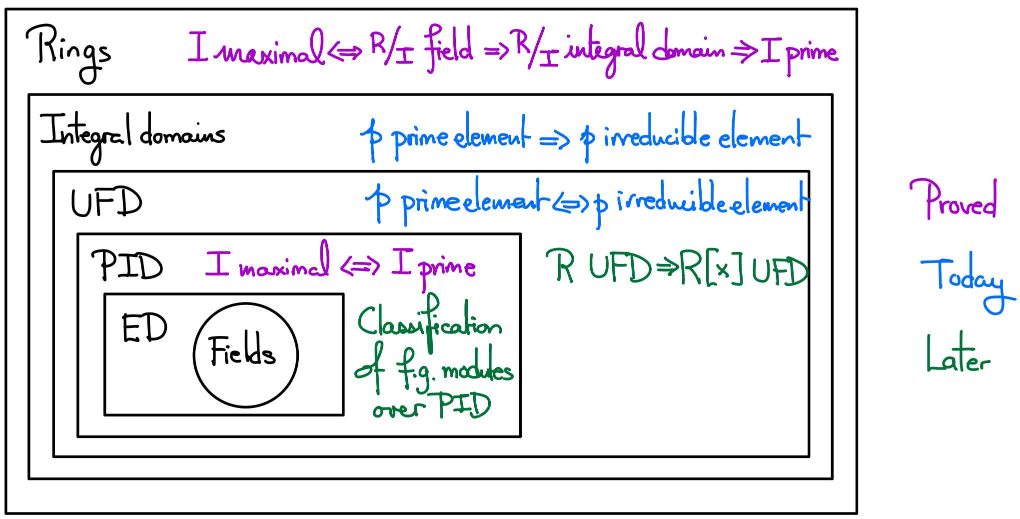
Euclidean domains and unique factorization domains

Today: R an integral domain

Goal: E.D $\Rightarrow$ P.I.D. $\Rightarrow$ U.F.D.



Q: How to prove an integral domain is a PID?

Definition An integral domain R is said to be an Euclidean domain (ED) (欧几里德整环)

if there is a norm $N: R \to \mathbb{Z}^+ \cup \{0\}$

s.t. (1) $N(0)=0$

(2) $\forall a, b^{\neq 0} \in R$, $\exists q, r \in R$, s.t. $a = bq + r$ & $r=0$ or $N(r) < N(b)$

q: quotient, r: remainder

Remark: We do not require q and r to be unique.

Remark: Can use Euclidean algorithm to find the "gcd" of two elements (辗转相除法)

Example ① Fields F, $N(a)=0$ $\forall a \in F$

② $\mathbb{Z}$, $N(a)=|a|$

③ $R=F[x]$, $N(f(x)) = \deg(f)$

④ $R=\mathbb{Z}[i]$ ring of <u>Gaussian integers</u> (高斯整数环)

$$N(x+yi)=x^2+y^2$$

When $a, b \overset{\neq 0}{\in} \mathbb{Z}[i]$, take $q\in\mathbb{Z}[i]$ such that

$$|\mathrm{Re}(q)-\mathrm{Re}(\tfrac{a}{b})|\leq \tfrac{1}{2}, \quad |\mathrm{Im}(q)-\mathrm{Im}(\tfrac{a}{b})|\leq\tfrac{1}{2}$$

Then $N(a-bq)=\|b\|^2\cdot\|\frac{a}{b}-q\|\leq\|b\|^2\cdot(\frac{1}{4}+\frac{1}{4})<\|b\|^2$ ✓

⑤ $R=\mathbb{Z}[\zeta_3]$ for $\zeta_3=\frac{-1+\sqrt{-3}}{2}$. $N(z)=\|z\|^2$

<u>Proposition</u> R ED $\Rightarrow$ PID

Proof. If $I\subseteq R$ is a nonzero ideal,

let $b:=$ an element of $I\setminus\{0\}$ with minimal possible norm.

<u>Claim</u> $I=(b)$, $(b)\subseteq I$ is clear.

Conversely, for $a\in I \rightsquigarrow a=bq+r$ with $q\in R$, $r=0$ or $N(r)<N(b)$

If $r\neq 0$, $r=a-bq\in I$, contradicting with minimality of $N(b)$.

So $r=0 \Rightarrow a\in(b)$. $\square$

<u>Generalization of prime numbers in $\mathbb{Z}$ to general integral domains</u>

<u>Definition</u> (0) For $a,b\in R$ with $a\neq 0$, we write $a|b$ if $b=ac$ for some $c\in R$.

