

1, Rings and ideals

5.1

Ring: $(R, +, \cdot)$

- $(R, +)$ abelian group
- $(R, \cdot)$ semigroup
- distributive law

All our rings will have a unit $1 \in R$

All our rings unless specified will be commutative

$0 \in R$ neutral element under $+$

The trivial ring $\{0\}$ has $1=0$

$u \in R$ is a unit (=invertible element) if there exist $\exists v \in R$ $uv = vu = 1$. This v is unique $v = u^{-1}$

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

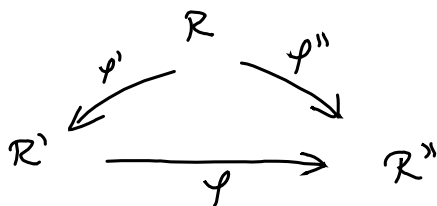
Ring homomorphism is a map $\varphi: R \rightarrow R'$ that preserves sums, product and ones

...

R -algebras: ring R' with a homomorphism
 $\varphi: R \rightarrow R'$
called *structure homomorphism*

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

R -algebra homomorphism between R', R'' is
a ring homomorphism that is compatible
with structure maps



Examples:

- $\mathbb{Z}_2$

- R ring, Y set

$R^Y = \{Y \rightarrow R\}$ is a ring with point wise operations $f, g \in R^Y$ $(f+g)(y) = f(y) + g(y)$
 $(f \cdot g)(y) = f(y) \cdot g(y)$

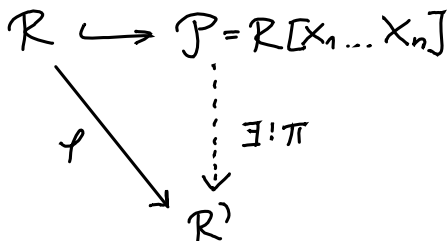
identity: $y \mapsto 1$

Ring of polynomials: $P = R[X_1, \dots, X_n]$

P has the following universal property (UL):

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

$\exists!$ homomorphism $\pi: P \rightarrow R' \ni \pi|_R = \varphi \wedge \pi(X_i) = a_i$



$$\pi\left(\sum_i r_i X_1 \cdots X_n\right) = \sum_i \varphi(r_i) a_1 \cdots a_n$$

- Ideal: $I \triangleleft R$ $0 \in I$
 $x, y \in I \Rightarrow x + y \in I$
 $r \in R, x \in I \Rightarrow rx \in I$

$S \subseteq R$ $\langle S \rangle \dots$ Ideal of R generated by S
 $\langle S \rangle = \left\{ \sum_{s \in S}^{finite} a_s s ; a_s \in R \right\}$
 $\langle a \rangle \dots$ principal ideals

Operations on ideals

- I_λ ($\lambda \in \Lambda$) ideals of R

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{\lambda \in \Lambda}^{finite} b_\lambda ; b_\lambda \in I_\lambda \right\}$$

- $\cap I_\lambda \triangleleft R$ $\cap I_\lambda = R$
- $\prod I_\lambda = \left\{ \prod_{\lambda \in \Lambda} b_\lambda ; \wedge \lambda \in \Lambda, b_\lambda \in I_\lambda \right\}$
- $(I : J) = \{ x \in R ; xJ \subseteq I \}$ transporter
- $I \cdot J \subseteq I \cap J \subseteq I, J \subseteq I + J$

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

$$I(J + K) = I \cdot J + I \cdot K \quad \forall n$$

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

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

($\Leftarrow$) obvious

$$(\Rightarrow) \langle x \rangle = R \Rightarrow \exists u \in R \quad ux = 1 \Rightarrow x \in R^\times$$

$$\varphi: R \rightarrow R' \quad I \triangleleft R$$

$\varphi(I)$ typically not ideal (

$$\mathbb{Z} \hookrightarrow \mathbb{Q}$$

$$\begin{array}{c} \mathbb{D} \\ \mathbb{Z} \nearrow \end{array}$$

$$\langle \varphi(I) \rangle =: I^e \quad \text{"extension of } I \text{"}$$

$$I' \triangleleft R'$$

$$\varphi^*(I') \triangleleft R \quad \text{"contraction of } I' \text{"} \quad I'^e = \varphi^*(I')$$

$$\varphi: R \rightarrow R' \Rightarrow \ker \varphi = \varphi^*(0) \triangleleft R$$

$$\ker \varphi = \{0\} \Leftrightarrow \varphi \text{ is injective}$$

$I \triangleleft R$ Form cosets $\{x+I; x \in R\} = R/I$

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

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

Quotient or factor ring

$$\begin{array}{ll} \kappa: R \rightarrow R/I & \text{canonical quotient} \\ x \mapsto x+I & \text{homomorphism} \end{array}$$

