HW 1 due Friday.
Discuss problem 8.

Current Goal:
- abstract (verb) properties of $\mathbb{Z}$
- to do number theory
- but it leads to more ... (algebraic geom.)

Some definitions:

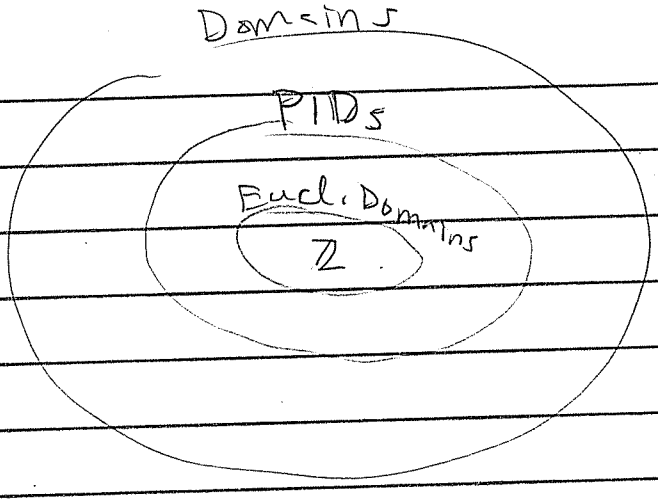
- An integral domain is (comm.) ring R with 1 and no zero divisors.
  i.e. $ab = 0 \Rightarrow a = 0$ OR $b = 0$.

[Note: In this class, almost all rings are integral domains.]

- An integral domain is a PID if all ideals are principal $(a) \subseteq R$.

- A domain R is Euclidean if $\exists$ function $N: R \setminus \{0\} \to \mathbb{N}$ such that
  $\forall\, a, b \neq 0$ in R $\exists\, q, r \in R$ such that
  - $a = qb + r$
  - $N(r) < N(b)$ OR $r = 0$

Relationships:



Examples of Euclidean Domains

① $\mathbb{Z}$ with $N(a) = |a|$.

IOU. ② Polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$ with $N(f) = \deg(f)$.

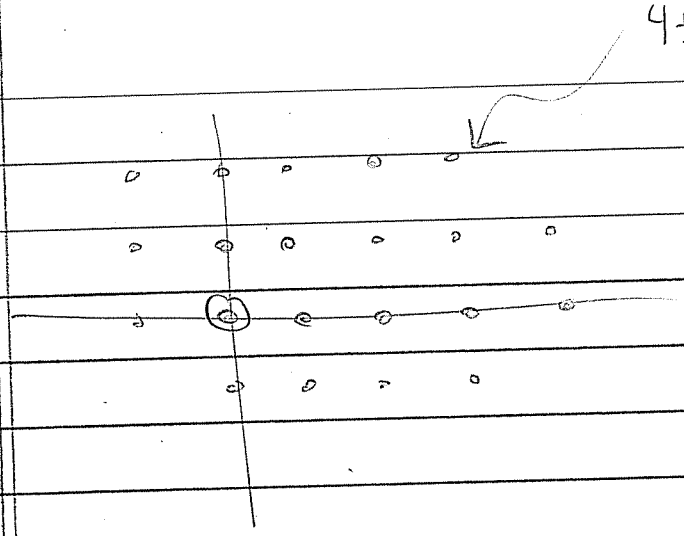
③ The Gaussian integers.

$$\mathbb{Z}[i] := \{a+ib : a, b \in \mathbb{Z},\ i^2 = -1\}.$$

with $N(a+ib) = a^2 + b^2$.

Proof that $\mathbb{Z}[i]$ is Euclidean:

Think of $\mathbb{Z}[i]$ as a square lattice. (Warning: "lattice" means two different things) in the complex plane,



Consider $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0 = 0+i0$.

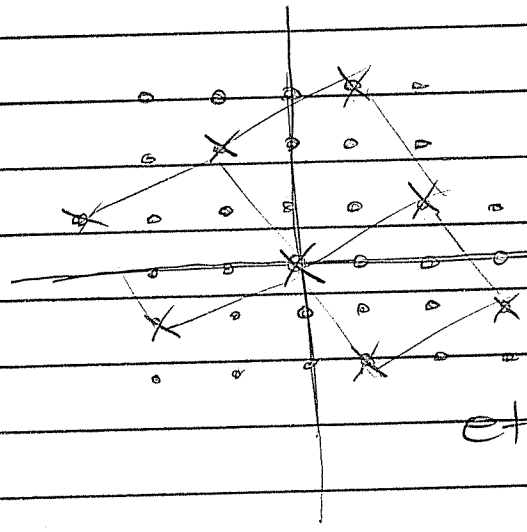
Claim: $\exists\ \mu, \rho \in \mathbb{Z}[i]$ with

- $\alpha = \mu\beta + \rho$
- $N(\rho) < N(\beta)$ OR $\rho = 0+i0$.

Here $N(a+ib) = a^2+b^2 = |a+ib|^2$
length squared.

It is enough to find ρ with $0 \leq |\rho| < |\beta|$.
So consider the principal ideal $(\beta) \subseteq \mathbb{Z}[i]$
What does it look like?

