

RINGS

Definition: $(R, +, \cdot)$ is a **ring** if $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup and we have distributive law between $+$ and $\cdot$.

All our rings will be unital: $1 \in R$ neutral under $\cdot$.

All our rings will be commutative: $\forall x, y \in R: xy = yx$.

$0 \in R$ is a neutral element under $+$.

The trivial ring has $1 = 0$.

Definition: $u \in R$ is a **unit** (invertible element) if there exists $v \in R$ such that $uv = vu = 1$. Then $v = u^{-1}$.

$R^\times = R^{-1} = GL(R)$... units of R

Definition: **Ring homomorphism** is a map $\varphi: R \rightarrow R'$ that preserves $+$, $\cdot$ and 1 .

φ is **isomorphism** if it's a bijective homomorphism $\varphi: R \xrightarrow{\cong} R'$.

Endomorphism is homomorphism $R \rightarrow R$.

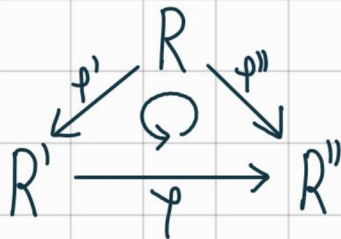
Automorphism is a bijective endomorphism $R \xrightarrow{\cong} R$.

Definition: $R'' \subseteq R$ is a **subring** if R'' is a ring (under $+$, $\cdot$ from R) and $R'' \hookrightarrow R$ is a homomorphism ($1_R \in R''$).

Definition: R -algebra is a ring R' with a homomorphism $\varphi: R \rightarrow R'$, we call it **structure homomorphism**.

Remark: Every ring is a $\mathbb{Z}$ -algebra.

Definition: R -algebra **homomorphism** between R' and R'' is a ring homomorphism that's compatible with structure maps:



Example: Smallest nontrivial ring has two elements:

$$F_2 = \{0, 1\}$$

Example: R ring, Y set

$R^Y = \{\text{maps } Y \rightarrow R\}$ is a ring with respect to pointwise operations:

$$f, g \in R^Y, y \in Y$$

$$(f+g)(y) := f(y) + g(y)$$

$$(f \cdot g)(y) := f(y) \cdot g(y)$$

Identity element of R^Y is the constant function 1.

Rings of polynomials:

R ring
 $n \in \mathbb{N}$

$$\mathcal{P} = R[X_1, \dots, X_n]$$

$\mathcal{P}$ has the following universal property (UL):

$\forall \varphi: R \rightarrow R'$ homomorphism : $\forall a_1, \dots, a_n \in R'$:

$\exists! \pi: \mathcal{P} \rightarrow R' \ni: \pi|_R = \varphi \wedge \forall i=1, \dots, n: \pi(X_i) = a_i$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \mathcal{P} = R[X_1, \dots, X_n] \\ & \searrow \varphi & \downarrow \exists! \pi \\ & & R' \end{array}$$

$$\pi\left(\sum_{\text{finite}} \overset{R}{r_i} X_i^{i_1} \dots X_n^{i_n}\right) = \sum \varphi(r_i) a_i^{i_1} \dots a_n^{i_n}$$

IDEALS

Definition: $I \triangleleft R$ is an ideal if:

1) $0 \in I$

2) $x, y \in I \Rightarrow x+y \in I$

3) $r \in R, x \in I \Rightarrow r \cdot x \in I$

$$S \subseteq R: \langle S \rangle = \left\{ \sum_{s \in S}^{\text{finite}} a_s s ; a_s \in R \right\} = \bigcap_{S \subseteq I \triangleleft R} I$$

... ideal of R , generated by S

$\sim$ smallest ideal that contains S

$$a \in R: \langle a \rangle = \{r \cdot a ; r \in R\} = R \cdot a$$

... principal ideal, generated by a

Operations on ideals:

$I_\lambda (\lambda \in \Lambda)$ ideals of R

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{\lambda \in \Lambda} b_\lambda ; b_\lambda \in I_\lambda \wedge \text{only finitely many } b_\lambda \neq 0 \right\}$$

= smallest ideal that contains all $I_\lambda (\lambda \in \Lambda)$

$$= \langle \bigcup_{\lambda \in \Lambda} I_\lambda \rangle$$

$$\bigcap_{\lambda \in \Lambda} I_\lambda \triangleleft R, \quad \bigcap_{\emptyset} I_\lambda := R$$

$$\prod_{\lambda \in \Lambda} I_\lambda = \langle \{ \prod_{\lambda \in \Lambda'} b_\lambda ; \Lambda' \text{ finite} \subseteq \Lambda, b_\lambda \in I_\lambda \} \rangle$$

If $\#\Lambda < \infty$, say $\Lambda = \{1, \dots, n\}$, then $\prod_{\lambda} I_\lambda = I_1 I_2 \dots I_n$.

For $I, J \triangleleft R$, the **transporter** is $(I:J) = \{x \in R; x \cdot J \subseteq I\} \triangleleft R$.

$$I \cdot J \subseteq I \cap J \subseteq I + J$$

$$\overline{I}, J \subseteq \overline{I} + J$$

$$I \subseteq (I:J)$$

For $I, J, K \triangleleft R$, we have $I \cdot (J + K) = I \cdot J + I \cdot K$.

