Algebra II: Feb 14, 2014.

Let R be an integral domain. Recall our terminology, phrased in terms of ideals:

a is a unit $\Leftrightarrow$ $(a) = (1)$

a divides b $\Leftrightarrow$ $(b) \subset (a)$

a properly divides b $\Leftrightarrow$ $(b) \subsetneq (a)$

a is irreducible $\Leftrightarrow$ a has no proper divisors.

a is prime $\Leftrightarrow$ (a) is a prime ideal.

Def: R is a Euclidean domain (ED) if there exists a function $\sigma: R \setminus \{0\} \to \mathbb{N} = \{0,1,2,\dots\}$ such that the following holds

- For every $a, b \in R$ with $b \neq 0$ we have $q, r \in R$ satisfying $a = bq + r$ and either $r = 0$ or $\sigma(r) < \sigma(b)$.

Rem: In other words, there is a "size function" which makes division with remainder work.

Last time I had $\mathbb{R}_{\geq 0}$ as the codomain of σ. But it should be $\mathbb{N}$.

Def: A principal ideal domain (PID) is a domain in which every ideal is principal.

Ex: $\mathbb{Z}$, $F[x]$ where F is a field.

Prop: ED $\Rightarrow$ PID. (i.e. Every Euclidean domain is a principal ideal domain.)

Pf: Mimicks the proof that $\mathbb{Z}$ or $F[x]$ is a PID using the division with remainder.

Ex. $\mathbb{Z}[i]$ is a ED $\Rightarrow$ $\mathbb{Z}[i]$ is a PID.

In a PID we can make sense of the gcd.

<u>Def</u>: We say that d is a gcd of a and b if

$$(d) = (a,b).$$

<u>Remk</u>: The gcd is unique, except up to multiplication by a unit.

Our goal is to generalize the Fundamental Theorem of Arithmetic (every integer factors into a product of primes uniquely, except up to ordering of the factors.)

Let R be a domain. We can attempt factoring $a \in R$.

$a \longrightarrow$ Is it irreducible

No — Then factor

<u>Yes</u> : Then STOP.

$a = a_1 b_1$ (Neither is a unit).

Repeat the same process for a_1 and b_1 .....

This may never terminate (we won't encounter this phenomenon much in this class, but here is an example:

Let R be the ring of "fractional power polynomials" with coeff in $\mathbb{R}$

$$R = \{ \sum_{i=0}^{n} a_i x^{b_i} \mid b_i \in \mathbb{Q} \quad b_i \geq 0 \}.$$

It includes functions like $x^{1/2}$, $x^{1/2} + 5 \cdot x^{1/3} + x^{2.3}$ etc.

It's not ~~too~~ hard to check that R is a domain. But when we try factoring, we fail:

$$x = x^{1/2} \cdot x^{1/2} = x^{1/4} \cdot x^{1/4} \cdot x^{1/2}$$
$$= x^{1/8} \cdot x^{1/8} \cdot x^{1/4} \cdot x^{1/2} \; \ldots\ldots)$$

There is a useful characterization of when factoring fails to terminate.

<u>Ascending Chain Condition</u> (for principal ideals)

There is no infinite increasing chain of principal ideals in R:

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots\cdots$$

<u>Prop</u>: Factoring terminates iff ACC holds. for principal ideals in R.

<u>Pf</u>: Say we factor $a = a_1 b_1$ where neither a_1, b_1 is a unit.
If factoring doesn't stop for a then it doesn't stop for a_1 or b_1.
Say a_1 is the culprit. Then we have

$$(a) \subsetneq (a_1)$$

And by factoring a_1 further, we can extend this chain further by the same argument, indefinitely. Thus

$$\text{Failure of termination} \Rightarrow \text{Failure of ACC.}$$

Conversely, failure of ACC means we have

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots\cdots \qquad \text{No } a_i \text{ is a unit}$$

Thus
$$a_1 = a_2 b_2 \qquad b_2 \text{ not a unit}$$
$$a_2 = a_3 b_3 \qquad b_3 \text{ not a unit}$$
$$\vdots$$

showing that factoring $a_1 = a_2 b_2$
$= (a_3 b_3) b_2 \quad \cdots$ does not terminate.