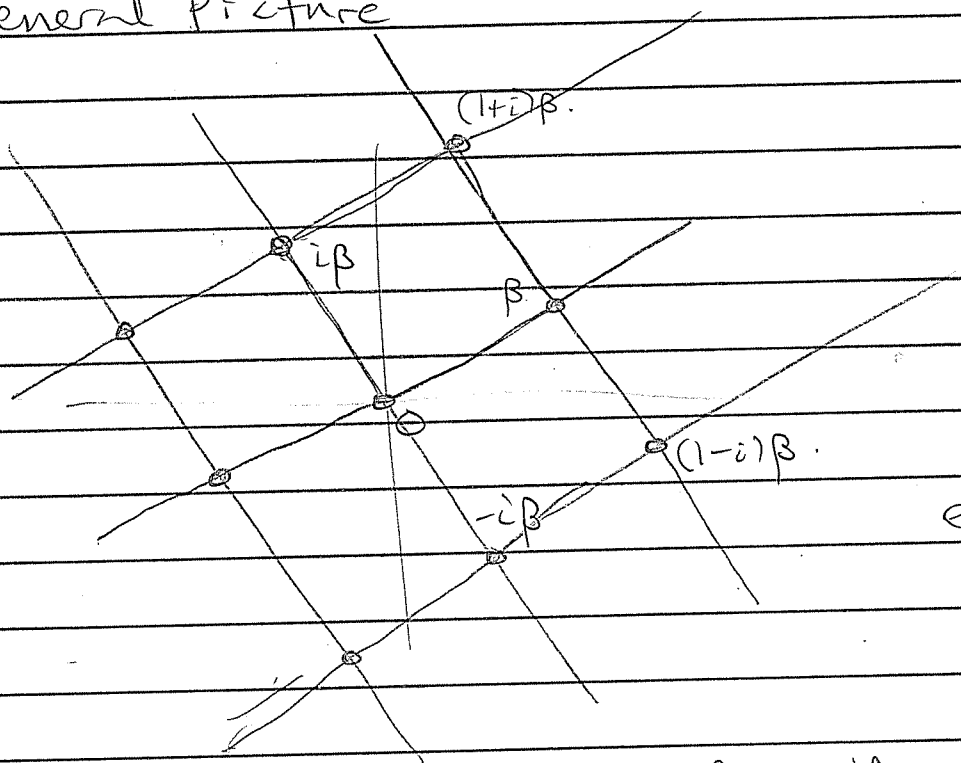
Eg. $\beta = 2+i$



The ideal $(2+i)$ is a square sublattice.

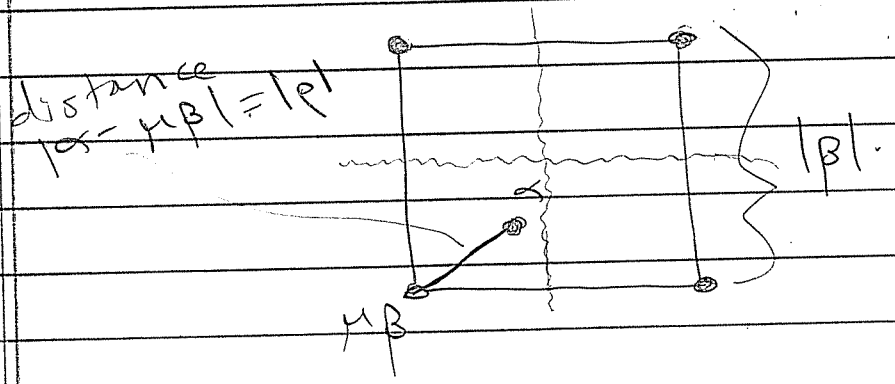
etc.

General Picture



(All principal ideals look like this).

Now given $\alpha \in \mathbb{Z}[i]$ choose $\mu \in \mathbb{Z}[i]$ so $|\alpha - \mu\beta|$ is minimized.



Let $\rho = \alpha - \mu\beta$.

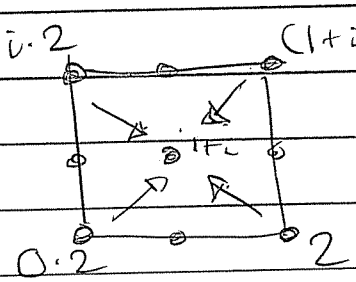
$\Longrightarrow \alpha = \mu\beta + \rho$ with

$|\rho| = |\alpha - \mu\beta| \leq \frac{\sqrt{2}}{2}|\beta| < |\beta|$ ▨

Note: Division with remainder is not unique.

Ex. Let $\alpha = 1+i$, $\beta = 2$.

Divide α by β $\longrightarrow$ 4 choices



$|1+i| < |2|$.

$(1+i) = 0 \cdot 2 + (1+i)$.

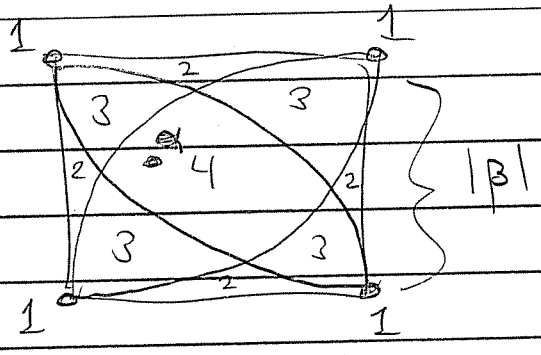
$(1+i) = 1 \cdot 2 + (-1+i)$

$(1+i) = i \cdot 2 + (1-i)$

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

In general

possible remainders



But that's OK ☺

//

Theorem (Prop 12.2.7).
Euclidean Domain $\Rightarrow$ PID.

