Ex: $\mathbb{Z}[i]/(i-2)$ $\qquad$ $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

If we quotient R by (a), then

$a = 0$ in $R/(a)$

$\mathbb{Z}[i] \cong \underbrace{\mathbb{Z}[x]/(x^2+1)}$.

because $x^2+1=0$ and $x^2=-1$

x is the square root of -1

$$\mathbb{Z}[x]/(x^2+1) \Big/ (x-2)$$

$$= \mathbb{Z}[x]/(x^2+1, x-2)$$

$\mathbb{Z}[x]$, kill x^2+1, $x-2$.

$$\begin{cases} x^2+1=0 \\ x-2=0 \end{cases} \iff \begin{cases} x=2 \\ 2^2+1=0 \end{cases}$$

$$\iff \begin{cases} x=2 \\ 5=0 \end{cases} \quad \text{in } \mathbb{Z}[x].$$

$$\mathbb{Z}[x]/(x-2, 5) = \mathbb{Z}/5\mathbb{Z}.$$

Fields   maximal ideal   adjoining elements

solve equations

Ex: $\mathbb{R}$ ring of real numbers.

We don't have a solution to x^2+1.

Goal: Find a "larger" ring. R'.

($\mathbb{R} \subset R'$, $\mathbb{R}$ is a subring
or $\mathbb{R} \hookrightarrow R'$)

and x^2+1 has a solution in R',

$$\mathbb{R}[x]/(x^2+1) = R'.$$

$\bar{x} \in R'$, $\bar{x} = x + (x^2+1)$

$\bar{x}^2 + 1 = 0$ in R'. $\bar{x}$ is a square root of (-1) in R'

$R' \ni f(x) = a_0 + a_1 x + \dots + a_n x^n$.
$= (x^2+1) \cdot q(x) + r(x)$

$r(x) = ax + b$.

any element in R' has the form

$a\bar{x}+b$. and

if $a_1\bar{x}+b_1 = a_2\bar{x}+b_2$.

then $(a_1-a_2)\bar{x}+(b_1-b_2) = 0$ in R',

$$\underbrace{(a_1-a_2)x+b_1-b_2}_{\text{is a multiple of } x^2+1} \in (x^2+1)$$

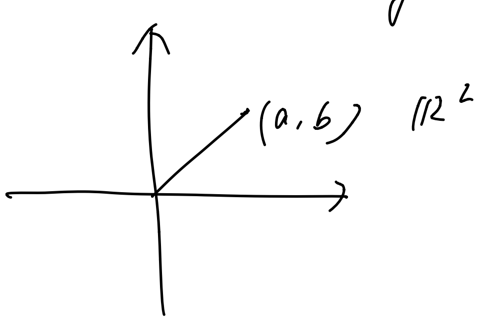
$= 0$, $\Rightarrow$ $a_1 = a_2$, $b_1 = b_2$.

Conclusion: $R' \xrightarrow[\text{as a set}]{1:1} \mathbb{R}^2$

$f(x) \longmapsto (a, b)$

$f(x) = (x^2+1)q(x) + ax+b$.

R' is actually $\mathbb{C}$.



$a+bi \in \mathbb{C}$.

$(a_1+b_1\bar{x})(a_2+b_2\bar{x})$ $\qquad \bar{x}^2=-1$

$= a_1a_2+a_1b_2\bar{x}+b_1a_2\bar{x}+b_1b_2\bar{x}^2$

$=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)\bar{x}$

$R' \cong \mathbb{C}$.

This method is called adjoining elements.

R is a ring.

$f(x)$ is a polynomial with leading coefficient $=1$.

$f(x)=x^n+a_{n-1}x^{n-1}\dots+a_0 \in R[x]$.

Goal: solve $f(x)=0$

Idea: consider $R'=R[x]/(f(x))$

(Defn) $f(x)$ is monic iff "leading coefficient of $f(x)$" $= 1$.

