Unique Factorization in Principal Ideal Domains

Due to time constraints from the snow day, I omitted the full details proving the following theorem, and will not base any exam problems on the proof. However, I'm providing here a proof, for your own interest (it may also be useful review of the concepts involved). I've aimed to streamline the book's proof which moves more on the way (but is much longer).

Thm If a ring D is a PID, then it is a UFD.

The theorem follows readily from the following three lemmas.

Lemma 1 If D is a PID & $p \in D$, then

$$p \text{ is prime iff } p \text{ is irreducible.}$$

Lemma 2 (irreducible factorization exists)

If D is a PID, ~~&~~ and $a \in D$ is nonzero & not a unit, then $\exists$ irreducible elements $q_1, \cdots, q_m \in D$ st. $a = q_1 q_2 \cdots q_m$.

Lemma 3 (prime factorization is unique)

If $p_1, \cdots, p_\ell \in D$ are prime, $q_1, \cdots, q_m$ are irreducible, w/ $p_1 \cdots p_\ell = q_1 \cdots q_m$ and D is an integral domain (eg. a PID), then $\ell = m$ & after reordering the q's if necessary, p_i & q_i are associates for $i = 1, 2, \cdots, \ell$.

(since this is true of irred. & primes by def'n)

Proof of lemma 1 (we did essentially all of this in class)

We'll prove a cycle of implications. Assuming $a \in D$ is nonzero throughout:

comment: only implication ④ requires D to be a PID. Implication ③ does require D to be an integral domain

$$\begin{array}{ccccl} a \text{ is irred.} & \overset{③}{\Longleftarrow} & a \text{ is prime} & \Big\} & \text{"element" point of view} \\ ④\Downarrow & & \Uparrow ② & & \\ \langle a \rangle \text{ is maximal} & \overset{①}{\Longrightarrow} & \langle a \rangle \text{ is prime} & \Big\} & \text{"ideal" point of view} \end{array}$$

① $\langle a \rangle$ maximal $\Rightarrow$ $\langle a \rangle$ prime.

If $\langle a \rangle$ is maximal, then $D/\langle a \rangle$ is a field (proved in class: I max'l $\Leftrightarrow$ D/I field)

so $D/\langle a \rangle$ is an integral domain, so $\langle a \rangle$ is prime. (I prime $\Leftrightarrow$ D/I is ID)

② $\langle a \rangle$ prime $\Rightarrow$ a is prime element.

$a \neq 0_D$ since we're assuming this throughout.

$a \notin D^\times$ since otherwise $1 = a \cdot a^{-1} \in \langle a \rangle$ & $\forall r \in R$, $r \cdot 1 \in \langle a \rangle$ (sticky property), but $\langle a \rangle \neq R$ (part of def'n of "prime ideal").

If $a | bc$, then $bc \in \langle a \rangle$. Since $\langle a \rangle$ is prime, either $b \in \langle a \rangle$ or $c \in \langle a \rangle$, ie. either $a|b$ or $a|c$.

So a is a prime element.

③ a is prime element $\Rightarrow$ a is irred. element.

Suppose a is prime and $a = bc$. Then $a | bc$, so either $a|b$ or $a|c$.

If $a|b$, then $\exists q \in D$ st $b = aq$, so $a = aqc$. Since $a \neq 0_D$ & D has no zero-divisors, cancellation applies: $1 = cq$. So c is a unit.

Similarly (exchange b&c above), if $a|c$ then b is a unit.

So either b or c is a unit.

Since $a \neq 0_D$ & $a \notin D^\times$, a is an irreducible element.

//pf. of lemma 1, cont.

(4) a is irred. element $\Rightarrow$ $\langle a \rangle$ is maximal. (also proved on PSet 11)

Suppose a is irreducible. Since $a \notin D^\times$ (part of def'n of "irreducible"), $a \nmid 1_D$ so $1_D \notin \langle a \rangle$ & $\langle a \rangle \neq R$. It remains to show that any ideal J w/ $\langle a \rangle \subseteq J \subseteq R$ is either $\langle a \rangle$ or R.

