2/8/2019>

(34) This relates to GCD's.

DEFIN: Given $a,b \in R$ a ring, a greatest common divisor (GCD) d of a,b is an element d dividing both a,b and such that any e dividing both a,b has e dividing d.

REMARKS (1) If one such d exists, it may not be unique, since any unit $c \in R^\times$ has $d' = cd$ another GCD for a,b

DEFIN: Two elements d, d' in R a ring that differ by a unit $c \in R^\times$ i.e. $d' = cd$ are called associates. Equivalently $(d) = (d')$ or d divides d' and d' divides d.

(2) Sometimes they don't exist, e.g. $a = 6$ and $b = 2(1+\sqrt{5})$ in $\mathbb{Z}[\sqrt{5}]$ $= 2 \cdot 3$ $= (1+\sqrt{-5})(1-\sqrt{5})$

have both 2 and $1+\sqrt{5}$ as common divisors, both maximal under divisibility among the common divisors of a,b, but neither divides the other.

(3) PROPOSITION (12.2.8): If R is a PID, then $GCD(a,b)$ always exists, and even $GCD(a_1, a_2, \dots, a_n)$, namely the ideal $I = (a,b) = (d)$ with $d = GCD(a,b)$ or $I = (a_1, \dots a_n) = (d)$ with $d = GCD(a_1, \dots a_n)$

and hence in this case, $GCD(a,b) = r \cdot a + s \cdot b$ for some $r,s \in R$

$GCD(a_1, \dots a_n) = r_1 a_1 + \dots + r_n a_n$ for some $r_i \in R$

Also $GCD(a_1, \dots, a_n) = GCD(a_1, a_2, \dots, GCD(a_{n-1}, a_n))$ lets one compute it pairwise, and if R is not just a PID but a Euclidean domain one can use Euclid's algorithm: $GCD(a,b) = GCD(r,a) = \dots$ if $b = qa + r$

EXAMPLE: $GCD(1000, 12, 30)$

$= GCD(1000, \underbrace{GCD(12,30)}) = GCD(6,12) = 6$

$= GCD(1000, 6)$

$= GCD(6, 4)$

$= GCD(4, 2) = 2$

$$\begin{array}{r} 2 \\ 12\overline{)30} \\ \underline{24} \\ 6 \end{array} \qquad \begin{array}{r} 166 \\ 6\overline{)1000} \\ \underline{600} \\ 400 \\ \underline{36} \\ 40 \\ \underline{36} \\ 4 \end{array} \qquad \begin{array}{r} 1 \\ 4\overline{)6} \\ \underline{4} \\ 2 \end{array}$$

NON-EXAMPLE: Later we'll see GCD's exist in $\mathbb{Z}[x]$, e.g. $GCD(2x, x^2) = x$, however $\nexists\, r(x), s(x) \in \mathbb{Z}[x]$ with $r(x)\cdot 2x + s(x)\cdot x^2 = x$

How does this P.I.D. property make factorization better?

Lack of unique factorization turns out to relate to the distinction between elements of R that are irreducible and are prime ..

DEF'N: Recall $r \in R$ is called irreducible if $r = ab$ forces at least one of a or b to be in $R^\times$

Equivalently, the principal ideal (r) has no principal ideals (a) with $(r) \subsetneq (a) \subsetneq R$ $\quad = (1)$

Say $r \in R$ is prime if r dividing ab implies either r divides a or r divides b

Equivalently, the principal ideal (r) is a prime ideal I (an ideal I for which $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$)

EXAMPLE: In $R = \mathbb{Z}$, irreducible $\overset{n}{\iff}$ prime $\overset{n}{\iff}$ n is a prime number p

PROPOSITION 12.2.10:

In any domain R, prime elements are always irreducible, but not conversely.

proof: If $p \in R$ is prime, it can't have a proper factorization $p = ab$, since primeness forces either a divisible by p $\Rightarrow (a) \supset (p)$ and $(p) \supset (a)$, so a, p are associates. (or b divisible by p)

In $R = \mathbb{Z}[\sqrt{-5}]$, can check $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible, and none are associates to each other, but $2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 6$

$$\Rightarrow \quad 2 \cdot 3 \in (1+\sqrt{-5})$$

even though $2 \notin (1+\sqrt{-5})$
$3 \notin (1+\sqrt{-5})$.

So $1+\sqrt{-5}$ is irreducible, but not prime ∎
(same for $2, 3, 1-\sqrt{-5}$)

PROPOSITION: (12.2.9(b)) In a P.I.D. an element is prime if and only if it is irreducible.

proof: By above PROP, only need to show r irreducible in R implies r is prime. So assume r divides ab, but $r \nmid a$, and we'll show $r \mid b$.

Since R is a P.I.D., $(r, a) = (g)$ for some $g = GCD(r, a)$

Since r is irreducible, $(g) = (1)$ or (r), but $(g) \neq (r)$ since $g \mid a$ but $r \nmid a$.

Hence $(r, a) = 1$, so $1 = xr + ya$ for some $x, y \in R$

mult. by b ↓

$b = \underbrace{xrb}_{\text{divisible by } r} + \underbrace{yab}_{\text{divisible by}} \Rightarrow b$ is divisible by r. ∎

Now we can define what unique factorization means and see why PID's have it.

DEF'N (12.2.12): A domain R is a unique factorization domain (U.F.D.) if for every $r \in R$

(a) there exists a factorization $r = p_1 p_2 \cdots p_n$ with p_i irreducible in R

(b) it is unique in the sense that if $r = p_1 \cdots p_n$ with p_i, q_j irreducibles $= q_1 \cdots q_m$

then in fact $n = m$ and one can re-index so that p_i, q_i are associates ($p_i = u_i q_i$ with $u_i \in R^\times$) for $i = 1, 2, \ldots, n$

EXAMPLE: In $\mathbb{Z}$, this is usual uniqueness of prime factorization

e.g. $40 = 2 \cdot 2 \cdot 5 \cdot 5$
$= (-2) \cdot 5 \cdot (-2) \cdot 5$
$= (-5) \cdot 2 \cdot (-2) \cdot 5$
$= \cdots$

2/20/2019

Parts (a) & (b) in the UFD definition are really separate issues, and PID's avoid the problem for both.

PROPOSITION (12.2.13): (i) A domain R has existence of factorizations $r = p_1 p_2 \cdots p_n$ into irreducibles p_i $\forall r \in R$ if $\nexists$ an infinite (strictly) ascending chain of principal ideals

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \text{ in } R$$

(ii) In particular, P.I.D.'s have no such chains of principal ideals, so they do have (irred.) factorizations.

NON-EXAMPLE: $R = \mathbb{R}[t, t^{1/2}, t^{1/4}, t^{1/8}, \ldots]$

contains elements like $7t + 20t^{5/16} - 109t^{\frac{13}{256}}$

and t has no irreducible factorization, e.g. $t = t^{1/2} \cdot t^{1/2}$
$= (t^{1/4} \cdot t^{1/4})(t^{1/4} \cdot t^{1/4})$
$= (t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})$
$= \cdots$

also $(t) \subsetneq (t^{1/2}) \subsetneq (t^{1/4}) \subsetneq (t^{1/8}) \subsetneq \cdots$