Prop: $R' = R[x]/(f(x))$ $\left(\text{or } \underbrace{R[\alpha]}_{\alpha = x + (f(x))},\ f(\alpha) = 0 \right)$ adjoining a root of $f(x)$

① R' has a basis $(1, \alpha, \alpha^2, \dots \alpha^{n-1})$

any element β in R' can be written as $\beta = a_0 + a_1 \alpha + a_2 \alpha^2 \dots a_{n-1} \alpha^{n-1}$ with $a_i \in R$. uniquely.

$a_0 \dots a_{n-1}$ are determined by β uniquely

② $R[\alpha]$, $f(\alpha) = 0$

$R[\alpha] \xrightarrow{1:1} R \times R \times \dots \times R = R^n$.

$\beta \longmapsto (a_0, a_1, \dots a_{n-1})$

③ multiplication in $R[\alpha]$ is determined by DWR

$\beta_1 = g_1(\alpha)$, $\quad \beta_2 = g_2(\alpha)$

$$\beta_1\beta_2 = g_1(\alpha)\cdot g_2(\alpha)$$
$$= f(\alpha)\cdot q(\alpha) + r(\alpha)$$
$$= r(\alpha)$$

Pf: ① Existence (DWR)

$$g(\alpha) = f(\alpha)\cdot q(\alpha) + \underbrace{r(\alpha)}_{\deg \le n-1.}$$

Uniqueness : if $g(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i = 0$

then $g(x) \in (f(x))$

$$g(x) = f(x)\cdot q(x)$$

$\deg f(x) q(x) \geq n$, $g(x) = 0$.

if $\beta = \underbrace{\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i}_{a_i, b_i \in R.}$ $\quad g(\alpha) = \sum_{i=0}^{n-1} (b_i - a_i)\alpha^i = 0$

Prop: α is a root of $f(x)=0$ in R'.

$R \hookrightarrow R'$. is a subring of R'.

$a_0 \mapsto a_0$

Rmk: $\deg f(x)\cdot g(x) = \underline{\deg} f + \underline{\deg g}$

is not always true.

Ex: $f(x) = 2x+1$. in $\mathbb{Z}/6\mathbb{Z}[x]$.

$g(x) = 3x+1$.

$$f(x)\,g(x) = (2x+1)(3x+1)$$
$$= 6x^2+5x+1.$$
$$= 5x+1.$$

$\deg f(x)\,g(x) = 1$.

$\deg f(x)\cdot g(x) = \deg f + \deg g$

if product of leading coefficients $\neq 0$.

Fields

Defn (units). R, ring. $s \in R$.

s is a unit iff s has a multiplicative inverse s^{-1}. $s^{-1} \cdot s = s \cdot s^{-1} = 1$. (unique)

Def (Fields). F ring. $F \neq \{0\}$

F is a field iff $F \setminus \{0\}$ is the set of units. $\frac{a}{b}$ makes sense

Ex: $\mathbb{Z}/6\mathbb{Z}$ $0, 1, 2, 3, 4, 5$.   2 unit?

$\times 2$ 0 2 4 0 2, 4.

2 has no multiplicative inverse

$\Rightarrow$ $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Criterion of fields in terms of ideals

Prop: F is a field iff F has only two trivial ideals $\{0\}$, F.

Pf: "$\Rightarrow$" $I \subset F$ is an ideal.

$I \neq \{0\}$. $a \neq 0$, $a \in I$.

$1 = a^{-1} a \in (a)$

$s \in R$, $s = 1 \cdot s \in (a)$

$\Rightarrow$ $I \supset (a) = F$.

$I = F$.

"$\Leftarrow$". Any $a \neq 0$, $a \in F$.

$(a) \neq \{0\}$, $(a) = F$.

$\exists b \in F$, s.t. $a \cdot b = 1$.

Prop: $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is a prime number.

Pf: Ideals in $\mathbb{Z}/n\mathbb{Z} \longleftrightarrow$ ideals (m) in $\mathbb{Z}$ containing $n\mathbb{Z}$.

$m | n$, if n is a prime number

$m = \pm 1, \pm n$.

