Some properties of $\mathbb{Z}$

Recall.

1. Every ideal in $\mathbb{Z}$ is a principal ideal.

2. Unique factorization theorem (Fundamental theorem of arithmetic). For an integer $n$ with $n > 1$, then

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$$

for some distinct prime numbers $p_1, p_2, \ldots p_r$, and some $e_i \in \mathbb{Z}_{>0}$.

3. Division algorithm. Let $a$ and $b$ be two integers with $b \neq 0$. Then there exist two integers $q$ and $r$ such that

3.1 $a = bq + r$, and
3.2 either $r = 0$ or $|r| < |b|$. 
Some properties of $\mathbf{F}[x]$ with $\mathbf{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Recall. Let $\mathbf{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

1. **Division algorithm.** Let $f(x)$ and $g(x) \in \mathbf{F}[x]$. Suppose that $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that
   1.1 $f(x) = g(x)q(x) + r(x),$
   1.2 $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

2. Every ideal in $\mathbf{F}[x]$ is a principal ideal.

3. **Unique factorization.** Every polynomial in $\mathbf{F}[x]$ can be uniquely represented as a product of irreducible polynomials, up to scalar multiples and the order of factors.
Euclidean Domain

**Definition.** A Euclidean norm on an integral domain $D$ is a function $N : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist $q$ and $r$ in $D$ such that
   1.1 $a = bq + r$, and
   1.2 either $r = 0$ or $N(r) < N(b)$.

2. For all $a, b \in D$, where neither $a$ nor $b$ is 0, $N(a) \leq N(ab)$.

An integral domain $D$ is a Euclidean domain (or possess a Division Algorithm) if there exists a Euclidean norm on $D$. 
Examples

1. Define \( N : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \) by \( N(n) = |n| \). Then \( N \) is a Euclidean norm.

2. Let \( F \) be a field. Define \( N : F[x] - \{0\} \to \mathbb{Z}_{\geq 0} \) by \( N(f(x)) = \deg f(x) \). Then \( N \) is a Euclidean norm.

3. Consider the set of all Gaussian integers,

\[ \mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}. \]

Define the norm \( N(a + bi) \) to be

\[ N(a + bi) = a^2 + b^2. \]

Then \( N \) is a Euclidean norm.
$\mathbb{Z}[i]$ is a Euclidean domain

**Lemma**

*For all $\alpha, \beta \in \mathbb{Z}[i]$, we have*

1. $N(\alpha) \geq 0$,
2. $N(\alpha) = 0$ if and only if $\alpha = 0$,
3. $N(\alpha \beta) = N(\alpha)N(\beta)$.

**Theorem**

1. $\mathbb{Z}[i]$ is an integral domain.
2. *The function $N$ given by $N(a + bi) = a^2 + b^2$ is a Euclidean norm on $\mathbb{Z}[i]$.*
Example
Let $\alpha = 7 + 13i$ and $\beta = 5 + 3i$. Find $q, r \in \mathbb{Z}[i]$.

Solution. We have

$$\frac{\alpha}{\beta} = \frac{(7 + 13i)(5 - 3i)}{(5 + 3i)(5 - 3i)} = \frac{74 + 44i}{34} = \frac{37 + 22i}{17}$$

The closest integer to $37/17$ is 2, while that to $22/17$ is 1. Thus, set $q = 2 + i$. Then we have

$$r = \alpha - \beta q = (7 + 13i) - (5 + 3i)(2 + i) = 2i.$$  \[\square\]
Proposition. Let $D$ be a Euclidean domain with Euclidean norm $N$. Then

1. $N(1)$ is minimal among all $N(a)$ for nonzero $a \in D$.
2. $u \in D$ is a unit if and only if $N(u) = N(1)$.

Example
The units of $\mathbb{Z}[i]$ are $\pm 1$, and $\pm i$. 
Proposition. Every ideal in a Euclidean Domain is principal.

Ideas.

1. Given an ideal $I$, if $I = \{0\}$, then $I = \langle 0 \rangle$.
2. If $I \neq \{0\}$, let $b$ be an element of $I$ of minimal norm. We claim that $I = \langle b \rangle$.
3. Given $a \in I$, there exist $q$ and $r$ in $D$ such that

$$a = bq + r$$

with $r = 0$ or $N(r) < N(b)$.
4. The possibility $N(r) < N(b)$ can not occur. Thus $a = bq \in \langle b \rangle$. 
**Principal ideal domains (PID)**

**Definition.** An integral domain $D$ is a **principal ideal domain (PID)** if every ideal in $D$ is principal.

**Example**

1. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PIDs.
2. If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a PID.

