MATH H113: Honors Introduction to Abstract Algebra

2016-04-20

- Unique factorization domains

For Friday:
Skip "Factorization in the Gaussian Integers" (p. 289-292) Read Sect. 9.1 and 9.2

Last time: In a P.I.D., every nonzero prime ideal is a maximal ideal.
Corollary: If F is a field, then $F[x,y]$ $(= F[x][y])$ is not a P.I.D.
Proof: Since $F[x,y]/(y) \cong F[x]$, and $F[x]$ is an integral domain, but not a field, the ideal (y) is prime but not maximal. $\therefore$ $F[x,y]$ is not a P.I.D. because P.I.D.'s don't have such ideals.

Unique Factorization Domains

Definition: Let R be an integral domain. Then:

a. An element $r \in R$ is *irreducible* if it's nonzero, not a unit, and $r = ab \implies a$ or b is a unit. a'. An element $r \in R$ is *reducible* if it's nonzero, not a unit, and $r = ab$ with a, b not units.
b. An element $p \in R$ is prime if the ideal (p) is a nonzero prime ideal; equivalently, if p is nonzero, p is not a unit, and $p \mid ab \implies p \mid a$ or $p \mid b$.

Examples: 0. In a field, there are no irreducible, reducible, or prime elements. Everything's either a unit or 0. 1. In $\mathbb{Z}$, the prime elements are $\pm p$, where p is a prime number (as in grade school: $2, 3, 5, 7, \ldots$).
The reducible elements are $\pm$ composite numbers
The irreducible elements are $\pm 2, \pm 3, \pm 5, \ldots$ 2. The book gives some examples of irreducible elements that are not prime.

Proposition: In an integral domain, all prime elements are irreducible.
Proof: Let R be an integral domain and let $p \in R$ be prime. Then $p \neq 0$ and p is not a unit. Suppose $p = ab$. Then $a \in (p)$ or $b \in (p)$ (by primeness of (p)). If $a \in (p)$, then $p \mid a$, but also $a \mid p$, so a and p are associates; since $a \neq 0$, $b = \frac{p}{a}$ is a unit. Similarly, $b \in (p) \implies (a)$ is a unit. $\therefore$ p is irreducible.
The converse is true in a P.I.D. (proof later).

Remark: Let R be an integral domain, and let a and b be associates in R. Then:
$a = 0 \iff b = 0$;
a is a unit $\iff$ b is a unit

a is irreducible $\iff$ b is irreducible
a is reducible $\iff$ b is reducible
a is prime $\iff$ b is prime $((a) = (b))$

Definition: A *unique factorization domain* is an integral domain R for which every nonzero nonunit element $r \in R$ has the following properties:

i. r can be written $r = p_1 p_2 \cdots p_n$, in which all p_i are irreducible elements of R; and
ii. Any two such factorizations are unique up to *associates*: if $r = q_1 q_2 \cdots q_m$ also, then $m = n$ and after renumbering the q_i, each q_i is associate to some p_i.

Big Theorem of the Day

Theorem: Every P.I.D. is a U.F.D.

Key Lemma: Let R be a P.I.D. Then every nonempty collection of ideals of R has a maximal element (not necessarily a max ideal).
Proof: Let R be a P.I.D. and let A be a nonempty collection of ideal of R. Partially order A by inclusion. Let B be a nonempty chain in A. We need to find an upper bound for B in A: Let $J = \bigcup_{I \in B} I$. As before, J is an ideal of R.
Clearly, J is an upper bound for B.
We need to check that $J \in A$.
Since R is a P.I.D., $J \in (r)$ for some $r \in R$.
Since $J = \bigcup_{I \in B} I$, r occurs in some $I \in B$.
So $J \subseteq I$ (because $J = (r)$ and $r \in I$),
and $I \subseteq J$ (because I is among the ideal whose union is J), $J = I \in B \subseteq A$, so $J \in A$.
Therefore, by Zorn's lemma, A has a maximal element.

Theorem: Every P.I.D. is a U.F.D.
Proof: Let R be a P.I.D.
Step 1: Factorization.
Assume that not every nonzero nonunit $r \in R$ can be written as a (finite) product of irreducibles. Let $A = \{(r) : r \in R, r \neq 0, r$ is not a unit, and r is not equal to a (finite) product of irreducibl
Then (by assumption) $A \neq \emptyset$, so it has a maximal element (r). Then $r \neq 0$, r is not a unit, and r is not a finite product of irreducibles.
In particular, r is not irreducible (otherwise $r = r$ would be a factorization).
So r is reducible, so $r = ab$ such that neither a nor b is a unit.
Now $a \mid r$, so $(r) \subseteq (a)$. Also b is not a unit, so r and a are not associates. $\therefore$ $(r) \neq (a)$. So $(a) \notin A$ (by maximality of (r)). We know that $a \neq 0$ ($r \neq 0$), and a is not a unit, so $(a) \notin A \implies a = p_1 p_2 \cdots p_n$ with p_i irreducible $\forall i$.
Similarly, $b = q_1 q_2 \cdots q_m$ with q_j irreducible $\forall j$.
Then $r = ab = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m$ is a factorization of r into irreducibles,

contradiction.
$\therefore$ every nonzero nonunit in R can be factored into irreducibles.
Step 2: Friday.
See how Step 1 plays out if $R = \mathbb{Z}$. Just work with positive numbers, $n \geq 2$ (avoids units). Proof that every $n \geq 2$ has a prime factorization:
Method 1: Strong induction: If all $m < n$ have prime factorizations, then:

a. if n is prime, then $n = n$ is a prime factorization.
b. otherwise $n = ab$ with $a, b \geq 2$. Each of these has prime factorization, $\therefore$ so does n.

Conclude by induction.

Method 2: By contradiction: Let $n \geq 2$ be the smallest number not having a prime factorization. THen n is not prime, so $n = ab$; $a, b < n$, so they have prime factorizations, $\therefore$ so does n, :(.