3-5-25 (WEEK 3)

Shun / 翔海 (@shun4midx)

# PID AND UFD

Today, assume $R$ is an integral domain.

## DEFINITION

Let $p \in R \setminus \tilde{R}$ ($\tilde{R} = R^\times \cup \{0\}$). We say $p$ is a **prime** if "$p \mid ab \Rightarrow p \mid a$ or $p \mid b$", and we say $p$ is **irreducible** if "$p = ab \Rightarrow a \in R^\times$ or $b \in R^\times$"

## FACT 1

1. Prime $\Rightarrow$ irreducible

   Proof

   $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Say $p \mid a$, then $a = pc \Rightarrow p = pcb \Rightarrow cb = 1$, so $b \in R^\times$. Similar for $p \mid b \Rightarrow a \in R^\times$

2. **Irreducible $\not\Rightarrow$ prime** (☆ important)

   mod 4 ⇒ -1, so norm has no ½

   Example: In $A_{-5}$, we have $2(3) = (1+\sqrt{-5})(1-\sqrt{-5})$

   $\alpha \in A_{-5}^\times$ $\quad$ $\beta \in A_{-5}^\times$

   ↳ "$1+\sqrt{-5}$ is irred": $1+\sqrt{-5} = \alpha\beta \Rightarrow N(1+\sqrt{-5}) = 6 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = 1$ or $N(\beta) = 1$

   ↳ $(1+\sqrt{-5}) \nmid 2, 3$: If $2 = (1+\sqrt{-5})\alpha$, then $N(2) = N(1+\sqrt{-5})N(\alpha) \Rightarrow N(\alpha) = \frac{2}{3} \notin \mathbb{N}$ $\divideontimes$

## PROPOSITION 1

Let $R$ be a PID and $p \in R \setminus \tilde{R}$. TFAE:

(a) $p$ is irr

(b) $\langle p \rangle \in \operatorname{Max} R$

(c) $\langle p \rangle \in \operatorname{Spec} R$

(d) $p$ is a prime

Proof

"(a) $\Rightarrow$ (b)": $\exists M \in \operatorname{Max} R$, s.t. $\langle p \rangle \subseteq M \overset{\text{PID}}{=} \langle m \rangle \Rightarrow$ "$p = um \Rightarrow u \in R^\times$ or $m \in R^\times$" $\overset{1 \in \langle m \rangle = R}{}$ $\Rightarrow m = u^{-1}p \Rightarrow \langle m \rangle \subseteq \langle p \rangle \Rightarrow \langle p \rangle = \langle m \rangle = M$ $\in \operatorname{Max} R$

"(b) $\Rightarrow$ (c)": OK

"(c) $\Rightarrow$ (d)": $p \mid ab \Rightarrow ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle \Rightarrow p \mid a$ or $p \mid b$

"(d) $\Rightarrow$ (a)": By fact

## DEFINITION

$R$ is a **unique factorization domain** (UFD) if:

- $\forall a \in R \setminus \tilde{R}$, $\exists u \in R^\times$, irr $p_i$ $\forall i = 1, \ldots, r$, s.t. $a = u p_1 p_2 \cdots p_r$
- If $a = u p_1 \cdots p_r = v q_1 \cdots q_\ell$, then $r = \ell$ and $p_i \sim q_i$ ("associates", i.e. differ by a unit) after some change of the indecies $\forall i = 1, \ldots, r$

## PROPOSITION 2

$R$ is a UFD $\Leftrightarrow \begin{cases} \text{ACC (Ascending Chain Condition) on principal ideals, i.e. } \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots \text{ and } \exists k \text{, s.t. } \langle a_k \rangle = \langle a_{k+1} \rangle = \ldots \\ \text{irr} \Rightarrow \text{prime} \end{cases}$

Proof

"$\Rightarrow$": $\cdot$ Assume that $0 \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \ldots$

$\because \langle a_1 \rangle \neq R$, $\langle a_2 \rangle \neq R$

$\therefore a_1, a_2 \in R \setminus \tilde{R}$, say $a_1 = u p_1 \cdots p_n$, $a_2 = v q_1 \cdots q_m$

Now, $a_1 \in \langle a_2 \rangle \Rightarrow a_2 \mid a_1 \Rightarrow a_1 = a_2 b \Rightarrow u p_1 \cdots p_n = v q_1 \cdots q_m b$

$\langle a_1 \rangle \neq \langle a_2 \rangle \Rightarrow a_1 \nmid a_2 \Rightarrow b \notin R^\times \Rightarrow b = v' q_1' \cdots q_r'$, $r \geq 1$.

