Rings.

① Factoring (Fermat's Last theorem)

$x^n + y^n = z^n$ $(n \geq 3)$ no nontrivial solutions in $\mathbb{Q}$.

② Modules (finite generated abelian group
Jordan form)

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$. addition and multiplication.

Defn (ring). A ring R is a set with two compositions (binary operations) $+$, $\times$, such that:

① With $+$, R is an abelian group, identity is denoted by 0. inverse of x is $-x$.

② $\times$ is commutative, associative and has identity 1.

③ Distributive law $a(b+c) = ab + ac$.

Subring. subset closed under $+, \times, -$,
and contains 1.

Note: non commutative ring
$\times$ is ~~not~~ commutative.
Example: $M_{n\times n}(\mathbb{R})$ matrices.
We use "ring" to mean "commutative ring"
Zero Ring $R=\{0\}$.
Prop: If $1=0$, then $R=\{0\}$.

Prop: $(0+0)a = 0a+0a = 0a$
so $0\cdot a = 0$.

$(-b)\cdot a = -ba$.

Let $n = \underbrace{1+1+\cdots+1}_{n}$ in R.
then $n\cdot a = (1+1+\cdots+1)a = \underbrace{a+\cdots+a}_{n}$.

unit an element that has a multiplicative inverse.

$\mathbb{Z}$. units $\{\pm 1\}$.

$\mathbb{R}$ units $\mathbb{R}-\{0\}$

Polynomial ring.

R ring.

$f(x) = a_n x^n + a_{n-1} x^{n+1} + \cdots + a_0$.

(formal polynomial)

x^i monomial

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$

$f = g$ iff $m = n$, $a_i = b_i$

$\left(\prod_{i=0}^{n} R\right) \ni (a_0 \cdots a_n, a_{n+1} \cdots -)$

finitely many non-zero elements.

First non-zero element a_n is leading coefficient.

monic polynomial has leading coefficient equal to 1

$$f+g = (a_0+b_0)+(a_1+b_1)x+\cdots$$

$$f\cdot g = a_0b_0 + (a_1b_0+a_0b_1)x + (a_1b_1+a_2b_0+a_0b_2)x^2 + \cdots$$

Division with Remainder.

$$g(x) = f(x)q(x)+r(x). \quad \deg r < \deg f.$$

Prop (DWR) Division with remainder can be done if leading coefficient of f is a unit.

Non Example: $g(x) = x^2+1$, $f(x) = 2x+1$ in $\mathbb{Z}[x]$.

(Fields) $R - \{0\}$ are all units. $R \neq \{0\}$.

Example: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$. p prime.

$\mathbb{Z}/p\mathbb{Z}$ is a field because

(Fermat little theorem) (FLT)

$a \neq 0$, $a^{p-1} \equiv 1 \pmod p$.

Proof for FLT relies on the following cancellation property

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

(or equivalently. non existence of zero divisor)

Defn of zero divisor.

If $ab = 0$, $a \neq 0$, $b \neq 0$. Both a, b are zero divisor.

Zero divisor can not be units. If a has an inverse

$ab = 0 \Rightarrow a^{-1} \cdot a \cdot b = 0 \Rightarrow b = 0$.

If there is no zero divisor, then

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

$\Rightarrow$ $a(b-c) = 0 \Rightarrow b-c=0 \Rightarrow b=c$.

$R = \mathbb{Z}/p\mathbb{Z}$ satisfies this property.

This means the map $m_a: R \to R$
$b \mapsto ab$

is injective.

Since R is finite set.

m_a is also surjective.

so 1 has an preimage.

so $\exists b$. s.t. $ab = 1$.

Choose all the non zero elements.

$b_1, \cdots, b_{p-1}$.

$m(a)$: $ab_1, \cdots, ab_{p-1}$. are also all the non zero elements.

$b_1 b_2 \cdots b_{p-1} = ab_1 \cdot ab_2 \cdots ab_{p-1}$

$\Rightarrow (b_1 \cdots b_{p-1}) = a^{p-1} \cdot (b_1 \cdots b_{p-1})$

$\Rightarrow a^{p-1} = 1$ in R

Homomorphism: $\varphi : R \to R'$.

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1) = 1.$$

Example: $\varphi : \mathbb{Z} \to \mathbb{F}_p$

Prop: There is exactly one homomorphism $\mathbb{Z} \to R$.

$\varphi : R \to R'$.

$\ker \varphi = \{ s \in R \mid \varphi(s) = 0 \}$.

Property of $\ker(\varphi)$:

1. closed under addition
2. If $s \in \ker(\varphi)$, then $rs \in \ker(\varphi)$ for all $r \in R$.

Ex: evaluation map

$$\mathbb{R}[x] \to \mathbb{R}$$
$$p(x) \mapsto p(a).$$

Prop (substitution principle)

$\varphi: R \to R'$ ring homomorphism.

$\forall \alpha \in R'$, there is a unique homomorphism

$\Phi: R[x] \to R'$, such that

$$\Phi(x) = \alpha.$$

More generally. $\forall \alpha_1, \alpha_2, \cdots \alpha_n$.

