110A Notes

Jerry Luo

Winter 2024

1 Fun Integer Facts!

We begin this course by discussing some important facts about integers.
But... why?
Before discussing rings in a more abstract settings, we will ground ourselves in a particular ring that we all know and love — the integers. The ring of integers (often denoted by $\mathbb{Z}$) is a particularly important ring. For example, it is an *initial object*[1] in the category of rings! We will discuss properties of integers, before seeing how these properties abstract to the general setting of rings.
We begin with the following theorem, which should look very obviously true.

Theorem 1.1 (Well-Ordering Principle) *Every nonempty set of nonnegative integers contains a smallest element.*

Thankfully, this isn't one of those weird theorems that sound obvious but are a pain to prove.

Proof: Let S be a set of nonnegative integers. Suppose S does not have a smallest element. We claim that S is empty.
We proceed by induction. It is clear that given $s \in S$, we must have $0 \leq s$ (since s is nonnegative). Therefore, $0 \notin S$, as otherwise 0 would be the smallest element.
By induction, suppose $0, 1, \cdots, k \notin S$. Then given $s \in S$, we must have $s \geq k+1$. Therefore, $k+1 \notin S$, as otherwise, $k+1$ will be the smallest in S. □
Even though this fact seems obvious, it turns out that it's actually useful!

1.1 Division Business

Our first use of the well-ordering principal is to prove another easy-sounding fact.

Theorem 1.2 *Let a and b be integers, such that $b > 0$. There exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < b$.*

The idea of this is fairly straight forward. If $a \geq 0$, we can subtract b (and keep track of how many times we do so!) until doing so will yield something negative. The number of times that we can do this would be our q, and the remainder (yes, that remainder!) is r. If $a < 0$, we can perform a similar (but opposite) procedure!
Of course, we need a more formal way to say this.

[1] The meaning of this is way beyond the scope of this course, unfortunately. Basically, this means there is a unique map (homomorphism) from the integers into any rings.

Proof: Let $a, b \in \mathbb{Z}$ such that $b > 0$. Consider $S = \{a - bx | x \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$.
The idea here, of course, is that the x that yields the smallest $a - bx$ will be our q, and $a - bx$ will be our r. But to even be able to pick that, we need to show that S is nonempty!
To show $S \neq \emptyset$, we note that $a + b|a| \geq 0$. To see this, if $a \geq 0$, then $a + b|a| = a + ba \geq 0$. If $a < 0$, then $a + b|a| = a - ba = a(1 - b)$. Since $b > 0$, we must have $1 - b \leq 0$, and since $a < 0$, we must have $a(a - b) \geq 0$. This implies S is not empty.
We can now choose the smallest $a - bx$ in S, and as we stated before, we let $q = x$ and $r = a - bx$. Clearly, we see that $a = qb + r$. To see $0 \leq r < b$, we note that if $r > b$, then $r - b > 0$. However, we then have $r - b = a - bx - b = a - b(x + 1) \in S$, which contradicts the fact that $a - bx$ was the smallest element in S.
What is left is to show that q and r are unique. Suppose we have $a = bq + r = bq' + r'$, where we have $r, r' < b$. This implies that $b(q - q') = r' - r$, which in turn, implies $b|r' - r$. However, since $0 \leq r' < b$ and $-b < -r \leq 0$, we have $-b < r' - r < b$, which implies $r' - r = 0$, which yields $r = r'$. This also implies $b(q - q') = 0$, and as $b \neq 0$, we have $q' = q$ as well. This concludes our proof. □
In fact, we can relax the above theorem to allow for $b \neq 0$ (i.e., allow b to be negative!). This will be homework. :0
We use the word "divide" above. Let us formally define it!

Definition 1.1 *Let $a, b \in \mathbb{Z}$. We say b divides a if we can find $c \in \mathbb{Z}$ such that $a = bc$.*

If b divides a, we say $b|a$. Otherwise, we say $b \nmid a$.

Lemma 1.1 *If $b|a$ and $a \neq 0$, then $|b| \leq |a|$.*

Proof: Homework! Hint: recall that $|xy| = |x||y|$. □

Definition 1.2 *Let $a, b \in \mathbb{Z}$, with a and b not both 0. The greatest common divisor, denoted as $\gcd(a, b)$ (or just (a, b)) is the largest integer that divides both a and b. That is,*

- $\gcd(a, b)|a$ *and* $\gcd(a, b)|b$
- *If $c > 0$ divides a and b (i.e., $c|a$ and $c|b$), then $0 < c \leq \gcd(a, b)$*

It turns out, given $a, b \in \mathbb{Z}$, we can write $\gcd(a, b)$ as a "linear combination" of a and b!

Theorem 1.3 *Let $a, b \in \mathbb{Z}$ be integers (not both 0). Suppose $d = \gcd(a, b)$. We can find $r, s \in \mathbb{Z}$ such that $ar + bs = d$.*

Proving this (slightly more nontrivial) theorem also requires the well-ordering principle!

Proof: Let $S = \{am + bn | m, n \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$. The idea here is that we pick the smallest thing, and the m and n that yields it is the r and s that we seek!
As before, we first need to show S is nonempty. This isn't hard to show, as $a^2 + b^2 > 0$.
Now, let $m.n \in \mathbb{Z}$ such that $t = am + bn$ is the smallest positive element in S (we note that there are positive elements in S, because $a^2 + b^2 > 0$). We first show that $t|a$ and $t|b$. We note that we can write $a = tq + r$, with $0 \leq r < t$. This yields

$$\begin{aligned} r &= a - tq \\ &= a - (am + bn)q \\ &= a - amq - bnq \\ &= a(1 - mq) + b(-nq)\,. \end{aligned}$$

This implies $r \in S$, and since t is the smallest *positive* element of S, this implies $r = 0$. As such, $t|a$. We can similarly show that $t|q$.
We now show that if $c|a$ and $c|b$ such that $c > 0$, that $c \leq t$. Suppose $a = cx$ and $b = cy$ We note that

$$\begin{aligned} t &= am + bn \\ &= cxm + cyn \\ &= c(xm + yn)\,. \end{aligned}$$

It therefore follows that $c|t$, and as $t \neq 0$, we see that $|c| < |t|$. As both are positive, we have $c < t$. □

Definition 1.3 *Let $a, b \in \mathbb{Z}$. We say that a and b are relatively prime if $(a, b) = 1$.*

Theorem 1.4 *Let $a, b, c \in \mathbb{Z}$. Suppose $a|bc$ and $(a, b) = 1$. Then $a|c$.*

Proof: Because $(a, b) = 1$, we can find $x, y \in \mathbb{Z}$ such that $ax + by = 1$. It therefore follows that $axc + byc = c$. Because $a|bc$, we can find z such that $bc = az$. Therefore, we have

$$\begin{aligned} c &= axc + byc && (1)\\ &= axc + azy && (2)\\ &= a(xc + zy)\,, && (3) \end{aligned}$$

which implies $a|c$, as desired. □

Corollary 1.1 *Let $a, b, c \in \mathbb{Z}$ such that $(a, b) = 1$. Suppose $a|c$ and $b|c$. Then $ab|c$.*

Proof: Homework! □

1.2 Primes and Unique Factorization

Perhaps one of the most important sets of integers is the set of prime numbers! In a nontrivial sort of way, they are the (multiplicative) building blocks for integers! The classical definition is that a prime number is one that is divisible only by 1 and itself. However, that definition only really works if we consider natural numbers (i.e., positive integers).

