Abstract Algebra
Lecture 16
Monday, 12/1/2010

1 Unique Factorization Domains

Recall: Let R be an integral domain. We say $p \in R$ is **prime** if p is not a unit and if $p|ab \to p|a$ or $p|b$. We say p is **irreducible** if p is not a unit and $p = ab$ implies a is a unit or b is a unit.

Recall: A **unique factorization domain** is an integral domain where every non-zero non-unit can be factored uniquely into irreducibles.

Theorem: In a UFD, every irreducible element is prime.

Proof: Let R be a UFD and let $p \in R$ be irreducible. Assume $p|ab$. Since R is a UFD, we can write $ab = q_1^{n_1} \cdots q_k^{n_k}$ for some q_i, irreducible, with $n_i \in \mathbb{N}$. Specifically, $a = q_1^{m_1} \cdots q_k^{m_k}$, and $b = q_1^{j_1} \cdots q_k^{j_k}$ with $m_i + j_i = n_i$. Since $p|ab$, we know that $ab = rp$ for some $r \in R$. Then $r = p_1^{c_1} \cdots p_j^{c_j}$. But by uniqueness, these must be the same as the factorization of ab up to multiplication by units. In particular, $p = uq_i$ for some i and some unit u. That q_i appears with positive exponent in either a or b (or both), so $p|a$ or $p|b$, so p is prime. ∎

Theorem: Every PID is a UFD.

Theorem: Lemma: Let R be a PID. If we have a chain of ideals $a_1 \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$, there exist $N \in \mathbb{Z}$ such that $(a_N) = (a_{N+1}) = \cdots$.

Proof: (of Lemma): Let $(a_1) \subseteq (a_2) \subseteq \cdots$ be a chain of ideals. Let $I = \bigcup_{i \in \mathbb{Z}} (a_i)$. Show I is an ideal. Let $b, c \in I$. Then $b \in (a_j)$ and $c \in (a_k)$. Say $j \leq k$. Then $(a_i) \subseteq (a_k)$. So $b \in (a_k)$, so $b - c \in (a_k) \subseteq I$. I is also clearly absorptive, so I is an ideal. Since R is a PID, we know that $I = (a)$ for some single element $a \in R$. Since $a \in I$, we know $a \in (a_N)$ for some N, and $a \in (a_m)$ for all $m \geq N$. So we have $(a) \subseteq (a_m)$ and $(a_m) \subseteq (a) = I$, so we have $I = (a) = (a_N) = (a_{N+1}) = \cdots$, as desired. ∎

Proof: Let $r \in R$ (a PID) so that $r \neq 0$, r not a unit. First, show r has an irreducible factor. If r is irreducible, then we're done. Otherwise, r factors into non-units $r = r_1 r_1'$. Do the same to r_1. Either it is irreducible, or it factors into $r_1 = r_2 r_2'$, both non-units. Repeat ad nauseum. If this process went on forever, we would have $(r) \subset (r_1) \subset (r_2) \subset \cdots$, which can't happen, so the process must terminate at some point. That is, some r_N is irreducible. So, pick an irreducible factor s_1 of r: $r = s_1 t_1$. Repeat the process on t_1: $r = s_1 s_2 t_2$, etc. If this went on forever, we would have $(r) \subset (t_1) \subset (t_2) \subset \cdots$. This can't happen, so some t_N is irreducible, so $r = s_1 s_2 \cdots s_N t_N$. This factorization is what we want. But we still need to show uniqueness.
Proceed by induction on the number of irreducible factors. For the case $n = 1$, uniqueness is clear. Assume any factorization $r = a_1 \cdots a_n$ into irreducibles is unique. Let $p_1 \cdots p_{n+1} = r = q_1 \cdots q_m$ be two factorizations. Now we have $p_1 | r$, so $p_1 | q_1 \cdots q_m$. In a PID, irreducible implies prime, so $p_1 | q_i$ for some i. Assume $i = 1$. Then $q_1 = p_1 s$, where s must be a unit. So $p_1 \cdots p_{n+1} = s p_1 q_2 \cdots q_m$, or equivalently $p_2 \cdots p_{n+1} = s q_2 \cdots q_m$, so by the inductive hypothesis, $m = n + 1$, and the q_i are equal to the p_i up to multiplication by units. ∎

Theorem: In a UFD, GCDs exist. Moreover, if $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{n_1} \cdots p_k^{n_k}$, then

$$\gcd(a, b) = p_1^{\min\{m_1, n_1\}} \cdots p_k^{\min\{m_k, n_k\}}.$$

Field $\Rightarrow$ Euclidean Domain $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ Integral Domain.