$\exists ! \, \Phi: R[x_1, \ldots x_n) \to R'$, such that
$$\Phi(x_i) = \alpha_i.$$

Ex: $R \xrightarrow{\varphi} R' \hookrightarrow R'[x)$. (change of coefficients)

$$x \mapsto x.$$

$$f(x) = \sum a_i x^i \mapsto \sum \varphi(a_i) x^i$$

Defn: (Ideal) $I \subset R$.

① closed under addition

② If $s \in I$, $r \in R$, then $rs \in I$.

If $s_1, s_2, \dots s_n \in I$, then

$\sum r_i s_i \in I$, $\forall r_1 \dots r_n \in R$.

Defn: (Ideal generated by $s_1 \dots s_n$)

$$I = \{ \sum r_i s_i \mid r_i \in R \} = (s_1, \dots s_n)$$

principal ideal: $(a) = Ra = \{ ra \mid r \in R \}$.

(0) zero

(1) unit ideal $= R$.

proper neither (1) or (0)

Prop:

ⓐ Field F has exactly two ideals (0) and (1)

ⓑ any ring has only two ideals is a field.

Ideals in $\mathbb{Z}$,

Any subgroup in $\mathbb{Z}^+$ is an ideal.

$$n \cdot x = x + \cdots + x.$$

Classification of subgroups in $\mathbb{Z}^+$, (n).

all ideals are principal. ($I \subset \mathbb{Z}$, Find $x \in I$, $x \neq 0$, with minimal $|x|$)

Ideals in $F[x]$. F is a field.

any ideal in $F[x]$ is principal.

Find $0 \neq f(x) \in I$, such that.

$f(x)$ has minimal deg

G.C.D (Greatest common divisor) $f, g \in F[x]$.

$$(f, g) = (d(x))$$

a). $(d) = (f, g)$.

b) d divides f, d divides g.

c). If $e = e(x)$ divides f and g then $e(x)$ divides $d(x)$

d) $\exists\, p, q$, s.t. $d(x) = f p + g q$

use Euclidean algorithm to find $d(x)$.

$f(x) = x^2 - 2x - 3 = (x-3)(x+1)$

$g(x) = (x-3)(x^2+x+1)$

$= x^3 - 2x^2 - 2x - 3$.

$g(x) = x(x^2-2x-3) + (x-3)$

$(f, g) = (f, r) = (0, x-3) = (x-3)$

Quotient ring. R/I.

$R/I = R^+/I^+ = \{a+I \mid a \in I\}$

Defn and Thm: There is a unique ring structure on R/I, s.t. $R \to R/I$ is a ring homomorphism.

Defn: $(a+I)(b+I) = ab+I$.

check well-defined.

$a+I = a'+I$ then $a = a'+u$ $u, v \in I$.
$b+I = b'+I$ $b = b'+v$

$$ab = a'b' + \underbrace{ub' + va' + uv}_{\in I}.$$

First isomorphism Thm:

If $f: R \to R'$ surjective ring homo

then $R/I \xrightarrow{\sim} R'$. $I = \ker f$.

Mapping property. If $f: R \to R'$ ring homo with $\ker f = K$. $\pi: R \to R/I$.

a) If $I \subset K$, then $\exists!$ $\bar{R} = R/I \to R'$.

s.t. $\bar{f}\pi = f$.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & R' \\
R/I \arrow[ur, dashed, "\bar{f}"'] &
\end{tikzcd}$$

b) If $K = I$, $\bar{f}$ is isomorphism and f surjective.

Thm (Correspondence Thm)

$\varphi : R \to R'$ is surjective ring homomorphism. $K := \ker\varphi$

$\{\text{ideals in } R \text{ containing } K\} \longleftrightarrow \{\text{ideals in } R'\}$

- If $I \supset K$, then $\varphi(I)$ is an ideal in R'
- If $\bar{I}$ is an ideal in R', then

$\varphi^{-1}(\bar{I})$ is an ideal in R.

step 1. $\varphi(I)$ is an ideal in R'.

$\varphi^{-1}(\bar{I})$ is an ideal in R

step 2: $\varphi(\varphi^{-1}(\bar{I})) = \bar{I}$. $\quad \varphi^{-1}(\varphi(I)) = I$

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

$x \mapsto t$.

$y \mapsto t^2$.

$\ker\varphi = (y - x^2)$.

why? $\quad g(x,y) \mapsto 0$.

$g(t, t^2) = 0$.

$f = y - x^2 \in \mathbb{C}[x][y]$

$g = f \cdot q + r \qquad r \in \mathbb{C}[x][y]$

$\deg$ in $y < 1$.

so $r(x,y) = r(x)$, and $r(t,t^2) = r(t) = 0$

and $r(t) = 0 \Rightarrow r = 0$.

so $g = f \cdot q$.

Ideals containing $(y - x^2)$

$\longleftrightarrow$ ideals in $\underset{\sim}{\mathbb{C}[t]}$.

$(f(t))$.

$\varphi^{-1}(f(t)) = (f(x), y - x^2)$.

Ex: $\mathbb{C}[t]/(t^2-1) = R'$

f monic.

any ideal in R' is (f). f divides $t^2 - 1$.

If $\deg f = 0$. $f = 1$.

