MATH 403/503 L25

Factorization in IDs §18.2

Let R be a comm ring. Let $a, b \in R$.

Def i) $a|b$ if $ac = b$, some $c \in R$

ii) a is a unit if $a|1$

iii) a, b are associates if $a = bu$, some unit u.

Note In an ID, a, b are associates iff $a|b$ and $b|a$. (Exercise!)

Def Let D be an ID.

i) $p \in D$ is prime if $p|ab \Rightarrow p|a$ or $p|b$.

ii) $p \in D$ is irreducible if $p = ab \Rightarrow a$ or b is a unit

Example Let R be the subring of $\mathbb{Q}[x,y]$ generated by x^2, xy, y^2. Then x^2, xy, y^2 are irreducible in R

But xy is not prime; $xy \mid x^2y^2$ in R but $xy \nmid x^2$ and $xy \nmid y^2$.

An integral domain D is a unique factorization domain (UFD) if

Every nonzero non-unit $a \in D$ is a product of (finitely many) irreducible elements

If $a = p_1 \cdots p_r = q_1 \cdots q_s$ where p_i, q_i are irreducible, then $r = s$ and $\exists \pi \in S_r$ such that p_i and $q_{\pi(i)}$ are associates $\forall i = 1, \ldots, r$.

Example $\mathbb{Z}$ is a UFD (by Fund. Th. Arithm.)

Example $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ (check!) hence an integral domain ($\mathbb{C}$ being a field). ($\sqrt{-3} = i\sqrt{3}$)

Define $\nu : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}_{\geq 0}$ by $\nu(z) = |z|^2 = a^2 + 3b^2$, for $z = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$.

$\nu(zw) = \nu(z)\nu(w)$ by properties of $|\cdot|$ on $\mathbb{C}$.

Can check: $z \in \mathbb{Z}[\sqrt{-3}]$ is a unit iff $\nu(z) = 1$ which holds iff $z = \pm 1$. ($\nu(z) = a^2 + 3b^2$)

We claim $4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$ are two distinct factorizations into irreducibles.

If 2 were not irreducible then $2 = zw$ for some non-units z, w. Then

$$4 = \nu(2) = \nu(zw) = \nu(z)\nu(w)$$

So $\nu(z) = \nu(w) = 2$. But $c^2 + 3d^2 = 2$ has no sol $(c, d) \in \mathbb{Z}^2$ contradiction. Similarly $1 \pm \sqrt{-3}$ are irreducible. (± 1 "a unit" times $1 \pm \sqrt{-3}$)

2 is not a unit

So $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

PIDs

Lem D integral domain, $a, b \in D$

i) $a|b \iff (a) \supseteq (b)$

ii) a, b associates $\iff (a) = (b)$

iii) a is a unit $\iff (a) = D$.

Th 18.12 Let D be a PID, and (p) a ideal in D.

Then i) (p) is maximal iff p is irreducible.

$\Leftrightarrow$ ii) (p) is prime ideal iff p is prime and nonzero

Proof i) Spse (p) maximal. Let $a, b \in D$ with $p = ab$. Then $(p) \subseteq (a)$ so either $(p) = (a)$ in which case b is a unit, or $(a) = D \Rightarrow a$ is a unit. So p is irreducible.

Conversely, spse p is irreducible. Let (a) be an ideal of D with $(p) \subseteq (a) \subseteq D$.

Then $p = ab$, some $b \in D$, So either a is a unit ($\Rightarrow (a) = D$) or b is a unit ($\Rightarrow (p) = (a)$).

ii) Exercise. ∎

Corollary Let D be a PID.
If p is irreducible then p is prime.

Pf p irr $\Rightarrow$ (p) maximal and $p \neq 0$
$\Rightarrow$ (p) prime and $p \neq 0$
$\Rightarrow$ p prime. ∎

Lemma 18.14
Let D be a PID. Let $I_1, I_2, \ldots$ be a sequence of ideals of D such that

$$I_1 \subseteq I_2 \subseteq \cdots$$

Then $\exists N > 0$ s.t. $I_n = I_N$ $\forall n \geq N$.

Proof We claim $I := \bigcup_{k=1}^{\infty} I_k$ is an ideal of D. $0 \in I_1 \subseteq I$ so $I \neq \emptyset$.
If $a, b \in I$ then $a, b \in I_k$ some $k \gg 0$.
$\Rightarrow a - b \in I_k \subseteq I$ so I is closed under subtraction. Similarly, if $a \in I$ then $a \in I_k$ some $k > 0$ $\Rightarrow ra \in I_k \subseteq I$ $\forall r \in D$. ∎

Since D is a PID, $I = (\bar{a})$ for some $\bar{a} \in D$. Since $\bar{a} \in I$, we have $\bar{a} \in I_N$, some $N > 0$. Then $I = I_N$ so $I_n = I_N$ $\forall n \geq N$ ∎