κ is surjective

$$\ker \kappa = I$$

$$R/\ker \kappa \cong \text{im } \kappa$$

$$R \quad I \triangleleft R \quad I \subseteq J \triangleleft R \quad \kappa: R \rightarrow R/I$$

$$J/I = \{y+I \mid y \in J\} = \kappa(J) \triangleleft R/I$$

maps $J \mapsto J/I$ in $J' \mapsto \kappa^{-1}(J)$

are inverse hence bijection

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

Proposition: $\mathcal{P} = R[X]$; $a \in R$. Let $\pi: \mathcal{P} \rightarrow R$ be the R -ring homomorphism $X \mapsto a$

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

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

Proof: $G := X - a$

$$\underline{\forall F \in \mathcal{P}. \exists H \in \mathcal{P}. \exists r \in R \ni F = GH + r}$$

B; linearity it suffices to prove this for $f = X^n$

$$f = X^n - aX^{n-1} = X^{n-1}(G + a) = GX^{n-1} + aX^{n-1}$$

Repeat this starting with X^{n-1}

$$a) \quad \pi(F) = \underbrace{\pi(G)}_0 \pi(H) + \underbrace{\pi(r)}_r = r$$

$$\begin{aligned} \text{Hence } F \in \ker(\pi) &\Leftrightarrow r = 0 \Leftrightarrow F(X-a) \cdot H \\ &\Leftrightarrow F \in \langle X-a \rangle \end{aligned}$$

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



$$\deg F = \max \{ \deg(M) : M \text{ monomial in } F \}$$

$$M = X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

$$\deg(M) = \sum \alpha_i$$

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

$$\deg(F \cdot G) \leq \deg F + \deg G$$

Idempotents if $e^2 = e$

Poglej si pri Filipu, če je potrebno

Prop: Let R be a ring and e, e' complementary idempotents ($e' = 1 - e$). Set $R' = Re'$ in $R'' = Re$

Define $\varphi: R \rightarrow R' \times R''$

$$x \mapsto (xe', xe'')$$

Then R is isomorphic to $R' \cong R/Re''$, $R'' \cong R/Re'$

Proof:

Consider $\varphi': R \rightarrow R'$

$$x \mapsto xe'$$

φ' is homomorphism $\varphi'(xy) = xye' = xye'^2 = \varphi(x)\varphi(y)$

$\ker \varphi' = R''$

$$(\subseteq) \varphi'(x) = 0 \Rightarrow xe' = 0$$

$$x \cdot 1 = x(e' + e'') = 0 + xe'' \in R''$$

$$(\supseteq) \varphi(xe'') = \underbrace{xe''}_{=0}e' = 0$$

Then $\text{im } \varphi' = R'$ and $R' \cong R/Re''$

Similarly we have $\varphi'': x \mapsto xe''$

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

$\ker \varphi = 0$

$$x \in \ker \varphi \Rightarrow xe' = 0 \text{ and } xe'' = 0$$

$$\Rightarrow 0 = x(e' + e'') = x \cdot 1 = x \quad \checkmark$$

$\text{im } \varphi = R' \times R''$

$$(xe', xe'') = \varphi(xe' + xe'')$$

$\Rightarrow \varphi$ is isomorphism

II Prime ideals

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

$$\text{zdiv } R = \{x \in R \text{ zero divisor}\}$$

Def $S \subseteq R$ is multiplicative if $1 \in S$ & $S \cdot S \subseteq S$

$P \subseteq R$ is prime if $R - P$ is multiplicative

Eg: $P \nsubseteq R$ is prime

Ring is a field if $0 \neq 1$ and an every non zero element is invertible

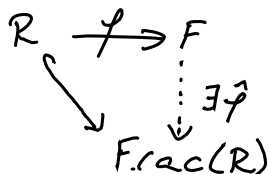
Ring where $\langle 0 \rangle$ is prime ideal is integral domain ← cel kelobar
such ring has no zero divisors