$\deg f = 1$. $f = t - \alpha$.

$t-\alpha$ divides $h(t)$ means

$h(\alpha)=0$. (Use division with remainder).

So $f=(t-1)$. or $(t+1)$.

If $\deg f=2$. $f=t^2-1$.

Useful facts: $I=(a)$.
$J=(b)$

$I\subset J$ iff b divides a.

Adjoining elements.

$$R/(a\cdot b) \cong {}^{R/(a)}\big/_{(\bar b)}$$

Ex: $\left(\mathbb{Z}[i]/i-2\right)$

$\mathbb{Z}[i]$ is the image of
$\mathbb{Z}[x]\to\mathbb{C}$.
$x\mapsto i$.

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

why: $\varphi: \mathbb{Z}[x] \to \mathbb{C}$
$x \mapsto i$.

$\ker \varphi = (x^2+1)$,

if $g(x) \in \ker \varphi$

then $g(i)=0$, $g(-i)=0$.

so $g(x) = (x^2+1) \cdot q(x) + r(x)$

$\deg r \le 1$, but $i \notin \mathbb{Z}$,

so $r(x)=0$.

$$\left.\mathbb{Z}[x]/(x^2+1)\right/ x-2 \cong \frac{\mathbb{Z}[x]/(x-2)}{(x^2+1)}$$

$$\cong \mathbb{Z}/(5)$$

Here we use $\mathbb{Z}[x]/(x-2) \cong \mathbb{Z}$.
$x \mapsto 2$.

Important facts

If u is a unit. $a \in R$.

$$(a) = (ua)$$

$\forall\ a, b, c \in R$, u, v units

$$(a, b) = (a, b+ac).$$

or $(a, b) = (ua, v(b+ac))$

This is based on the following.

If $A_1, A_2 \dots A_n$ are represented by $a_1 \cdots a_m$

$$A_i = \sum c_{ij} a_j$$

then $(A_1 \dots A_n) \subset (a_1 \cdots a_m)$.

Example $\mathbb{Z}[x] \big/ (x^2-3,\ 2x+4)$

$$\mathbb{Z}[x] \big/ (x^2-3\ ,\ 2(x+2))$$

Change of variable

$$\mathbb{Z}[t] \longrightarrow \mathbb{Z}[x]$$
$$t \longmapsto x+2.$$

$$\mathbb{Z}[t] \big/ ((t-2)^2-3\ ,\ 2t)$$
$$= \mathbb{Z}[t] \big/ (t^2-4t+1,\ 2t).$$
$$= \mathbb{Z}[t] \big/ (t^2+1,\ 2t).$$
$$= \mathbb{Z}[t]/(t^2+1) \Big/ (2t) \cong \mathbb{Z}[t]/(t^2+1) \Big/ (2).$$
$$\cong \mathbb{Z}[t]/(2) \Big/ (t^2+1) = (\mathbb{Z}/2\mathbb{Z})[t] \Big/ (t+1)^2$$
$$\cong \mathbb{Z}/2\mathbb{Z}[t] \Big/ (t^2)$$

Characteristic of a ring:

Adjoining elements

Goal: solve equation $f(x)=0$. in R.

Ex: $\mathbb{R}$. no solution for $f(x)=x^2+1=0$

New ring $\mathbb{R}[x]/(x^2+1) =: \bar{R}$

Now $\bar{x} \in \bar{R}$ satisfies

$$\bar{x}^2+1=0.$$

Ex:

solve the inverse equation

$$a \in R, \quad ax-1=0.$$

so $R[x]/(ax-1)$.

$R=\mathbb{Z}$

$a=3$. $\mathbb{Z}[x]/(3x-1) \cong \mathbb{Z}[\frac{1}{3}] \subset \mathbb{Q}$.

Bad ex: $R=\mathbb{Z}/6\mathbb{Z}$

$a=3$. $R[x]/(3x-1) =$ zero ring.

$R \to R[x]/(3x-1)$ is a zero morphism.

Good case: $f(x)$ is monic.

$R[x]/f(x)$. or $\left(\begin{array}{l} R[\alpha] \\ f(\alpha)=0 \end{array} \right)$

(1) $R[\alpha]$ has basis

$(1, \alpha, \alpha^2 \cdots \alpha^{n-1})$.

i.e. $\forall \ \beta \in R[\alpha]$

$\beta = g(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$ a_i are uniquely determined by β.

If $\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i$, then

$a_i = b_i$.

(2) Can view $R[\alpha]$ the same as the set of n-tuples in R

$(a_0, a_1, \cdots a_{n-1})$

Addition is component wise addition.

3 Multiplication is defined as follows.

$\beta_1 = g_1(\alpha)$. $\beta_2 = g_2(\alpha)$

$\beta_1 \cdot \beta_2 = g_1(\alpha) \cdot g_2(\alpha)$

$= f \cdot q + r$.

Pf: 1 reduce to. uniqueness of 0

$0 = \sum_{i=0}^{n} a_i \alpha^i = g(\alpha)$

$g(\alpha) = f(\alpha) \cdot h(\alpha) \Rightarrow g(\alpha) = 0$.