$I \triangleleft R$ is **proper** if $I \neq R$.

$I \triangleleft R$ is **trivial** if $I = \{0\}$.

$$\underline{I \triangleleft R} : \underline{I = R} \Leftrightarrow \underline{1 \in I}$$

($\Rightarrow$) Obvious.

($\Leftarrow$) If $1 \in I$, take $r \in R$.

$$\text{Then } r = \underbrace{r}_{\in R} \cdot \underbrace{1}_{\in I} \in I.$$

$$\text{Similarly: } I = R \Leftrightarrow I \cap R^\times \neq \emptyset$$

$$\underline{x \in R: \langle x \rangle = R \Leftrightarrow x \in R^\times}$$

($\Leftarrow$) Easy.

$$(\Rightarrow) \langle x \rangle = R \Rightarrow \exists y: xy = 1 \Rightarrow y = x^{-1}, x \in R^\times$$

$$\varphi: R \rightarrow R', I \triangleleft R: \langle \varphi(I) \rangle =: I^e \triangleleft R'$$

... extension of I

$$I' \triangleleft R': \varphi^{-1}(I') =: I'^c \triangleleft R$$

... contraction of I'

Quotient/factor rings:

$$\varphi: R \rightarrow R': \ker \varphi = \varphi^{-1}(0) \triangleleft R$$

$$\ker \varphi = \langle 0 \rangle \Leftrightarrow \varphi \text{ is injective (1-1, one-to-one, one-one)}$$

Have $I \triangleleft R$.

For cosets $\{x + I; x \in R\} = R/I$ we add:

$$(x+I) + (y+I) := (x+y) + I$$

$$(x+I) \cdot (y+I) := (x \cdot y) + I$$

This makes R/I into a ring. We call it a **quotient** or **factor ring**.

$\mathcal{K}: R \rightarrow R/I$ is the canonical quotient homomorphism:
 $x \mapsto x+I$

$\mathcal{K}$ is surjective

$$\ker \mathcal{K} = I$$

$$\varphi: R \rightarrow R' \Rightarrow R/\ker \varphi \cong \operatorname{im} \varphi$$

$$R, I \triangleleft R, I \subseteq J \triangleleft R, \mathcal{K}: R \rightarrow R/I$$

$$J/I = \{y+I; y \in J\} = \mathcal{K}(J) \triangleleft R/I$$

Maps $J \mapsto J/I$ and $J' \mapsto \mathcal{K}^{-1}(J')$ are inverse to each other, hence bijections of {ideals of R that contain I } and {ideals of R/I }:

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

Proposition: Have $\mathcal{P} = R[X]$, $a \in R$. Let $\pi: \mathcal{P} \rightarrow R$ be the R -algebra homomorphism sending X to a . Then:

$$a) \ker \pi = \{F \in \mathcal{P}; F(a) = 0\} = \langle X-a \rangle$$

$$b) \mathcal{P}/\ker \pi \cong R$$

Proof: $G := X - a$

$$\forall F \in \mathcal{P} : \exists H \in \mathcal{P} : \exists r \in R \ni F = G \cdot H + r$$

By linearity, it's sufficient to prove this for $f = X^n$.

$$f = X^{n-1} \cdot X = X^{n-1} (G + a) = G \cdot X^{n-1} + a \cdot X^{n-1}$$

Repeat this, now starting with X^{n-1} ...

$$a) \pi(F) = \underbrace{\pi(G)}_{=0} \pi(H) + \underbrace{\pi(r)}_{=r} = r$$

$$\text{Hence: } F \in \ker \pi \Leftrightarrow \pi(F) = 0$$

$$\Leftrightarrow r = 0$$

$$\Leftrightarrow F = (X - a) \cdot H$$

$$\Leftrightarrow F \in \langle X - a \rangle$$

$$b) \mathcal{P} / \ker \pi \cong \text{im } \pi = R$$

Degree of a polynomial:

R ring, $n \in \mathbb{N}$

$$\mathcal{P} = R[X_1, \dots, X_n]$$

$0 \neq F \in \mathcal{P} : \deg(F) := \max \{ \deg(M) \mid M \text{ is a monomial appearing in } F \}$

$$M = X_1^{\alpha_1} \dots X_n^{\alpha_n} \quad (\alpha_i \in \mathbb{N}_0)$$

$$\deg M = \sum_{i=1}^n \alpha_i \quad (\text{total degree})$$

$$\deg(0) := -\infty$$

$$F, G \in \mathcal{P}, F \cdot G \neq 0 \Rightarrow \deg(F \cdot G) \leq \deg F + \deg G$$

Every monomial that appears in $F \cdot G$ is of the form $M_1 \cdot M_2$ for a monomial $M_1 \in F$ and $M_2 \in G$.

Beware: In general $\deg(F \cdot G) \neq \deg F + \deg G$:

$$\mathbb{Z}_4[X]:$$

$$F = 2X$$

$$G = 2X$$

IDEMPOTENTS

$e \in R$ is *idempotent* if $e^2 = e$.

Form $R \cdot e = \langle e \rangle$ is a ring with identity element e :

$$(x \cdot e) \cdot e = x e^2 = x e$$

Unless $0=1$, Re is *not* a subring of R !

