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 $2 \mid p$, $p = 2k$.

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

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

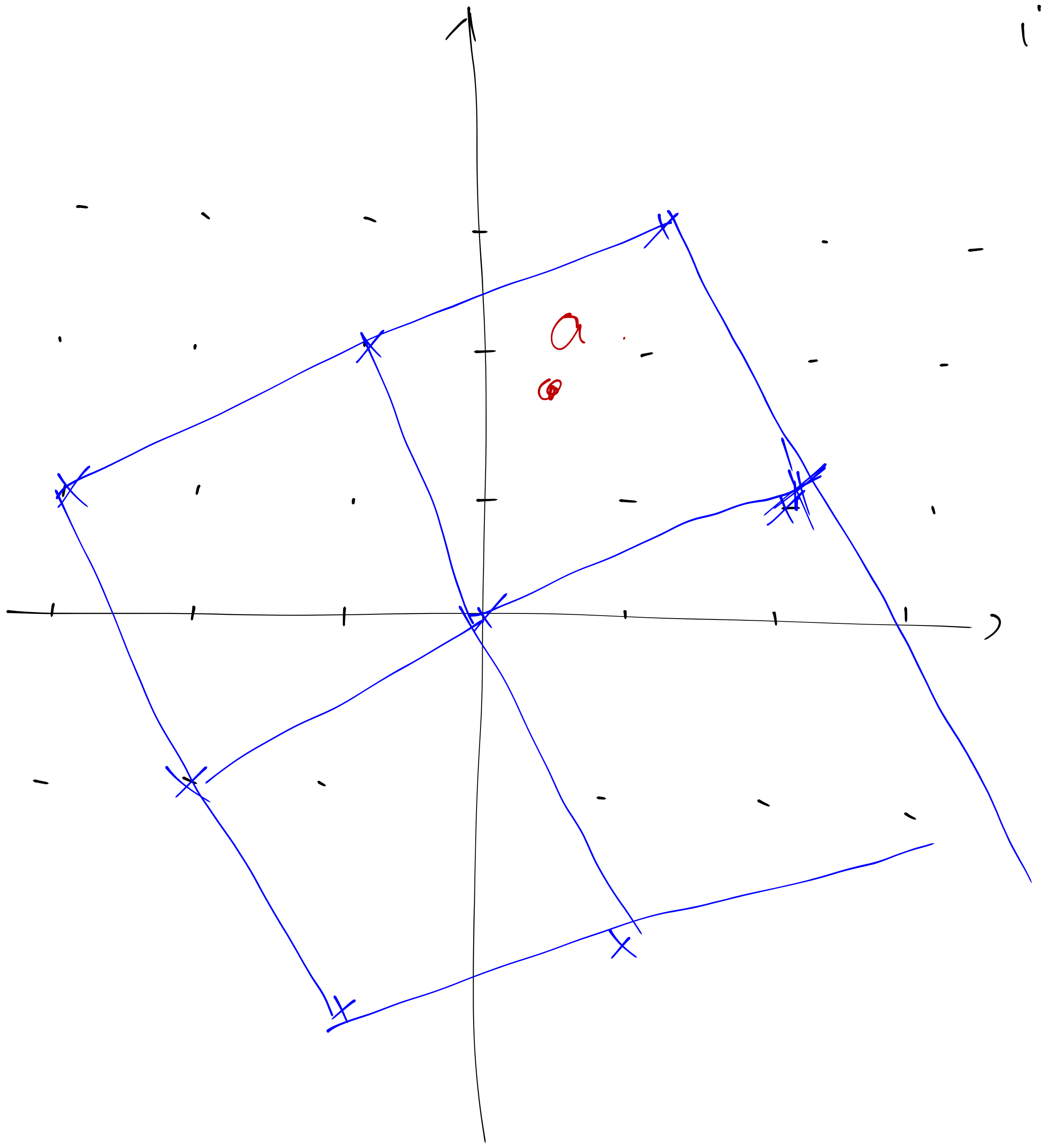
$\mathbb{Z}[i] = \{ a = m + ni \mid m, n \in \mathbb{Z} \}$.

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

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 $\min \{ \sigma(x) \mid x \in I, x \neq 0 \} = n$.

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

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

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 $\sigma(x)$, $x \in I \setminus \{0\}$