Example: $\mathbb{R}$ $\qquad \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$$\mathbb{F}_2[x]/(x^2+x+1)$$

$0, 1, x, 1+x$

$$x(x+1) = 1 \Rightarrow x^{-1} = 1+x$$

field of order 4

Product ring

Def: $R \times R'$ has a ring structure.

$$(x, x')\cdot(y, y') = (xy, x'\cdot y')$$

$$(x, x') + (y, y') = (x+y, x'+y').$$

$$(0, 0')$$

$$(1, 1')$$

(Idempotent element) $e \in R$, $e^2 = e$.

Prop: a). $e' = 1-e$ is also idempotent.

b). eR is also a ring with identity e.

(Notice that eR is not a subring)

c). $R \cong eR \times e'R$

Pf: a) $(1-e)^2 = 1-2e+e^2 = 1-e$.

b). $\forall\, ea \in eR$.

$e \cdot (ea) = e^2 a = ea$

c). $R \longrightarrow eR \times e'R$.

$a \mapsto (ea, e'a)$

idea $e+e' = 1$.

$(e+e')a = ea + e'a$

bijection.

ring homomorphism.

Example of product ring and idempotent elements

Ex: $\mathbb{F}_2[x]/x^2+x = R$

$0, 1, x, x+1$.

$x^2 = x$, $(x+1)^2 = x^2+2x+1$
$= (x^2+x)+x+1 = x+1$

So $\mathbb{F}_2[x]/(x^2+x) \cong \underbrace{Rx} \times R(x+1)$

Ex:

$\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

Non Ex. $\mathbb{Z}/8\mathbb{Z} \not\cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$

(Chinese Remainder theorem). $I + J = R$.
Then, $IJ = I \cap J$,

$$R/IJ \cong (R/I) \times (R/J).$$

(Hint: $R \to (R/I) \times (R/J)$ is surjective.
$a \mapsto (a+I, a+J)$)

Maximal ideal.

$I \subsetneq R$ is a maximal ideal.

iff Any ideal $J \supset I$, $J = I$ or R.

Prop: $I \subseteq R$ is a maximal ideal iff R/I is a field

Pf: Use correspondence thm and the fact that any ring F is a field iff F has only two ideals (0) and F itself.

Example: $R = \mathbb{C}[x, y]$. (Find maximal ideals in R)

Define $\varphi: R \to \mathbb{C}$. $(\alpha_1, \alpha_2) \in \mathbb{C}^2$

$x \mapsto \alpha_1$ a ring homo

$y \mapsto \alpha_2$.

then $\ker\varphi = (x-\alpha_1, y-\alpha_2)$ (Think why?)

Since φ is a surjective map.

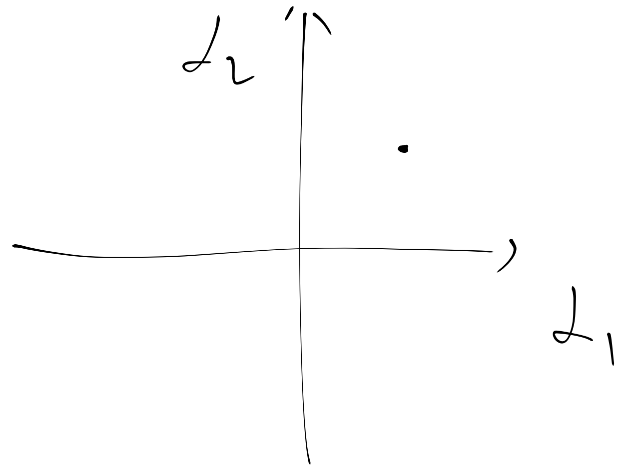
1st isomorphism Thm $\Rightarrow R/\ker\varphi \cong \mathbb{C}$.

So $(x-\alpha_1, y-\alpha_2)$ is a maximal ideal.

The converse is also true, this is the famous Hilbert's Nullstellensatz.

Thm: All the maximal ideals in $\mathbb{C}[x_1 \ldots x_n]$ are of the form $(x_1-\alpha_1, x_2-\alpha_2, \ldots, x_n-\alpha_n)$ for some $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{C}^n$

Picture



maximal ideals in $\mathbb{C}[x,y]$

Ex: $\mathbb{C}[x,y]/(y-x^2) =: R$

$\{$maximal ideals in $R\} \xleftrightarrow{1:1}$

$\{$maximal ideals in $\mathbb{C}[x,y]$ containing $(y-x^2)\}$

All the maximal ideals in R are in the form $(x-\alpha_1, y-\alpha_2)$ such that $\alpha_2 = (\alpha_1)^2$

Pf: If $(x-\alpha_1, y-\alpha_2) \supset (y-x^2)$

Then $\varphi: \mathbb{C}[x,y] \to \mathbb{C}$.

$$x \mapsto \alpha_1$$
$$y \mapsto \alpha_2$$

$(y - x^2) \subset \ker \varphi$.

then $\varphi(y - x^2) = 0 \Rightarrow \alpha_2 - \alpha_1^2 = 0$.

The converse is also true.

$$\boxed{\begin{array}{l}\text{Properties of maximal ideals in } \mathbb{F}[x].\\ (f(x)).\quad f(x) \text{ is irreducible}\end{array}}$$

Some definitions to clarify:

① Integral domain (domain)
ring without zero divisors.