Proof: Let R be Euclidean with norm
$N: R\setminus\{0\} \to \mathbb{N}$.
Let $I \subseteq R$ be any ideal. If $I=(0)$, done.
So choose $0 \neq a \in I$ with minimum $N(a)$.
(exists by well-ordering; not unique)

Know $(a) \subseteq I$. Want $I \subseteq (a)$.
So take any $d \in I$ and divide by a to get

$$d = qa + r \quad \text{with } r=0 \text{ or } N(r) < N(a).$$

But $r = d - qa \in I \Rightarrow N(r) \not< N(a)$.
$\Rightarrow r = 0 \Rightarrow d \in (a)$

$\blacksquare$

HW 1 due NOW.
HW 2 out on Mon
due Wed Feb 15
Exam 1 Fri Feb 17

Today: More $\mathbb{Z}[i]$.

What are the units of $\mathbb{Z}[i]$?

Note: $\mathbb{Z}[i]$ is a subring of $\mathbb{C} = \mathbb{R}[i]$ under the inclusion homomorphism

$$\mathbb{Z}[i] \xrightarrow{\iota} \mathbb{R}[i]$$
$$a+ib \longmapsto a+ib.$$

Suppose $\alpha = a+ib \in \mathbb{Z}[i]^\times$. So $\exists\ \beta \in \mathbb{Z}[i]$ with $\alpha\beta = 1+0i$.
But then $\alpha\beta = 1$ in $\mathbb{C}$ also.

$$\Rightarrow \beta = \frac{\overline{\alpha}}{|\alpha|^2} = \frac{1}{a^2+b^2}(a-ib).$$

But $\beta \in \mathbb{Z}[i]$

$$\Rightarrow \frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Z}.$$

$$\Rightarrow (a,b) = (1,0), (-1,0), (0,1), (0,-1)$$
$$\alpha = 1, \quad -1, \quad i, \quad -i.$$

Conclusion:

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$$
$$= \{1, i, i^2, i^3\} \cong \mathbb{Z}/4\mathbb{Z}.$$
(the cyclic group generated by i)

Know: $\mathbb{Z}[i]$ is Euclidean with norm
$N(a+ib) = |a+ib|^2 = a^2+b^2$.

It follows that: if $I \subseteq \mathbb{Z}[i]$ is an ideal and if $\alpha \in I$ satisfies

$$N(\alpha) = \min\{N(\beta) : \beta \in I\}$$

Then $I = (\alpha)$. ($\mathbb{Z}[i]$ is a PID) ///

Now suppose $(\alpha) = (\beta)$. Then
$\alpha \in (\beta) \Rightarrow \alpha = \gamma\beta$ } they divide
$\beta \in (\alpha) \Rightarrow \beta = \delta\alpha$ } each other.

$\Rightarrow \alpha = \gamma\beta = \gamma\delta\alpha$
$\Rightarrow 0 = (\gamma\delta - 1)\alpha$
$\Rightarrow \gamma\delta - 1 = 0$ (if $\alpha \neq 0$)
$\Rightarrow \gamma\delta = 1$
(γ, δ are units).

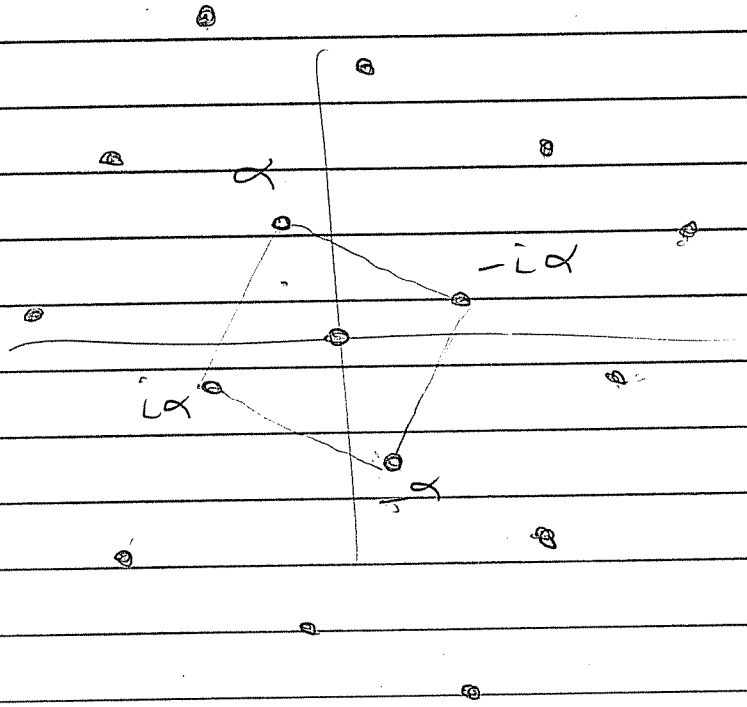
Prop. In an integral domain,

$(a) = (b) \iff a = ub$ for some unit u.

Proof: Homework 2 ☒

Corollary: Every nonzero ideal $I \subseteq \mathbb{Z}[i]$ has exactly 4 generators $\pm\alpha, \pm i\alpha$, which are also the "shortest" elements of the ideal.

