Recall:
Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD.

$\Downarrow$

DWR.

$\Downarrow$ (from PID)

$s \in R$ irreducible $\Leftrightarrow$ s prime

$\Leftrightarrow$ (s) prime ideal

$\Leftrightarrow$ (s) maximal ideal.

$\not\Leftarrow$ is not true.

$\not\Leftarrow$ is not true.

Two examples: $\mathbb{Z}[i]$. Gauss integers.

$F[x]$ F field.

Last time $\mathbb{Z}[i]$ Euclidean domain

size function $\sigma(m+ni) = |m+ni|^2$

$= m^2+n^2$.

Questions: ① what are the units?

② what are the prime element?

③ How to factor an element?

The prime elements or factorization is related to number theory:

When is p prime number equal to sum of two squares?

$$p = m^2 + n^2 \quad (p \text{ prime}).$$

---

① Units in $\mathbb{Z}[i]$.

Prop: If $s = m + ni$, $m, n \in \mathbb{Z}$, is a unit in $\mathbb{Z}[i]$, then $s = \pm 1, \pm i$.

Pf: $s \cdot s^{-1} = 1$. (norm square)

$$|s|^2 |s^{-1}|^2 = 1. \qquad s^{-1} = a + bi.$$

$$a, b \in \mathbb{Z}.$$

$$\underline{(m^2+n^2)}\,\underline{(a^2+b^2)} = 1.$$

$$m^2 + n^2 = 1. \qquad m = \pm 1,\ n = 0$$

$$m = 0,\ n = \pm 1.$$

Check if $m^2 + n^2 = 1$, then $s \cdot \bar{s} = 1$.

Question 2. $\mathbb{Z} \subset \mathbb{Z}[i]$.

$\mathbb{Z}$ is a subring of $\mathbb{Z}[i]$.

The prime elements in $\mathbb{Z}$ are all prime numbers.

prime numbers may have more divisors in $\mathbb{Z}[i]$.

Ex: 5 prime element in $\mathbb{Z}$.

but not prime element in $\mathbb{Z}[i]$.

$$5 = (1+2i)(1-2i)$$

Prop: p prime number in $\mathbb{Z}$,

p is sum of two squares iff

p is reducible in $\mathbb{Z}[i]$.
not irreducible

Pf: "if". $p = (a+bi)(c+di)$. $a+bi$, $c+di$ are not units in $\mathbb{Z}[i]$.

$a, b, c, d \in \mathbb{Z}$.

Norm square: $p^2 = (a^2+b^2)(c^2+d^2)$.

$a^2+b^2 = 1,\ p,\ p^2.$

$c^2+d^2 = p^2,\ p,\ 1$

$c+di$ unit.

$a+bi$ unit.

$a^2+b^2=p$. and $c^2+d^2=p$.

"only if" $p = m^2+n^2$, $m, n \in \mathbb{Z}$.

$p = (m+ni)(m-ni)$

$m^2+n^2 = p \neq 1$, so $m+ni$, $m-ni$ are not units

p reducible.

Prop: p is a prime element in $\mathbb{Z}[i]$

iff $p \equiv 3 \pmod 4$.

pf: $p=2$. $2 = 1^2+1^2$. p not prime element in $\mathbb{Z}[i]$.

p odd prime. $p \equiv 1$ or $3 \pmod 4$.

Goal: " p is not a prime $\iff$ $p \equiv 1 \pmod 4$ "

p is not a prime $\iff$ $\mathbb{Z}[i]/(p)$ is not a field.

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

$x \longmapsto i$.

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

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

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

$\cong \mathbb{Z}/(p)\,[x] \Big/ (x^2+1)$ $\qquad \mathbb{Z}/(p) \cong \mathbb{F}_p$. finite field.

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

$\mathbb{F}_p[x]$ is a PID.

whether x^2+1 is irreducible or not?

x^2+1 reducible in $\mathbb{F}_p[x]$

$\Leftrightarrow$ $p \equiv 1 \pmod 4$.

In $\mathbb{F}_p[x]$, the units are $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$

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

$f(x)g(x) = 1$. then $\deg f = \deg g = 0$.

x^2+1 reducible $\Leftrightarrow$ $x^2+1 = (x-a)(x-b)$

a, b are roots of x^2+1.

$a^2+1 = 0$, $b^2+1 = 0$

If x^2+1 has root $x=a$. $a^2+1=0$

then DWR $x^2+1 = (x-a)q(x)+r$.

$\deg r = 0$. then $r=0$.

x^2+1 reducible in $\mathbb{F}_p[x]$ $\Leftrightarrow$ x^2+1 has a root $x=a$, i.e. $a^2+1=0$

$a \in \mathbb{F}_p$

Lemma: p odd prime

(1). The multiplicative group $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$.

contains an element of order 4 iff $p \equiv 1 \pmod 4$

(2) The integer $a \in \mathbb{Z}$ solves $a^2 \equiv -1 \pmod p$

iff $\bar{a}$ in $\mathbb{F}_p$ is an element of order 4.
in $\mathbb{F}_p^\times$

Pf: (useful fact $\mathbb{F}_p^\times$ is a cyclic group of order $(p-1)$)

①: If $\bar{a}$ has order 4 in $\mathbb{F}_p^\times$

$4 \mid p-1$. $\Rightarrow$ $p \equiv 1 \pmod 4$

If $p \equiv 1 \pmod 4$, then consider homomorphism

$\varphi: \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ group homomorphism.

$x \mapsto x^2$.

$\ker\varphi = \{\pm 1\}$. $\quad \ker\varphi = \{x \mid x^2 = 1\}$

$= \{x \mid (x-1)(x+1) = 0\}$

$= \{\pm 1\}$.

