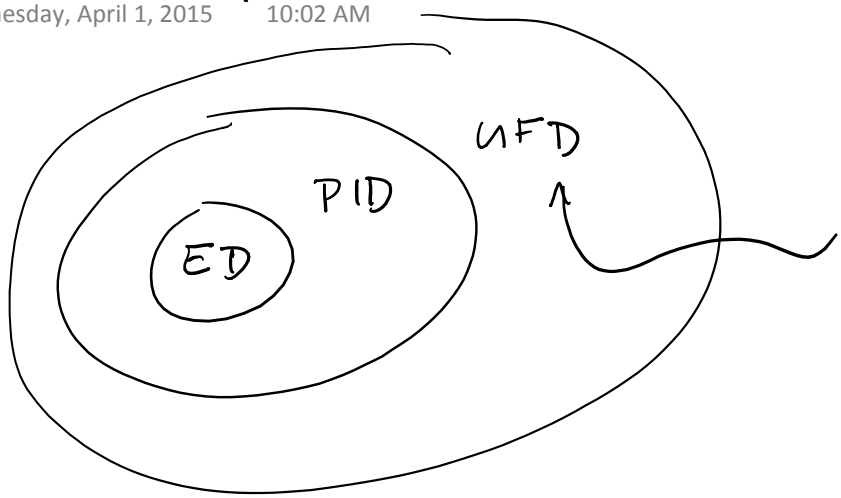
Lecture 34

Wednesday, April 1, 2015 10:02 AM



Defn R integral domain.

(1) $0 \neq r \in R \setminus R^\times$ is irreducible when

$r = ab$ (for $a, b \in R$) $\Rightarrow$ a or $b \in R^\times$

(2) $p \in R$ is prime if (p) is a prime ideal

$\Leftrightarrow$ $\left(p \mid ab \Rightarrow p \mid a \text{ or } p \mid b \right)$

(3) $a, b \in R$ are associate if $a = ub$ for some $u \in R^\times$.

Prop In an integral domain nonzero prime elts are irreducible.

Pf If (p) is prime and $p = ab$, then

a or $b \in (p)$. If $a \in (p)$, then

$a = pr$ for some $r \Rightarrow p = ab = prb$

Cancel p: $1 = rb \Rightarrow b \in R^\times$.

If $b \in (p)$, then $a \in R^\times$. Thus p is irreducible. ∎

Fact $R = \mathbb{Z}[\sqrt{-5}]$ has 3 as an irreducible elt but $3 \mid 9 = (2+\sqrt{-5})(2-\sqrt{-5})$ & $3 \nmid 2 \pm \sqrt{-5}$

so 3 is <u>not</u> prime in R.

Prop In a PID, a nonzero elt is prime $\iff$ it is irreducible.

Cor By the fact, $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Pf of Prop Suppose p is irreducible in a PID R.

We show (p) is a maximal ideal in R.

If $I \supseteq (p)$ is an ideal of R, then $I = (m)$

& $p = rm$ for some $r \in R$.

By irreducibility, r or $m \in R^\times$.

If $m \in R^\times$, then $I = R$. If $r \in R^\times$, then

$(p) = (rm) = (m) = I$.

Thus (p) is maximal and hence prime.

Defn A unique factorization domain (UFD) is an integral domain R in which every $0 \neq r \in R - R^\times$ has the following properties:

(1) $r = \prod_{i=1}^{n} p_i$, $p_i \in R$ irreducible

(2) The factorization in (1) is unique up to reordering and associates:

if $r = \prod_{j=1}^{m} q_j$, q_j irred,

then $m = n$ & $\exists\, \sigma \in S_n$ s.t.

$q_{\sigma(j)} = u_j p_j$ for $u_i \in R^\times$.

$6 = 2 \cdot 3$
$= (-3)\cdot(-2)$

Prop In a UFD, nonzero elts are prime $\Leftrightarrow$ irr.