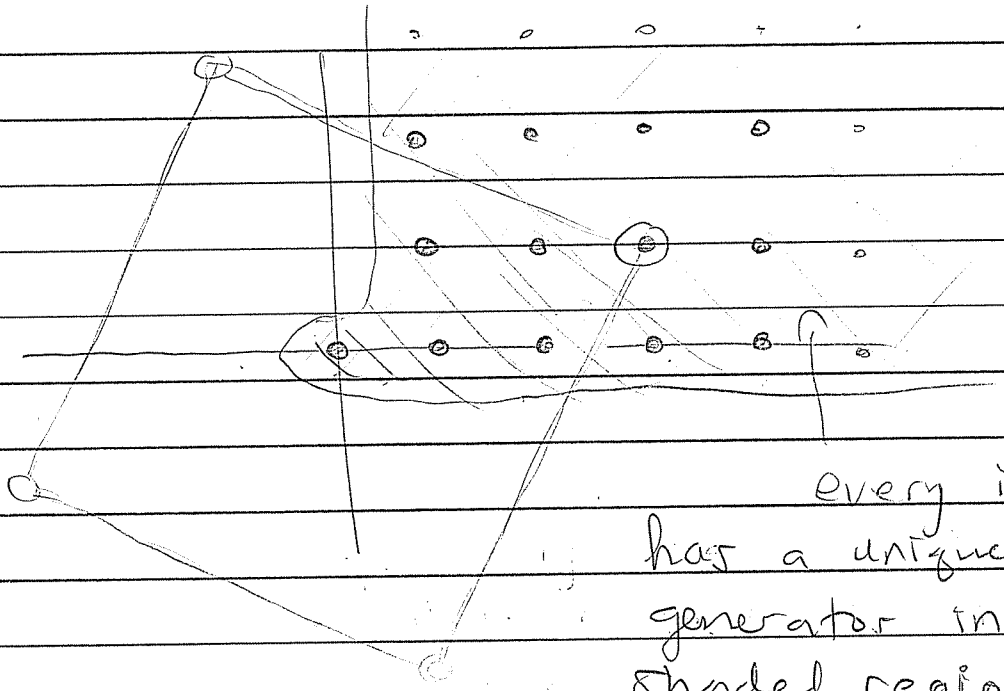
Picture of (α), eg.,



all nonzero ideals look like this

Corollary: The ideals of $\mathbb{Z}[i]$ are in bijection with the set

$$\{a+ib : a>0,\ b\geq 0\} \cup \{0+0i\}$$



every ideal has a unique generator in the shaded region

HW 2 due Wed Feb 15
Exam 1 Fri Feb 17.

Today: Factoring.

Language of principal ideals is useful (see pg. 360)

Let R be a domain. Then

u is a unit $\iff (u) = (1)$

a divides b $\iff (b) \subseteq (a)$.

DEF: • Say a is a proper divisor of b if $b = qa$ with q & a nonunits.

• Say a, b are associates if $\exists$ unit u with $b = ua$.

• Say a is irreducible if it has no proper divisor.
i.e. $d \mid a \implies d \in R^\times$ or d, a are assoc.

• Say p is prime if $\forall a, b \in R$.
$p \mid ab \implies p \mid a$ OR $p \mid b$.

Translation:

a is proper divisor of b (HW2)
$\iff (b) < (a) < (1)$
↑ ↑ strict containment.

a, b are associates $\iff (a) = (b)$ (HW2)

a is irreducible
$\iff (a) < (1)$ (a not a unit)
& $\nexists (c)$ with
$(a) < (c) < (1)$ (a has no proper divisor)

p is prime
$\iff ab \in (p) \implies a \in (p)$ OR $b \in (p)$. ///

Lemma: In a domain, prime $\implies$ irreducible.

Proof: Suppose p is prime with $p = ab$.
Show that a or b is a unit.
Well $p \mid ab$ & p prime $\implies p \mid a$ OR $p \mid b$.
W.l.o.g. say $p \mid a$, $pk = a$.
But then $p = ab = pkb$ ↯

$\Rightarrow \quad p(1-kb) = 0$

$\Rightarrow \quad 1 - kb = 0$

$\Rightarrow \quad kb = 1. \Rightarrow b$ is a unit. ∎

The converse is not true.

Ex. Consider the domain (subring)

$$\mathbb{Z}[\sqrt{-3}] = \{ a + b\sqrt{-3} \; ; \; a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$$

Claim: $1+\sqrt{-3}$ is NOT prime.

Proof: Note that

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$$

$$\Rightarrow \quad (1+\sqrt{-3}) \mid 2 \cdot 2$$

If $1+\sqrt{-3}$ were prime, then would have $(1+\sqrt{-3}) \mid 2$. i.e. $\exists \; a, b \in \mathbb{Z}$ with.

$$(1+\sqrt{-3})(a+b\sqrt{-3}) = 2 + 0\sqrt{-3}.$$

$$a + a\sqrt{-3} + b\sqrt{-3} + b(-3) = 2 + 0\sqrt{-3}.$$

$$(a-3b) + (a+b)\sqrt{-3} = 2 + 0\sqrt{-3}.$$

$\Rightarrow$ $\left.\begin{array}{l} a-3b=2 \\ a+b=0 \end{array}\right\} \Rightarrow 4a=2$. Garbage.

Hence $1+\sqrt{3}$ is NOT prime.

BUT. You will show that

$1+\sqrt{-3}$ is irreducible.

Summary: In a domain

prime $\Rightarrow$ irreducible

$\not\Leftarrow$ need something more (PID)

Motivation: The FTA.

Fundamental Theorem of Arithmetic
(Euclid, long time ago)

Every nonzero, nonunit $n \in \mathbb{Z}$ has a "unique" factorization into irreducibles.