$1-e = e' = e^\perp$ is the *complementary* idempotent:

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$$

$$\text{Also: } e(1-e) = e - e^2 = e - e = 0$$

If $e_1, e_2 \in R$ satisfy $e_1 + e_2 = 1$ and $e_1 e_2 = 0$, then they are complementary idempotents:

$$e_1 = e_1 \cdot 1 = e_1(e_1 + e_2) = e_1^2 + e_1 e_2 = e_1^2$$

$$\text{Idem}(R) = \{\text{idempotents of } R\}$$

Example: From R', R'' rings, form $R = R' \times R''$ with componentwise $+, \cdot$.

Then:

- $(0, 0)$ is neutral element for $+$
- $(1, 1)$ is neutral element for $\cdot$

$e' = (1, 0)$ and $e'' = (0, 1)$ are complementary idempotents.

Proposition: Let R be a ring and $e', e'' \in R$ complementary idempotents. Set $R' = Re'$ and $R'' = Re''$.

$$\text{Define } \varphi: R \rightarrow R' \times R'' \\ x \mapsto (xe', xe'')$$

Then φ is an isomorphism and $R' \cong R/Re''$, $R'' \cong R/Re'$.

Proof: Consider $\varphi': R \rightarrow R'$ $x \mapsto xe'$.

φ' is a homomorphism.

$$\varphi'(xy) = xy \cdot e'$$

$$\varphi'(x) \cdot \varphi'(y) = xe' ye' = xy (e')^2 = xy e'$$

$$\underline{\ker \varphi' = R'' = Re''}$$

$$x \in \ker \varphi' \Leftrightarrow xe' = 0$$

$$\Rightarrow x = x \cdot 1 = x(e' + e'') = xe' + xe'' = xe'' \in Re''$$

$$x \in Re'' : x = ye'' \Rightarrow xe' = y \underset{=0}{e''} e' = 0$$

$$\Rightarrow \operatorname{im} \varphi = R' \quad \wedge \quad R' \cong R/Re''$$

Similarly, we have:

$$\begin{aligned} \varphi'' : R &\rightarrow R'' \\ x &\mapsto xe'' \end{aligned}$$

$$\ker \varphi'' = R'$$

$$\operatorname{im} \varphi'' = R''$$

$$\Rightarrow R'' \cong R/Re'$$

Then $\varphi = (\varphi', \varphi'')$ is a homomorphism.

$$\underline{\ker \varphi = \langle 0 \rangle}$$

$$x \in \ker \varphi \Rightarrow xe' = 0 \quad \wedge \quad xe'' = 0$$

$$\Rightarrow x \underset{=1}{(e' + e'')} = x \cdot 1 = x$$

$$\underline{\operatorname{im} \varphi = R' \times R''}$$

$$(x'e', x''e'') = \varphi(x'e' + x''e'')$$

Then φ is an isomorphism.

PRIME IDEALS

$x \in R$ is a zero divisor $\Leftrightarrow \exists y \in R \setminus \{0\} : xy = 0$

Otherwise: x is a non zero divisor

$$Z \text{div } R := \{x \in R \text{ zero divisor}\}$$

$$S_0 := \{x \in R \text{ non zero divisor}\} \text{ multiplication set}$$

Definition: $S \subseteq R$ is multiplicative if $1 \in S$ and $S \cdot S \subseteq S$.

Definition: $P \triangleleft R$ is prime if $R \setminus P$ is multiplicative.

Equivalently, $P \triangleleft R$ is prime if whenever $a \cdot b \in P$, we have $a \in P$ or $b \in P$.

Terminology: Ring is called a field if $0 \neq 1$ and every nonzero element is invertible (ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_2$).

Ring where $\langle 0 \rangle$ is a prime ideal is an (integral) domain (cel kolobar). Such a ring has no nonzero zero divisors.

If R is integral domain, we can form its field of fractions:

$$\text{Frac}(R) = \left\{ \frac{a}{b} ; a \in R, b \in R \setminus \{0\} \right\}$$

Every integral domain is a subring of a field:

$$r \mapsto \frac{r}{1}$$

Conversely, if R is a subring of a field F , then R is an integral domain:

$$xy = 0, x \neq 0, x, y \in R$$

$$\Rightarrow \exists \frac{1}{x} \in F$$

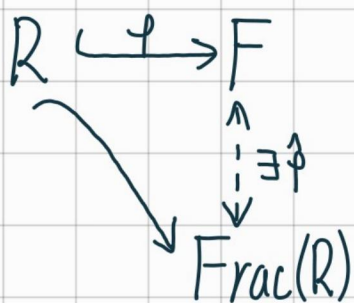
$$\Rightarrow \frac{1}{x} \cdot xy = 0$$

$$\Rightarrow y = 0$$

$$\Rightarrow y = 0$$

Universal property for $\text{Frac}(R)$:

Each embedding of a domain R into a field F ,



extends to $\text{Frac}(R) \hookrightarrow F$.

$$\hat{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$$

We can form polynomial rings over integral domains, $\mathcal{P} = R[x]$.