$\operatorname{Im}\varphi \cong \mathbb{F}_p^\times / \{\pm 1\}$. has order $\frac{p-1}{2}$. is an even number, $\quad 2 \mid \frac{p-1}{2}$.

$\operatorname{Im}\varphi$ has a 2-Sylow group and element of order 2.

$\operatorname{Im}\varphi$ has an element of order 2.

$x^2 = 1$, and $x \neq 1$, so $x = -1$.

$\operatorname{Im}\varphi \ni -1$. $\quad a^2 = -1$, $\quad a^3 = -a$,

$a^4 = 1$.

a itself $\neq 1$. $\quad a^2 \neq 1$. (p odd, so $-1 \neq 1$).

a has order 4.

b). If $\bar{a}$ has order 4 in $\mathbb{F}_p^\times$,

then $\bar{a}^2$ has order 2 in $\mathbb{F}_p^\times$.

So $\bar{a}^2 = -1$ in $\mathbb{F}_p$

If $\bar{a}^2 = -1$, then $\bar{a}^2$ has order 2 in $\mathbb{F}_p^\times$, so $\bar{a}$ has order 4

$\mathbb{Z}[i]$. ① p prime number in $\mathbb{Z}$. $p \equiv 3 \pmod 4$

$\pm p, \pm pi$ also a prime element in $\mathbb{Z}[i]$.

Prop: $p = 2$ or $p \equiv 1 \pmod 4$

$p = m^2 + n^2 = (m+ni)(m-ni)$. $m, n \in \mathbb{Z}$.

$m+ni$ is a prime element in $\mathbb{Z}[i]$.

Pf: If $m+ni = (a+bi)(c+di)$. $a, b, c, d \in \mathbb{Z}$

$p = m^2+n^2 = \underline{(a^2+b^2)}\underline{(c^2+d^2)}$

$a^2+b^2 = 1$ or $c^2+d^2 = 1$

$\Rightarrow$ $a+bi$ or $c+di$ is a unit.

$m+ni$ irreducible.

② $m+ni$. $m, n \in \mathbb{Z}$. $m^2+n^2 = p$.

$p \equiv 1 \pmod 4$, $p = 2$.

Prop: ①, ② give all the irreducible elements in $\mathbb{Z}[i]$.

Pf: Take $a+bi$ an irreducible element in $\mathbb{Z}[i]$. $a, b \in \mathbb{Z}$.

$\varphi: \mathbb{Z}[i] \to \mathbb{Z}[i]$ is a bijective ring homomorphism (automorphism)

$z \mapsto \bar{z}$

$a+bi \mapsto a-bi$.

$a-bi$ is also irreducible.

$\underbrace{(a+bi)(a-bi)}_{\text{irreducible factrization for } a^2+b^2 \text{ in } \mathbb{Z}[i]} = a^2+b^2 \in \mathbb{Z}$.

$a^2+b^2 = p_1 \cdots p_m$ p_j primes in $\mathbb{Z}$.

If $p_j \equiv 3 \pmod 4$, p_j irred. in $\mathbb{Z}[i]$.

If $p_j \equiv 1 \pmod 4$, or $p_j = 2$,

$$p_j = \underbrace{(m_j + n_j i)}\underbrace{(m_j - n_j i)}$$

irreducible in $\mathbb{Z}[i]$

$$a^2+b^2 = \underbrace{p_1 \cdots (m_j+n_j i)(m_j - n_j i)}_{\text{irreducible factorization of } a^2+b^2} \cdots$$

$\mathbb{Z}[i]$ is UFD $\Rightarrow$ $a+bi$ is the associate with prime p_j. $p_j \equiv 3 \pmod 4$

or $m_j + n_j i$. $m_j^2 + n_j^2 = p_j$ prime

$F[x]$ F field.

Units in $F[x] = \{ a \in F \mid a \neq 0 \}$

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

Defn (irreducible polynomials) irreducible elements in $F[x]$.

Important question: How to find irred. poly's?

Depends on F.

F finite field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ of p elements

p prime # in $\mathbb{Z}$.

<u>Sieve method</u>. $F = \mathbb{F}_2 = \{0, 1\}$

deg 0 No.

deg 1. x, $x+1$.

deg 2, $\cancel{x^2}$, $\cancel{x^2+x}$, x^2+x+1, $\cancel{x^2+1}$.

Find products of deg-1 polynomials

deg 3, x^3, x^3+x, x^3+x+1, x^3+1,

x^3+x^2, x^3+x^2+x, x^3+x^2+x+1, x^3+x^2+1.

Find products of deg-1 and deg-2 polynomials

Cross out these products

$\vdots$

$\mathbb{Z}$, $\quad 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}$

Greatest common divisor. exists in PID

Defn (g.c.d) $f, g \in R$, $d = \text{g.c.d}(f, g) \in R$

iff d is the divisor of both f, g.

and if s is the common divisor of f and g, then s is the divisor of d.

In PID, we look at the ideal (f, g)

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

$\Rightarrow$ $d \mid f$, $d \mid g$, and if

$s \mid f$, $s \mid g$, $\Rightarrow (s) \supset (f, g)$

$\Rightarrow (s) \supset (d) \Rightarrow s \mid d$.

$\exists\, r, s \in R$, s.t. $rf + sg = d$.

DWR can be used to find d, r, s.

$\underline{g = fq + r}$ assume $\deg f \leq \deg g$.

$\underline{(f, g)} = \underline{(f, r)}$

$\max(\deg f, \deg r) < \max(\deg q, \deg f)$

Next time $\mathbb{Z}[x]$. $\mathbb{Z}$ is not a field

$\mathbb{Z}[x]$ is not PID

but is still UFD