• R integral domain $\Rightarrow$ can form a field of fractions

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

- every integral domain is a subring of a field
- every subring of a field is integral

UL for $\text{Frac}(R)$: Each embedding of R into F Field extends to $\text{Frac}(R) \xrightarrow{\hat{f}} F$



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

- Polynomial rings over integral domains

R domain, $P = R[x]$

P is also a domain and $\deg(FG) = \deg F + \deg G$

We order P with so-called graded lexicographic (glex) ordering:

order first by degree, then lexicographically

$$x_1^4 x_2 < x_1^3 x_2^3 x_3 < x_1^2 x_2 x_3^4$$

Among all the monomials pick the largest one. This is $\text{LM}(F)$ = leading monomial of F

$\text{LT}(F)$ = leading term of F $a \cdot \text{LM}(F)$

if $a \cdot \text{LM}(F)$ appears in F

$\text{LC}(F)$ = leading term of F a

$$F, G \in \mathcal{P} \Rightarrow \underbrace{LT(FG)}_{a \cdot m} = \underbrace{LT(F)}_{a \cdot m} \cdot \underbrace{LT(G)}_{a \cdot n}$$

Then $a \cdot b \neq 0$ bcos R is a domain

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

if $m' \neq m$ or $n' \neq n$ then $m' \cdot n' \leq_{\text{lex}} m \cdot n$ by
max of m, n !

$$\text{Hence } LT(F \cdot G) = abmn = LT(F) \cdot LT(G)$$

$\mathcal{P}$ domain $\Rightarrow$ hen form $\text{Frac}(\mathcal{P}) =: K(X)$,
 $K = \text{Frac}(R)$ $\uparrow$

field of rational
functions

$$\underbrace{\mathcal{P}^\times = R^\times}_{\text{if } F \cdot G = 1}$$

then $\deg(FG) = 0$
 $\deg(F) + \deg(G) = 0$

lemma: let $\varphi: R \rightarrow R'$ is homomorphism and $T \in R'$.

a) if T is multiplicative then $\varphi(T)$ is too

b) if φ is surjective (onto), then also the converse holds

Proof:

a) $S = \varphi^*(T)$

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

For $x, y \in S$ we have

$$\varphi(xy) \in \varphi(S) \subseteq T$$

"

$$\varphi(x) \cdot \varphi(y) \in \varphi(S) \cdot \varphi(S) = T \cdot T$$

$$\Rightarrow T \cdot T \subseteq T$$

b) Now assume $S = \varphi^*(T)$ is multiplicative

T is multiplicative

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

• given $x', y' \in T$ then $\exists x, y \in S$ $x' = \varphi(x), y' = \varphi(y)$

Then $x \cdot y \in S$ and $\varphi(x \cdot y) = \varphi(x) \varphi(y) = x' y' \in T$

Corollary:

$\varphi: R \rightarrow R'$ hom, $J \triangleleft R'$, $I := \varphi^*(J)$

a) if J is a prime ideal then so is I

b) if φ is onto (surj) $\wedge I$ is prime $\Rightarrow J$ is prime

Proof: Apply the lemma to the complement of J

Corollary: Let $P \triangleleft R$. Then

P prime $\Leftrightarrow R/P$ is a domain

Definition: $M \triangleleft R$ is a maximal ideal of $M \neq R$
and $\nexists I \triangleleft R$, $M \subsetneq I \subsetneq R$

Proposition:

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

Proof:

$(\Rightarrow)$ $\exists 0 \neq x \in I$. Then $\exists x^{-1} \in R$ Hence $1 = x \cdot x^{-1} \in I$
So $I = R$