Definition 1.4 *A nonzero and non-unit (i.e., $\neq \pm 1$) integer p is prime if its only divisors are ± 1 and $\pm p$.*

Theorem 1.5 *Let $p \in \mathbb{Z}$ such that $p \neq 0, \pm 1$. The following are equivalent:*

1. *p is prime*
2. *If $p|bc$ where $b, c \in \mathbb{Z}$, then $p|b$ or $p|c$.*

We note that this should theorem is eerily similar to one of the theorems we showed above!

Proof: Suppose p is prime. Suppose $p \not| b$. We wish to show that $p|c$.
Note that the only possible values of (p, b) are 1 and $|p|$. Because $p \not| b$, we must have $(p, b) = 1$. Therefore, because we simultaneously have $p|bc$ and $(p, b) = 1$, we must have $p|c$.
The other direction is homework! (Hint: contrapositive/contradiction should do the trick.) □
It is not difficult to see that we can extend one direction of this result to the following:

Corollary 1.2 *If p is prime and $p|a_1 \cdots a_n$, then there must be at least one a_i such that $p|a_i$.*

Proof: Homework! □
As stated above, primes are effectively the building blocks for integers! The precise statement for this fact is in the following theorem:

Theorem 1.6 *Let $n \in \mathbb{Z}$ be nonzero, with $n \neq \pm 1$. n can be written as a product[2] of primes.*

Proof: We consider $n > 1$ (note that $n < -1$ can be treated similarly).
Let S be the set of positive non-zero non-unit integers that cannot be written as a product of primes. We seek to show that S is empty.
Seeking a contradiction, suppose S is not empty. By the well ordering principle, we can find a smallest element of S, which we denote m. We note that m cannot be prime (indeed, $m \in S$). Therefore, we can find divisors $a, b \in \mathbb{Z}$ with $1 < a, b < m$ such that $m = ab$.
Because $a, b \notin S$, we can express them as a product of primes. However, this implies that m can also be expressed as a product of primes, as $m = ab$. We have therefore reached a contradiction, which implies S is empty, as desired. □
Not only can all (nonzero and non-unit) integers be expressed as a product of primes, the way in which integers can be expressed as a product of primes is unique! This fact is known as the fundamental theorem of arithmetic:

Theorem 1.7 (Fundamental Theorem of Arithmetic) *Let $n \in \mathbb{Z}$ be nonzero and non-unit, and suppose $n = p_1 \cdots, p_r$ and $n = q_1 \cdots, q_s$ are both prime factorizations of n. Then $r = s$ and we can find a permutation σ on $\{1, \cdots, r\}$ (i.e., a bijection from $\{1, \cdots, r\}$ to itself) such that $p_i = \pm q_{\sigma(i)}$ for all i.*

Proof: [sketch] Suppose $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ and both prime factorizations for n. Then we have $p_1 \cdots, p_r = q_1 \cdots, q_s$. Without loss of generality, suppose $r \leq s$.
Because $p_1 | q_1 \cdots q_s$, we must have p_1 dividing one of the q_j. Without loss of generality, suppose $p_1 | q_1$. Because p_1 and q_1 are both primes, we must have $q_1 = \pm p_1$. This implies $p_1 p_2 \cdots, p_r = q_1 \cdots, q_s = \pm p_1 q_2 \cdots q_s$, and after dividing by p_1, we have $p_2 \cdots, p_r = q_2 \cdots, q_s$.
We can continue this process, from which, without loss of generality, we get $p_i = \pm q_i$, for $1 \leq i \leq r$. We claim that $r = s$. Seeking a contradiction, suppose not (i.e., $r < s$). Following the above process, we get $1 = \pm q_{r+1} q_{r+2} \cdots q_s$, where q_j is prime. This implies $q_j | 1$ for each j, a contradiction. Therefore, we must have $r = s$. □

[2] In this context, we consider "products of one thing" as products.

Proof: [more formal] Suppose $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two prime factorizations of n, and without loss of generality, assume $r \leq s$. We induct on r.
For $r = 1$, we have $p_1 = q_1 \cdots q_s$. Because $p_1 | q_1 \cdots q_s$ and p_1 is prime, we must have $p_1 | q_j$ for some j. Without loss of generality, suppose $p_1 | q_1$. Because q_1 is prime, we must have $q_1 = \pm p_1$. To see that $s = 1$, suppose not. By dividing both sides by p_1, we have $1 = \pm q_2 \cdots q_s$, which further implies $q_j | 1$ for each $2 \leq j \leq s$. This is impossible, because q_j, a nonzero non-unit, cannot divide 1. So, indeed, we have $s = 1$.
Suppose whenever we have $p_1 \cdots p_{r-1} = q_1 \cdots q_s$, for $s \geq r - 1$ and p_i, q_j prime, we have $s = r - 1$ and $p_i = \pm q_{\sigma(i)}$ for some permutation σ. Consider $p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_j are prime and $s \geq r$. We first note that $p_1 | q_1 \cdots q_s$, and so, $p_1 | q_j$ for some q_j. Without loss of generality, say $p_1 | q_1$. Because both p_1 and q_1 are primes, it follows that $q_1 = \pm p_1$, and by dividing by p_1 on both sides, we have $p_2 \cdots p_r = \pm q_2 \cdots q_s$. By the induction hypothesis (and noting that we can absorb the $\pm$ into one of the q_j), we have $s - 1 = r - 1$ (so $s = r$), and furthermore, $p_i = \pm q_{\sigma(j)}$ for some permutation sigma (on $2, \ldots, r$). Our desired result follows. □
We end this excursion on primes with the following fact:

Theorem 1.8 *Let $n \in \mathbb{Z}$ be positive and non-unit. Suppose there is no prime divisor p of n such that $|p| \leq \sqrt{n}$. Then n is prime.*

Proof: Seeking a contradiction, suppose n is not prime. Then we can find prime a prime p such that $p | n$. We write $n = pm$, and because n is not prime, $m \neq \pm 1$, and so, we can find a prime q such that $q | m$. Write $m = qr$. We note that $n = pqr$, in which p and q are both prime divisors of n. Because n has no prime divisors with absolute value less than or equal to $\sqrt{n}$, we have $|p|, |q| > \sqrt{n}$. From this, we see that

$$\begin{aligned} n = |n| &= |p| \cdot |q| \cdot |r| \\ &\geq |p| \cdot |q| \\ &> \sqrt{n} \cdot \sqrt{n} = n \,, \end{aligned}$$

a contradiction. We are now done. □

Remark 1.1 *The above theorem tells us that if we want to check if n is prime, we only need to check whether $1, 2, \ldots \lfloor \sqrt{n} \rfloor$ divide n (i.e., there is no need to go all the way up to n).*

1.3 Modular Arithmetics!

We now discuss modular arithmetics, which more or less piggybacks off of our excursion in division. In modular arithmetics, two integers a and b are "congruent" modulo n if $a - b$ is divisible by n. Another way to think about this notion of congruence is that a and b leave the same remainder when dividing by n.

