Lecture L: Unique factorization domains

TODAY'S GOAL: Study a new class of rings (UFDs) & relate them to the other notions.

§50.1 Definition:

In order to state what U.F.D.'s are, we need some terminology

Definition: Let R be an integral domain

- $a \in R$ is said to be an irreducible element if $a \neq 0$, $a \notin R^\times$ and for any $x, y \in R$ we have: if $a = xy$, then either x or y is a unit in R.
- $a \in R$ is said to be a prime element if $0 \neq (a) \subsetneq R$ is a prime ideal (ie $xy \in (a) \Rightarrow x \in (a)$ or $y \in (a)$)

Lemma: Prime elements in a domain are irreducible.

Proof: Fix $a \in R$ a prime element, so $a \neq 0$, $a \notin R^\times$.

Assume $a = xy$ with $x, y \in R$. Then $xy \in (a) \underset{a \text{ prime}}{\Longrightarrow} x \in (a)$ or $y \in (a)$

Without loss of generality, assume $x \in (a)$, so $\exists\, z \in R$ with $x = az$.

$\Rightarrow$ $a = xy = azy$, ie $a(1 - zy) = 0$

Since R is a domain and $a \neq 0$, we conclude $1 - zy = 0$, ie $y \in R^\times$.

Thus a is irreducible $\square$

Proposition: Let R be a PID, and $a \neq 0$. Then, a is prime if, and only if a is irreducible

Proof: ($\Rightarrow$) Follows from the Lemma

($\Leftarrow$) We assume $a \in R$ is irreducible, so $a \neq 0$ & $a \notin R^\times$. We want to show (a) is prime

We show that (a) is maximal

Pick $I \subseteq R$ ideal with $(a) \subseteq I$. Since R is a PID, then $\exists\, x \in R$ with $I = (x)$

Thus $a \in (x)$, meaning $\exists\, r \in R$ with $a = xr$

Since a is irreducible, we have either $x \in R^\times$ (so $I = R$) or $r \in R^\times$ (so $x = ar^{-1}$, thus $(a) \subseteq (x) \subseteq (a)$, giving $(a) = I$).

We conclude: if I is an ideal with $(a) \subseteq I$, then $I = (a)$ or $I = R$.

This implies (a) is maximal, hence prime. $\square$

<u>Definition:</u> We say a ring R is a <u>unique factorization domain</u> (UFD for short) if for every $n \in R$, $n \neq 0$, $n \notin R^{\times}$ we have

(1) n can be written as a (finite) product of irreducible elements (not necessarily distinct) $p_1, \dots, p_m \in R$: $n = p_1 p_2 \cdots p_m$

(2) if $n = q_1 \cdots q_\ell$ for $q_1, \dots, q_\ell$ irreducible, then $n = \ell$ and, up to permutations, the q_i's are related to p_j's by units of R.

Meaning: $\exists\ \sigma \in S_m$ and units $u_1, \dots, u_m \in R^{\times}$ st $u_i q_i = p_{\sigma(i)}$ $\forall i = 1, \dots, m$

§50.2 Examples:

① $R = \mathbb{Z}$

- Prime elements of R $\longleftrightarrow$ prime numbers
- Irreducible elements of R $\longleftrightarrow$ prime numbers

$\mathbb{Z}$ is a UFD (Fundamental Theorem of Arithmetic) $\mathbb{Z}^{\times} = \{\pm 1\}$

② $R = \mathbb{Z}[\sqrt{-5}]$ is not a PID (Theorem §48.4). Using Proposition §50.1, we can give an alternative proof.

<u>Lemma:</u> $3 \in R = \mathbb{Z}[\sqrt{-5}]$ is irreducible, but not prime

<u>Proof:</u> First, we show 3 is irreducible. Assume $3 = \alpha \cdot \beta$ with $\alpha, \beta \in R$.
Then applying $N(\ ) = |\ |^2$ $(-5<0)$, we get

$$9 = |3|^2 = |\alpha|^2 |\beta|^2 \text{ with } |\alpha|, |\beta| \in \mathbb{Z} \quad (R = \mathcal{O}_{(\sqrt{-5})} \text{ since } -5 \equiv 3 \bmod 4)$$

We get 2 options (1) $|\alpha|^2 = 1$ or $|\beta|^2 = 1$

(2) $|\alpha|^2 = |\beta|^2 = 3$.

By construction $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$ $\Rightarrow$ $|\alpha|^2 = a^2 + 5b^2 \geq 5$ if $b \neq 0$.
In addition, if $b = 0$, we get $|\alpha|^2 = a^2 \neq 3$ since $a \in \mathbb{Z}$.
Thus, option (2) is impossible, ie either $|\alpha|^2 = 1$ (so $\alpha \in R^{\times}$ by Corollary §48.1), or $|\beta|^2 = 1$ (so $\beta \in R^{\times}$)

- Next, we show 3 is not a prime element. Indeed, $(1+\sqrt{-5})(1-\sqrt{-5}) = 1+5 = 6 \in (3)$ but $1 \pm \sqrt{-5} \notin (3)$. Otherwise, $1 \pm \sqrt{-5} \in (3)$ so $\exists\ a, b \in \mathbb{Z}$ with $1 \pm \sqrt{-5} = 3(a + b\sqrt{-5})$.
Thus $1 = 3a$ with $a \in \mathbb{Z}$ Contradiction!

§50.3 Main result:

Theorem: Every PID is a UFD. In particular, every Euclidean domain is a UFD.

In order to prove this statement, we will need the following result

Proposition: In a UFD, a non-zero element is a prime if, and only if, it is irreducible

Proof: ($\Rightarrow$) is true for any domain by Lemma §50.1.

($\Leftarrow$) Let $a \in R$ be an irreducible element and assume $x, y \in R$ with $xy \in (a)$

Thus $\exists\, z \in R$ with $xy = az$

Writing x & y as a product of irreducibles & using the fact that a is irreducible, the uniqueness factorization says a agrees (up to a unit in $R^\times$) with an irreducible of either x or y. Note that we cannot have both $x, y \in R^\times$ since $a \notin R^\times$.

Assume it is x. Thus, we have $x = (ua)\, p_2 \cdots p_n$ with $u \in R^\times$ and $\{p_2, p_3, \ldots, p_n\}$ (a possibly empty) set of irreducibles. Thus $a \mid x$ ie $x \in (a)$ as we wanted.

Proof of Theorem: Since any Euclidean domain is a PID, we need only prove the first part of the statement.

Let $r \in R$ with $r \neq 0$ & $r \notin R^\times$. We want to show existence and uniqueness of the factorization of r.

Existence: We treat 2 cases, depending on whether r is irreducible or not.

CASE 1: If r is irreducible, there is nothing to do

CASE 2: If r is not irreducible, then $\exists\, r_1, r_2 \notin R^\times$ with $r = r_1 r_2$, so $r \in (r_i)$

- If both these elements are irreducible, there is nothing to do
- Otherwise, one of them is reducible, say r_1. We have $r_1 \notin (r)$ because $r_2 \notin R^\times$.

Then $\exists\, r_{11}, r_{12} \notin R^\times$ with $r_1 = r_{11} r_{12}$

We can continue in this way to produce an ascending chain of ideals

$$\underset{I_1}{\underset{\parallel}{(r)}} \subsetneq \underset{I_2}{\underset{\parallel}{(r_1)}} \subsetneq \underset{I_3}{\underset{\parallel}{(r_{11})}} \subsetneq \cdots \subseteq R \qquad (*)$$

Take $J := \bigcup_{k \geq 1} I_k$. This is an ideal of R. Since R is a PID, we know $\exists\, a \in R$ with $J = (a)$. Let $n \in \mathbb{N}$ with $a \in I_n \Rightarrow J \subseteq I_n$

Then $I_n \subseteq I_{n+s} \subseteq J \subseteq I_n \Rightarrow I_n = I_{n+1} = I_{n+2} = \cdots = (a)$

This shows the chain (*) is stationary, so at some point the construction of irreducible factors of r stops.

Uniqueness: We proceed by induction on the number of irreducible factors of some factorization of r.

Base case: $n=0$, then $r \in R^\times$. If $r = qc$ for some other factorization with q irred, then q divides the unit r, meaning q is also a unit. Contr!

Inductive Step: Assume $n \geq 1$ & r has 2 factorizations

$$r = p_1 \cdots p_n = q_1 q_2 \cdots q_m \qquad (*)$$

with $m \geq n$. Since p_1 is irreducible, Proposition implies it is prime.

Then, since $p_1 \mid (q_1 \cdots q_m)$ we can find $j \in \{1, \ldots, m\}$ with $p_1 \mid q_j$.

After reshuffling, we may assume $j=1$. Then, $q_1 = p_1 u$ with $u \in R$.

Since q_1 is irreducible & $p_1 \notin R^\times$, we conclude that $u \in R^\times$. Thus, p_1 & q_1 are associates. Thus (*) becomes $p_1 p_2 \cdots p_n = u p_1 q_2 \cdots q_m$

Cancelling p_1 from both sides, we conclude that $s = p_2 \cdots p_n = (uq_2) q_3 \cdots q_m$ has 2 factorizations with $n-1 \leq m-1$ irreducibles ((uq_2) is irreducible), the (IH) ensures $n-1 = m-1$ & $\exists\, \sigma \in S_{n-1}$ and $u_2, \ldots, u_n \in R^\times$ such that $u_i q_i = p_{\sigma(i)}$ for all $i = 2, \ldots, m$. Combining this with $u_1 = u$ & $\sigma(1) = 1$, the statement follows. $\square$

Corollary 1 (Fundamental Theorem of Arithmetic) $\mathbb{Z}$ is a UFD.

Corollary 2: For every field K, $K[x]$ is a UFD.

Corollary 3: $\mathbb{Z}[i]$ is a UFD

(If you are curious about what do factorizations in $\mathbb{Z}[i]$ look like, you can look at Section §8.3 in the textbook)

Some comments:

(1) For the proof of the Theorem, we didn't need to invoke the Lemma since we know that on a PID every irreducible element is automatically prime.

(2) We used the PID to show the existence of a factorization but we didn't need the PID condition for the proof of uniqueness. Uniqueness did use that irreducible elements are prime.

(3) As a consequence of this, our proof applies to more general cases. More precisely

Corollary 4: Assume R is a domain satisfying

(1) every $a \in R$, $a \neq 0$, $a \notin R^\times$ admits a factorization as a finite product of irreducible elements

(2) every irreducible element of R is prime.

Then, R is a UFD