② Polynomial ring: $R[x]$
"constant" means $R \subset R[x]$

③ monic polynomial
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots - a_0$.
leading coefficient $=1$.

④ Field. F
the set of units is $F \setminus \{0\}$

$$\boxed{\begin{array}{l}\text{Criterion for maximal ideals.} \\ \quad I \subset R \text{ is an ideal in } R. \\ \quad I \text{ is maximal ideal iff } R/I \text{ is a field.}\end{array}}$$

Example 1: $R = \mathbb{Z}$.

All the ideals in $\mathbb{Z}$ are in the form of (n). $n \geq 0$. $n \in \mathbb{Z}$

① If n is a prime number.

then $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ is a field $\mathbb{F}_n$

(We proved this before)

so (n) is an maximal ideal.

A more direct approach from definition.

If $J \supset (n)$ is another ideal containing (n). We write $J = (m)$.

Then $(n) \subset (m)$. so $n = m \cdot k$.

since n is a prime number, according to fundamental theorem of arithmetic

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

If $m = \pm n$, then $(m) = (n)$

If $m = \pm 1$. then $(m) = \mathbb{Z}$

Another fact we usually use:

$(x) = R$ iff x is a unit.

① If x is a unit, $1 = x \cdot x^{-1} \in (x)$

$r = r \cdot 1 \in (x)$.

② If $(x) = R$, then $1 = x \cdot a$ for some a.

(2) If n is not a prime.

$n = m_1 m_2$, $m_i \neq \pm 1$

so $\overline{m_1} \in \mathbb{Z}/n\mathbb{Z} \neq \overline{0}$

$\overline{m_2} \in \mathbb{Z}/n\mathbb{Z} \neq \overline{0}$

$\overline{m_1} \cdot \overline{m_2} = \overline{n} = \overline{0}$

so $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

$\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

hence not a field.

Example: $R = F[x]$. F is a field.

What are the maximal ideals in R?

All the ideals in R are in the form

$(f(x))$ $f(x)$ is a monic polynomial.

Def: $f(x)$ is irreducible polynomial in $F[x]$ iff

(F is a field)

① $f(x) \neq 0$ $f(x)$ is not a constant.

② If $f(x) = g(x) \cdot h(x)$. $g(x), h(x) \in F[x]$

then $g(x)$, or $h(x)$ must be constant.

Claim: $(f(x))$ is a maximal ideal iff

$f(x)$ is irreducible.

Pf: "$\Leftarrow$" If $f(x)$ is irreducible.

Assume $J = (g(x)) \supset (f(x))$.

then $f(x) = g(x) \cdot h(x)$

① If $g(x)$ is constant.

then $g(x)$ is invertible.

$(g(x)) = F(x)$

② If $h(x)$ is constant.

$g(x) = (h(x))^{-1} \cdot f(x)$

$(g(x)) = (f(x))$

" $\Longrightarrow$ " If $(f(x))$ is a maximal ideal

Assume $f(x) = g(x) \cdot h(x)$

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

① $(g(x)) = F[x]$. then

$1 = g(x) \cdot m(x)$. $\deg g = 0$.

$g(x)$ is a constant

② $(g(x)) = (f(x))$. then

$g(x) = f(x) \cdot H(x)$.

so $f(x) = f(x) \cdot H(x) \cdot h(x)$.

$\deg H = \deg h = 0$

$h(x)$ is a constant

Ex: $\mathbb{F}_2[x] / (x^2+x+1)$

$f(x) = x^2+x+1$ is irreducible.

because if $f(x) = g(x) h(x)$

and $\deg g \neq 0$, $\deg h \neq 0$.

then $\deg g = \deg h = 1$.

$g(x) = x$ or $x+1$

If $g(x) = x$, $f(0) = g(0) h(0) = 0 \cdot h(0) = 0$

but $f(0) = 1$

If $g(x) = x+1$, $f(1) = g(1) \cdot h(1) = 0 \cdot h(1) = 0$

but $f(1) = 1$

so $f(x)$ is irreducible and

$\mathbb{F}_2[x] / (x^2+x+1)$ is a field.

Example (revisited).

$R = \mathbb{C}[x, y]$. Construct maximal ideal.

$\varphi_{\alpha_1, \alpha_2} : \mathbb{C}[x, y] \to \mathbb{C}$

$f(x, y) \mapsto f(\alpha_1, \alpha_2)$

surjective.

$\ker \varphi_{\alpha_1, \alpha_2} = (x - \alpha_1, y - \alpha_2)$.

(Why ?).

$\ker \varphi_{\alpha_1, \alpha_2} \supset (x - \alpha_1, y - \alpha_2)$. (use definition).

Look at the special case. $\alpha_1 = \alpha_2 = 0$

$$f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{11}xy + a_{20}x^2 + a_{02}y^2 + \cdots$$

$$\varphi_{0,0}(f(x,y)) = f(0,0) = a_{00}$$

$f \in \ker \varphi_{0,0} \iff f(0,0) = 0 \iff$

$f \in (x, y)$

For different (α_1, α_2).