$\Leftrightarrow b\in(a)$.

(1) A nonzero, nonunit element $p\in R$ is called a <u>prime element</u> (素元) if (p) is a prime ideal.

(i.e. if $p|ab\Rightarrow p|a$ or $p|b$.)

(2) Suppose $r\in R$ is nonzero and not a unit. Then r is called an <u>irreducible element</u> (不可约元)

if whenever $r=ab$, then either a or b is a unit

(3) Two elements $a,b\in R$ are said to be <u>associate</u> (相伴的) if $a=bu$ for some unit $u\in R^\times$

Proposition (1) Prime elements are always irreducible.

(2) If R is a PID, then irreducible elements are prime elements

Proof: (1) Let $p \in R$ be a prime element and $p = uv$.

Then $uv \in (p) \Rightarrow u \in (p)$ or $v \in (p)$

WLOG $u = ps \Rightarrow p = psv \Rightarrow 1 = sv \Rightarrow v$ is a unit.

So p is irreducible.

(2) If p is irreducible, we will show that (p) is maximal, so a prime ideal.

Indeed, if $(p) \subseteq (m)$, then $p = rm \Rightarrow$ either r is a unit $\Rightarrow (p) = (m)$

or m is a unit $\Rightarrow (m) = (1)$ $\square$

Definition A unique factorization domain (UFD) is an integral domain R in which

$\forall r \in R$ with $r \neq 0$ nonunit satisfies

not necessarily distinct

① r is a product of irreducibles $p_i \in R$: $r = p_1 p_2 \cdots p_m$

② the factorization in ① is unique to associates, i.e. if $r = q_1 q_2 \cdots q_n$ is another factorization into irreducibles, then $m = n$ and $\exists\, \sigma \in S_n$, s.t. p_i and $q_{\sigma(i)}$ are associates.

Examples $\mathbb{Z}$, $F[x_1, \dots, x_n]$

Remark: Why associates? $6 = 2 \cdot 3 = (-2) \cdot (-3)$

Two main theorems: (1) PID $\Rightarrow$ UFD

(2) If R is a UFD, so is $R[x_1, \dots, x_n]$ — not a PID if $n \geq 2$

Typical non-example: $R = \mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$

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

<u>Proposition</u> In a UFD R, $p \overset{\neq 0}{\in} R$, p is a prime element $\Longleftrightarrow$ p is irreducible

Proof: "$\Rightarrow$" ✓

"$\Leftarrow$" If $p \mid ab \Rightarrow pc = ab$

Then writing ab as products of irreducibles, in which an associate of p must appear

$\Rightarrow a = pr$ or $b = pr$ for some $r \in R$ ✓. $\square$

<u>Definition/Proposition</u> In a UFD, one can define gcd of $\overset{\neq}{a}, \overset{\neq 0}{b} \in R$, as

* an element $d \overset{\neq 0}{\in} R$ s.t. $d \mid a$, $d \mid b$, and $\forall d'^{\neq 0}$, $d' \mid a, d' \mid b \Rightarrow d' \mid d$.

<u>note</u>: if d is a gcd of a, b, then du is a gcd of a, b for $u \in R^\times$

Explicitly, write $a = u p_1^{c_1} \cdots p_r^{c_r}$ $\quad p_i$ irreducible, pairwise non-associate

$b = v p_1^{d_1} \cdots p_r^{d_r}$ $\quad u, v \in R^\times$, $c_i, d_i \in \mathbb{Z}_{\geq 0}$

then $d := p_1^{\min(c_1, d_1)} \cdots p_r^{\min(c_r, d_r)}$ is a gcd of a, b.

Can define lcm similarly.

<u>Theorem</u> R PID $\Rightarrow$ UFD

Proof: <u>Existence of factorization</u>: Suppose $r \overset{\neq 0}{\in} R$ nonunit is not a finite product of irreducibles.

Certainly r is not irreducible, $r = a_1 b_1$ with a_1, b_1 nonzero, nonunit

Then one of a_1, b_1 is not a finite product of irreducibles

WLOG b_1 is not. Continue the proof above to write

$r = a_1 b_1 = a_1 a_2 b_2 = a_1 a_2 a_3 b_3 = \cdots$ $\leftarrow$ needs Axiom of Choice.

Then $(r) \subseteq (b_1) \subseteq (b_2) \subseteq \cdots R$

So $\bigcup_{n \geq 0} (b_n) =$ some ideal (b)

But this b must be contained in one of (b_n) & thus $(b_n) = (b_{n+1}) = \cdots$

Then $b_n = a_{n+1} \cdot b_{n+1} \Rightarrow a_{n+1}$ is a unit. Contradiction!