$\mathcal{P}$ is also a domain & $\deg(F \cdot G) = \deg(F) + \deg(G)$

We order $\mathcal{P}$ with graded lexicographical ordering (grlex):

Order monomials first by degree, then lexicographically within the same degree.

Among all monomials of $F \in \mathcal{P}$, pick the largest one. This is $LM(F)$ or leading monomial of F .

Leading term of F or $LT(F)$ is then $a \cdot LM(F)$ if $a \cdot LM(F)$ for $a \in R$ appears in F .

We call a the lead coefficient of F or $LC(F)$.

$$F, G \in \mathcal{P} \Rightarrow \underline{LT(F \cdot G)} = \underline{LT(F)} \cdot \underline{LT(G)}$$

$= a \cdot m \quad = b \cdot n$

Then $a \cdot b \neq 0$ because R is a domain.

$$\deg(m \cdot n) = \deg(m) + \deg(n) = \deg(F) + \deg(G)$$

$$\deg(m \cdot n) \geq \deg(m' \cdot n') \text{ for any monomials } m' \in F, n' \in G$$

If $m' \neq m$ and $n' \neq n$, then $m' \cdot n' \not\leq_{\text{grlex}} m \cdot n$ by max of m, n .

$$\text{Hence } LT(F \cdot G) = ab \cdot mn = LT(F) \cdot LT(G).$$

$\Rightarrow \mathcal{P}$ is a domain

If $\mathcal{P}$ is a domain, we can form field of rational functions $\text{Frac}(\mathcal{P}) =: K(x)$ where $K = \text{Frac}(R)$.

$$\underline{\mathcal{P}^\times = R^\times}$$

If $F \cdot G = 1$ for $F, G \in \mathcal{P}$, then $\deg(F \cdot G) \stackrel{=0}{=} \deg F \stackrel{\geq 0}{+} \deg G \stackrel{\geq 0}{}$,
so $\deg F = \deg G = 0$, so $F, G \in R$.

Beware, if R is not a ring, the above equation will not hold:

If $a \in R$ satisfies $a^2 = 0$, then $(1-aX)(1+aX) = 1$.

Lemma: Let $\varphi: R \rightarrow R'$ be a homomorphism and $T \subseteq R'$.

a) If T is multiplicative, then so is $\varphi^{-1}(T)$.

b) If φ is **onto** (surjective), then also the converse holds.

Proof: a) $S := \varphi^{-1}(T)$

Since $\varphi(1) = 1$, we have $1 \in S$.

For $x, y \in S$, we have $\varphi(xy) = \varphi(x)\varphi(y) \in T \cdot T = T$,
so $xy \in \varphi^{-1}(T) = S$.

b) Now assume $S = \varphi^{-1}(T)$ is multiplicative. We are proving T is multiplicative.

- $1 \in T$ since $1 \in S$ and $\varphi(1) = 1$.

- Given $x', y' \in T$, then there exist $x, y \in S$ such that $x' = \varphi(x)$ and $y' = \varphi(y)$. Then $x \cdot y \in S$ and $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = x' y' \in T$.

Corollary: Have $\varphi: R \rightarrow R'$ homomorphism, $J \triangleleft R'$ and $I := \varphi^{-1}(J)$.

a) If J is a prime field, then so is I .

b) If φ is onto and I is prime, then J is prime.

Proof: Apply lemma to $T = R' \setminus U$.

Corollary: Let $P \triangleleft R$. Then P prime iff R/P is a domain.

Example: R ringy
 $\mathcal{P} = R[x, y]$
 $P = \langle x \rangle$

Then: $\mathcal{P}/P \cong R[x]$

So: P is a prime ideal $\Leftrightarrow R$ is a domain

MAXIMAL IDEAL

Definition: $M \triangleleft R$ is a maximal ideal if $M \neq R$ and there is no $I \triangleleft R$ such that $M \subsetneq I \subsetneq R$.

Proposition: Ring R is a field $\Leftrightarrow (0)$ is a max ideal

Proof: $(\Rightarrow)$ Suppose $(0) \subsetneq I \triangleleft R$.

Then there exists $0 \neq x \in I$. Then there exists $x^{-1} \in R$ since R is a field. Hence $1 = \underbrace{x \cdot x^{-1}}_1 \in I$ and $I = R$.

$(\Leftarrow)$ Pick $x \in R \setminus (0)$. Then $(0) \subsetneq \langle x \rangle \triangleleft R$. In particular, $1 \in \langle x \rangle$, so there is $y \in R$ such that $xy = 1$. That is, $x \in R$ is invertible.

Corollary: Let R be a ring, $M \triangleleft R$. Then M is a max ideal iff R/M is a field.

Proof: M is a max ideal in $R \iff (0)$ is a max ideal in R/M
 $\stackrel{\text{prop}}{\iff} R/M$ is a field

Corollary: Every max ideal is prime.

Proof: Every field is an integral domain.