$(x-\alpha_1, y-\alpha_2)$ is different.

i.e. If $(\alpha_1, \alpha_2) \neq (\beta_1, \beta_2)$.

then $(x-\alpha_1, y-\alpha_2) \neq (x-\beta_1, y-\beta_2)$.

Pf: assume $\alpha_1 \neq \beta_1$, and

$(x-\alpha_1, y-\alpha_2) = (x-\beta_1, y-\beta_2) = I$.

then $(x-\alpha_1)-(x-\beta_1) = \beta_1-\alpha_1 \neq 0 \in I$.

$\beta_1-\alpha_1$ is a unit, so $I = \mathbb{C}[x,y]$

contradiction!

Hilbert's Nullstellensatz says

There is a one-to-one correspondence:

$$\mathbb{C}^2 \longleftrightarrow \{\text{maximal ideals in } \mathbb{C}[x,y]\}$$

$$(\alpha_1, \alpha_2) \longmapsto (x-\alpha_1, y-\alpha_2)$$

(we proved "well-defined", "injective".
Hilbert proved surjectivity)

Corollary: consider $R = \mathbb{C}[x,y]/V$.

$$V = (f_1, f_2, \cdots f_n)$$

then there is a bijection

$$\left\{ (\alpha_1, \alpha_2) \;\middle|\; \begin{array}{c} f_1(\alpha_1, \alpha_2) = 0 \\ \vdots \\ f_n(\alpha_1, \alpha_2) = 0 \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{maximal} \\ \text{ideals} \\ \text{in } R \end{array} \right\}$$

$$(\alpha_1, \alpha_2) \longmapsto (x-\alpha_1, y-\alpha_2)$$

Pf: Use correspondence theorem:

$$\{\text{maximal ideals in } R\}$$

$$\xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{maximal ideals in } \mathbb{C}[x,y] \\ \boxed{\text{containing } V} \end{array} \right\}$$

How to check containing V?

$f_i(x,y) \in (x-\alpha_1, y-\alpha_2) \iff f_i \in \ker \varphi_{\alpha_1,\alpha_2}$

$\varphi_{\alpha_1,\alpha_2}(f_i(x,y)) = 0 \iff f_i(\alpha_1,\alpha_2) = 0$

So we have the correspondence above

Factoring (Integral domain)

① How to factor integers?

$12 = 2^2 \cdot 3$ (prime numbers)

(factorization is unique).

② Why useful? $\sqrt{2}$ irrational.

If $\sqrt{2}$ is rational

$\sqrt{2} = \frac{p}{q}$ $(p, q) = 1$.

$2q^2 = p^2$ 2 is a prime.

so $2 | p$, $p = 2k$.

$q^2 = 2k^2 \Rightarrow 2 | q$.

Contradiction

③ factor elements in $\mathbb{Z}[i]$.

Why is a prime p has the form

$p = x^2 + y^2$, $x, y \in \mathbb{Z}$

Answer: $p \equiv 1 \pmod 4$. Yes

$p \not\equiv 1 \pmod 4$ No.

(4) Fermat's last theorem.

(Kummer's appoach)

Terminology:

u is a unit $\Leftrightarrow$ $(u) = (1) = R$

a divides b $\Leftrightarrow$ $b = ac$ for some c.

$\Leftrightarrow$ $(b) \subset (a)$

a is a proper divisor of b

$\Leftrightarrow$ $b = ac$, Neither a or c is a unit.

$\Leftrightarrow$ $(b) \subsetneq (a) \subsetneq (1)$

a. b associates $\Leftrightarrow$ $(a) = (b)$

a irreducible if a is not a unit. a has no proper divisor.

$\Leftrightarrow$ $(a) < (1)$,

No principal ideal (c)

$(a) \subsetneq (c) \subsetneq (1)$.

p is a prime element

if p divides ab, then p divides a or b.

$(\Leftrightarrow)$ $ab \in (p) \Rightarrow a \in (p)$ or $b \in (p)$

$(\Leftrightarrow)$ $R/(p)$ is integral domain.

Defn: (PID) Principal ideal domain. R

R : every ideal in R is a principal ideal (a)

Goal: Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD

(unique factorization Domain)

Defn:

Euclidean domain R.

R is a domain with size function

$\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. such that.

$\forall$ $a, b \in R$, $b \neq 0$.

$\exists\, q, r \in R$, s.t. $a = bq + r$.

$r = 0$ or $\sigma(r) < \sigma(b)$.

Example: $\mathbb{Z}$, σ = absolute value.

$F[x]$. F field.