Definition 1.5 *Let $a, b \in \mathbb{Z}$, and let $n \in \mathbb{Z}$ be positive. We say a and b are congruent modulo n if $n | (a - b)$. We write this as $a \equiv b \mod n$.*

Proposition 1.1 *Congruence modulo n is an equivalence relation.*

Proof: To show that congruence modulo n is an equivalence relation, we must show that it is reflexive, symmetric, and transitive.
To see reflexivity, we note that $a \equiv a \mod n$, because $a - a = 0$ is clearly divisible by n.
To see symmetry, suppose $a \equiv b \mod n$. This implies $a - b$ is divisible by n. To show $b \equiv a \mod n$, we note that $b - a = -(a - b)$, which is clearly also divisible by n.
To see transitivity, suppose $a \equiv b \mod n$ and $b \equiv c \mod n$. We wish to show $a \equiv c \mod n$. To see this, note that $a-b$ and $b-c$ are both divisible to n, which implies that their sum $(a-b)+(b-c) = a-c$ is divisible by n, as desired. □
For each $a \in \mathbb{Z}$, we refer to $[a]_n$ as the equivalence class in which a belongs. When there is no confusion on n, we will suppress it.
Since congruence modulo n is an equivalence relation, we can look at its equivalence classes, which we refer to as congruence classes. It turns out that we can do arithmetics on the congruence classes in the same sort of way we do arithmetics on integers! In particular, we can consider addition (resp. multiplication) of congruence classes to be the congruence class of the sum (resp. product) of representatives of the congruence classes in question.

Definition 1.6 *Let $n \in \mathbb{Z}$ be positive. The integers modulo n, which we abbreviate as $\mathbb{Z}_n$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/(n)$ or $\mathbb{Z}/n$, is the set of congruence classes of integers modulo n.*

The integers modulo n have similar operations to those of $\mathbb{Z}$, with the same properties!

Definition 1.7 *Let $n \in \mathbb{Z}$ be positive, and let $[a]$ and $[b]$ be congruence classes. We define $[a]+[b] = [a+b]$ and $[a] \cdot [b] = [ab]$.*

One may be wondering, does the sum and product of $[a]$ and $[b]$ depend on our choices of representatives for $[a]$ and $[b]$? That is, if $[a'] = [a]$ and $[b'] = [b]$, do we necessarily have $[a+b] = [a'+b']$ and $[ab] = [a'b']$? Because if not, these operations don't really make sense...
Thankfully, the above is true, so the operations are well defined!

Theorem 1.9 *Let $n \in \mathbb{Z}$ be positive, and let $[a]$ and $[b]$ be equivalence classes. Suppose $[a'] = [a]$ and $[b'] = [b]$. Then $[a+b] = [a'+b']$ and $[ab] = [a'b']$.*

Proof: We first show that $[a+b] = [a'+b']$, which is to say, $a + b \equiv a' + b' \mod n$.
To see this, we note that $(a+b) - (a'+b') = (a-a') + (b-b')$. Because $a - a'$ and $b - b'$ are both divisible by n, we have that $(a+b) - (a'+b')$ is also divisible by n.
We now show that $[ab] = [a'b']$, which is to say, $ab - a'b'$ is divisible by n. To see this, we note that

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= b(a-a') + a'(b-b') \,. \end{aligned}$$

Because $a' - a$ and $b - b'$ are both divisible by n,$ab - a'b'$ is as well. □
Because the inherited operations of addition and multiplication are well defined, arithmetics modulo n is very similar to arithmetics in $\mathbb{Z}$. In particular, addition and multiplication modulo n have the same associative and commutative properties that addition and multiplication of integers have. The distribution laws get inherited as well!

Proposition 1.2 *Let $n \in \mathbb{Z}$ be positive, and let $[a], [b], [c]$ be (any) congruence classes modulo $\mathbb{Z}$. The following hold:*

1. $[a] + [b] = [b] + [a]$
2. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$
3. $[a] + [0] = [a]$
4. $[a] + x = [0]$ *has a solution*
5. $[a] \cdot [b] = [b] \cdot [a]$
6. $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$
7. $[a] \cdot [1] = [a]$
8. $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$

Note, none of these are hard to prove.
We also have another operation for $\mathbb{Z}/n$, that's fairly straight forward.

Definition 1.8 *Let $n \in \mathbb{Z}$ be positive, and let $[a]$ be an equivalence class modulo n. Let $k \in \mathbb{Z}$ be positive. $[a]$ to the power k is given by*

$$[a]^k = [a] \cdot [a] \cdot \ldots \cdot [a] \text{ (k times)}.$$

Because the congruence classes modulo n can be uniquely represented by $0, 1, \cdots, n-1$, we will default to using these representations to represent $\mathbb{Z}/n$ elements.
It turns out that if p is a prime, then the integers modulo p are special. We will see why this is the case by the following examples.

Definition 1.9 *Let $n > 1$ be an integer, and consider $[a] \in \mathbb{Z}/n$. Suppose there is $[b] \in \mathbb{Z}/n$ such that $[ab] = [1]$ in $\mathbb{Z}/n$. We say that $[a]$ is a <u>unit</u> in $\mathbb{Z}/n$, and refer to $[b]$ as the <u>inverse</u> of $[a]$, which we denote $[a]^{-1}$.*

Theorem 1.10 *Let $p > 1$ be an integer. The following are equivalent.*

1. *p is prime.*
2. *Each nonzero element in $\mathbb{Z}/p$ has a multiplicative inverse. That is, for each nonzero $[a] \in \mathbb{Z}/p$, we can find $[b] \in \mathbb{Z}/p$ such that $[ab] = [1]$ in $\mathbb{Z}/p$.*
3. *Let $[a], [b] \in \mathbb{Z}/p$. If $[ab] = [0]$, then $[a] = [0]$ or $[b] = [0]$.*