Example: R integral domain
 $\mathcal{P} := R[X, Y]$

$$\langle X \rangle \subsetneq \langle X, Y \rangle \subsetneq \mathcal{P}$$

$\Rightarrow \langle X \rangle$ prime ideal that is *not* max

$$\langle X, Y \rangle \triangleleft \mathcal{P} \text{ is max } \iff \mathcal{P}/\langle X, Y \rangle \cong R \text{ is a field}$$

Example: R ring
 $\mathcal{P} = R[X_\lambda; \lambda \in \Lambda]$

$$\forall \lambda \in \Lambda: \text{ Pick } a_\lambda \in R$$

$$M := \langle X_\lambda - a_\lambda; \lambda \in \Lambda \rangle$$

$$\Rightarrow \mathcal{P}/M \cong R$$

$$\text{So: } M \text{ max } \iff R \text{ field}$$

Theorem: Every proper ideal is contained in a max ideal.

Proof: $I \subsetneq R$

$$\mathcal{Y} = \{J \not\subseteq R ; I \subseteq J\}$$

Since $I \subseteq \mathcal{Y}$, $\mathcal{Y} \neq \emptyset$.

Consider a chain $\{I_\lambda ; \lambda \in \Lambda\}$ in $\mathcal{Y}$.

Then let $J = \bigcup_{\lambda \in \Lambda} I_\lambda \triangleleft R$.

Since $1 \notin I_\lambda$, $1 \notin J$, so $J \not\subseteq R$.

^{Zorn}
 $\Rightarrow \exists M \in \mathcal{Y}$ max element

Then M is a max ideal that contains I .

Corollary: Have R ring and $x \in R$. Then $x \in R^\times$ iff x does not lie in a max ideal.

Proof: $x \in R^\times \Leftrightarrow \langle x \rangle = R$

Hence: $x \notin R^\times \Leftrightarrow \langle x \rangle \not\subseteq R$

$\Leftrightarrow \exists M^{\max} \triangleleft R : x \in \langle x \rangle \subseteq M \not\subseteq R$

FACTORIZATION

R integral domain

u unit $\Leftrightarrow \exists u^{-1} \in R \Leftrightarrow \langle u \rangle = R$

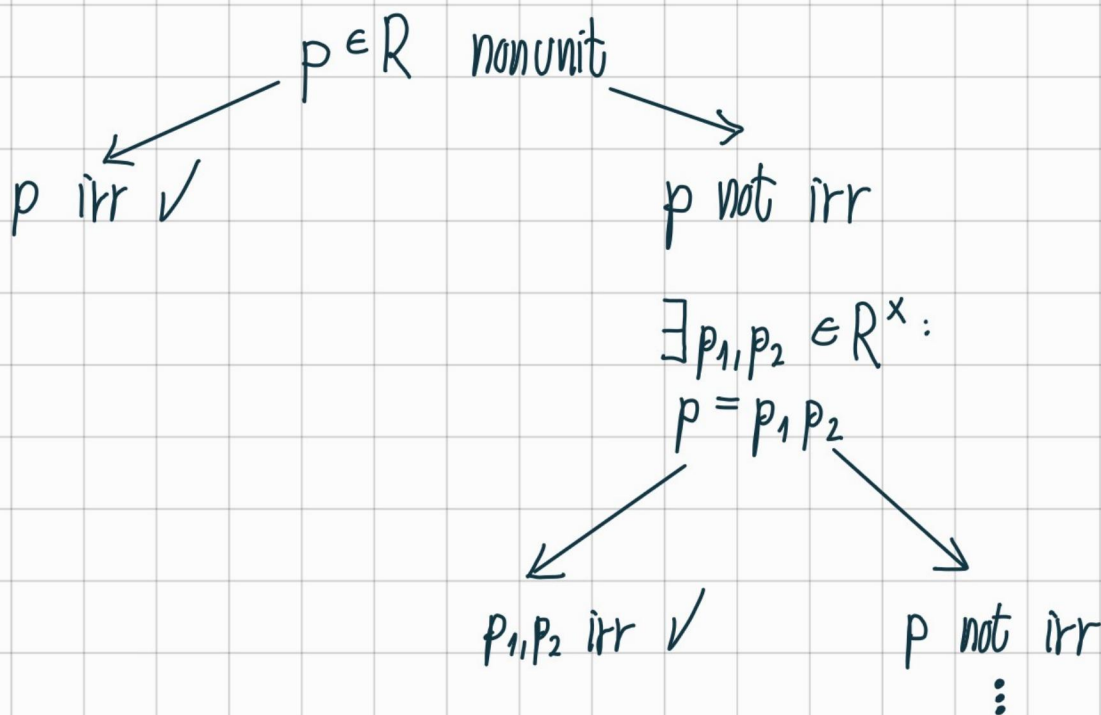
a divides b $\Leftrightarrow \exists g \in R : b = g \cdot a$ $b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$

a, b are associates $\Leftrightarrow \exists u \in R^\times: a = ub \Leftrightarrow \langle a \rangle = \langle b \rangle$
 $a|b$ & $b|a$

a is a proper divisor of $b \Leftrightarrow \exists u \in R: b = q \cdot a \Leftrightarrow \langle b \rangle \subsetneq \langle a \rangle \subsetneq R$
 & $a, q \notin R^\times$

a is irreducible $\Leftrightarrow a \notin R^\times$ & a has no proper divisors $\Leftrightarrow \langle a \rangle$ max among principal ideals

p is a prime element $\Leftrightarrow p \notin R^\times$ & $(p|ab \Rightarrow p|a \text{ or } p|b) \Leftrightarrow \langle p \rangle$ is a prime ideal



Definition: A domain R is **unique factorization domain (UFD)**, if:

1) Each nonzero element of R is a product of irreducible elements and units.