Suppose that $\langle a \rangle \subseteq J \subseteq R$, Since D is a PID, $\exists b$ s.t. $J = \langle b \rangle$.

Then $a \in \langle a \rangle \subseteq \langle b \rangle$, so $b | a$, ie. $\exists c$ s.t. $a = bc$.
Since a is irred., either $b \in D^\times$ or $c \in D^\times$.

Case 1: $b \in D^\times$. Then $\forall r \in R$, $r = b(b^{-1} \cdot r) \in \langle b \rangle$,
so $\underline{\langle b \rangle = R}$ in this case.

Case 2: $c \in D^\times$. Then $b = c^{-1} a \in \langle a \rangle$ (sticky prop.)
so $\forall$ element rb of $\langle b \rangle$, $rb = rc^{-1} a \in \langle a \rangle$.
So $\langle b \rangle \subseteq \langle a \rangle$ & $\langle a \rangle \subseteq \langle b \rangle$, hence $\underline{\langle b \rangle = \langle a \rangle}$.

So indeed $\langle a \rangle$ is a maximal ideal.

Proof of lemma 2 (done in §18.2 of the text)

Fix $a \in D$ nonzero & non-unit.

$\lightning$ Suppose a cannot factor into irreducibles.

Then it is not irred itself, so

$$a = bc$$

for some two elements b, c, both nonunits.

At least one of b, c cannot be factored into irreducibles, otherwise a could be. WLOG c cannot be factored into irreducibles.

Iterating this argument, we see that ~~$\forall n$, $\exists$ nonunits~~ we can find a sequence of factorizations as follows:

$$\begin{aligned} a &= b_1 c_1 \\ &= b_1 b_2 c_2 \\ &= b_1 b_2 b_3 c_3 \\ &\cdots \\ &= b_1 b_2 \cdots b_n c_n \\ &\cdots \end{aligned}$$

where all b_i & c_i are non-units. & $c_n = b_{n+1} c_{n+1}$ $\forall n \geq 1$.

Observe that $c_n | c_{n-1} | c_{n-2} | \cdots | c_1$, so we have a chain of ideals:

$$\langle c_1 \rangle \subseteq \langle c_2 \rangle \subseteq \cdots \subseteq \langle c_n \rangle \subseteq \cdots.$$

Let $I = \{ r \in D : r \in \langle c_n \rangle \text{ for some } n \}$.

I is an ideal: It's nonempty ($0 \in \langle c_n \rangle$ $\forall n$), closed under subtraction since $r_1 \in \langle c_n \rangle$, $r_2 \in \langle c_m \rangle \Rightarrow r_1, r_2$ are both in $\langle c_N \rangle$ where N = maximum of m & n. so $r_1 - r_2 \in \langle c_N \rangle \Rightarrow r_1 - r_2 \in I$,

// proof of lemma 2, cont.

and sticky since $a \in I \Rightarrow a \in \langle c_n \rangle$ for some n,

$\Rightarrow \forall r \in D$, $ar \in \langle c_n \rangle$ & thus $ar \in I$.

Since D is a PID, $\exists d$ s.t. $I = \langle d \rangle$. Then $d \in I$,

so $\exists n$ s.t. $d \in \langle c_n \rangle$. This means that

$$\langle d \rangle \subseteq \langle c_n \rangle \subseteq \langle c_{n+1} \rangle \subseteq \langle d \rangle,$$

so in fact $\langle c_n \rangle = \langle c_{n+1} \rangle = \langle d \rangle$.

This implies that $c_{n+1} \in \langle c_n \rangle$, so $\exists q \in D$ s.t.

$$c_{n+1} = q c_n \quad \& \quad c_n = c_{n+1} b_{n+1},$$

hence

$$c_n = c_n \cdot q b_{n+1}$$

$\Rightarrow$ since $c_n \neq 0_D$ & D is a PID, cancellation applies,

so $1 = q b_{n+1}$

$\Rightarrow$ b_{n+1} is a unit. $\lightning$

This contradiction shows that a must factor into irreducibles after all.