Then $(m) \supset (n)$ $\quad (m) = (1) = \mathbb{Z}$

or $(m) = (n)$

$\mathbb{Z}/n\mathbb{Z}$ only has two ideals

if n is not a prime number.

$n = a \cdot b$. $\underline{a \neq \pm 1,\ b \neq \pm 1}$

$\mathbb{Z} \neq (a) \supsetneq (n)$, $\mathbb{Z}/n\mathbb{Z}$ has more than two ideals. $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Prop: F is a field. then any ideal in $F[x]$ is $(f(x))$. (DWR).

Defn: $I \subsetneq R$ ideal. is called maximal ideal if $J \supset I$ is an ideal, then $J = I$, $J = R$.

Prop: $\underline{I \text{ is maximal iff } R/I \text{ is a field}}$

Pf: $\{$Ideals in $R/I\}$ $\xleftrightarrow{1:1}$ $\{$ideals J in R, $J \supset I\}$.

correspondence

Ex: $\varphi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}$.

$$a \in \mathbb{C} \longmapsto a \in \mathbb{C}$$

$$x \longmapsto 1.$$

$$y \longmapsto 2.$$

$$f(x,y) \longmapsto f(1,2)$$

IWR..

$\ker\varphi = (x-1, y-2)$ is a maximal ideal

why? $\quad \operatorname{Im}\varphi = \mathbb{C}$, $\quad \underline{\mathbb{C}[x,y]/\ker\varphi} \cong \underline{\mathbb{C}}$.

$$f(x,y) = g(x-1, y-2)$$

$$= a_0 + a_1(x-1) + a_2(y-2) + a_3(x-1)^2 + a_4(x-1)(y-2) + a_5(y-2)^2 + \cdots$$

$f \in \ker\varphi$, $\quad f(1,2) = 0$.

$\iff a_0 = 0$, $\quad f \in (x-1, y-2)$

Cancellation prop: $ab = ac$. $a \neq 0$.

If $a, b, c \in R$, R is a field.

$a^{-1}ab = a^{-1}ac \Rightarrow b = c$.

Defn (Integral domain) $R \neq \{0\}$

R is an integral domain iff

R has no zero divisors,

If $ab = 0$, $a, b \in R$,

then $a = 0$ or $b = 0$.

If $a \neq 0, b \neq 0$
$\Rightarrow ab \neq 0$

If $ab = 0$, $a, b \neq 0$,

both a, b are zero divisors.

Prop: R integral domain. then

$a \neq 0$, $ab = ac \Rightarrow b = c$.

Pf: $ab - ac = 0 \Rightarrow a(b-c) = 0$

$a \neq 0$, $\Rightarrow b - c = 0 \Rightarrow b = c$.

$|R| < \infty$.

Prop: R is a finite integral domain then R is a field.

Pf: $\forall a \neq 0 \in R$.

$$m_a : R \to R$$
$$s \mapsto as.$$

Want to see whether $1 \in m_a(R)$

Cancellation prop: $m_a(b) = m_a(c) \Rightarrow b = c$

m_a is injective. $|R| < +\infty$

m_a is also surjective.

Ex: $\mathbb{Z}$, $F[x]$, F field.

R integral domain $\Rightarrow$ so is $R[x]$

Defn (prime ideal) $I \subset R$ is a prime ideal iff

$a \notin I,\ b \notin I, \Rightarrow ab \notin I.$

or $ab \in I \Rightarrow a \in I$ or $b \in I$.

Prop: I prime $\Leftrightarrow$ R/I is an integral domain.

Prop: $\{\text{maximal ideals}\} \subset \{\text{prime ideals}\}$.

Ex: $\underline{\mathbb{C}[x,y]}$, $I = (y)$

$$\mathbb{C}[x,y]/(y) \cong \mathbb{C}[x]$$

$\Rightarrow$ I is a prime ideal, but not maximal.

Later:

$F[x]$, $(f(x))$ is prime ideal $\Leftrightarrow$ $(f(x))$ is maximal.