Proper ideal $I \subset R$: any ideal other than $R = (1)$, (0) is a proper ideal.

Prime and maximal ideals

(see Friedman, Ideals, section 2)

Def An ideal $I \subset R$ is a prime ideal if $I \neq R$ and if $rs \in I$ then $r \in I$ or $s \in I$, for $r, s \in R$.

Prop R/I is an integral domain if and only if I is a prime ideal in R.

$\bar{r} = r+I, \bar{s} = s+I$

Proof R/I has zero divisors $\Leftrightarrow \exists$ zero divisors $\underset{\neq I}{r+I}, \underset{\neq I}{s+I}$ $(r+I)(s+I) = I \Leftrightarrow r \notin I, s \notin I$

$\Leftrightarrow \exists r, s \quad rs + I = I, r \notin I, s \notin I \Leftrightarrow \exists r, s \quad rs \in I, r \notin I, s \notin I$

Examples 1) (0) is a prime ideal iff R is an integral domain.

2) $(21) \subset \mathbb{Z}$ is not a prime ideal, $3, 7 \notin (21)$, $3 \cdot 7 \in (21)$

3) $(nm) \subset \mathbb{Z}$ $n, m > 1$ is not a prime ideal $nm \in (nm)$ but $n, m \notin (nm)$

4) $(x^2+x) \subset F[x]$ is not a prime ideal $x, x+1$ $x(x+1) \in (x^2+x)$

Prime ideals in $\mathbb{Z}$: (0), $(p) = (-p)$

Prime ideals in $F[x]$: (0), $(p(x))$ monic irreducible.

Def $I \subset R$ is a maximal ideal if $I \neq R$ and for any ideal J, $I \subset J \subset R$, either $J = I$ or $J = R$.

Thm R/I is a field iff I is a maximal ideal.

Proof: Recall that F is a field iff the only ideals of F are (0) and F.

Assume R/I is a field. Let $I \underset{\text{proper}}{\subsetneq} J \subset R \Rightarrow J \supset I + (j)$, $j \in J \setminus I$. Since R/I is a field, $\exists k$ s.t. $jk = 1 + i$, some $i \in I$.

$j+I, k+I$ are inverses in R/I $\Rightarrow$ $j \neq 0, j \notin I$

$\Rightarrow (j) + I \ni 1 \Rightarrow (j) + I = (1) = R$. entire ring.

Exercise: Complete the proof. Assume R/I is not a field. $\exists$ noninvertible j. It has the property $jk \notin 1 + I$ $\forall k$. Consider ideal $I + (j)$.

$I \subset I + (j) \subsetneq R$ proper inclusions

Alternative proof. Use

Thm (Correspondence theorem for rings)

$R \xrightarrow{\alpha} R/I$
quotient map

$I \subset R$ proper ideal $\to R/I$ quotient ring

There is a bijection between intermediate ideals J, $I \subset J \subset R$ and ideals $K \subset R/I$

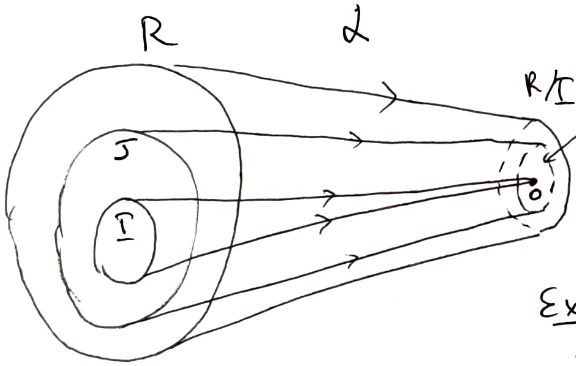
Intermediate ideals $\longleftrightarrow$ ideals of R/I

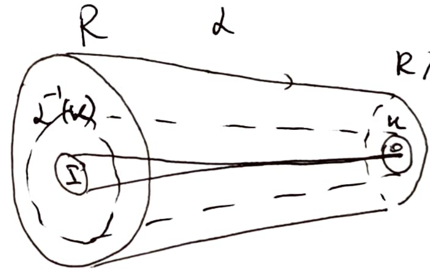
$I \subset J \subset R$

$J \longmapsto J/I = \{a + I : a \in J\}$, $J/I = \alpha(J)$

$\{j \in R \mid \alpha(j) \in K\} \longleftarrow K$

$= \alpha^{-1}(K)$ notation for inverse image of a set under a map α





__Exercise__ Prove Correspondence thm for rings. Compare with correspondence theorem for groups (see Ex. 38 in Rotman, p. 23)

__Second proof of Thm from page 1:__ Use Correspondence theorem. If $\exists J$, $I \subset J \subset R$, $J \neq I, R \Rightarrow \alpha(J)$ is a proper ideal of R/I
$(0) \subset \alpha(J) \subset R/I$

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & R/I \\ \cup & & \cup \\ J & \longrightarrow & \alpha(J) \end{array}$$
ideal that is neither (0) nor R/I

Any intermediate ideal J in R will produce an ideal in R/I other than (0), R/I and vice versa

$K \subset R/I$ ideal, $\alpha^{-1}(K) = \{a \mid \alpha(a) \in K\}$ is an intermediate ideal
$K \neq 0, R/I$

Corollary: A maximal ideal is a prime ideal

Holds, since any field is an integral domain

Example 1) $\mathbb{Z}$ $\quad (0), (p)$, p - prime are prime ideals

(p), p - prime are maximal ideals

(0) is a prime but not a maximal ideal

2) $\mathbb{Z}[x]$ $\quad (x)$ is prime ideal $\quad \mathbb{Z}[x]/(x) \cong \mathbb{Z}$ integral domain

(x) is not maximal, $\mathbb{Z}$ not a field

what happens if we change from $\mathbb{Z}$ to a field F in this example?