**Proposition.** Every nonzero prime ideal in a PID is a maximal ideal.
Greatest common divisor

Definition. Let $R$ be a commutative ring and $a, b \in R$ with $b \neq 0$.

- We say that $b$ divides $a$ if $a = bx$ for some $x \in R$. (Notation: $b \mid a$)
- A common divisor $d$ of $a$ and $b$ is a greatest common divisor of $a$ and $b$ if every common divisor of $a$ and $b$ divides $d$. (Notation: $d = \gcd(a, b)$)

Remark

GCD’s may not exist in general. For example, in $\mathbb{Z}[\sqrt{-3}]$, we have

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Thus, $1 + \sqrt{-3}$ and 2 both divide 4 and $2(1 + \sqrt{-3})$. However, there is no divisor of 4 and $2(1 + \sqrt{-3})$ that is divisible by both 2 and $1 + \sqrt{-3}$. 
Proposition. Let $D$ be a PID. For any nonzero $d, d'$, we have

1. $\langle d \rangle = \langle d' \rangle$ if and only if $d' = ud$ for some unit $u \in D$.
2. if $d$ and $d'$ are both GCDs of $a$ and $b$, then $d' = ud$ for some unit $u \in D$.
3. if $d$ is a GCD of $a$ and $b$, then there exists $x, y$ in $D$ such that $d = ax + by$.

Definition. Let $R$ be a commutative ring with unity. Let $a, b \in R$. $a$ and $b$ are associates if $a = ub$ for some unit $u \in R$. 
Euclidean algorithm

**Theorem**

Let $D$ be a Euclidean domain, and $a$ and $b$ be two elements of $D$.

1. Then a GCD of $a$ and $b$ can be obtained by the Euclidean algorithm.
2. $\langle a \rangle + \langle b \rangle = \langle \gcd(a, b) \rangle$.

**Remark**

In a Euclidean domain, $d$ is a GCD of $a$ and $b$ if and only if $d$ has the largest Euclidean norm among all common divisors of $a$ and $b$. 
Key ideas.

1. Assume $b \neq 0$. Consider the Euclidean algorithm

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$\vdots$$
$$r_{n-1} = r_nq_{n+1} + 0.$$  

(The process must stop because $N(r_1), N(r_2), \cdots$ is a series of strictly decreasing nonnegative integers.)

2. The element $r_n$ is a GCD of $a$ and $b$. 
Example
Find the GCD of $a = 19 + 33i$ and $b = 11 + 27i$.

1. We have $a/b = (22 - 3i)/17$. Thus, choose $q_1 = 1$ and $r_1 = a - b = 8 + 6i$.

2. Then $b/r_1 = (5 + 3i)/2$. We choose $q_2 = 2 + i$. (Any of $2 + i$, $3 + i$, $2 + 2i$, $3 + 2i$ will do.) Then
   
   $r_2 = b - r_1 q_2 = (11 + 27i) - (8 + 6i)(2 + i) = 1 + 7i$.

3. Then $r_1/r_2 = 1 - i \in \mathbb{Z}[i]$. Thus, a GCD of $a$ and $b$ is $r_2 = 1 + 7i$.

Remark
Other GCD’s are $-r_2$, and $\pm ir_2$, since the units in $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$. 
Irreducibles and Primes

Definition. Let $D$ be an integral domain.

- A nonzero non-unit element $p$ is an irreducible of $D$ if any factorization $p = ab$ in $D$ has the property that either $a$ or $b$ is a unit.
- A nonzero non-unit element $p$ is a prime if $p | ab$ implies $p | a$ or $p | b$.

Remarks

1. In $\mathbb{Z}$, an integer prime $p$ has two properties
   1.1 If $p = ab$, then $a = \pm 1$ or $b = \pm 1$ (i.e., either $a$ or $b$ is a unit).
   1.2 If $p | ab$, then $p | a$ or $p | b$.

2. In an integral domain, a prime is always an irreducible, but an irreducible may not be a prime.
Examples of irreducibles that are not primes

1. In \( \mathbb{Z}[2i] \), we have

\[
4 = 2 \cdot 2 = (2i) \cdot (-2i).
\]

The numbers \( \pm 2i \) are irreducibles, but not prime.