By uniqueness (UFD), $n = m + r$, $r \geq 1 \Rightarrow n > m$, $q_i \sim p_i$ $\forall i = 1, \ldots, m$. We conclude that $a_2 = u' p_1 \cdots p_m$

Similarly, $a_3 = u'' p_1 \cdots p_s$, $s \lneq m \lneq n$, etc... However, $\{p_i\}$ is a finite set $\divideontimes$

- Let $a$ be irr and $a|bc$, say $bc=ad$.
  - ↳ $b=0$ or $c=0$: $a|bc=0 \Rightarrow a|0 \Rightarrow a|b$ or $a|c$
  - ↳ $b\in R^\times$ or $c\in R^\times$: Say $b\in R^\times$, $c=adb^{-1} \Rightarrow a|c$. Similarly, $c\in R^\times \Rightarrow a|b$.
  - ↳ $b\in R\setminus\tilde{R}$ or $c\in R\setminus\tilde{R}$: Let $b=up_1\cdots p_n$, $c=vq_1\cdots q_m$, then $a$ is irr and $uvp_1\cdots p_nq_1\cdots q_m=ad \Rightarrow a|p_i$ or $a|q_j \Rightarrow a|b$ or $a|c$

"$\Leftarrow$": Existence: Let $a\in R\setminus\tilde{R}$.

Claim: $a$ has at least one irr factor

Proof

If $a$ is irr, then done. Otherwise, $a=a_1b_1$, $a_1,b_1\notin R^\times$.

$\Rightarrow$ If $a_1$ is irr, then done. Otherwise $a_1=a_2b_2$, $a_2,b_2\notin R^\times$.

$\vdots$

$\therefore$ Eventually, $\exists\, a_n$ that is irr. Otherwise, we find $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \langle a_3\rangle \subsetneq \cdots$ nonending $\rightarrow\!\times$

Now, if $a$ is irr, then done. Otherwise, $a=p_1a_1$ with irr $p_1$ and $a_1\notin R^\times$.

If $a_1$ is irr, then done. Otherwise, $a_1=p_2a_2$ with irr $p_2$ and $a_2\notin R^\times$.

$\vdots$

Eventually, $\exists$ irr $a_n$ and $a_{n-1}=\underbrace{p_n}_{\text{key}}a_n$. Otherwise, we find $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots$ nonending $\rightarrow\!\times$

Hence, $a=p_1\cdots p_na_n=p_1\cdots p_np_{n+1}$, which is a prime decomposition. ✓

Uniqueness: Let $a=up_1\cdots p_n=vq_1\cdots q_m$

By induction on $n$, $n=1 \Rightarrow up_1=vq_1\cdots q_m \Rightarrow p_1=u^{-1}vq_1\cdots q_m \Rightarrow m=1$ and $p_1\sim q_1$

For $n>1$, $\underbrace{p_1}_{\text{irr=prime}}|q_1\cdots q_m \Rightarrow p_1|q_i$ for some $i$, say $q_i=q_1$, write $q_1=p_1w$

Then, $up_1\cdots p_n=vwp_1q_2\cdots q_m \Rightarrow$ By induction hypothesis, $n-1=m-1 \Rightarrow n=m$ and $p_i\sim q_i$ $\forall i=2,\dots,m$. ✓

THEOREM

PID $\Rightarrow$ UFD

Proof

- "irr $\Rightarrow$ prime": Ref above
- "$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots$": Let $I=\bigcup_{i=1}^{\infty}\langle a_i\rangle$, which is also an ideal. Say $I=\langle a\rangle$ and $a\in\langle a_\ell\rangle$ for some $\ell$.
  Then, $I=\langle a\rangle \subseteq \langle a_\ell\rangle \subseteq \langle a_{\ell+1}\rangle \subseteq \cdots \subseteq I \Rightarrow \langle a_\ell\rangle = \langle a_{\ell+1}\rangle = \cdots$ ✓

# RING OF GAUSSIAN INTEGERS

Gaussian Integers: $A_{-1}$ is a ED, PID, and UFD. (We underline things to prove here in orange)

