Abstract Algebra
Lecture 14
Monday, 10/25/2010

1 Euclidean Domains

Euclidean domains are our way of saying "I wish all rings were as pretty as the integers." We abstract certain things that happen in the integers to other rings.

In $\mathbb{Z}$, we have the division algorithm. For any $a, b \in \mathbb{Z}$, $b \neq 0$, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$a = bq + r.$$

We also have the division algorithm in the polynomials. In particular, we can do this in $\mathbb{R}[x]$. For $f, g \in \mathbb{R}[x]$, with $g \neq 0$, there exists $q, r \in \mathbb{R}[x]$ such that

$$f = gq + r$$

and $r = 0$ or $\deg(r) < \deg(g)$.

This allows us to compute GCDs.

Ex: $GCD(48, 18)$:

$$\begin{aligned} 48 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + \boxed{6} \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Defn: Let R be an integral domain. A **norm** N on R is a function $N : R \to \mathbb{Z}_{\geq 0}$ such that $N(0) = 0$.

Defn: R is a **Euclidean Domain** if there is a norm N on R such that For any $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ with $a = bq + r$ and $N(r) < N(b)$ or $r = 0$ (i.e. the division algorithm works).

Ex: Trivially, $\mathbb{Z}$ is a Euclidean domain, with norm $N(a) = |a|$. $\mathbb{R}[x]$ is a Euclidean domain, with norm $N(a) = \deg(a)$. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain with norm $N(a + bi) = |a + bi|^2 = a^2 + b^2$.

Let's show that the division algorithm holds on this norm for the complex numbers. Let $a + bi, c + di \in \mathbb{Z}[i]$, $c + di \neq 0$. We know, in $\mathbb{C}$, that $\frac{a+bi}{c+di} = x + yi$, but x and y are probably not integers. But $x, y \in \mathbb{R}$, so round them to the nearest integers s and t. Then

$(a+bi) = (s+ti)(c+di) + [(x-s)+(y-t)i](c+di)$. Now we need to compute the norm of each of these terms.

$$\begin{aligned} N([(x-s)+(y-t)i](c+di)) &= N((x-s)+(y-t)i)N(c+di) \\ &= [(x-s)^2+(y-t)^2]N(c+di) \\ &\leq [0.5^2+0.5^2]N(c+di) \\ &\leq \frac{1}{2}N(c+di) \\ &< N(c+di) \end{aligned}$$

So we satisfy the requirements of the norm (namely that $N(r) < N(b)$).

Theorem: If R is a Euclidean Domain, then every ideal of R is principal. Specifically, any non-zero $I = (d)$ where d is a non-zero element of smallest possible norm.

Proof: Let I be an ideal in R. Let $d \neq 0$ have smallest possible norm among non-zero elements of I (relying on the well-ordering principle of the integers). Since $d \in I$, clearly $(d) \subseteq I$. To show $I \subseteq (d)$, let $i \in I$. Since R is a Euclidean Domain, we can write $i = qd + r$, where $N(r) < N(d)$. But then $r = i - qd \in I$. But $N(d)$ was minimal among nonzero elements of i, so $r = 0$. Thus $i = qd$, so $i \in (d)$. ∎

Ex: In $\mathbb{Z}$, we have $(18, 48) = (6)$. (Guess what! We denote taking the gcd and taking the ideal the same way. Woooooo this is why this class is called Abstract Algebra.)

Defn: In a commutative ring R, we say $a \mid b$ if $b = ra$ for some $r \in R$.
If $a, b \in R$, a GCD of a and b is an element $d \in R$ such that
i) $d \mid a$ and $d \mid b$
ii) If $d' \mid a$ and $d' \mid b$, then $d' \mid d$.
Or, in terms of ideals,
i) $(a) \subseteq (d)$ and $(b) \subseteq (d)$
ii) If $(a) \subseteq (d')$ and $(b) \subseteq (d')$, then $(d) \subseteq (d')$.
Basically, if $(a, b) = (d)$, then d is a GCD of a and b.

Ex: In $\mathbb{Z}[x]$, the ideal $(2, x)$ is not principal. But $\gcd(2, x) = 1$. This is because $\mathbb{Z}[x]$ is not a Euclidean Domain.

Theorem: Let R be a Euclidean Domain. Let $a, b \in R$, $a, b \neq 0$. Let r_n be the last non-zero remainder obtained from applying the Euclidean algorithm on a and b. Then
i) r_n is a GCD of a and b.
ii) $(a, b) = (r_n)$. In particular, $r_n = ax + by$ for some $x, y \in R$.

Proof:

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + \boxed{r_n} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

so r_n is a GCD of a and b. To show $(r_n) \subseteq (a, b)$, consider that $a, b \in (a, b)$, so $a - b_0 = r_0 \in (a, b)$, so etc. etc. so $r_{n-2}, r_{n-1} \in (a, b)$, so $r_n \in (a, b)$. To show the opposite inclusion, consider that $r_{n-1} \in (r_n)$ since $r_{n-1} = r_n q_{n+2}$, so $r_{n-2} \in (r_n)$, so etc. etc. so $b \in (r_n)$, so $a \in (r_n)$. ∎

Theorem: Let $a, b \in R$ (an integral domain). If d and d' are both GCDs of a and b, then $(d) = (d')$, so $d = ud'$ for some unit $u \in R$.

Proof: d and d' are both common divisors of a and b. So since d is a GCD and d' is a common divisor, we have $(d) \subseteq (d')$, and by the reverse argument $(d') \subseteq (d)$, so $(d) = (d')$. ∎

Defn: a **principal ideal domain** is an integral domain in which every ideal is principal. We proved today that every Euclidean domain is a principal ideal domain (PID). This is better than an integral domain, and almost as good as a Euclidean domain.

Theorem: In a PID, let $(d) = (a, b)$, then d is a GCD of a and b.