Proof: We first show (1) implies (2). Suppose p is prime, and take $[a] \in \mathbb{Z}/p$ to be nonzero. We seek to find $[b] \in \mathbb{Z}/p$ such that $[ab] = [1]$ in $\mathbb{Z}/p$. Because p is prime and $p \not| a$, we have $(a, p) = 1$. Therefore, we can find $c, d \in \mathbb{Z}$ such that $1 = ac + pd$, and because $[pd] = [0]$ in $\mathbb{Z}/p$, we note that $[ac] = [1]$ in $\mathbb{Z}/p$.
We now show (2) implies (3). Let $[a], [b] \in \mathbb{Z}/p$, and suppose $[ab] = [0]$. If $[a] = [0]$, then we are done. Otherwise, we can find a multiplicative inverse for $[a]$. So, we note that $[a]^{-1} \cdot [ab] = [a]^{-1} \cdot [0]$, so $[b] = [0]$, as desired.
We finally show (3) implies (1). Seeking a contradiction, suppose p is not prime. This means we can find a (positive) divisor a for p such that $a \neq \pm 1, \pm p$. Let $p = ab$; we have $1 < a, b < p$. This

implies that, $[a], [b] \neq [0]$, when viewed as elements of $\mathbb{Z}/p$. However, $[ab] = [p] = [0]$ in $\mathbb{Z}/p$, a contradiction. So, p must be prime. $\square$

The key idea in the proof of the theorem above is that given a (positive) prime number p and a such that $1 \leq a < p$, we have $(a, p) = 1$. Of course, this is not true if p was not prime. This idea informs us which elements in $\mathbb{Z}/n$ have multiplicative inverses!

Theorem 1.11 *Let $n > 1$ be an integer and take $[a] \in \mathbb{Z}/n$. $[a]$ has a multiplicative inverse if and only if $(a, n) = 1$.*

Proof: Suppose $(a, n) = 1$. Then we can find $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Because $[ny] = [0]$ in $\mathbb{Z}/n$, we have that $[ax] = [1]$ in $\mathbb{Z}/n$, which means $[a]$ has a multiplicative inverse in $\mathbb{Z}/p$.

Suppose now that $[a]$ has a multiplicative inverse. We may assume $0 < a < n$. Seeking a contradiction, suppose $(a, n) \neq 1$. This implies $1 < (a, n) < n$. We refer to $d = (a, n)$.

We can express $a = db$, and $n = dc$. We note that $1 < c < n$. Moreover, we note that $[ca] = [c(bd)] = [bn] = [0]$ in $\mathbb{Z}/n$. Because $[a]$ has a multiplicative inverse, $[a]^{-1}$, we have $[c] = [ca][a]^{-1} = [0]$. This implies $[c] = [0]$, a contradiction, as we then would simultaneously have c being a multiple of n, and $1 < c < n$, which is impossible. $\square$

We end our excursion on integers with the Chinese remainder theorem, an important fact used in number theory.

Theorem 1.12 (Chinese Remainder Theorem, simple version) *Let $m, n \in \mathbb{Z}$ be relatively prime and positive. Let $a, b \in \mathbb{Z}$. We can find $x \in \mathbb{Z}$ such that*

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n\,. \end{aligned}$$

Moreover, if y is another solution, then $y \equiv x \mod mn$.

Proof: Because $(m, n) = 1$, we can find $c, d \in \mathbb{Z}$ such that $cm + dn = 1$. We observe that because $cm \equiv 0 \mod m$, we have $dc \equiv 1 \mod m$. Similarly, $cm \equiv 1 \mod n$.

Consider $x = bcm + adn$. We observe that $x \equiv adn \equiv a \mod m$ and $x \equiv bcm \mod n = b$, as desired.

Suppose y is another solution. Then we have $y \equiv x \mod m$, which implies $y - x$ is a multiple of m. Similarly, $y - x$ is a multiple of n as well. Because m and n are relatively prime, it follows that $y - x$ is a multiple of mn, which implies $y \equiv x \mod mn$. $\square$

We can, in fact, show the more general fact:

Theorem 1.13 (Chinese Remainder Theorem, more general) *Let $m_1, \cdots, m_1 \in \mathbb{Z}$ be positive and pairwise relatively prime. Let $a_1, \cdots, a_n \in \mathbb{Z}$. We can find x such that*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n\,. \end{aligned}$$

Moreover, if y is another solution, then $y \equiv x \mod m_1 m_2 \cdots m_n$

Proof: Homework! Hint: Use induction. The less general case is quite useful here... $\square$

2 Rings

Now that we have discussed integers and their properties in quite a bit of depth, we now turn to rings, which were constructed in order to generalize the integers.

2.1 Definition and Basic Properties

Definition 2.1 *A ring R is a nonempty set with two operations, addition ($+$) and multiplication ($\cdot$, or just concatenation) such that, for all $a, b, c \in R$, the following hold:*

1. *$a + b \in R$ [closure of addition]*
2. *$a + (b + c) = (a + b) + c$ [associativity of addition]*
3. *$a + b = b + a$ [commutativity of addition]*
4. *There is an element $0 \in R$ such that $0 + a = 0$ for all $a \in R$. [existence of additive identity]*
5. *There is an element $-a \in R$ such that $(-a) + a = 0$ [existence of additive inverses]*
6. *$ab \in R$ [closure of addition]*
7. *$a(bc) = (ab)c$ [associativity of multiplication]*
8. *$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ [multiplication distributes over addition]*
9. *There is an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.*

Notation 2.1 *When there are multiple rings floating around, we will use 0_R and 1_R to denote the additive and multiplicative identities of R, respectively. Otherwise, when things are clear, we will not be using subscripts.*

Some books/authors do not require rings to satisfy condition (9). We refer to sets R that satisfy (1)–(8) but not (9) as non-unital rings, or rngs[3]. We will largely not be dealing with them.

Remark 2.1 *Given a ring R, it is possible for $0 = 1$. In this case, we must have $R = \{0\}$ (Homework!)*

Definition 2.2 *A ring R is commutative if for all $a, b \in R$, we have $ab = ba$.*

For this class, we will largely focus on commutative rings. However, it is important to acknowledge the fact that non-commutative rings exist.

Definition 2.3 *Let R be a ring. An element $a \in R$ is a zero divisor if we can find $b \in R$ such that $ab = 0$ or $ba = 0$.*

Definition 2.4 *Let R be a ring. An element $a \in R$ is a unit if we can find $b \in R$ such that $ab = ba = 1$. We refer to the b as the inverse of a, which we denote a^{-1}.*

[3]That is, a ring without identity (i). So basically, take the word 'ring' and remove 'i' and you get 'rng'. This may sound like a joke, but mathematicians sometimes do use this term!

