Definition 18.1 (Associates, Irreducibles, Primes)**.** *Let $a\ b \in D$ where D is an integral domain, a and b are called associates if $a = ub$ where u is a unit of D. If a is non-zero and not a unit, and whenever $a = bc$ for some $b\ c \in D$ implies b or c is a unit, then a is called irreducible. If a is non-zero and not a unit, and $a \mid bc$ implies $a \mid b$ or $a \mid c$, then a is called a prime.*

Theorem 18.1. *In an integral domain, every prime is an irreducible.*

Proof. Let D an integral domain and $p \in D$ a prime. Suppose $p = ab$ for some $a\ b \in D$, then $p \mid ab$ since $p = 1ab$, which implies $p \mid a$ or $p \mid b$, we may suppose $p \mid a$. Then $a = pc$ for some $c \in D$, therefore $p = pcb$. By cancellation (since we are in an integral domain) we know $1 = cb$, therefore b is a unit and $b^{-1} = c$. □

Theorem 18.2. *In a principal ideal domain, an element is irreducible iff it is a prime.*

Proof. Since a principal ideal domain is an integral domain, ($\Leftarrow$) is trivial.

($\Rightarrow$) Let P a principal ideal domain and $p \in P$, and suppose $I = \langle q \rangle$ an ideal (we know it has form $\langle q \rangle$ since we are in a principal ideal domain) such that $\langle p \rangle \subseteq \langle q \rangle$. Since $p \in \langle q \rangle$, we know $p = qr$ for some $r \in P$, according to p is irreducible, we know either q or r is unit. If q is unit, then $\langle q \rangle = P$. If r is unit, then $q = pr^{-1}$, therefore $q \in \langle p \rangle$ and $\langle p \rangle = \langle q \rangle$. This shows that $\langle p \rangle$ is a maximal ideal, therefore it is a prime ideal, and $\langle p \rangle$ is prime ideal implies p is prime. □

Lemma 18.1. *In a principal ideal domain, any strictly increasing chain of ideals $I_0 \subset I_1 \subset \ldots$ must be finite.*

Proof. This proof comes from textbook.

Let D be that principal ideal domain and $I = I_0 \cup I_1 \cup \ldots$, for any element $i \in I$ and $a \in D$, i must be an element of an ideal in the chain, say I_i, then $ia \in I_i \subseteq I$. Therefore I is an ideal.

then $I = \langle a \rangle$, and a must belongs to an ideal in the chain, say I_n. For any ideal I_m in the chain, we have $I_m \subseteq I_n$ since a divides the "generator" of I_m. Therefore I_n is the last member of the chain. □

Definition 18.2 (Unique Factorization Domain)**.** *An integral domain D is a unique factorization domain if:*

1. *Every non-zero element of D that is not a unit can be written as a product of irreducibles of D.*

2. *The factorization into irreducibles is unique up to* ***associates and the order of the factors****.*

Therefore, the factorization $4 = 2 \times 2 = (-2) \times (-2)$ is considered "the same", cause 2 is associated with -2 by $2 = (-1)2$ (or $\langle 2 \rangle = \langle -2 \rangle$).

Theorem 18.3 (PID implies UFD)**.** *Every pincipal ideal domain is a unique factorization domain.*

Proof. Let D a principal ideal domain and $a \in D$ a non-zero, non-unit element.

We first show that for any reducible, there is an irreducible divides it. Suppose $a \in D$ is reducible, then $a = bc$ where $b\ c \in D$ are non-zero and non-unit. If b or c is irreducible, then trivial. If both b and c are reducible, then $\langle a \rangle \subset \langle b \rangle$, it is trivial that $\langle a \rangle \subseteq \langle b \rangle$, if $b \in \langle a \rangle$, then $b = ad$, which means $a = bc \to a = adc$, which implies c is a unit but it isn't. Then we perform this algorithm on b, and we have a strictly increasing chain of ideals $\langle a \rangle \subset \langle b \rangle \subset \dots$. According to the Lemma 18.1, we know the chain is finite, therefore the algorithm must stop at some point. We found that the algorithm only stops when it meets an irreducible, therefore there is a irreducible divides a.

We repeat applying this algorithm to the factor of a, the factor of the factor of a and so on, then we have a series $a = p_0 p_1 p_2 \dots$ where p_i are irreducibles. If this series is infinite, then $b = p_1 p_2 \cdots$ and $\langle a \rangle \subset \langle b \rangle$ (properly containing by p_0 is not a unit). Therefore, we have a infinite strictly increasing chain $\langle p_0 p_1 p_2 \dots \rangle \subset \langle p_1 p_2 p_3 \dots \rangle \subset \dots$ which is impossible. Therefore $a = p_0 p_1 \cdots p_n$ where p_i are irreducibles.

If $a = p_0 p_1 \cdots p_n = q_0 q_1 \cdots q_m$, we induction on n:

- Base: If $a = p_0 = q_0 q_1 \cdots q_m$, then p_0 must divides some q_i. Since q_i is irreducible, we know p_0 and q_i are associates. Then the product of the remaining irreducibles are a unit by cancellation, which only makes sense when there is no remaining irreducibles. Therefore $0 = m$.

- Induction: If $a = p_0 p_1 \cdots p_n = q_0 q_1 \cdots q_m$, then p_0 must divides some q_i and they are associates, that is, $cp_0 = q_i$, we may suppose $i = 1$ since an integral domain is commutative, then by cancellation, we have $(cp_1)p_2 \cdots p_n = q_1 q_2 \cdots p_m$. By induction hypothesis, we know $n = m$, and they are unique up to associates.

□

Definition 18.3 (Euclidean Domain)**.** *An integral domain D is called a Euclidean domain if there is a function $d : D^* \to \mathbb{N}$ (called measure) where D^* is D without 0, such that:*

1. *$d(a) \leq d(ab)$ for all non-zero a $b \in D$.*
2. *For any a $b \in D$ and $b \neq 0$, then a can be written in the form of $a = bq+r$ where q $r \in D$ and either $r = 0$ or $d(r) < d(b)$.*

Example. *The ring $\mathbb{Z}$ is an Euclidean domain with $d(a) = |a|$.*

Example. *For any field F, $F[x]$ is an Euclidean domain with $d = \deg$*

Theorem 18.4. *Every Euclidean domain is a principal integral domain.*

Proof. Let D an Euclidean domain and I a non-zero ideal of D. Let $b \in I$ with $d(b)$ is minimal, we claim $I = \langle b \rangle$. For any element a in I, a can be written in the form of $a = bq + r$, if $r = 0$, then $a \in \langle b \rangle$; if $r \neq 0$, then $d(r) < d(b)$, since $r \in I$ (cause a $b \in I$ and I is an ideal), it contradicts the assumption that $d(b)$ is minimal. □