- $A_{-1}^\times=\{\pm1,\pm i\}$: $N(\alpha)=N(a+bi)=a^2+b^2=1 \Leftrightarrow a=\pm1, b=0$ or $a=0, b=\pm1$ ✓
- $\alpha\in A_{-1}\setminus\tilde{A}_{-1}$ is a Gauss prime $\Rightarrow N(\alpha)=p$ or $p^2$ for some prime integer $p$.
  - ↳ Write $N(\alpha)=\alpha\bar{\alpha}=p_1\cdots p_n$, prime integers $p_i$. Then, $\alpha|p_1\cdots p_n \Rightarrow \alpha|p_i$ for some $i$.
    Say $p_i=\alpha\beta \Rightarrow p_i=\overline{p_i}=\bar{\alpha}\bar{\beta} \Rightarrow \bar{\alpha}|p_i$. So, $\alpha\bar{\alpha}=N(\alpha)|p_i^2 \Rightarrow N(\alpha)=p$ or $p^2$ ✓
- If $N(\alpha)=p^2$, say $p=\alpha\beta \Rightarrow \bar{p}=\bar{\alpha}\bar{\beta}$. So, $p^2=N(\alpha)N(\beta) \Rightarrow N(\beta)=1 \Rightarrow \beta\in A_{-1}^\times \Rightarrow p\sim\alpha$ is a Gauss prime

CLAIM

$p\sim\alpha$ is a Gauss prime $\Leftrightarrow x^2+1$ is irr in $\mathbb{Z}/p\mathbb{Z}[x]$

Proof

Consider $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]=A_{-1}$

$f(x) \longmapsto f(i)$

Then, $\ker\varphi=\{f(x)\mid f(i)=0\}=\langle x^2+1\rangle$ (Proof: Gauss Lemma in the next section)

By 1st isom thm, $\mathbb{Z}[x]/\langle x^2+1\rangle \cong \mathbb{Z}[i]=A_{-1}$.

Now, $p$ is a Gauss prime $\Leftrightarrow \langle p\rangle\in\operatorname{Max}A_{-1}$

By 3rd isom thm, $\mathbb{Z}[x]/\langle p,x^2+1\rangle \cong \left(\mathbb{Z}[x]/\langle p\rangle\right)/\left(\langle p,x^2+1\rangle/\langle p\rangle\right) \cong \left(\mathbb{Z}[x]/\langle p\rangle\right)/\langle x^2+1\rangle$ is a field, i.e. $\mathbb{Z}[i]/\langle p\rangle$ is a field $\Leftrightarrow \langle x^2+1\rangle\in\operatorname{Max}\mathbb{Z}/p\mathbb{Z}[x]$

## CLAIM

$p$ is not a Gauss prime $\Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

**Proof**

Say $p=\bar{\alpha}\alpha \Leftrightarrow x^2+1$ is irr in $\mathbb{Z}/p\mathbb{Z}[x]$

$\Leftrightarrow x^2\equiv -1 \pmod p$ has integer solution

$\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $a^2\equiv -1 \pmod p$

$\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $O(\bar{a})=4$ in $(\mathbb{Z}/p\mathbb{Z}^\times, \bar{1})$ or $p=2$

(Lagrange) $\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $4 \mid |\mathbb{Z}/p\mathbb{Z}^\times| = p-1 \Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

Opposite direction: $2^2=4 \mid p-1 = |\mathbb{Z}/p\mathbb{Z}^\times|$. By Sylow I, $\exists H \leq \mathbb{Z}/p\mathbb{Z}^\times$ (cyclic), s.t. $|H| = |\langle\bar{a}\rangle| = 4$

$\therefore p=a^2+b^2=N(a+bi) \Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

## CLAIM

$n=A^2+B^2 \Leftrightarrow n=2^k p_1^{a_1}\cdots p_r^{a_r} q_1^{b_1}\cdots q_s^{b_s}$, $p_i\equiv 1 \pmod 4$, $q_j\equiv 3 \pmod 4$, $b_i\equiv 0 \pmod 2$

**Proof**

"$\Rightarrow$": For $n=N(A+Bi)=N(\alpha_1)N(\alpha_2)\cdots N(\alpha_k)$, write $A+Bi=\alpha_1\cdots\alpha_k$, $\alpha_i$: Gauss prime

Here, $N(\alpha_i)=p$ or $p^2 \Leftrightarrow \underbrace{(p=2 \text{ or } p\equiv 1 \pmod 4)}_{\text{Related to } p \text{ as norm}}$ or $\underbrace{p\equiv 3 \pmod 4}$ — related to $p^2$ as norm

"$\Leftarrow$": $2=(1-i)(1+i)$, $(1+i)\sim(1-i)$, write $p_i=\alpha_i\bar{\alpha_i}$

Let $(1+i)^k \alpha_1^{a_1}\cdots\alpha_r^{a_r} q_1^{\frac{b_1}{2}}\cdots q_s^{\frac{b_s}{2}} = A+Bi$, then $(1-i)^k \bar{\alpha}_1^{a_1}\cdots\bar{\alpha}_r^{a_r}\bar{q}_1^{\frac{b_1}{2}}\cdots\bar{q}_s^{\frac{b_s}{2}} = A-Bi$

Multiplying the two, we get $n=A^2+B^2$