Abstract Algebra
Lecture 15
Wednesday, 10/27/2010

Note: Some people would define Euclidean Domains so that the norm satisfies $N(a) \leq N(ab)$ if $ab \neq 0$ under the usual other constraints: $N : R \to \mathbb{Z}$, $N(0) = 0$, $a = bq + r$, $r = 0$ or $N(r) < N(b)$.

1 Principal Ideal Domains

Theorem: Let R be a PID and $a, b \in R$ are non-zero elements. Let d be a generator of (a, b). Then

i) d is a GCD for a and b.
ii) $d = ax + by$ for some $x, y \in R$.
iii) d is unique up to multiplication by a unit.

Proof:

i) $(d) = (a, b)$, so $d|a$ and $d|b$. If $d'|a$ $d'|b$, then $(a, b) \subseteq (d')$. Thus $(d) \subseteq (d')$, so $d'|d$.

■

Theorem: If R is a PID, then a non-zero ideal I of R is prime if and only if it is maximal.

Proof: The fact that maximal implies prime is always true in commutative rings, and has been previously shown. So we need to show prime $\Rightarrow$ maximal.
Let P be a prime ideal of a PID R. Assume that $P \subset M \subseteq R$ for some ideal M. Since R is a PID, we can write $P = (p)$ and $M = (m)$. We have $(p) \subset (m) \subseteq R$. So we can write $p = mr$ for some $r \in R$. But since P is prime, either m or r is in P. But since $M = (m)$ is strictly larger than P, it can't be that $m \in P$, hence $r \in P$, so $r = ps$ for some $s \in R$. This gives $p = mr = mps$, or that $1 = ms$. Then, since m is a unit, $(m) = R$. Thus P is maximal.

■

Theorem: Assume $R[x]$ is a PID. Then R is a field.

Proof: $R[x]$ has an identity. It must be a constant polynomial 1_R. Note that $R[x]/(x) \cong R$ (we have shown this is a proper isomorphism before). Since $R[x]$ is a PID, we just have to show that (x) is prime. There are no zero-divisors in $R[x]$, so there are no zero-divisors in R. Thus, if two elements of $R[x]$ with non-zero constant term are multiplied, their product must also have non-zero constant term. Thus, no two elements outside of (x) can be multiplied to fall inside (x), so (x) is prime. Thus (x) is maximal, so $R[x]/(x)$ is a field. Alternatively: $R[x]$ has no zero divisors, therefore R has no zero divisors, therefore R is an integral domain, therefore (x) is prime, therefore (x) is maximal, therefore R is a field.

■

2 Factoring in Rings

What are primes in $\mathbb{Z}$? If we write $p = ab$, then a or b is ± 1. Or, if $p|ab$, then either $p|a$ or $p|b$. Note that this second definition is much closer to the ring-theoretic definition of a prime ideal.

Defn: In general commutative rings (actually we're only looking at Integral Domains right now), we say x is **irreducible** if $x = ab$ implies a or b is a unit. We say that x is **prime** if $x|ab$ implies $x|a$ or $x|b$.

Theorem: If $x \in R$ is prime, then x is irreducible.

Proof: Let x be prime, and assume $x = ab$. So $x|ab$, so either $x|a$ or $x|b$. Assume without loss of generality that $x|a$. Then $a = rx$, so we have $x = ab = rxb$, which gives $1 = rb$, so b is a unit. ∎

Ex: Note that irreducible does not necessarily imply prime. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. In this ring, 3 is irreducible but not prime. First, note that our norm is $N(a + b\sqrt{-5}) = a62 + 5b^2$. This does not satisfy the Euclidean algorithm, but it is multiplicative: $N(xy) = N(x)N(y)$. The units in R are those elements that have a norm of 1, namely just ± 1. If $xy = 3$, then $N(x)N(y) = N(3) = 9$. If $N(x) = 1$, it is a unit, so we're done. Can we have $N(x) = N(y) = 3$? But no element of norm 3 can exist due to our definition of a norm. Note also that $3|9$, and $9 = (2 + \sqrt{5})(2 - \sqrt{5})$, but 3 does not divide either of those factors, so 3 is not prime.

Theorem: If R is a PID, then irreducible implies prime.

Proof: Let $x \in R$ be irreducible. We want to show that if $x|ab$, then $x|a$ or $x|b$. In other words, show that (x) is prime, or since R is a PID, show that (x) is maximal. Assume $(x) \subset M \subseteq R$. But $M = (m)$, so $m|x$, or $x = mr$ for some $r \in R$. But since x is irreducible, one of m or r must be a unit. If r is a unit, then x and m are only off by a unit, so $(x) = (m)$, which is false. Thus m must be a unit, so $(m) = M = R$, so (x) is maximal. ∎

Defn: A **unique factorization domain** is an integral domain in which every element x can be written as a product of irreducibles: $x = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ where all a_i are irreducible, all $n_i \in \mathbb{Z}^+$, such that the factorization is unique up to units: if $x = b_1^{m_1} b_2^{m_2} \cdots b_r^{m_r}$ then $k = r$ and there is some reordering of the b_i so that $b_i = u_i a_i$ and $m_i = n_i$ where u_i are units.

Ex: $\mathbb{Z}$, $F[x]$ are unique factorization domains, but $\mathbb{Z}[\sqrt{-5}]$ is not, because $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$.