Here are some examples of rings, both commutative and non-commutative:

- The set $\{0\}$ forms a (technically commutative) ring. In this case, the additive and multiplicative identity is the same thing. In fact, one can show that if a ring R satisfies $1 = 0$, then $R = \{0\}$ (Homework!).
- The integers, $\mathbb{Z}$, form a commutative ring! $\mathbb{Z}$ is commutative. We observe that there are no nonzero zero divisors. The units in $\mathbb{Z}$ are ± 1.
- The integers modulo n, $\mathbb{Z}/n$, is also commutative. By some of what we showed earlier, we see that the units are precisely the congruence classes $[a]$ such that $(a, n) = 1$. In fact, if $(a, n) > 1$, then $[a]$ is a zero divisor.
- The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all rings. In fact, none of them have nonzero zero divisors.
- Let R and S be rings. The cartesian product of R and S, given by $R \times S = \{(r, s) | r \in R, s \in S\}$ is also a ring. Moreover, if R and S are both commutative, then so is $R \times S$. The zero divisors of $R \times S$ are elements of the form (r, s) where r and s are both zero divisors. Likewise, the units of $R \times S$ are elements of the form (r, s) where r and s are both units.
- Let R be any ring. Given $n \in \mathbb{Z}$ with $n > 0$, the $n \times n$ square matrices with real entries, given by $M_n(R)$, form a ring. Here, addition is entry-wise; that is, given $A, B \in M_n(R)$, we have $(A + B)_{ij} = A_{ij} + B_{ij}$. Multiplication, as we recall, is a bit more complicated; We have

  $$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} \, .$$

  The zero divisors are precisely the non-invertible matrices, and the units are the invertible ones.

  Even if R is commutative, $M_n(R)$ may not be. For example, if $n > 1$, $M_n(R)$ is not commutative! For example, given $n = 2$, and $R = \mathbb{R}$ we can consider $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. We note that $AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, whereas $BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.
- Let R be any ring, and let X be a nonempty set. Consider $\mathcal{F}(X, R)$, the set of all functions $f : X \to R$. Addition and multiplication are defined pointwise: given $f, g \in \mathcal{F}(X, R)$, we have $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. If R is commutative, then so is $\mathcal{F}(X, R)$. The zero divisors are functions f such that $f(x) = 0$ for some x. The units are the functions f such that $f(x) \neq 0$ for all x.
- Let R be a ring. The set of polynomials over R, written $R[x]$, forms a ring. The set of polynomials are defined as

  $$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n | a_i \in R, n \in \mathbb{Z}_{>0}\} \, .$$

  We can think of polynomials as formal linear combinations[4] of $\{1, x, x^2, \cdots\}$. We are essentially taking R and adding in an extra element, x, which commutes with everything in R (i.e.,

[4]Recall that linear combinations are always finite! In particular, something like $\sum_{i=0}^{\infty} x^i = 1 + x + x^2 + ...$ is NOT a polynomial!

given $a \in R$, $ax = xa$). $R[x]$ is commutative if and only if R is commutative (Homework!). The units of $R[x]$ are precisely the units of R. The zero divisors are a bit more complicated, which we won't get into.

We now discuss some basic properties of rings.

Proposition 2.1 *Let R be a ring. Let $a, b, c \in R$. The following hold:*

1. *The additive identity is unique.*
2. *An additive inverse is unique.*

   NOTATION: We denote the additive inverse of a by $-a$. Additionally, $a-b$ refers to $a+(-b)$.
3. *If $a + b = a + c$, then $b = c$.*
4. *The multiplicative identity is unique.*
5. *If a is a unit, then its inverse is unique.*

   NOTATION: If a is a unit, then we denote its inverse as a^{-1}
6. $0 \cdot a = a \cdot 0 = 0$
7. $a(-b) = -ab$ *and* $(-a)b = -ab$
8. $-(-a) = a$
9. $-(a + b) = -a - b$
10. $-(a - b) = -a + b$
11. $(-a)(-b) = ab$

Proof: These are fairly straight forward to do. We will prove five of them and leave the rest for homework. Let $a, b, c \in R$.

1. Let 0 and $0'$ both be additive identities. Then by definition of additive identity, we note that $0 = 0 + 0' = 0'$.
2. Let b and c both be additive identities of a. Then $c = (a+b)+c = (b+a)+c = b+(a+c) = b$.
3. If $a + b = a + c$, then we can add the additive inverse of a to both sides to yield the desired result.
6. Observe that $0+0 = 0$. Therefore, we have $0a = (0+0)a = 0a+0a$. We can add the additive inverse of $0a$ to yield $0a = 0$.
7. Observe that $b - b = 0$. Because $0a = 0$, we see that $ab + a(-b) = a(b - b) = 0$. By additing $-ab$ to both sides, we see that $a(-b) = -ab$.

□

Proposition 2.2 *Let R be a ring. Suppose a is an unit. Then a cannot be a zero divisor.*

Proof: Seeking a contradiction, suppose a is a zero divisor. Then we can find a nonzero b such that $ab = 0$ or $ba = 0$. We consider the case of $ab = 0$, and note that the case $ba = 0$ can be treated similarly.
Because a is a unit, we can find c such that $ac = ca = 1$. As such, we note that $0 = 0 \cdot c = c(aB) = (ca)b = b$, a contradiction, as b was given to be nonzero. Therefore a cannot be a zero divisor. □
Just like how in the vector space setting, we have subspaces, we also have subrings for rings.

Definition 2.5 *Let R be a ring. A subring $S \subseteq R$ is a subset such that S is a ring with the same addition and multiplication operations, as well as the same additive and multiplicative identities. If S forms a non-unital ring with the same addition and multiplication operations, or forms a ring but with a different multiplicative identity than that of R, then we say that S is a non-unital subring.*

Just like how, to show a subset of vector space is a subspace, we didn't need to show *all* the vector space axioms, the same holds for showing a subset of a ring is a subring.

Proposition 2.3 *Let $S \subseteq R$ be a subset. S is a subring if and only if S satisfies the following properties:*

1. *$1 \in S$*
2. *S is closed under addition: for all $a, b \in S$, we have $a + b \in S$.*
3. *S is closed under multiplication: for $a, b \in S$, we have $ab \in S$*
4. *S is closed under additive inverses: For $a \in S$, we have $-a \in S$.*

Proof: We get properties 1, 5, and 6, and 9 for free. Properties 2, 3, 7, and 8 all get inherited from R. Property 4 is satisfied because if $1 \in S$ and S is closed under additive inverses, we also have $-1 \in S$; Using closure of addition, we then get $0 = 1 + (-1) \in S$ □

Remark 2.2 *Let R be a ring and $S \subseteq R$ be a subring. As stated above, 1_R and 1_S must be the same. For example, if we take $R = R_1 \times R_2$, and $S = \{(r_1, 0) | r_1 \in R_1\}$, then $1_S = (1, 0)$ whereas $1_R = (1, 1)$. In this case S is NOT a subring of R, even though it is a subset that satisfies the ring axioms.*

Remark 2.3 *If we wish to show a subset $S \subseteq R$ is a non-unital subring, we need to show that $0 \in S$, and that S is closed under addition, multiplication, and additive inverses. The reason why we need an additional condition of $0 \in S$ is because we need to ensure S is nonempty*

We will now discuss some special rings: integral domains and fields. Integral domains have the special property that one cannot take products of nonzero elements and yield 0. Fields have the special property that nonzero elements have multiplicative inverses.

Definition 2.6 *A nonzero commutative ring R is an integral domain if it has no nonzero zero divisors. That is, given $a, b \in R$ such that $ab = 0$, we must have $a = 0$ or $b = 0$.*

One of the nice properties of integral domains is that one can "cancel" elements.