↑ up to order and units

Ex. $12 = 2 \cdot 2 \cdot 3$
$= (-2) \cdot (-2) \cdot 3$
$= (-2) \cdot 2 \cdot (-3)$
} and reorderings of these

Maybe better... $(12) = (2)(2)(3)$ ...
ideals

Sketch Proof of FTA.

(1) Existence of factorization.

If n is irreducible, done ✓.
So take $n = ab$, a, b proper divisors
Then inductively factor a & b.
Why does the process terminate ?

Idea: If $d \mid a$ is a proper divisor then $|d| < |a|$.

∞ Not very general.
Only works for Euc dom. with multiplicative norm.

(2) Uniqueness of Factorization.

Follows from... ↓

Euclid's Lemma: In $\mathbb{Z}$,

irreducible $\Rightarrow$ prime. (T.O.U.)

Then suppose:

$$n = a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_\ell$$

two irred. factorizations.

$$a_1 \mid b_1 \cdots b_\ell \underset{\text{Euclid}}{\Longrightarrow} a_1 \mid b_i \text{ for some } i$$

w.l.o.g. $a_1 \mid b_1$

Then b_1 irred. $\Rightarrow$ a_1, b_1 associates

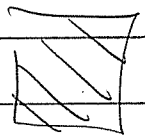
$b_1 = u a_1$.

Cancel $a_1 = b_1$ to get

$$a_2 \cdots a_k = b_2 \cdots b_\ell \cdot u$$

Induct to get

- $k = \ell$
- a_i, b_i associates $\forall i$



HW 2 due Wed Feb 15

Exam 1 due Fri Feb 17

Welcome Prof. Dvorsky!

Current Goal:

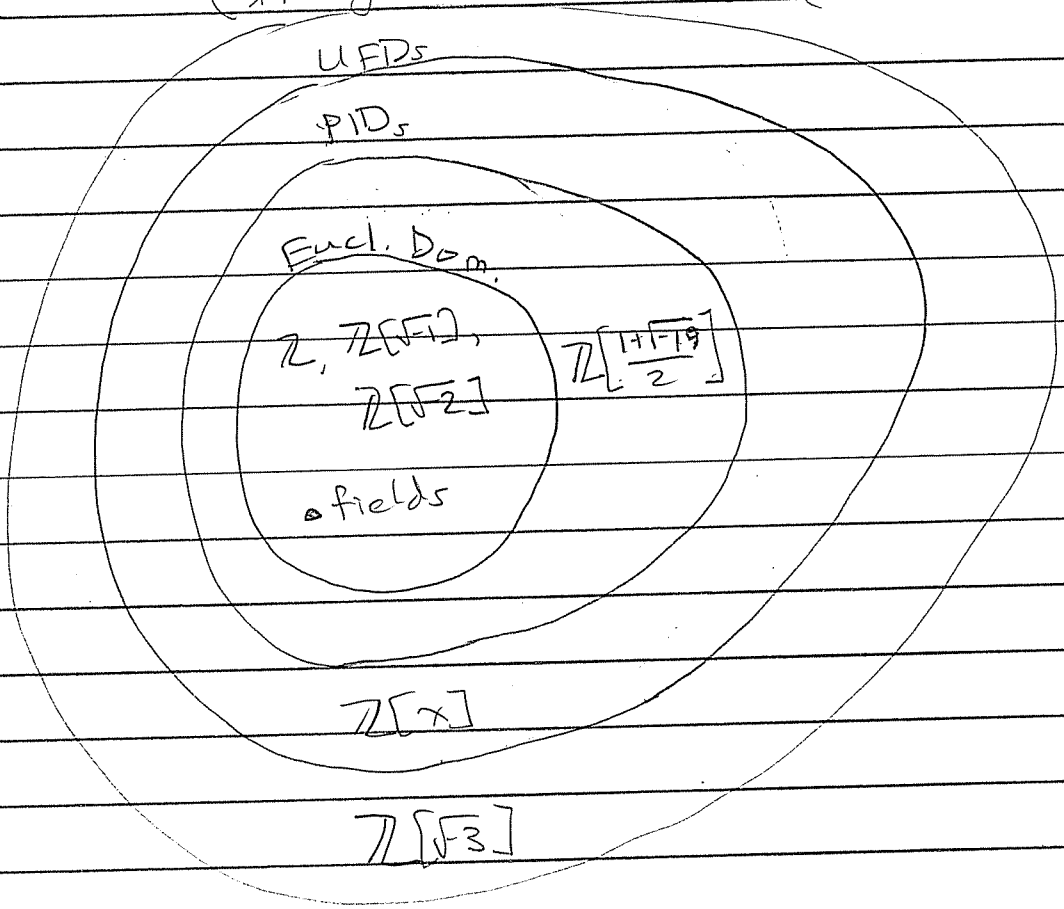
Generalize the concept "integer"

Number Theory ~~~?~~~> Geometry

What happens?

~~for us,~~ $\mathbb{C}$ ↓

(Integral) Domains (i.e. $\subseteq \mathbb{F}$)



Today: UFD.

Definition: A domain R is called UFD if

$\exists$ (1) Every $r \in R$ is a (finite) product of irreducibles

$!$ (2) such a factorization is unique up to associates.

Example: $\mathbb{Z}$ (Euclid)

What causes UFD?

(1) Try to factor a.
If r irreducible, done ✓.
Otherwise $r = ab$ for a, b nonunits.
Repeat.
Hope the process terminates in finite time.

Theorem: Factoring terminates in a PID.