2) Such factorizations are unique up to order and units.

Proposition: An int. domain R is UFD $\Leftrightarrow$

i) Every ascending chain of principle ideals $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$ stabilizes (ACCP)

&

ii) Every irreducible element is prime

Proof:

($\Rightarrow$) i) If $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$, then $a_{i+1} | a_i$ and a_i / a_{i+1} is not a unit.

So the number of irreducible factors of a_i strictly decreases at each step.

This cannot happen indefinitely, so ACCP holds.

ii) Suppose p is irreducible and $p | ab$. Factor a, b .

Then the uniqueness of factorization forces p to be associate with one of a or b . Thus pla or plb .

($\Leftarrow$) i) Suppose $a \in R$ does not factor into irreducibles. In particular a is not irreducible.

So there exist $a_1, b_1 \in R^\times$, so $a = a_1 b_1$. Thus $\langle a \rangle \subsetneq \langle a_1 \rangle$, $\langle a \rangle \subsetneq \langle b_1 \rangle$.

Without loss of generality (wlog), a_1 is also not a factor of irreducibles. So, as above, $a_1 = a_2 b_2$ for $a_2, b_2 \notin R^\times$. Thus $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$. Repeat this on $a_2 \dots$

So we have $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$ infinite chain of prime ideals.

~~ACCP~~

ii) Suppose $p_1 \dots p_n \stackrel{(*)}{=} q_1 \dots q_n$ for irreducibles p_i, q_i .

If p_i is irreducible, p_i is prime. So $p_i \mid q_1 \cdots q_n$.
As p_i is prime, $p_i \mid q_j$ for some j .

But q_j is irreducible, so it cannot have proper divisors.
So p_i and q_j are associates:

$$q_j = u_j p_i \text{ for some } u_j \in R^\times$$

So cancel p_i and q_j in (*) and continue by induction.

Example: Examples of UFDs:

$$\text{Fields, } \mathbb{Z}, R \text{ UFD} \Rightarrow R[x_1, \dots, x_n]$$

Example: Examples of not UFDs:

$$F[x, y, z] / \langle xy - z^2 \rangle$$

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} ; a, b \in \mathbb{Z}\},$$

because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

Definition: A domain R is a **principal ideal domain (PID)** if every ideal is principal.

Example: Examples of PIDs:

$$\text{Fields, } \mathbb{Z}, F[x] \text{ (polynomials on one variable over fields)}$$

Example: Examples of not PIDs:

$$F[x, y]$$

Proposition: Let R be a PID. Then:

a) Every irreducible element is prime.

b) Every nonzero prime ideal is max.

c) R is UFD.

Proof:

a) Have q irreducible. Suppose $\langle q \rangle \subseteq I \subsetneq R$. Say $I = \langle a \rangle$ (by PID). Hence $\langle q \rangle \subseteq \langle a \rangle$, so $a \mid q$. Hence a only one associate or a is a unit. Since $\langle a \rangle = I \subsetneq R$, $a \in R^\times$. So a, q are associate, i.e. $I = \langle q \rangle$ and $\langle q \rangle$ is a max ideal. Thus $\langle q \rangle$ is a prime ideal, and q is a prime element.

b) If $(0) \neq P = \langle p \rangle \triangleleft R$ is a prime ideal. Then p is a prime element. By (a), $\langle p \rangle$ is a max ideal.

c) To prove R is UFD, it suffices (by (a)) to show ACCP. Suppose $(I_n; n \in \mathbb{N})$ is an ascending chain of ideals in R :

$$I_1 \subseteq I_2 \subseteq \dots$$

Let $I := \bigcup_j I_j \triangleleft R$. By PID there exists $d \in R$, such that $I = \langle d \rangle$. Thus there exists $n \in \mathbb{N}$, such that $d \in I_n$. Then $I_n \supseteq \langle d \rangle = I = \bigcup_j I_j$. So chain stabilizes at I_n .

Example: Suppose R is PID and pick $p \in P$ prime element.

Then $\overset{(0) \neq}{\langle p \rangle} \triangleleft R$ is a prime ideal, so max by (b) of proposition.

$$R/\langle p \rangle = k \text{ field}$$

$$\mathcal{S} = R[x]$$

$$\bar{G} \in \mathcal{P}$$

$\rightsquigarrow \bar{G} \in k[x]$ reduce coefficients mod $\langle p \rangle$

Suppose $\bar{G}$ is irreducible. Form $M = \langle p, \bar{G} \rangle \triangleleft \mathcal{S}$.