Proposition 2.4 *Let R be an integral domain, and let $a, b, c \in R$ such that a is nonzero. If $ab = ac$, then $b = c$.*

Proof: Because $ab = ac$, we also have $a(b-c) = ab - ac = 0$. Because a is nonzero, we must have $b - c = 0$, which implies $b = c$. □

Definition 2.7 *A nonzero commutative ring R is a field if every nonzero element is unit. That is, given nonzero $a \in R$, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.*

Proposition 2.5 *Every field is an integral domain.*

Proof: As previously shown, given a ring R, units of R are not zero divisors. Because every nonzero element of R is a unit, R has no nonzero zero divisors. □
We see that all fields are integral domains, but not all integral domains are fields. For example $\mathbb{Z}$ is an integral domain (no nonzero elements are zero divisors), but it is clearly not a field (e.g., $2 \in \mathbb{Z}$ is not a unit). However, it turns out that finite integral domains *are* fields.

Theorem 2.1 *Every finite integral domain is a field.*

Proof: Let R be a finite integral domain. We can list out it elements $R = \{r_1, \cdots, r_n\}$. Take $r_i \in R$ to be nonzero. We wish to show that it has an inverse.
To see this, consider the set $r_iR = \{r_ir_1, r_ir_2, \cdots, r_ir_n\}$ By closure of multiplication in R, we note that $r_i \subseteq R$. Therefore, $|r_iR| \leq n$.
We show that $|r_iR| = n$. To see this, we need to show that every r_ir_j is unique. Suppose $r_ir_j = r_ir_k$. Because r_i is nonzero, we must have $r_j = r_k$. Therefore, $j = k$, so $r_ir_j = r_ir_k$.
Therefore, because $|r_iR| = |R| = n < \infty$ and $r_iR \subseteq R$, it follows that $r_iR = R$. Therefore, we must have $r_ir_j = 1$ for some $r_j \in R$, as desired.

□

2.2 Ring Homomorphisms and Ideals

We now turn to ring homomorphisms, which are maps between rings. The reason for considering ring homomorphism is that they "preserve" the structure of a ring.

Definition 2.8 *Let R and S be rings. A function $f : R \to S$ is a ring homomorphism if given $a, b \in R$ the following hold:*

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$.

We note that some books/authors define ring homomorphisms to not require condition (3) to be met. We refer to functions that satisfy (1) and (2) but not (3) as non-unital ring homomorphisms.
It is also worth noting that condition (3) puts quite a bit of restriction on which maps can be homomorphisms. In particular, if R and S are rings such that R is additively generated by 1_R, then there is at most one ring homomorphism from R to S.
Here are some basic properties of ring homomorphism:

Proposition 2.6 *Let R and S be rings, and let $f : R \to S$. Let $a, b \in R$. The following hold:*

1. *$f(0_R) = 0_S$.*
2. *$f(-a) = -f(a)$.*
3. *$f(a-b) = f(a) - f(b)$.*
4. *If $a \in R$ is a unit, then $f(a)$ is a unit as well, with $f(a^{-1}) = f(a)^{-1}$.*

Proof: Let $a, b \in R$.

1. We observe that $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$. By adding $-f(0_R)$ to both sides, we see $f(0_R) = 0_S$, as desired.
2. We observe that $0 = f(0_R) = f(a + (-a)) = f(a) + f(-a)$. By adding $-f(a)$ to both sides, we see $f(-a) = -f(a)$.
3. Homework!
4. Homework!

□

Definition 2.9 *Let $f : R \to S$ be a ring homomorphism. We say that f is an isomorphism if f is bijective, in which case, we also say that R and S are isomorphic, which we write $R \cong S$.*

Similar to linear transformations between vector spaces, ring homomorphisms yield images and kernels. While images are certainly subrings, kernels need not be.

Definition 2.10 *Let $f : R \to S$ be a ring homomorphism. The kernel of f is defined by $\ker(f) = \{a \in R | f(a) = 0\}$ and the image of f is defined by $Im(f) = \{f(a) | a \in R\}$.*

Proposition 2.7 *Let $f : R \to S$ be a ring homomorphism. The image of f is a subring of S, wheras the kernel of f is a non-unital subring of R.*

Proof: We first show that $Im(f)$ is a subring of S. First, we note that $1_S \in Im(f)$, because $1_S = f(1_R)$. To see that $Im(f)$ is closed under addition and multiplication, take $f(a), f(b) \in Im(f)$. We observe that $f(a) + f(b) = f(a+b) \in Im(S)$, and $f(a)f(b) = f(ab) \in Im(S)$. Finally, to see that $Im(S)$ is closed under additive inverses, we observe that $f(-a) = -f(a)$, which implies that $-f(a) \in Im(f)$.
To see that $\ker(f)$ is a non-unital subring, we show that it is closed under addition, multiplications, and additive inverses. Let $x, y \in \ker(f)$. To see $x + y, xy \in \ker(f)$, we observe that $f(x+y) = f(x) + f(y) = 0_S + 0_S = 0$, and $f(xy) = f(x)f(y) = 0_R \cdot 0_R = 0$. To see closure of additive inverses, we observe that $f(-a) = f(-a) + 0_S = f(-a) + f(a) + f(-a+a) = f(0_R) = 0_S$. □

Theorem 2.2 *Let $f : R \to S$ be a ring homomorphism. f is injective if and only if $\ker(f) = \{0\}$.*

The proof of this is very similar to the linear algebra proof.

Proof: The forward direction is clear, by definition: we always have $f(0_R) = 0_S$, and if f is injective, then 0_R is the only thing that maps to 0_S.
Suppose now that $\ker(f) = \{0\}$, and suppose $f(r_1) = f(r_2)$. From this, we observe that $f(r_1 - r_2) = 0_S$, which implies $r_1 - r_2 \in \ker(f) = \{0_R\}$. This implies $r_1 = r_2$. □
Here are examples of ring homomorphisms, as well as examples of rings that do not have ring homomorphism.

- Let R be a ring, and let $a \in R$. Consider $\Phi_a : R[x] \to R$ be defined by $f \mapsto f(a)$ (i.e., $r \mapsto r$ for $r \in R$ and $x \mapsto a$). We clearly have $\Phi_a(1) = 1$. To see closure of addition and multiplication, take $f, g \in \Phi$. We note that $\Phi_a(f + g) = (f + g)(a) = f(a) + g(a) = \Phi_a(f) + \Phi_a(g)$, and $\Phi_a(fg) = (fg)(a) = f(a)g(a) = \Phi_a(f)\Phi_a(g)$.

  We note that $\ker(f)$ is the set of polynomials with a as a root, and $Im(f)$ is all of R.

