LECTURE 21.

ALIREZA SALEHI GOLSEFIDY

1. Recall

On Monday, we defined a UFD and proved that in a PID any non-zero, non-unit element is a product of irreducibles.

2. PID is UFD

Theorem 1. *Every PID is a UFD.*

Proof. We have already proved the existence. So it is enough to prove the uniqueness. Let a be a non-zero, non-unit element and assume that p_i and q_i are irreducibles such that

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_r = q_1 \cdot q_2 \cdot \cdots \cdot q_s.$$

In a PID, any irreducible is a prime. So p_1 dividing $q_1 \cdot \cdots \cdot q_s$, implies p_1 divides q_{j_1} for some j_1. Since q_{j_1} is irreducible, we have p_1 and q_{j_1} are associates. Now we can cancel them and repeat this argument. $\square$

3. Pell's equation and $\mathbb{Z}[\sqrt{d}]$

Lot's of problems in number theory are naturally connected to ring theory. For instance, Pell's equations: what are the integer solutions of $x^2 - dy^2 = \pm 1$ for a given integer d?

Definition 2. (1) Let $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}^{\geq 0}$ be

$$N(x + \sqrt{d}y) := |x^2 - dy^2|.$$

N is called the norm map.

(2) Let $\tau : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ be

$$\tau(x + \sqrt{d}y) := x - \sqrt{d}y.$$

$\tau(z)$ is called the conjugate of z.

Lemma 3. (1) *τ is a ring isomorphism.*
(2) *$N(z) = |z \cdot \tau(z)|$ for any $z \in \mathbb{Z}[\sqrt{d}]$.*
(3) *$N(zz') = N(z)N(z')$ for any $z, z' \in \mathbb{Z}[\sqrt{d}]$.*

Proof. 1. One can easily check this.

2. Let $z = x + \sqrt{d}y$. So

$$N(z) = N(x + \sqrt{d}y) = |x^2 - dy^2| = |(x + \sqrt{d}y)(x - \sqrt{d}y)| = |z \cdot \tau(z)|.$$

3. $N(zz') = |(zz' \cdot \tau(zz')| = |zz'\tau(z)\tau(z')| = |z\tau(z)||z'\tau(z')| = N(z)N(z').$ $\square$

Theorem 4. $U(\mathbb{Z}[\sqrt{d}]) = \{x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}] |\ x^2 - dy^2 = \pm 1\}$.

Date: 3/7/2012.

Proof. We have to show two directions. First assume that $x^2 - dy^2 = \pm 1$ and we have to prove that $x + \sqrt{d}y$ is a unit in $\mathbb{Z}[\sqrt{d}]$. But it is clear as

$$(x + \sqrt{d}y)(\pm(x - \sqrt{d}y)) = 1,$$

and $\pm(x - \sqrt{d}y) \in \mathbb{Z}[\sqrt{d}]$.

Now we have to show the other direction: if $z = x + \sqrt{d}y$ is a unit in $\mathbb{Z}[\sqrt{d}]$, then $N(z) = |x^2 - dy^2| = 1$.

If z is a unit, then there is $z' \in \mathbb{Z}[\sqrt{d}]$ such that $zz' = 1$. Hence

$$N(zz') = N(1) = 1 \Rightarrow N(z)N(z') = 1.$$

This means the product of two non-negative integers $N(z)$ and $N(z')$ is one. Thus both of them are one. So $N(z) = 1$ and we are done. $\square$

This shows solving Pell's equation is the same as finding units of the ring $\mathbb{Z}[\sqrt{d}]$.

4. How can we check if an integral domain is PID?

So far we know two important PIDs: $\mathbb{Z}$ and $F[x]$, where F is a field. In some sense, we proved both of them in the same way: using "division algorithm". Let's generalize it.

Definition 5. An integral domain D is called a Euclidean Domain (ED) if there is a function $d : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ (sometimes called a measuring function) with the following properties:

(1) $d(ab) \geq d(a)$ for any $a, b \in D \setminus \{0\}$.
(2) For any $a \in D$ and $b \in D \setminus \{0\}$, there are q and r in D such that $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$.

Example 6. $d : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}^{\geq 0}$, $d(n) = |n|$ *satisfies the above properties. And so* $\mathbb{Z}$ *is a ED.*

$d : F[x] \to \mathbb{Z}^{\geq 0}$, $d(f(x)) = \deg(f)$ *satisfies the above properties. And so* $F[x]$ *is a ED.*

Theorem 7. *Every ED is a PID.*

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

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

Claim $I = \langle a \rangle$. If not, there is $b \in I$ which is not a multiple of a. So there is a non-zero r such that $b = aq + r$ and $d(r) < d(a)$. This means $r \in I$, which is a contradiction. $\square$

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

E-mail address: golsefidy@ucsd.edu