M is a max ideal

$\mathcal{S}/M \cong k[x]/(\bar{G})$ is a field since $k[x]$ is a PID and $\bar{G}$ is irreducible

RADICAL IDEALS

Definition: Jacobson radical of a ring R , $J(R)$, $\text{Jac}(R)$, $\text{rad}(R)$, is the intersection of all max ideals of R :

$$\text{rad } R = \bigcap_{M \triangleleft R} M$$

Proposition: R ring, $I \triangleleft R$, $u \in R^\times$
 $x \in R$

$$x \in \text{rad } R \iff \forall y \in R: u - xy \in R^\times$$

In particular:

$$\bullet R^\times + \text{rad } R \subseteq R^\times$$

$$\bullet 1 - I \subseteq R^\times \Rightarrow I \subseteq \text{rad } R$$

Proof: $(\Rightarrow)$ Suppose $x \in \text{rad} R$, $M \triangleleft^{\text{max}} R$ and suppose $u - xy \in M$ for some $y \in R$.

Since $x \in \text{rad} R \subseteq M$, we have $u \in xy + M \subseteq M$.



$(\Leftarrow)$ If $x \notin \text{rad} R$, then there exists $M \triangleleft^{\text{max}} R$ such that $x \notin M$.

Then $M + \langle x \rangle = R$ by maximality of M .

Hence there exist $y \in R$ and $m \in M$ such that $xy + m = u$.

So $u - xy = m \in M$, that is $u - xy \in R^x$.

In particular:

$$\bullet \ x \in \text{rad} R, u \in R^x, y = -1$$

$$\Rightarrow u + x \in R^x$$

$$\bullet \ x \in I, y \in R$$

$$\Rightarrow 1 - xy \in 1 - I \subseteq R^x$$

$$\stackrel{\text{above}}{\Rightarrow} x \in \text{rad} R$$

Corollary: $I \triangleleft R$, $\mathcal{K}: R \rightarrow R/I$ quotient homomorphism
 $I \subseteq \text{rad} R$

$$\Rightarrow \mathcal{K}|_{\text{Idempotents}(R)}: \text{Idem}(R) \rightarrow \text{Idem}(R/I) \text{ injective}$$

Proof: Let $e, e' \in R$ be idempotents with $\mathcal{K}(e) = \mathcal{K}(e')$.
Set $x := e - e'$.

$$\begin{aligned} x^3 &= e^3 - 3e^2e' + 3e(e')^2 - (e')^3 \\ &= e - 3ee' + 3ee' - e' \\ &= e - e' = x \end{aligned}$$

$$\Rightarrow x - x^3 = 0 = x(1 - x^2)$$

From $\mathcal{K}(x) = 0$ we have $x \in I$.

By the proposition, $1 - x^2 \in R^\times$, because $x \in \text{rad } R$.

$$\Rightarrow x = 0$$

Definition: Ring R is **local**, if it has only one max ideal.

Ring R is **semilocal**, if it has finitely many max ideals.

The **residue field** of a local ring $(R, \overset{\text{max ideal}}{M})$ is R/M .

Lemma: R ring, $N = R \setminus R^\times$ the set of non-units

$$R \text{ local} \Leftrightarrow N \triangleleft R$$

In this case: N is the max ideal of R

Proof: $(\Leftarrow)$ Each $I \triangleleft R$ is contained in N since $I \cap R^\times = \emptyset$.
If $N \triangleleft R$, then it must be a max ideal and thus the max ideal of R .

$$(\Rightarrow) (R, M) \text{ local} \Rightarrow R \setminus M = R^\times = R \setminus N \Rightarrow N = M \triangleleft R$$

Example: $R' \times R'' =: R$ for nontrivial R', R'' is not local:

$$(1, 1) = (1, 0) + (0, 1) \text{ is sum of two non-units}$$

Example: Have R ring and $n \in \mathbb{N}$. Formal power series in $X_1, \dots, X_n$ are formal (∞) series of the form $\sum_i a_i X_1^{i_1} \dots X_n^{i_n}$, where $i \in \mathbb{N}_0$ and $a_i \in R$.

$a_0 =:$ const coeff

We add and multiply FPS as we do with polynomials.

Ring of FPS is denoted as $R[[X_1, \dots, X_n]]$ or $R[[X_1, \dots, X_n]]$.

$$I := \langle X_1, \dots, X_n \rangle \triangleleft R[[X]]$$

Then $\sum a_i X_1^{i_1} \dots X_n^{i_n} \mapsto a_0 : R[[X]] \rightarrow R$ is a surjective homomorphism with kernel I :

$$R[[X]]/I \cong R$$

$$\bullet M \triangleleft R, N := I + M \cdot R[[X]] \triangleleft R[[X]]$$

$$\Rightarrow R[[X]]/N \cong R/M$$

$$\bullet F = \sum a_i X_1^{i_1} \dots X_n^{i_n} \in R[[X]]$$

$$\underline{F \in R[[X]]^\times \Leftrightarrow a_0 \in R^\times}$$

($\Rightarrow$) Suppose $F' = \sum a_i' X_1^{i_1} \dots X_n^{i_n}$ satisfies $F \cdot F' = 1$.

$$\begin{aligned} \text{Thus } 1 = F \cdot F' &= \left(\sum a_i X_1^{i_1} \dots X_n^{i_n} \right) \left(\sum a_i' X_1^{i_1'} \dots X_n^{i_n'} \right) \\ &= a_0 a_0' + I. \end{aligned}$$

Hence $a_0 a_0' = 1$, i.e. $a_0 \in R^\times$.

$$(\Leftarrow) F = a_0(1 - G) \text{ for some } G \in I$$

$$F' := a_0^{-1}(1 + G + G^2 + \dots) \in R[[X]]$$

$$\Rightarrow F \cdot F' = 1$$

$$\Rightarrow F \in R[[X]]^\times$$

- Have (R, M) local ring. For $F \in R[[X]]$, if $F \notin N$, then its const term $a_0 \notin M$. Hence $a_0 \in R^\times$ and thus $F \in R[[X]]^\times$.