<u>Uniqueness of factorization</u>: We make induction on the number of irreducible factors

$$r = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \qquad p_i, q_j \text{ irreducible}, \ n \geq m.$$

Note: p_1 divides one of $q_1, q_2, \dots, q_n$

WLOG $p_1 | q_1 \Rightarrow q_1 = p_1 \cdot u$ for u unit

$\Rightarrow p_2 \cdots p_m = u \cdot q_2 \cdots q_n$. by induction, we are done.

<u>Remark</u>: Typical examples of ED $\Rightarrow$ PID $\Rightarrow$ UFD

$$\mathbb{Z}[i] \quad \mathbb{Z}[\sqrt{-19}] \quad \mathbb{Z}[x_1, \dots, x_n]$$

<u>Application to Gaussian integers</u>

$R = \mathbb{Z}[i]$, ED $\Rightarrow$ PID $\Rightarrow$ UFD

$N: R \longrightarrow \mathbb{Z}_{\geq 0} \qquad N(x+iy) = x^2 + y^2 = \|x+iy\|^2$

$R^\times = \{a \in R, N(a) = 1\} = \{\pm 1, \pm i\}$

<u>Theorem</u> (1) (Fermat's Theorem on sums of squares)

A prime p is the sum of two squares of integers $p = x^2 + y^2$, $x, y \in \mathbb{Z}$

if and only if $p = 2$ or $p \equiv 1 \pmod 4$

Such x, y are unique, up to signs & swapping x with y.

(2) Irreducible elements in $\mathbb{Z}[i]$ are as follows (up to associates)

(a) $1+i$ (with norm 2)

(b) the primes $p \in \mathbb{Z}$, $p \equiv 3 \bmod 4$ (with norm p^2)

(c) $x+yi$ and $x-yi$ if $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$ for a prime $p \equiv 1 \bmod 4$ (with norm p)

Proof: <u>Step 1</u> If $\pi \in \mathbb{Z}[i]$ is so that $N(\pi)$ is a prime number p, then π is irreducible

If $\pi = ab \Rightarrow \underset{\underset{p}{\parallel}}{N(\pi)} = N(a)N(b)$ so either $N(a)=1$ or $N(b)=1$

$\Rightarrow$ either a or b is a unit.

<u>Step 2</u>. For every irreducible element $\pi \in \mathbb{Z}[i]$, $N(\pi) = p$ or p^2 for some prime p, and more

Look at $(\pi) \cap \mathbb{Z}$ = a prime ideal in $\mathbb{Z}$ (as preimage of $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$)

So $(\pi) \cap \mathbb{Z} = (p)$ for some prime number p.

$\Rightarrow p = \pi a$ for some $a \in \mathbb{Z}[i]$

$\Rightarrow p^2 = N(p) = N(\pi) \cdot N(a) \Rightarrow N(\pi) = p$ or p^2

- If $N(\pi) = p^2$, then $N(a) = 1 \Rightarrow a = \pm 1, \pm i$ is a unit $\Rightarrow \pi$ is an associate of p

  If $N(\pi) = p$, then $p = \pi \cdot \bar{\pi}$, both π and $\bar{\pi}$ are irreducible elements in $\mathbb{Z}[i]$.

<u>Step 3</u> $p = 2 \Rightarrow 2 = (1+i)(1-i)$, Yet $(1-i) = -i(1+i)$ is associated to $(1+i)$

$p \equiv 3 \mod 4 \Rightarrow p$ is irreducible in $\mathbb{Z}[i]$

b/c otherwise $p = N(\pi) = a^2 + b^2$. But $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$ $\divideontimes$

$p \equiv 1 \mod 4 \rightsquigarrow$ <u>WTS</u> $p = \pi\bar{\pi}$ for some π irreducible, then $p = (x+iy)(x-iy) = x^2 + y^2$

Just need to show p is <u>not</u> irreducible in $\mathbb{Z}[i]$

<u>Fact</u>: $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ $\leftarrow$ a multiple of 4

$\Rightarrow \exists\, a \in (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $a^4 = 1$ but $a^2 \neq 1$ in $\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow a^2 + 1 \equiv 0 \pmod p$

If p is irreducible in $\mathbb{Z}[i]$, then $p \mid a^2 + 1 = (a+i)(a-i)$

$\Rightarrow$ either $p \mid a+i$ or $p \mid a-i$

But $p\mathbb{Z}[i] = \{px + pyi\}$. Contradiction!