σ = deg of a polynomial

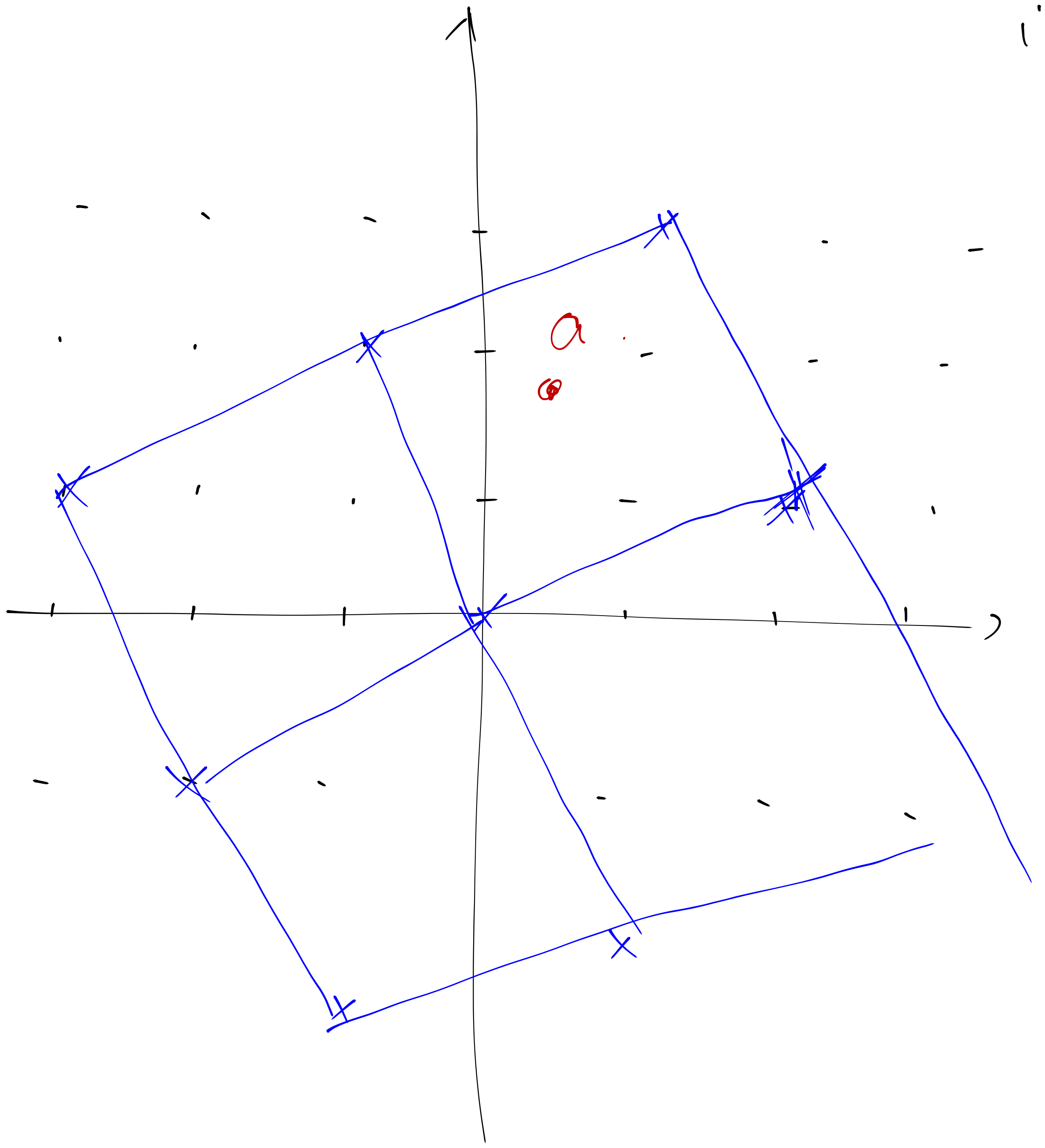
$\mathbb{Z}[i] = \{ a = m + ni \mid m, n \in \mathbb{Z} \}$.

$\sigma(a) = |a|^2$.

Let $b \neq 0$.

then (b) is the vertices of squares on $\mathbb{C}$

$b = 2+i$. The side of each square is $|b|$



a is lying in some of the squares.

so there exist one vertex of the square such that. $|a - bq|^2 < |b|^2$

so let $r = a - bq$.

$a = bq + r$. $\sigma(r) < \sigma(b)$

Thm. An Euclidean ring R is PID.

Pf: $I \subset R$ is an ideal.

then let $\min\left\{\sigma(x) \,\middle|\, \begin{matrix} x \in I \\ x \neq 0 \end{matrix}\right\} = n$.

Assume $\sigma(a) = n$.

Claim $I = (a)$.

① $(a) \subset I$ because $a \in I$.

② If $I \not\subset (a)$, then $\exists\, b \in I$, $b \notin (a)$.

$b = a \cdot q + r$.

2 I $r = 0$, $b = aq \in (a)$

2 II $r \neq 0$, $\sigma(r) < \sigma(a)$.

On the other hand $r = b - aq \in I$.

because $b \in I$, $a \in I$.

Contradict with $\sigma(a) = n$ is the minimal value for $\sigma(x)$, $x \in I \setminus \{0\}$.

$$\boxed{\begin{array}{l}\text{Euclidean domain} \Rightarrow \text{Principal Ideal domain} \\ \qquad\qquad \Rightarrow \text{uniquely factorization domain.}\end{array}}$$

Defn (UFD). $\forall a \in R$. if a is not irreducible

$a = a_1 b_1$. neither a_1. nor b_1 is unit

$a_1 = c_1 d_1$, $b_1 = c_2 d_2$ ....

Factoring terminates if after finite steps, all the factors are irreducible.

$a = p_1 p_2 p_3 \cdots p_m$. p_i are irreducible.