So $\quad$ Failure of ACC $\Rightarrow$ Failure of termination

$\square$.

<u>Def</u>: A domain R is a <u>Unique Factorization Domain</u> (UFD) if
(1) ACC holds (2) factorization is unique in the following sense:

if $a = p_1 \cdots p_m$ where p_i are irred.
$= q_1 \cdots q_n$ where q_i are irred.

Then $m = n$ and (possibly after a permutation)

$$p_1 = \text{unit}_1 \cdot q_1, \quad p_2 = \text{unit}_2\, q_2, \quad \ldots, \quad p_m = \text{unit}_m\, q_m.$$

Thm: PID $\Rightarrow$ UFD.

Lemma 1: PID $\Rightarrow$ ACC.

Pf: Suppose we have a chain of (not necessarily strict) inclusions

$$(a_1) \subset (a_2) \subset \cdots\cdots$$

Let $I = \bigcup_{i=0}^{\infty} (a_i) = \{ r \in R \mid r \in (a_i) \text{ for some } i \}$.

Then I is an ideal. $\Rightarrow$ $I = (b)$ for some b.

But then $b \in (a_n)$ for some n.

$\Rightarrow$ $(b) \subset (a_n)$ But clearly $(a_n) \subset I = (b)$

$\Rightarrow$ $(b) = (a_n)$ and similarly $(b) = (a_{n+1}) = (a_{n+2}) = \cdots\cdots$

So the chain is not really infinite; it stabilizes after n. $\square$.

Lemma 2: In a PID irreducible $\Rightarrow$ prime.

Pf: Let p be irreducible and $p \mid ab$.

Suppose $p \nmid a$. We must show $p \mid b$.

Let $(d) = (p, a)$. Then $d \mid p$ and $d \mid a$.

Since p has no proper divisors and $p \nmid a$, d must be a unit.

We can take $d = 1$. So $1 \in (p, a)$.

Thus we can write $1 = px + ay$ $x, y \in R$.

Then $b = pbx + bay$,

which is div. by p as $p \mid pbx$ and $p \mid aby$.

$\square$.

Thm: ~~Lemma 3~~: ~~ACC *~~ ~~In~~ A domain ~~A~~ ~~ring~~ where ACC holds and every irred elem. is prime is a UFD.

Pf: We have to prove uniqueness of factorization. This is completely analogous to the proof for $\mathbb{Z}$.

Say $p_1 \cdots p_m = q_1 \cdots q_n$. p_i, q_i irred.

Then $p_1 \mid q_1 \cdots q_n$. But then $p_1 \mid q_i$ for some i.

But q_i is also irred. $\Rightarrow$ $q_i = \text{unit} \cdot p_1$

re arrange the numbering so that $q_i = q_1$. We have

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

$q_1 = \text{unit} \cdot p_1$

$$\Rightarrow \quad \cancel{p_1} p_2 \cdots p_m = \text{unit} \cdot \cancel{p_1} \cdot q_2 \cdots q_m \qquad \underline{\text{cancel}}.$$

$$\Rightarrow \quad p_2 \cdots p_m = (\text{unit } q_2)\, q_3 \cdots q_m .$$

Repeat . . .

$\square$.

Conclusion.

$$\begin{tikzcd}
 & \text{UFD.} & \\
\underline{\text{ACC}} & + \arrow[u, Rightarrow] & \underline{\text{Irreducible} \Leftrightarrow \text{Prime.}} \\
 & \underline{\text{PID}} \arrow[ul, Rightarrow] \arrow[ur, Rightarrow] & \\
 & \underline{\text{ED.}} \arrow[u, Rightarrow] &
\end{tikzcd}$$

Ex. Unique factorization holds in $\mathbb{Z}[i]$.
(Q: What are the "primes" ??)

~~Ex. (Without PF)~~