MATH H113: Honors Introduction to Abstract Algebra

2016-04-22

- U.F.D.'s
- Polynomials

For Monday:
Read Sections 9.2 and 13.1

Homework due April 29:
8.3: 2
9.1: 8, 10, 13
9.2: 7, 9
13.1: 2, 7

We were proving: **Theorem**: Every P.I.D. is a U.F.D.
Proof: On Wednesday, we showed every nonzero nonunit element in R factors into a product of irreducibles (where R is a P.I.D.)
Step 2: Uniqueness. Suppose $r \in R$ is nonzero, not a unit, and has all factorizations $r = p_1 p_2 \cdots p_n$ and $r = q_1 q_2 \cdots q_m$, where all p_i and all q_i are irreducible, and $m, n \in \mathbb{N}$. Now if $m = 0$or $n = 0$ then $r = 1$, which is a unit, so $m, n > 0$.
We may assume $n \leq m$ (otherwise integerchange the two factorizations). We'll prove this by induction on n.
Base case: $n = 1$. Then $r = p_1$, so r is irreducible. If $r = q_1 q_2 \cdots q_m$ with $m > 1$ then $r = ab$ where $a = q_1$ is not a unit and $b = q_2 \cdots q_m$ $(m \geq 2)$ is not a unit (that would imply q_2 is a unit, but it's not). This contradicts irreducibility of $r = p_1$. $\therefore m = 1$, so $p_1 = q_1$ and we're done.
Inductive Step: Assume that if two products of $n-1$ and $m-1 \geq n-1$ irreducibles are equal then $n - 1 = m - 1$ and all factors are associates after rearranging them.
We have p_1 is irreducible and $p_1 \mid q_1 \cdots q_m$.
Lemma (Prop. 11): In a P.I.D., an element, every irreducible element is prime.
Proof: Let $p \in R$ be irreducible. Then the ideal (p) is nonzero, and we'll show that it's prime by showing that it's maximal. Let M be an ideal of R that contains (p). $M \supseteq (p)$. Write $M = (m)$ (R is a P.I.D.). Then $p \in (m)$, so $p = mr$ for some $r \in R$. Since p is irreducible, (m is a unit $\implies (m) = M = R$) or (r is a unit $\implies m$ and p are associates $\implies (m) = M = (p)$).
Back to our proof: $p_1 \mid q_1 \cdots q_m$, so $p_1 \mid q_j$ for some j. After some rearranging, we may assume $j = 1$, so $p_1 \mid q_1$. Then $q_1 = p_1 r$ for some $r \in R$. Since q is irreducible, r must be a unit (because p_1 isn't). $\therefore p_1$ and q_1 are associates; $q_1 = r p_1$, $r \in R^\times$
Then $p_2 \cdots p_n = q_2' q_3 \cdots q_m$ where $q_2' = r q_2$ is irreducible. Conclude by induction.

$\therefore$ R is a U.F.D.
(Not every U.F.D. is a P.I.D.; later (I hope) we'll see that $F[x, y]$ is a U.F.D. for any field F; we already know it's not a P.I.D.)

Proposition: In a U.F.D. an element is prime if and only if it's irreducible.
Proof:

- prime $\implies$ irreducible: already proved (on Wed.)
- irreducible $\implies$ prime: Let p be irreducible. Then $p \neq 0$ and p is not a unit, so we need to show only that if $p \mid ab$ then $p \mid a$ or $p \mid b$. Suppose $p \mid ab$, so $pr = ab$ for some $r \in R$. Then p occurs in a factorization of the left-hand side into irreducibles, so it must occur in a factorization of a or b into irreducibles (by uniqueness of the factorization of $pr = ab$). $\therefore$ $p \mid a$ or $p \mid b$. (need to handle special cases: r, a or b may be units. Exercise.)

Suppose R is a U.F.D. and every nonzero $r \in R$ can be written $r = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where u is a unit, $p_1, \cdots, p_n$ are irreducibles (or prime), $\alpha_i \in \mathbb{Z}_{>0}$ for all i, and no p_i is an associate of any p_j with $i \neq j$.
Proof: If r is a unit then let $u = r$ and $n = 0$. Otherwise, write $r = p_1 \cdots p_n$ as a product of irreducibles. Then $r = up_1 \cdots p_r$ with $u = 1$. If none of the p_i, p_j are associates with $i \neq j$, then done; otherwise $p_j = p_i \cdot v$ for some unit v; replace p_j with p and n with uv and compine the p_is and (decrease n). Repeat until you're done.
Example:
$-36 = (-2) \cdot 2 \cdot 3 \cdot 3 \setminus = (-2) \cdot 2 \cdot 3^2 \setminus = -1 \cdot 2^2 \cdot 3^2$

Proposition: Let R be a U.F.D., and let $a, b \in R$
We can write $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = vp_1^{\beta_1} \cdots p_n^{\beta_n}$ where u, v are units, $p_1, ldots, p_n$ are irreducibles with no associates, and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}$. (Combine primes in factorizationsof a and b, and include 0 exponents when necessary.) THen $a \mid b \iff \alpha_i \leq \beta_i$ for all i and $\prod p_i^{\min(\alpha_i, \beta_i)}$ is a gcd of a and b. (Just like in $\mathbb{Z}$).
Proof: See the book.

More on Polynomials

Assume for the rest of today's class that R is a commutative ring with $1 \neq 0$ (though most if not all will also be true for the trivial ring (where $1 = 0$)).

Proposition: Let R be as above, and let I be an ideal in R. Then

a. the ideal $IR[x] = (I)$ in $R[x]$ generated by the elements of I equals $\{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x] : a_i \in I \ \forall i\}$ (call this $I[x]$).
b. The natural map $R[x] \to (R/I)[x]$ induces an isomorphism $R[x]/(I) \cong (R/I)[x]$, and

c. If I (ideal in R) is prime, then so is (I) (ideal in $R[x]$).

Proof:

a. Let $f(x) = a_n x^n + \cdots + a_0 \in R[x]$. If $f(x) \in I[x]$ then $a_i \in I$ for all I, and $\therefore f(x) = \sum_{i=0}^{n} a_i \cdot x^i \in IR[x] = (I)$.

   Conversely, if $f(x) \in IR[x]$ then $f(x) = \sum_{j=1}^{m} b_j g_j(x)$ with $b_j \in I$ and $g_j(x) \in R[x]\ \forall j$. Then all coefficients of $b_j g_j(x)$ lie in I, so $b_j g_j(x) \in I[x]\ \forall j$. $\therefore$ so is the sum, which is $f(x)$.

b. Let $\phi : R[x] \to (R/I)[x]$ be the map that applies the natural projection $R \to R/I$ to each coefficient. This is a ring homomorphism, by formals for addition and multiplication in polynomial rings, and the fact that π is a homomorphism. This is onto (because π is onto). Its kernel is $I[x]$. $\therefore$ it gives an isomorphism $R[x]/(I) \xrightarrow{\sim} (R/I)[x]$ by the First Isomorphism Theorem.

c. I is prime in $R \implies R/I$ is an integral domain
   $\implies (R/I)[x]$ is an integral domain
   $\implies R[x]/(I)$ is an integral domain
   $\implies (I) is prime (in R[x])$