LECTURE 22.

ALIREZA SALEHI GOLSEFIDY

1. Recall

Last time we defined a Euclidean Domain and we were proving that every ED is a PID.

2. A Euclidean domain is a PID

Theorem 1. *Every ED is a PID.*

Proof. Let I be a non-zero proper ideal of D. Let $a \in I$ be such that

$$d(a) := \min_{0 \neq x \in I} d(x). \tag{1}$$

We claim that I is generated by a. Assume the contrary. So there is $b \in I$ which is not a multiple of a. Hence by the properties of a ED, there is a non-zero $r \in D$ such that $b = aq + r$ and $d(r) < d(a)$. This implies that $r = b - aq \in I$ which contradicts Equation (1). □

So we have that ED implies PID and PID implies UFD. The converse of neither of these is true.

Example 2 (A UFD which is not PID)**.** *We have seen that $\mathbb{Z}[x]$ is not PID. In fact we proved that $\langle 2, x\rangle$ is not a principal ideal. However one can prove that $\mathbb{Z}[x]$ is a UFD. I will give it as an exercise. It is essentially based on Gauss's Lemma and the fact that a primitive polynomial is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.*

Example 3 (A PID which is not ED)**.** $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ *can be showed to be a PID and not a ED.*

Lemma 4. *Let N be the norm map of $\mathbb{Z}[\sqrt{d}]$. If $N(z) = p$ is prime, then z is irreducible in $\mathbb{Z}[\sqrt{d}]$.*

Proof. If $z = z_1 z_2$, then $p = N(z) = N(z_1)N(z_2)$. Since p is prime and $N(z_1)$ and $N(z_2)$ are non-negative integers, $N(z_i) = 1$ for some i. Hence z_i is unit for some i. Thus z is irreducible. □

Example 5.
1. *In $\mathbb{Z}[i]$, $2 + i$ is irreducible.*
2. *In $\mathbb{Z}[i]$, $3 + 2i$ is irreducible.*
3. *In $\mathbb{Z}[\sqrt{6}]$, $2 + \sqrt{6}$ is irreducible.*
4. *In $\mathbb{Z}[\sqrt{6}]$, $2 + \sqrt{6}$ is irreducible.*

Lemma 6.
1. *There is no $z \in \mathbb{Z}[\sqrt{10}]$ such that $N(z) = 2$.*
2. *There is no $z \in \mathbb{Z}[\sqrt{10}]$ such that $N(z) = 5$.*

Proof. 1. Assume the contrary. So there are $x, y \in \mathbb{Z}$ such that $x^2 - 10y^2 = \pm 2$. Look at both sides modulo 5. So $x^2 \equiv \pm 2 \pmod 5$, which is a contradiction (square of any element in $\mathbb{Z}/5\mathbb{Z}$ is either 0 or ± 1).

2. Assume the contrary. So there are $x, y \in \mathbb{Z}$ such that $x^2 - 10y^2 = 5$. Looking at both sides modulo 5, we can deduce that x is a multiple of 5, i.e. $x = 5x'$. Hence $25x'^2 - 10y^2 = 5$ and so $5x'^2 - 2y^2 = 1$. Again look at both sides modulo 5. So $-2y^2 \equiv 1 \pmod 5$, which is a contradiction. □

Date: 3/9/2012.

Lemma 7. *2, 5 and $\sqrt{10}$ are irreducibles in $\mathbb{Z}[\sqrt{10}]$.*

Proof. If $2 = z_1z_2$, then $4 = N(2) = N(z_1)N(z_2)$. Since by the previous Lemma $N(z_i)$ cannot be equal to 2, one of the norms has to be one and the other one 4, which implies one of them is a unit. So 2 is an irreducible.

If $5 = z_1z_2$, then $25 = N(5) = N(z_1)N(z_2)$. Since by the previous Lemma $N(z_i)$ cannot be equal to 5, one of the norms has to be one and the other one 25, which implies one of them is a unit. So 5 is an irreducible.

If $\sqrt{10} = z_1z_2$, then $10 = N(\sqrt{10}) = N(z_1)N(z_2)$. Since by the previous Lemma $N(z_i)$ cannot be equal to 2, one of the norms has to be one and the other one 10, which implies one of them is a unit. So $\sqrt{10}$ is an irreducible. □

Lemma 8. *In $\mathbb{Z}[\sqrt{d}]$ if a and b are associates, then $N(a) = N(b)$.*

Proof. By the definition, there is a unit u such that $a = ub$. So $N(a) = N(u)N(b) = N(b)$. □

Example 9. *In $\mathbb{Z}[\sqrt{10}]$, 2 and $\sqrt{10}$ are not associates and neither are 5 and $\sqrt{10}$.*

Lemma 10.
(1) *In $\mathbb{Z}[\sqrt{10}]$, 2, 5 and $\sqrt{10}$ are not primes.*
(2) *$\mathbb{Z}[\sqrt{10}]$ is not a UFD.*

Proof.
(1) 2 divides $\sqrt{10} \cdot \sqrt{10}$ but 2 does not divide $\sqrt{10}$. 5 divides $\sqrt{10} \cdot \sqrt{10}$ but it does not divide $\sqrt{10}$. $\sqrt{10}$ divides $2 \cdot 5$ but it does not divide either 2 nor 5.
(2) $2 \cdot 5 = 10 = \sqrt{10} \cdot \sqrt{10}$ by the previous lemmas, these are two different irreducible factorizations of 10.

□

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu