MATH 403/503 L26

Thm Every PID is a UFD.

Proof Existence of factorization: Let D be a PID and $a \in D$ be a nonzero nonunit. If a is irreducible, we are done. Otherwise, $a = a_1 b_1$ where neither a_1 nor b_1 is a unit. Then $(a) \subsetneq (a_1)$.

Suppose $a_1 = a_2 b_2$ where neither a_2 nor b_2 is a unit. As before, $(a_1) \subsetneq (a_2)$. Continuing this way we get

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_N)$$

By Lemma, this cannot continue forever. So eventually we come to an element a_N which cannot be factored into non-units. That is, a_N is irreducible.

Thus:

$$a = a_1 b_1 = a_2 b_2 b_1 = \cdots = a_{N-1} b_{N-1} \cdots b_2 b_1$$
$$= a_N (b_N \cdots b_2 b_1)$$

We have shown that every non-unit $a \neq 0$ is divisible by an irreducible element.

Now suppose $a = p_1 c_1$, where p_1 is irreducible. If c_1 is a nonunit we have $c_1 = p_2 c_2$ for some irreducible $p_2 \in D$.

Repeating this we get

$$(a) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_r)$$

Eventually we find $c_{r-1} = p_{r-1} c_r$ where c_r is also irreducible. Put $p_r = c_r$. Then:

$$a = p_1 p_2 \cdots p_r, \quad p_i \text{ irreducible.}$$

Uniqueness of factorization: Suppose

$$a = p_1 \cdots p_r = q_1 \cdots q_s \qquad p_i, q_j \text{ irr.}$$

WLOG $r \le s$. Then, since p_1 is irr and D is a PID, p_1 is prime (by a Corollary last time). Since $p_1 | a$ we get $p_1 | q_j$, for some j. After relabeling WLOG $p_1 | q_1$. So $p_1 u_1 = q_1$ for some $u_1 \in D$, which must be a unit since q_1 is irreducible.

$$a = p_1 p_2 \cdots p_r = u_1 p_1 q_2 q_3 \cdots q_s$$

$$\Rightarrow \quad p_2 \cdots p_r = (u_1 q_2) q_3 \cdots q_s$$

Continuing in this way we can relabel the q_j's so that $q_2 = u_2 p_2$, ..., $q_r = u_r p_r$. This gives

$$p_1 \cdots p_r = u_1 \cdots u_r \, p_1 \cdots p_r \, q_{r+1} \cdots q_s$$

$$\Rightarrow u_1 \cdots u_r \, q_{r+1} \cdots q_s = 1$$

If $s > r$ we get that q_{r+1} is a unit contradicting that q_{r+1} is irreducible.

So $s = r$ and $q_i = u_i p_i \quad \forall i = 1, \ldots, r$ ∎

Corollary Let F be a field. Then $F[x]$ is a UFD. (Recall that $F[x]$ is a PID.)

Euclidean Domains.

Idea: The division algorithm(s) in $\mathbb{Z}$ and in $F[x]$, are very useful. Let's axiomatize it.

Def Let D be an integral domain.

(i) A **Euclidean valuation** $v : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ is a function such that

1) For any nonzero $a, b \in D$:
$$v(a) \leq v(ab).$$

2) Let $a, b \in D$, $b \neq 0$. Then there exist $q, r \in D$ such that
$$a = bq + r$$
and $v(r) < v(b)$ when $r \neq 0$.

(ii) D is a **Euclidean domain** if there exists a Euclidean valuation on D.

Example On $\mathbb{Z}$, define $v(a) = |a|$ for all $a \neq 0$. Then v is a Euclidean valuation on $\mathbb{Z}$. So $\mathbb{Z}$ is a Euclidean domain.

Example. On $F[x]$, define

$$v(p(x)) = \deg p(x)$$

for all nonzero $p(x) \in F[x]$. Then v is a Euclidean valuation, so $F[x]$ is a Euclidean domain.

Example The Gaussian integers

$$\mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

has a Euclidean valuation

$$v(a+bi) = a^2 + b^2$$

(This requires proof, see Example 18.20 in Judson.)

So $\mathbb{Z}[i]$ is a Euclidean domain.

ED := Euclidean domain.

Theorem Every ED is a PID.

Proof Let D be a ED. Let $I \subseteq D$ be an ideal. If $I = \{0\}$ then $I = (0)$ which is principal. Otherwise, let $a \in I \setminus \{0\}$ with minimal $v(a)$. (Here v is any Euclidean valuation on D that we fix.) Let $x \in I$. By property of v,

$$x = aq + r$$

for some q, r and $v(r) < v(a)$ when $r \neq 0$. But $r = \underbrace{x}_{\in I} - \underbrace{aq}_{\in I} \in I$.

So $v(r) < v(a)$ is not possible by minimality of $v(a)$. Therefore $r = 0$. So $x \in (a)$. Since x was arbitrary, $I \subseteq (a)$, but $(a) \subseteq I$ too so $I = (a)$. Thus I is principal. So D is a PID. ∎

We have shown:

$$ED \Longrightarrow PID \Longrightarrow UFD \Longrightarrow ID$$

The converse of each implication is false:

1) We saw $\mathbb{Z}[\sqrt{-3}]$ is an ID which is not a UFD.

2) Next time we'll show $\mathbb{Z}[x]$ is a UFD. We have seen $\mathbb{Z}[x]$ is not a PID.

3) It can be shown that

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

is a PID which is not a ED but it's not easy.