- Consider $f : \mathbb{Z} \to \mathbb{Z}/n$, where $a \mapsto [a]$. We note that this is the *only* homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n$, because $1 \mapsto [1]$ forces the value of each $f(n)$. We know that f is a homomorphism, because $f(1) = [1]$ (by definition), $f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$, and $f(ab) = [ab] = [a] \cdot [b] = f(a)f(b)$.

  Observe that $\ker(f) = n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$, and $Im(f) = \mathbb{Z}/n$.

- There is *no* homomorphism from $\mathbb{Z}_3$ to $\mathbb{Z}_6$. This is because if there were a ring homomorphism $f : \mathbb{Z}_3 \to \mathbb{Z}_6$, we would need $[1]_3 \to [1]_6$. However, this would mean that $[0]_6 = f([0]_3) = f([3]_3) = [3]_6$, which is not possible.

- Let R be any ring. We have a homomorphism $f : \mathbb{Z} \to R$ given by

  $$f(n) = 1_R + \cdots + 1_R \ (n \text{ times})$$

  if $n \geq 0$ and

  $$f(n) = -1_R - \cdots - 1_R \ (-n \text{ times})$$

  if $n < 0$. It is not difficult (albeit a bit tedious) to see that this is a ring homomorphism. In fact, this is the *only* ring homomorphism from $\mathbb{Z}$ to R, as we must have $1 \mapsto 1_R$, which forces the function values for the rest of the integers.

- Consider the Gaussian integers, given by $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, where $i^2 = -1$. Consider the map $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$ where $a + bi \mapsto a - bi$. Homework: check this is an isomorphism!

Given a ring homomorphism $f : R \to S$, an important observation about $\ker(f)$ is that it's not just a nonunital subring of R. It also has the following 'absorbing" property!

Proposition 2.8 *Let $f : R \to S$ be a ring homomorphism. For any $a \in \ker(f)$ and $x \in R$, we have $ax, xa \in \ker(f)$.*

Proof: We observe that $f(ax) = f(a)f(x) = 0_S \cdot f(x) = 0_S$. Similarly, $f(xa) = f(x)f(a) = f(x) \cdot 0_S = 0_S$ □
Kernels of ring homomorphism are an example of an "ideal", which is a non-unital subring with the "absorbing" property above. In fact, as we will see later on, *all* ideals can be realized as kernels of ring homomorphisms.

Definition 2.11 *Let R be a ring, and let $I \subseteq R$ be a nonempty subset. I is an ideal of R if I is a non-unital subring such that for all $a \in I$ and $x \in R$, we have $xa, ax \in I$.*

Remark 2.4 *We refer to non-unital subrings that have the absorption property for multiplication on the left (resp. right) side as left (resp. right) ideals. This only matters for the non-commutative rings. In particular, for commutative rings, left ideals and right ideals are the same.*

One of the most examples of an ideal for commutative rings is a principal ideal, which is "generated" by an element of R. Given $a \in R$, the principal ideal generated by R is the set of all "multiples" of a.

Definition 2.12 *Let R be a commutative ring, and let $a \in R$. The principal ideal generated by a is the set $(a) = \{ar | r \in R\}$.*
Notation: We sometimes refer to (a) as aR.

As one would hope, principal ideals are ideals!

Theorem 2.3 *Let R be a commutative ring, and let $a \in R$. Then the principal ideal (a) is an ideal.*

Proof: To see that (a) is a subring of R, we first show that it forms a nonunital ring. To see that $0 \in (a)$, we note that $0 = a \cdot 0 \in (a)$. To see closure under addition and multiplication, we note that given $ar_1, ar_2 \in (a)$, we have $ar_1 + ar_2 = a(r_1 + r_2) \in (a)$, and $(ar_1)(ar_2) = a(r_1 ar_2) \in (a)$. To see closure under additive inverses, take $ar \in (a)$. We note that the additive inverse of a is $-ar = a(-r) \in (a)$.
To see that (a) satisfies the absorbing property, take $ar_1 \in (a)$ and $r \in R$. Clearly, we see that $(ar_1)r = a(r_1 r) \in (a)$, as desired. □
Herer are some examples of ideals:

1. Let R be any ring. Then $\{0\}$ and R are both ideals. In particular, $\{0\} = (0)$ and $R = (1)$, which means they are principal ideals!

2. Consider $\mathbb{Z}$. The set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \cdots\}$ forms an ideal, and can be written (n).

3. Let F be a field, and consider $R = F[x]$ be the polynomials with coefficients in F. Consider the polynomial $x - a$, for $a \in F$. The (principal) ideal $(x - a)$ is the set of all polynomials that has a as a root.

4. Let S be a set and R a commutative ring, and consider the set $\mathcal{F}(S, R)$ of functions from S to R. Let $T \subseteq S$ be a subset, and consider $A_T = \{f \in \mathcal{F}(S, R) | f(x) = 0 \text{ for } x \in T\}$. A_T forms an ideal.

5. Let F be a field, and let $R = F[x][y]$, which is usually written $F[x, y]$. The set $(x, y) = \{p(x, y)x + q(x, y)y | p, q \in F[x, y]\}$ forms an ideal. We note that (x, y) is not principal (homework!).

Theorem 2.4 *Let R be a ring, and let $I_1, \cdots, I_k$ be ideals. Then*

1. *The set $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k | i_j \in I_j\}$ is an ideal.*

2. *The set $I_1 \cap I_2 \cap \cdots \cap I_k$ is an ideal.*

Proof: Homework! □

Definition 2.13 *Let R be a commutative ring, and let $a_1, \ldots, a_k \in R$. The ideal generated by $a_1, \cdots, a_n$ is given by $(a_1) + \cdots + (a_k)$. We denoted this ideal as $(a_1, \ldots, a_n)$.*

A special property of fields is that they only have two ideals:

Proposition 2.9 *Let F be a field. The only ideals of F are F and $\{0\}$.*

Proof: Let I be a nonzero ideal, and take $a \in I$. We then observe that $1 = a \cdot a^{-1} \in I$. Because $1 \in I$, it follows that $R = I$. □

2.3 Quotient Rings

In the section above, we noted that kernels of ring homomorphisms are ideals. As hinted earlier, it turns out that all ideals can be realized as kernels of homomorphisms!
To start off, let's remind ourselves of a more familiar setting: integers. It turns out that all ideals in $\mathbb{Z}$ are of the form (n), where $n \in \mathbb{Z}$ (we can even assume that n is non-negative!). By taking integers modulo n, we get $\mathbb{Z}/n$, which consists of congruence classes modulo n. We also recall that we have a homomorphism $\mathbb{Z} \to \mathbb{Z}/n$, where the kernel is precisely $n\mathbb{Z} = (n)$.
In a similar way, given a ring R, we can also consider congruence modulo an ideal I. This yields a ring of congruence classes modulo I, which is constructed in the same sort of way we constructed $\mathbb{Z}/n$. We call such a ring a quotient ring.