Thm $I \subset F[x]$ an ideal. TFAE:

(1) I is a maximal ideal

(2) I is a prime ideal and $I \neq \{0\}$

(3) there exists an irreducible polynomial p such that $I = (p)$

Proof (for more details see Friedman, Thm 3.1. in Factorizations section)

(1) $\Rightarrow$ (2) $\quad$ maximal implies prime; $(0) \subset F[x]$ is not maximal.

(2) $\Rightarrow$ (3) $\quad F[x]$ is a PID $\Rightarrow I = (p)$ some p. What to show p is irreducible. Otherwise $p \in F$ a constant $\begin{cases} p \in F^* & (1) = F[x] \text{ not maximal} \\ p = 0 & (0) \text{ not maximal} \end{cases}$

or $p = fg$ $\quad \deg f, \deg g < \deg p. \Rightarrow fg \in (p)$, but $f \notin (p), g \notin (p)$ due to their degrees.

(3) $\Rightarrow$ (1) $\quad$ If $I = (p)$, p irreducible $\Rightarrow p$ not a unit, $(p) \neq 0, F[x]$

if $(p) \subset J \subset F[x]$ intermediate ideal, $J = (f)$, some f

$(p) \subset (f) \Rightarrow \quad p = fq$, but p is irreducible $\Rightarrow J = F[x]$ or $J = (p)$.

<u>Corollary</u> Let $f \in F[x]$. Then $F[x]/(f)$ is a field iff f is irreducible.

<u>Explanation</u>: How to find the inverse of $g + (f) \in F[x]/(f)$?

$g \notin (f)$

$\gcd(f, g) = 1$ $1, f$ are the only factors of f.

$\Rightarrow 1 = af + bg$ some a, b.

$\Rightarrow bg = 1 - af$, $bg \in 1 + (f)$. $\Rightarrow$

b is the inverse of g in $F[x]/(f)$.

Get a large supply of fields that contain F, one for each irreducible polynomial. Can assume f monic

$c \in F^*$ $(cf) = (f) \Rightarrow F[x]/(fc) \simeq F[x]/(f)$.

$\deg f = 1$ $f = x + a$ $F[x]/(x+a) \simeq F$ exercise.

need irreducible polynomials of $\deg \geq 2$ for interesting examples

$\mathbb{R}[x]$, $f = x^2 + 1$ $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ a field

$\mathbb{F}_2[x]/(x^3+x+1) \simeq \mathbb{F}_8$ field with 8 elements, see last lecture

$\mathbb{F}_2[x]/(x^2+x+1) \simeq \mathbb{F}_4$ 4-element field $\{0, 1, x, x+1\}$ $x(x+1) = 1$. $x+1 = x^{-1}$ in $\mathbb{F}_4$.

irreducible, no roots in $\mathbb{F}_2$

relabel x into y

$E = \mathbb{F}_2[y]/(y^2+y+1)$ $\qquad \{0,1,y,y+1\}$.

E is a field, $E = \mathbb{F}_4$

Polynomial $\quad f(x) = x^2+x+1 \quad$ irreducible in $\mathbb{F}_2$

$f(x) = (x+y)(x+y+1)$ factors in E.

$(x+y)(x+y+1) = x^2 + (y+1)x + yx + y(y+1) = x^2+x+1$.

Made the field of constants larger, polynomial factors.

$f(x)$ - irreducible $\Rightarrow F[x]/(f(x))$ is a field

we use a different variable $\quad E = F[y]/(f(y))$.

$$\begin{array}{ccc} F[x] & \subset & E[x] \\ \cup & & \cup \\ F & \subset & E \end{array}$$

constants $\qquad y$

still free to use x.

In $F[x]$, no relations on powers of x

In E, relation on powers of y.

E is a field, since f is irreducible

evaluation homomorphism $\quad E[x] \xrightarrow{ev_y} E$

x - formal variable

$y \in E$ "constant"

$f(x) \longmapsto f(y)$

$$\begin{tikzcd} F[x] \arrow[r, phantom, "\subset"] \arrow[dr, "ev_y"] & E[x] \arrow[d, "ev_y"] \\ F \arrow[u, phantom, "\cup"] \arrow[r, phantom, "\subset"] & E \end{tikzcd}$$

$f(y) = 0$ in E

$ev_y(f(x)) = 0$

$\Rightarrow y$ is a root of $f(x)$. $\Rightarrow f(x)$ factors nontrivially in E.

$x-y \mid f(x)$, $\qquad f(x) = (x-y)g(x) \qquad g(x) \in E[x]$

coefficients in E

$f(x) = x^2+1$ irreducible in $\mathbb{R}[x]$

$E = \mathbb{R}[y]/(y^2+1)$ or $\mathbb{R}[i]/(i^2+1)$ secretly $i = \sqrt{-1}$

$y = \sqrt{-1}$.

y constant in E, $f(y) = y^2+1 = 0$ in E $\Rightarrow$ y a root of $f(x)$ in E.

$f(x) = (x-y)(x+y)$ factors in E.

We enlarge our field of constants from F to $\overset{E}{\overset{\shortparallel}{F[y]/(f(y))}}$

$f(x)$ must be irreducible in F, otherwise E is not a field.

now y is a root of $f(x)$ in E, $x-y \mid f(x)$

$f(y) = 0$.

$f(x) = (x-y)\,g(x)$.