$= q_1 q_2 \cdots q_m$ q_m are irreducible.

The irreducible factorization is unique.

if $m = n$, and after rearranging $q_1 \cdots q_m$ suitably, q_i is an associate of p_i for each i.

Example:

In $\mathbb{Z}[i]$. $5 = (1+2i)(1-2i)$

$= (2+i)(2-i)$.

$1-2i$ and $2+i$ are associates.

$(2+i)i = 1-2i$.

$i(-i) = -1$ i is a unit in $\mathbb{Z}[i]$.

Lemma 1: In an integral domain R, any prime element is irreducible

Pf: p prime element, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

p irreducible if $p = ab$ one of a, b must be unit. (or one of a, b is an associate of p)

If p is prime and $p = ab$, then

$p \mid a$ or $p \mid b$.

Assume $a = p \cdot c$.

then $p = p \cdot cb \Rightarrow bc = 1$.

Lemma 2: If R is PID, then every irreducible element is a prime element.

Pf: Assume p is irreducible, then there is no principal ideal

$$(p) \subsetneq (c) \subsetneq (1).$$

so (p) is maximal ideal.

$R/(p)$ is a field.

So p is prime.

Prop: i) Suppose factoring process terminates in R. Then R is UFD iff every irreducible element is a prime element.

ii) PID is UFD.

i) Pf: $\Leftarrow$ $a = p_1 p_2 \cdots p_m$

$= q_1 q_2 \cdots q_n$.

$m \le n$, induction on n.

$n = 1$, then $a = p_1 = q_1$.

$n \geq 2$, q_1 irreducible $\Rightarrow$ q_1 prime $\Rightarrow$

q_1 divides $p_1 \cdots p_m$, then

q_1 divides p_j.

Assume $q_1 \mid p_1$. since p_1 is irreducible.

q_1 is a unit or associates with p_1.
Since q_1 is irreducible. q_1 is not a unit. so q_1, p_1 are associates.
We can assume $q_1 = p_1$ by multiplying a unit to p_1.

so $q_2 q_3 \cdots q_n = p_2 \cdots p_m$.

(ii) We only need to prove that factoring terminates.

Prop: ① and ② are equivalent:

① Factoring terminates

② R does not contain an infinite strictly increasing chain

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq \cdots$$

① ⇒ ②. $(a_1) \subsetneq (a_2)$

$\Rightarrow \quad a_1 = a_2 b_1$ $\quad b_1$ not unit.

$= a_3 b_2 b_1$

$= \cdots\cdots$

② ⇒ ①. $a_1 = a_2 b_1$

$= a_3 b_2 b_1$

$= \cdots\cdots$

then $(a_1) \subsetneq (a_2) \subsetneq \cdots$

For PID, if $(a_1) \subseteq (a_2) \cdots$

Take the union $\bigcup (a_i) = I$.

I is an ideal, and $I = (a)$.

so $a \in \bigcup (a_i)$. assume

$a \in (a_j)$, then $(a_j) = \bigcup (a_i)$

so $(a_j) = (a_{j+1}) = \cdots$

Non UFD.

$\mathbb{Z}[\sqrt{-5}]$.

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

2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are all irreducible.

Review:

Defns: Rings, units ideals, principal ideals,

polynomial ring $R[x]$, quotient ring.

homomorphism, subring, kernel.

Product ring, maximal ideals.

idempotent element. characteristic

integral domain. , divisor. prime element, zero divisor

irreducible element, associates.

Euclidean ring $\Rightarrow$ PID $\Rightarrow$ UFD

Fractions.

Thms: ① substitution principle, extend $\underbrace{\varphi: R \to R'}_{\text{homomorphism}}$.

to $R[x] \to R'$.

$x \mapsto a$

② correspondence thm

Ex: Find ideals containing $(y-x^2)$ in $\mathbb{C}[x,y]$

$\varphi: \mathbb{C}[x,y] \to \mathbb{C}[t]$.

$x \mapsto t$

$y \mapsto t^2$.

$\ker \varphi = (y-x^2)$

Find maximal ideals in $\mathbb{Z}/8\mathbb{Z}$.

③ Adding relations.

$$R/(a,b) \cong R/(a) \Big/ (b)$$

$$\cong R/(b) \Big/ (a)$$

$$\mathbb{Z}[i]/(i+3)$$

④ Adjoining elements.

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

then $R[x]/(f(x))$ has a basis

$1, \alpha, \dots \alpha^{n-1}$

⑤ Division with remainder.

5.1 How to calculate in $\mathbb{F}[x]$

5.2. How to calculate in $\mathbb{Z}[i]$

(6) Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD

$\mathbb{Z}[i]$ is Euclidean domain

(7) Hilbert's Nullstellensatz.

(8) Maximal ideals in $\mathbb{Z}$, and $\mathbb{F}[x]$ ($\mathbb{F}$ a field)

(9) I is maximal ideal iff R/I is a field.

(10) In PID, prime $\Leftrightarrow$ irreducible.

Useful techniques.

① change of variable in $\mathbb{C}[t]$, or

$\mathbb{C}[x,y]$

② If R is an integral domain.

In $R[x]$. $\deg f(x) + \deg g(x)$

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