Proof of lemma 3 We'll prove a slightly stronger fact: if $p_1 p_2 \cdots p_\ell = u q_1 \cdots q_m$, where u is a unit in D, then the same conclusion holds.

By induction on ℓ.

Base case: $\ell = 1$

Suppose $p_1 = u q_1 \cdots q_m$. Then $p_1 \mid u q_1 \cdots q_m$,

so either $p_1 \mid \cancel{q_1}^{u}$ or $p_1 \mid q_1 q_2 \cdots q_m$

$\Rightarrow$ either $p_1 \mid \cancel{q_1}^{u}$ or $p_1 \mid \cancel{q_2}^{q_1}$ or $p_1 \mid q_2 \cdots q_m$

$\Rightarrow \cdots \Rightarrow$ either $p_1 \mid \cancel{q_1}^{u}$ or $p_1 \mid \cancel{q_2}^{q_1}$ or $\cdots$ or $p_1 \mid \cancel{q_m}^{q_m}$.

So $p_1 \mid q_i$ for some i. Reordering the q's, we may assume $p_1 \mid q_1$. So $q_1 = p_1 \cdot b$ for some $b \in D$.

since $p_1 \mid u$ is impossible (it would imply $p_1 \mid 1_D$, but $p_1 \notin D^\times$)

~~By lemma~~

So $q_1 \mid p_1 b$, hence either $q_1 \mid p_1$ or $q_1 \mid b$.

If $q_1 \mid p_1$ then $p_1 = q_1 c$ for some $c \in D$, & thus

$p_1 = p_1 bc \Rightarrow 1 = bc$ (cancellation valid since D is an ID & $p_1 \neq 0$, so p_1 isn't a zero-divisor)

so b is a unit w/ $q_1 = p_1 b$, so p_1 & q_1 are associates.

Then $p_1 = (ub) p_1 q_2 \cdots q_m$

$\Rightarrow 1_D = (ub) q_2 \cdots q_m$

& thus $q_2, \cdots, q_m$ are units. This is impossible unless $m = 1$. So we're done in this case.

If $q_1 \mid b$ then $b = q_1 c$ for some $c \in D$, so

$q_1 = q_1 p_1 c \Rightarrow 1 = \cancel{bc}^{p_1 c}$ (q_1 not zero or zero-divisor)

$\Rightarrow p_1$ is a unit. This is impossible,

so this case never occurs.

That establishes the base case.

//pf of lemma 3, cont.

Inductive step. Suppose the ~~lemma~~ stronger claim holds for equations of the form

$$p_1 \cdots p_{\ell-1} = u q_1 \cdots q_m.$$

Now suppose

$$p_1 \cdots p_\ell = u q_1 \cdots q_m.$$

Then $\underline{p_1 \mid u q_1 \cdots q_m}$. Repeating the argument in the base case word-for-word shows that

$$p_1 \mid q_i \quad \text{for some } i, \text{ w/ } q_i = p_1 b \text{ for some unit } b,$$

so upon reordering to place q_i first,

$$q_1 = b p_1$$

$$\& \quad p_1 p_2 \cdots p_\ell = (ub) p_1 q_2 \cdots q_m.$$

Since $p_1 \neq 0_D$ in an integral domain, cancellation applies:

$$p_2 p_3 \cdots p_\ell = (ub) q_2 \cdots q_m$$

w/ $ub \in D^\times$. By inductive hypothesis, $\ell - 1 = m - 1$ & after reordering p_2 & q_2 are assocs, & $\cdots$ & p_ℓ & q_ℓ are assocs.

Hence $\ell = m$ & p_i & q_i are associates for $i = 1, \cdots, \ell$,

This completes the induction.