Pf p irr, $p \mid ab \Rightarrow ab = pc$ and thus by uniqueness of fact'n into irreducibles p is an associate of some irr factor of a or b. WLOG,

$a = (up)\, p_2 p_3 \cdots p_n$, $u \in R^\times \Rightarrow p \mid a$ so p is prime. $\square$

Prop $a, b \neq 0$ in a UFD R w/ prime factorizations

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

w/ p_i distinct irreducibles, $e_i, f_i \geq 0$.

[e.g. $30 = 2 \cdot 3 \cdot 5 \cdot 7^0$ $\quad 105 = 2^0 \cdot 3 \cdot 5 \cdot 7$]

Then if $g_i = \min\{e_i, f_i\}$, then

$c = p_1^{g_1} p_2^{g_2} \cdots p_n^{g_n}$ is a gcd of a & b.

[$\gcd(30, 105) = 3 \cdot 5 = 15$]

Pf Exc. □

Thm Every PID is a UFD.

Pf **Step 1** Factor.

Take $0 \neq r \in R \setminus R^\times$. If r is irr, done.

If r is not irr, write $r = r_1 r_2$ with $r_1, r_2 \notin R^\times$.

If r_1 & r_2 are irr, done. If not, assume r_1 is reducible

Then $r_1 = r_{11} r_{12}$, $r_{11}, r_{12} \notin R^\times$. Continue ...

Does this process terminate ?

Suppose not. Get $(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq (r_{111}) \subsetneq \cdots \subsetneq R$

Claim Any ascending chain of ideals in a PID terminates, i.e. if

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$$

then $I_n = I_N$ for all $n \geq$ some fixed N.

take $I = \bigcup_{n \geq 1} I_n \trianglelefteq R$ Since R is a PID,

$I = (a)$. Since $a \in I$, $a \in I_N$ for some N.

Thus $I_N \subseteq I = (a) \subseteq I_N \Rightarrow I = I_N$.

$\rightsquigarrow$ factorization algorithm terminates.

Step 2

Remains to show factorization is unique.

$r = \prod_{i=1}^{n} p_i$. If $n = 0$, then r is a unit.

If $r = qc$, q irr, then $q \mid$ unit $\Rightarrow q$ a unit $\lightning$.

For $n \geq 1$, if $r = p_1 \cdots p_n = q_1 \cdots q_m$, $m \geq n$.

Since $p_1 \mid q_1 \cdots q_m$, $p_1 \mid$ some q_i. WLOG,

assume $p_1 \mid q_1 \Rightarrow q_1 = p_1 u \Rightarrow u \in R^\times$.

Thus $p_1 \cdots p_n = (p_1 u)\, q_2 \cdots q_m$

Cancel p_1,

$$p_2 \cdots p_n = \underbrace{(u q_2)}_{\text{irr.}} \cdots q_m .$$

By induction on minimal # of irr factors, we're done. □

Cor [Fundamental Thm of Arithmetic] $\mathbb{Z}$ is a UFD.

pf $\mathbb{Z}$ is a ED $\Rightarrow$ PID $\Rightarrow$ UFD. □

Cor R a PID then $\exists$ multiplicative D-H norm on R.

pf Define $N: R \to \mathbb{N}$ by

$N(0) = 0$

$N(u) = 1$ for $u \in R^\times$

$N(a) = 2^n$ if $a = p_1 \cdots p_n$, p_i irr.

$N(ab) = 2^{n+m}$ if $b = q_1 \cdots q_m$

$= 2^n \cdot 2^m = N(a)\,N(b)$.

$a, b \in R \setminus \{0\}$. $(a, b) = (r)$. $a \notin (b) \Rightarrow (r) \neq (b)$.

Since $b = xr$, we must have that $x \in R^\times$

$\Rightarrow N(b) = N(x)N(r) > N(r)$.

Thus (a,b) contains a nonzero elt of norm $< N(b)$.

□