Hence $N = \text{non-units of } R[[X]]$, so $(R[[X]], N)$ is a local field.

Proposition: Let R be a ring, $S \subseteq R$ multiplicative set and $I \triangleleft R$ with $I \cap S = \emptyset$. Form $\mathcal{J} = \{J \triangleleft R; I \subseteq J \wedge J \cap S = \emptyset\}$.

Then $\mathcal{J}$ contains max elements (wrt $\subseteq$) and each such max element is a prime ideal.

Proof: Suppose $I \in \mathcal{J} \neq \emptyset$.

Let $(J_\lambda)_\lambda$ be a chain in $\mathcal{J}$. Define $J = \bigcup_\lambda J_\lambda$.

Then $J \triangleleft R$, $I \subseteq J$, $J \cap S = \emptyset$, so J is upper bound in $\mathcal{Y}$ of $(J_\lambda)_\lambda$.

Thus Zorn's lemma applies to give that $\mathcal{Y}$ has max elements.

Let $P \in \mathcal{Y}$ be a max element.

Take $x, y \in R \setminus P$. Then $P + \langle x \rangle, P + \langle y \rangle \notin \mathcal{Y}$ by max of $\mathcal{Y}$. By definition of $\mathcal{Y}$, $P + \langle x \rangle \cap S \neq \emptyset$ and $P + \langle y \rangle \cap S \neq \emptyset$:

$$\exists p, q \in P : \exists a, b \in R : p + ax \in S \wedge q + by \in S$$

S multiplicative

$$\Rightarrow (p + ax)(q + by) \in S$$

$$\underbrace{pq + pby + axq + abxy}_{\in R} \in S$$

$P \cap S = \emptyset$

$$\Rightarrow abxy \notin P$$

$$\Rightarrow xy \notin P$$

$$\Rightarrow P \text{ is prime ideal}$$

Definition: Radical of ideal $I \subseteq R$ is:

$$\sqrt{I} = \{x \in R ; \exists n \in \mathbb{N} : x^n \in I\}$$

Obviously:

$$\bullet I \subseteq \sqrt{I}$$

- $\sqrt{\sqrt{I}} = \sqrt{I}$

- $J \subseteq I \Rightarrow \sqrt{J} \subseteq \sqrt{I}$

Definition: An ideal $I \triangleleft R$ is **radical** when $I = \sqrt{I}$.

Lemma: If $I = \bigcap_{\lambda} P_{\lambda}$ where each P_{λ} is a prime ideal, then I is ideal.

Proof: Suppose $x \in \sqrt{I}$. Then $x^n \in I = \bigcap P_{\lambda}$ for some $n \in \mathbb{N}$. Thus $x^n \in P_{\lambda}$ for each λ . Because P_{λ} is prime, this implies $x \in P_{\lambda}$. So $x \in \bigcap P_{\lambda} = I$.

Definition: $\text{nil}(R) := \sqrt{(0)}$ is the **nilradical**.

Note $\text{nil}(R) = \sqrt{(0)} = \{x \in R ; \exists n \in \mathbb{N} : x^n = 0\}$ are nilpotents of R .

$I \triangleleft R$ is **nilpotent** $\Leftrightarrow \exists n \in \mathbb{N} : x^n = 0$

Since $\text{rad} R = \bigcap_{\text{max } R} M$ is an intersection of max (hence prime) ideals, it holds:

- $\text{rad} R$ is a radical ideal:

$$\sqrt{\text{rad} R} = \text{rad} R$$

- $(0) \subseteq \text{rad} R$

$$\sqrt{\Rightarrow} \sqrt{(0)} = \text{nil} R \subseteq \sqrt{\text{rad} R} = \text{rad} R$$

Definition: Ring R is **reduced** if $\text{nil} R = (0)$.

Theorem: If $I \triangleleft R$, then $\sqrt{I} = \bigcap_{\substack{I \subseteq P \\ P \text{ prime ideal}}} P$.

Proof: Suppose $x \in \sqrt{I}$. Define $S = \{1, x, x^2, x^3, \dots\}$. Then S is multiplicative and $S \cap I = \emptyset$. By proposition, a max ideal P among ideals of R that contain I and avoid S is a prime ideal.

From $S \cap P = \emptyset$ we get $x \notin P$, so $x \notin \bigcap_{I \subseteq P \text{ prime}} P$.

Suppose $x \in \sqrt{I}$, say $x^n \in I$ and $P \supseteq I$ is a prime ideal, then $x^n \in I \subseteq P$.

As P is prime, $x \in P$. That is $x \in \bigcap_{I \subseteq P \text{ prime}} P$.

Corollary: If $I \triangleleft R$, then $\sqrt{I} \triangleleft R$.

Proof: By theorem, $\sqrt{I}$ is the intersection of (prime) ideals, so an ideal.