Proof: If not, we get an infinite chain of proper divisors

$$(a_1) < (a_2) < (a_3) < \cdots$$

strict containment.

Lemma: given ideals $I_1 \subseteq I_2 \subseteq \cdots$ in any ring. the union $J = \bigcup_{n=1}^{\infty} I_n$ is an ideal.

Proof: Let $u, v \in J$, $r \in R$. By definition $\exists\, n$ with $u, v \in I_n$. Then $u+v \in I_n \subset J$. and $ru \in I_n \subseteq J$. ∎

Let $J = \bigcup_{i=1}^{\infty} (a_i)$

PID $\Rightarrow$ $J = (d)$ for some $d \in R$.

Then $d \in J \Rightarrow d \in (a_n) \Rightarrow (d) \subseteq (a_n)$ for some n.

But $(a_n) < (a_{n+1}) \subseteq J = (d)$ ✗ contradiction ∎

Most generally, we say R is Noetherian if it has no infinite chain of ideals

$$I_1 < I_2 < I_3 < \cdots$$

(a finiteness condition).

Noetherian $\Rightarrow$ Factoring terminates.

(2) When is factorization unique?

A: We need

"Euclid's Lemma": irreducible $\Rightarrow$ prime.

Assuming this, consider.

(*) $r = a_1 a_2 \cdots a_m = b_1 \cdots b_n$

($a_1 a_2 \cdots a_m$: irreducible (hence prime).)

$a_1 \mid b_1 \cdots b_n \Rightarrow a_1 \mid b_1$ (WLOG)

b_1 irred. $\Rightarrow$ a_1, b_1 associates, say

$a_1 = u b_1$

Divide * by $a_1 = u b_1$ to get

$$a_2 a_3 \cdots a_m = b_2 b_3 \cdots b_n \cdot u^{-1}$$

Induct to get

- $m = n$
- a_i, b_i associate $\forall\ i$. ✓

$\Rightarrow$ UFD.

Theorem: Euclid's Lemma holds for PID.

Proof: Let p be irred so $\nexists$ proper factor d with $(p) < (d) < (1)$.

Now suppose $p \mid ab$ and $p \nmid a$.
Claim: $p \mid b$. (i.e. p is prime)

Well $p \nmid a \Rightarrow (a) \subseteq (p)$.
$\Rightarrow (p) < (p) + (a)$.

PID $\Rightarrow (p) < (p) + (a) = (d)$ for some d.
p irred. $\Rightarrow (d) = (1)$.

Hence $(p) + (a) = (1)$ [say p, a are coprime]

$1 \in (p) + (a) \Rightarrow \exists\, x, y$ with $ax + py = 1$
(Bézout's Identity).

Multiply by b to get

$$abx + pby = b.$$
$$pkx + pby = b \quad \text{since } p \mid ab.$$
$$p(kx + by) = b$$

$\Rightarrow p \mid b$. ∎

Corollary: PID $\Rightarrow$ UFD.

(More generally,

Noetherian & Euclid's Lemma $\Rightarrow$ UFD)

$\exists$!

$\Longrightarrow$

You will show: in $\mathbb{Z}[\sqrt{-3}]$

$$4 = (1+\sqrt{-3})(1+\sqrt{-3}) = 2 \cdot 2$$

$\Longrightarrow$ $\mathbb{Z}[\sqrt{-3}]$ NOT UFD.

$\Longrightarrow$ NOT PID

$\Longrightarrow$ NOT Euclidean.

HW 2 due next Wed.
Exam 1 next Fri
Welcom Prof. Pestien!

We have seen:

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD.

But so what?
What is UFD good for?

In 1637, Fermat claimed that for $n \geq 3$
$\nexists\ x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ s.t.

$$x^n + y^n = z^n. \quad (*)$$

"I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

Euler tried and failed.
- he proved $n=3$ in 1770
but it had a gap.

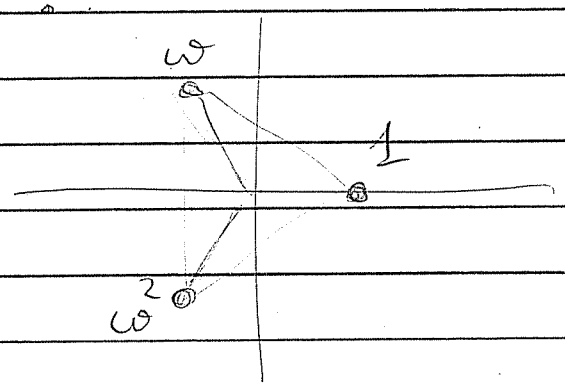
$\rightsquigarrow$ Fermat's "Last" Theorem.

Look at $n = 3$.

$$x^3 + y^3 = z^3 \quad ?$$

Let $\omega = e^{2\pi i/3}$

$$= -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$



$\{1, \omega, \omega^2\}$

= 3rd roots of 1.

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$$

Put $x \to -x/y$.

$$-\frac{x^3}{y^3} - 1 = \left(-\frac{x}{y} - 1\right)\left(-\frac{x}{y} - \omega\right)\left(-\frac{x}{y} - \omega^2\right)$$

Multiply by $-y^3$.

$$(*) \qquad x^3 + y^3 = (x+y)(x+\omega y)(x+\omega^2 y) = z^3$$

DEF: Given $\omega_n = e^{2\pi i/n}$, let

$$\mathbb{Z}[\omega_n] := \{a_0 + a_1\omega_n + \cdots + a_{n-1}\omega_n^{n-1} : a_0, \ldots, a_{n-1} \in \mathbb{Z}\}$$

The ring of cyclotomic integers

Ex. $\omega_4 = e^{\pi i/2} = i$.