$(\Leftarrow)$

Pick $x \in R - (0)$ then $(0) \subsetneq \langle x \rangle \triangleleft R$

Since (0) is a max ideal $\langle x \rangle = R$

in particular $1 \in \langle x \rangle$ so $\exists y \in R. xy = 1$

So x is invertible

Coro. Let R be a ring. $\mathfrak{M} \triangleleft R$. Then $\mathfrak{M}$ is
max ideal $\Leftrightarrow R/\mathfrak{M}$ is a field

Proof: $\mathfrak{M}$ is a max ideal $R \Leftrightarrow (0)$ is a max ideal

$R/\mathfrak{M} \stackrel{\text{prop}}{\Leftrightarrow} R/\mathfrak{M}$ is a field

Cor. Every max ideal is prime

Proof Every field is an int domain

Examples:

a) R int domain: $R[x, y] \neq P$. Then $\langle x \rangle \triangleleft P$
is a prime ideal that is not maximal

$$\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq P$$

$\langle x \rangle$ is prime since $P/\langle x \rangle = R[y]$ is a domain

$\langle x, y \rangle$ is max $\Leftrightarrow P/\langle x, y \rangle \cong$ is a field

b) R ring, $P = R[x_\lambda; \lambda \in \Lambda]$. For each $\lambda \in \Lambda$

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

Then $P/M \cong R$

Theorem: Every proper ideal is contained in a maximum ideal

Proof:

$$I \subsetneq R$$

$$\mathcal{J} = \{ J \subsetneq R; I \subseteq J \}$$

We want to use Zorn lemma

- $I \in \mathcal{J} \Rightarrow \mathcal{J} \neq \emptyset$

- every chain has an upper bound

chain $\{I_\lambda; \lambda \in \Lambda\}$ in $\mathcal{J}$

upper bound: $J = \bigcup_{\lambda \in \Lambda} I_\lambda \subsetneq R$

Since $1 \notin I_\lambda \forall \lambda \Rightarrow 1 \notin J \Rightarrow J \neq R$

According to Zorn lemma the set $\mathcal{J}$ has the max element (maximal ideal) and it contains I

Cor:

R ring, $x \in R$ Then

$x \in R^* \Leftrightarrow x$ does not lie in max ideal

Proof

$$x \in R^* \Leftrightarrow \langle x \rangle = R \Rightarrow$$

$$x \in R \Leftrightarrow \langle x \rangle \neq R \Leftrightarrow \exists M \text{ max ideal } x \in R \subseteq M \subsetneq R$$

II.1 Factorisation

R ring, integral domain

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

$a|b \Leftrightarrow \exists g \in R. b = g \cdot a \Leftrightarrow b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$

a and b are associates $a|b \wedge b|a \Leftrightarrow a = bu \Leftrightarrow \langle a \rangle = \langle b \rangle$

a is a proper divisor of $b \Leftrightarrow b = a_2, a, g \notin R^\times$
 $\Leftrightarrow \langle b \rangle \subsetneq \langle a \rangle \subsetneq R$

a is irreducible $\Leftrightarrow a \notin R^\times$ and has no proper divisors
 $\Leftrightarrow$ maximal among principal ideals

p is prime element $\Leftrightarrow p \in R^\times \wedge (p|ab \Rightarrow p|a \vee p|b)$
 $\Leftrightarrow \langle p \rangle$ is prime ideal

Definition Domain R is UFD (unique factorisation domain) if

- 1) each element is a product of irreducibles and units
- 2) factorisation is unique up to units and order

Prop: An int-domain R is UFD $\Leftrightarrow$

1) every ascending chain of principal ideals stabilizes

2) every irreducible element is prime

Proof:

$\Rightarrow$ if $\langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$

then $a_{i+1} | a_i$ & a_i / a_{i+1} is not a unit

so the number of factors strictly decreases

This cannot happen so 1 holds

• Suppose p is irreducible and $p | ab$ Factor a, b . The uniqueness of factorization

Filipovi zpisu

Def: A domain R is principal ideal domain (PID)
if every ideal is principal

Prop: R PID. Then

- a) Every irreducible element is prime
- b) Every nonzero ideal is max

Proof:

Filip zgrski

III Radical ideals

Def: Jacobson radical of ring R $\text{rad}(R)$ is the intersection of all max ideals of R .

$$\text{rad} R = \bigcap_{M \in \text{Max} R} M$$