2. In \( \mathbb{Z}[\sqrt{-5}] \), \( 2, 3, 1 \pm \sqrt{-5} \) are all irreducibles, but neither of them is a prime. We have

\[
6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),
\]

but 2 does not divide \( 1 + \sqrt{-5} \) nor \( 1 - \sqrt{-5} \) in \( \mathbb{Z}[\sqrt{-5}] \).
Lemma

1. An element $p$ in an integral domain $D$ is a prime if and only if $\langle p \rangle$ is a prime ideal.

2. An ideal $\langle p \rangle$ in a PID is a maximal ideal if and only if $p$ is an irreducible.

3. In a PID, an element $p$ is a prime if and only if $p$ is an irreducible.

Corollary. In a PID, if an irreducible $p$ divides $a_1 \ldots a_n$, then $p \mid a_i$ for at least one $i$. 
Unique Factorization Domains

**Definition.** An integral domain $D$ is a unique factorization domain (UFD) if

1. Every nonzero non-unit element of $D$ can be factored into a product of a finite number of irreducibles.
2. If $a \in D$ has two factorizations $p_1 \ldots p_r$ and $q_1 \ldots q_s$ into products of irreducibles, then $r = s$ and $q_j$ can be renumbered so that $p_i$ and $q_i$ are associates.

**Example**

1. $\mathbb{Z}$ is a UFD. (Fundamental theorem of arithmetics.)
2. The integral domain $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. (We have

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

where $2, 1 \pm \sqrt{-3}$ are all irreducibles, but mutually non-associates.)
Theorem. Every PID is a UFD.

Key Lemmas.

1. Let $R$ be a commutative ring. Suppose that $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in $R$. Then $I = \bigcup_i I_i$ is an ideal of $R$.

2. Ascending Chain Condition for a PID: Let $D$ be a PID. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Then there is a positive number $N$ such that $I_n = I_N$ for all $n \geq N$.
Proof of PID $\Rightarrow$ UFD, first part

**Claim.** Every nonzero non-unit element $a$ has an irreducible factor.

1. Assume that $a$ is not an irreducible.
2. Then we have $a = a_1 b_1$, where neither $a_1$ nor $b_1$ is a unit. This implies that $\langle a \rangle \subsetneq \langle a_1 \rangle$.
3. If $a_1$ is not an irreducible, then $a_1 = a_2 b_2$ for some non-unit $a_2$ and $b_2$, and we have $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$.
4. Continuing this way, we obtain a strictly ascending chain of ideals $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$.
5. By ACC, this chain of ideals cannot go on forever.
6. Therefore, at some point $a_n$ must be an irreducible.
Claim. Every nonzero non-unit element $a$ is a product of irreducibles.

1. Assume that $a$ is not an irreducible. Then $a$ has an irreducible factor, say, $a = p_1 a_1$ for some irreducible $p_1$ and $a_1$ is not a unit. Then $\langle a \rangle \subsetneq \langle a_1 \rangle$.

2. If $a_1$ is an irreducible, we are done; otherwise, $a_1 = p_2 a_2$ for some irreducible $p_2$ and some non-unit $a_2$. We have $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$.

3. Continuing this way, we obtain a strictly ascending chain of ideals $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$.

4. By ACC, this process terminates at some point, i.e., $a = p_1 \cdots p_r$, where $p_i$ are all irreducibles.
Proof of PID ⇒ UFD, second part

We have seen that every nonzero non-unit element is a product of irreducibles. We now show the uniqueness.

1. Assume that $a = p_1 \ldots p_r$ and $a = q_1 \ldots q_s$ are two factorizations into products of irreducibles.
2. Then $p_1$ divides one of $q_i$. By rearranging the index, we assume that $p_1 \mid q_1$.
3. Then $q_1 = p_1 u_1$ for some $u_1 \in D$. Since $q_1$ is an irreducible, $u_1$ must be a unit. That is, $p_1$ and $q_1$ are associates.
4. We then have $p_2 \ldots p_r = u_1 q_2 \ldots q_s$.
5. Applying the same argument to $p_2$, we find $q_2 = p_2 u_2$ for some unit $u_2$, and $p_3 \ldots p_r = u_1 u_2 q_3 \ldots q_s$.
6. Continuing this way, we find $r = s$ and $p_i$ are associates of $q_i$ for each $i$. \qed