$\Rightarrow \mathbb{Z}[\omega_4] = \mathbb{Z}[i]$ Gaussian integers

$\mathbb{Z}[\omega_3]$ = "Eisenstein integers".

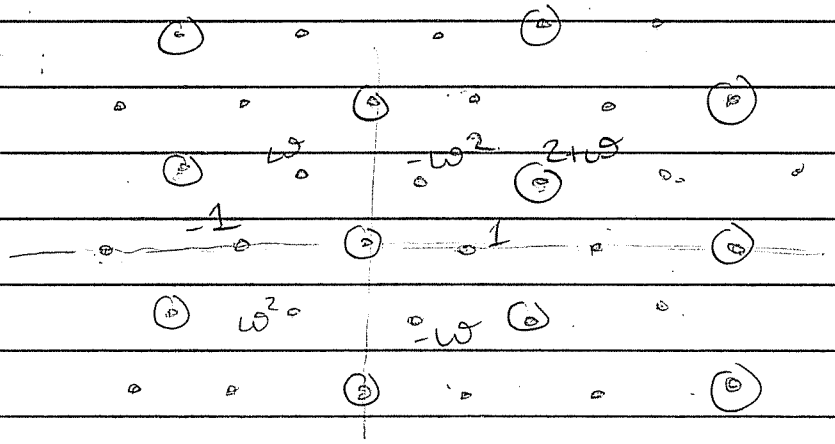
Note: $\omega_3 + \omega_3^2 = -1$ & $\omega_6 = -\omega_3^2$, so.

$$\mathbb{Z}[\omega_6] = \mathbb{Z}[\omega_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \supseteq \mathbb{Z}[\sqrt{-3}]$$

UFD ✓ NOT UFD ✗

Theorem: $\mathbb{Z}[\omega_3]$ is Euclidean ☺

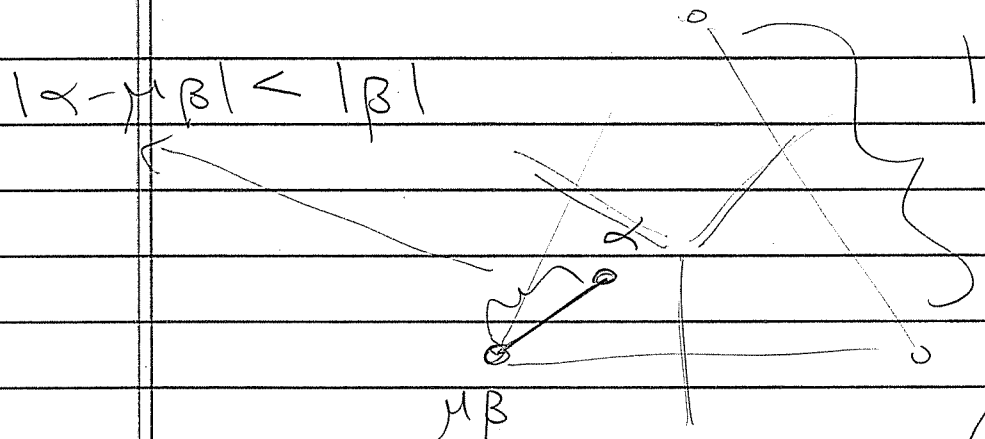
Proof:



$\mathbb{Z}[\omega_3] \subseteq \mathbb{C}$ "triangular" lattice.

Every $(\beta) \subseteq \mathbb{Z}[\omega_3]$ is a "triangular" sublattice. eg. $(2+\omega)$.

To divide α by $\beta \neq 0$, consider α relative to the ideal (β) and let μ minimize $|\alpha - \mu\beta|$.



$$\alpha = \mu\beta + (\alpha - \mu\beta)$$

quotient — remainder

Corollary: $\mathbb{Z}[\omega_3]$ is UFD

Back to Fermat for $n = 3$

Theorem: Given $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ we have

$$x^3 + y^3 \neq z^3$$

Proof Sketch (tricky details omitted):

Suppose for contradiction that $x^3+y^3=z^3$

Step (1) Factor $x^3+y^3=(x+y)(x^2-xy+y^2)=z^3$
Work mod 9 to show that

$$x^2-xy+y^2 = 3c^3 \quad \text{for some } c,d\in\mathbb{Z}$$
$$x+y = 9d^3 \qquad (3\nmid c).$$

(2) Shift to Eisenstein $\mathbb{Z}[\omega_3]$ UFD

$$x^2-xy+y^2=(x+\omega y)(x+\omega^2 y)=3c^3.$$

and note $\gcd(x+\omega y, x+\omega^2 y) = 1-\omega$.

$$\Rightarrow \underbrace{(x+\omega y)}_{1-\omega}\ \underbrace{(x+\omega^2 y)}_{1-\omega} = \underbrace{(-\omega)}_{\text{unit}}(1-\omega)\,c^3$$

coprime

(3) By UFD, $\dfrac{x+\omega y}{1-\omega}$ is a cube $\in\mathbb{Z}[\omega_3]$

i.e. $\exists\, a,b\in\mathbb{Z}$, $(x+\omega y)=(1-\omega)(a+b\omega)$.

$\downarrow$

Expand and compare coefficients to get

$$x + y = 9ab(a-b).$$

But $x + y = 9d^3$ from before.

(4) By UFD, a, b, $(a-b)$ are cubes, (say $a-b = x_1^3$, $b = y_1^3$, $a = z_1^3$) with

$$x_1^3 + y_1^3 = z_1^3.$$

(5) Show that

$$0 < |x_1 y_1 z_1| < |xyz|.$$

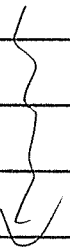
This can't go on forever.
"infinite regress."
CONTRADICTION

Whew...

(Yes, it's TRICKY.
Even Euler (1770) had
trouble with this.)

Theorem (Lamé, 1847).

$\mathbb{Z}[\omega_n]$ is UFD $\Rightarrow$ FLT(n) is true.



But Kummer had shown in 1844 that

$\mathbb{Z}[\omega_{23}]$ is NOT UFD !

Unique factorization was taken very seriously !

HW 2 due Wed

Exam 1 Friday

Today: A non-principal ideal

Recall: $\mathbb{Z}[\sqrt{-3}]$ is not UFD, but it can be fixed.

$$\mathbb{Z}[\sqrt{-3}] \rightsquigarrow \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\omega_3]$$

integral closure

Eisenstein integers

UFD ✓

Today we consider

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

with norm function

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2$$
$$= a^2 + 5b^2 \quad \in \mathbb{N}$$

Note: $N(\alpha\beta) = N(\alpha)N(\beta)$.

(multiplicative)

Fact : $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$

Proof : Suppose $u \in \mathbb{Z}[\sqrt{-5}]^\times$ i.e. $\exists\ uv = 1$

Then

$$N(uv) = N(u)\,N(v) = 1.$$

$$\Rightarrow N(u) = 1.$$

If $u = a + b\sqrt{-5}$ then $a^2 + 5b^2 = 1$.

$$\Rightarrow a = \pm 1,\ b = 0$$

Lemma : $\mathbb{Z}[\sqrt{-5}]$ contains NO element of norm 2 OR 3.

Proof : $a^2 + 5b^2 = 2$ & $a^2 + 5b^2 = 3$ have NO integer solution

Lemma : $2,\ 3,\ 1+\sqrt{-5},\ 1-\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ are all irreducible.

Proof: Suppose $2 = \alpha\beta$.

$\Rightarrow N(\alpha)N(\beta) = N(2) = 2^2 + 5\cdot 0^2 = 4$. ✓

trivial	1	4
impossible	2	2
trivial	4	1

Suppose $3 = \alpha\beta$.

$N(\alpha)N(\beta) = N(3) = 9$. ✓

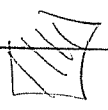
trivial	1	9
impossible	3	3
trivial	9	1

Suppose $1+\sqrt{-5} = \alpha\beta$.

$N(\alpha)N(\beta) = N(1+\sqrt{-5}) = 6$

triv	1	6
X	2	3
X	3	2
triv	6	1

$1-\sqrt{-5}$ is similar



Theorem: $6 \in \mathbb{Z}[\sqrt{-5}]$ has two different irreducible factorizations

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

(2 and 3 irreducible)

Since $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$,

2 NOT associate to $1 \pm \sqrt{-5}$. ∎

Remark: $\mathbb{Z}[\sqrt{-5}]$ is integrally closed

How can unique factorization be saved?

Idea: (Kummer ⇝ Dedekind)

Replace "element/number" with "ideal".

DEF: Given ideals $I, J \subseteq R$ (comm. with 1)

define the product ideal

$$IJ := \{ uv : u \in I,\ v \in J \}.$$

Hope: every nonzero ideal is a unique product of "prime" ideals.

(in a PID you won't notice)

Back to $\mathbb{Z}[\sqrt{-5}]$:

2 & $1+\sqrt{-5}$ have no common proper factor, but they're not really "coprime".

Consider the ideal.

$$(2)+(1+\sqrt{-5}) = A < (1).$$

↑ NOT principal.

Notation: $A = (2, 1+\sqrt{-5})$

the ideal generated by 2 & $1+\sqrt{-5}$.

Think: $A = \gcd(2, 1+\sqrt{-5})$.

Continue....

$$A = (2, 1+\sqrt{-5}), \quad \overline{A} = (2, 1-\sqrt{-5}).$$

$$B = (3, 1+\sqrt{-5}), \quad \overline{B} = (3, 1-\sqrt{-5}).$$

Lemma:

$$A\overline{A} = (2) \qquad AB = (1+\sqrt{-5})$$
$$B\overline{B} = (3) \qquad A\overline{B} = (1-\sqrt{-5})$$

Proof: HW 3.

Conclusion: At the level of ideals.

$$(6) = (2)(3) = (A\bar{A})(B\bar{B})$$
$$= (AB)(\bar{A}\bar{B})$$
$$= (1+\sqrt{-5})(1-\sqrt{-5}).$$

$$(6) = A\bar{A}B\bar{B}$$

Unique factorization restored ☺

Dedekind's Big Theorem

Let K be a "number field" i.e.

(1) $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

(2) $\dim(K/\mathbb{Q}) < \infty$

Let $\mathcal{O}_K \subseteq K$ be its "ring of integers"

$$\mathcal{O}_K = \{\alpha \in K : f(\alpha) = 0 \text{ for some monic polynomial } f(x) \in \mathbb{Z}[x]\}$$

Then $\mathcal{O}_K$ has unique ideal factorization.

↖ say it's a "Dedekind domain"