Definition 2.14 *Let R be a ring, let $a, b \in I$ and let $I \subseteq R$ be an ideal. We say that a and b are congruent modulo I if $a - b \in I$. We write this as $a \equiv b \mod I$, or $a + I = b + I$.*

Proposition 2.10 *Let R be a ring and let $I \subseteq R$ be an ideal. Congruence modulo I is an equivalence relation.*

Proof: First we show reflexivity. Given $a \in R$, we clearly have $a \equiv a \mod I$, as $a - a = 0 \in I$.
To see symmetry, take $a, b \in R$. If $a \equiv b \mod I$, this means $a - b \in I$. To see $b \equiv a \mod I$, we note that $b - a = (a - b) \cdot (-1) \in I$, because $a - b \in I$.
Finally, to show transitivity, suppose $a, b, c \in R$ such that $a \equiv b \mod I$ and $b \equiv c \mod I$. This implies that $a - b \in I$ and $b - c \in I$. Therefore, by closure of addition, we see that $a - c = (a - b) + (b - c) \in I$, which means $a \equiv b \mod I$. □

Notation 2.2 *Given a ring R, $a \in R$, and an ideal $I \subseteq R$, we refer to the congruence class modulo I containing a as $a + I$. This notation is sensible; it is not difficult to show that the congruence class modulo I containing a is precisely $\{a + r | r \in I\}$ (Homework!).*

Theorem 2.5 *Let R be a ring, $a, b, c, d \in R$, and $I \subseteq R$ be an ideal. Suppose $a \equiv c \mod I$ and $b \equiv d \mod I$. Then*

1. $a + b \equiv c + d \mod I$
2. $ab \equiv cd \mod I$

Proof:

1. Suppose $a \equiv c \mod I$ and $b \equiv d \mod I$. This means $a - c \in I$ and $b - d \in I$. Therefore, it follows that $(a + b) - (c + d) = (a - c) + (b - d) \in I$, which implies $a + b \equiv c + d \mod I$, as desired.

2. We observe that $ab - cd = ab - (bc + bc) - cd = b(a - c) + c(b - d)$. Because $a - c, b - d \in I$, it follows that $ab - cd \in I$, so $ab \equiv cd \mod I$.

□

The above theorem tells us that addition of congruence classes modulo an ideal is well defined, which allows us to construct quotient rings. The construction here is similar (in fact, nearly identical) to the construction $\mathbb{Z}_n$.

Definition 2.15 *Let R be a ring, $a, b \in R$, and $I \subseteq R$ be an ideal. The quotient ring Q/I is the ring consisting of congruence classes modulo I, with addition and multiplication operations given by $(a + I) + (b + I) = a + b + I$ and $(a + I)(b + I) = ab + I$, respectively.*

Remark 2.5 *The notation we have above is fitting; as sets, we have $(a + I) + (b + I) = a + b + I$ and $(a + I)(b + I) = ab + I$.*

Proposition 2.11 *Let R be a ring, $a, b \in R$, and $I \subseteq R$ be an ideal. The quotient ring Q/I is a ring.*

Proof: Closure of addition and multiplication (properties 1 and 6) are clear, by definition and because R is closed under addition and multiplication. Commutativity of addition (property 2), associativity of addition (property 3), associativity of multiplication (property 7), and multiplication distributing over addition (property 8) all hold because they hold for R. The additive identity here is just I (or $0_R + I$), the existence of additive inverses is clear (given $a + I$, its additive inverse is $-a + I$), and the multiplicative inverse is $1_R + I$. □

Lemma 2.1 *If R is commutative and $I \subseteq R$ is an ideal, then R/I is commutative.*

Proof: Let $a + I, b + I \in R/I$. Because R is commutative, we see that

$$\begin{aligned}(a + I)(b + I) &= ab + I \\ &= ba + I \\ &= (b + I)(a + I)\end{aligned}$$

as desired. □

Here are examples of quotient rings:

- Consider $\mathbb{Z}$, and $n \in \mathbb{Z}$. By considering the ideal $I = (n)$, we see that the quotient ring is none other than $\mathbb{Z}/n$.
- Consider $R = F[x, y]$, where F is a field. Consider the ideal $I = (x, y)$. We note that $R/I \cong F$, because $x, y \equiv 0 \mod I$.

- Consider $R = \mathbb{R}[x]$ and $I = (x^2 + 1)$. Note that $x^2 + 1$ is irreducible. By considering long division of polynomials, we observe all polynomials $p \in \mathbb{R}[x]$ can be written $p(x) = q(x)(x^2+1)+r(x)$, where $\deg(r) < \deg(x^2+1) = 2$. Therefore, each congruence class modulo I can be represented by $(ax + b) + I$.

  We moreover note that $x^2 \equiv -1 \mod I$, which should remind us of the complex numbers. In fact, R/I is isomorphic to the complex numbers: consider $\phi : \mathbb{C} \to R/I$ given by $ai + b \mapsto ax + b + I$.

Given a ring R and an ideal $I \subseteq R$, there is a natural map from $R \to R/I$ that takes each ring element to its congruence class modulo I. It turns out that this map is a homomorphism, with kernel precisely I.

Definition 2.16 *Let R be a ring and $I \subseteq R$ an ideal. Consider the map $\pi : R \to R/I$ such that $\pi(r) = r + I$. We refer to this map as the canonicalprojection from R onto R/I.*

Theorem 2.6 *Let R be a ring and $I \subseteq R$ an ideal. The canonical projection $\pi : R \to R/I$ is a surjective homomorphism with $\ker(\pi) = I$.*

Proof: We first note that π is surjective, because given $r + I \in R/I$, we have $\pi(r) = r + I$.
To see that R is a ring homomorphism, we note the following:

- $\pi(1_R) = 1_R + I$, and we note $1_R + I$ is the multiplicative identity for R/I.
- To see that addition and multiplication are respected, take $a, b \in R$. We have

$$\begin{aligned} \pi(a) + \pi(b) &= a + I + b + I \\ &= a + b + I \\ &= \pi(a + b) \end{aligned}$$

  and

$$\begin{aligned} \pi(a)\pi(b) &= (a + I)(b + I) \\ &= ab + I \\ &= \pi(ab)\,. \end{aligned}$$

Finally, we show that $\ker(\pi) = I$. We first observe that given $r \in I$, we have $\pi(r) = r + I$. We note that $r + I = I$, because $r \equiv 0 \mod I$, which implies that $r \in \ker(\pi)$.
Now, take $r \in \ker(\pi)$. We observe that $\pi(r) = 0 + I$. By definition, we have $\pi(r) = r + I$, and so, we have $r \equiv 0 \mod I$, or in other words, $r \in I$. □

Remark 2.6 *The theorem above tells us that every ideal in a ring can be realized as the kernel of some homomorphism. Moreover, we have previously shown that the kernel of any ring homomorphism is an ideal. Therefore, we can think of ideals and kernels as two ways to look at the same thing.*

Theorem 2.7 (First Isomorphism Theorem) *Let $f : R \to S$ be a ring homomorphism. The following hold:*

1. *There is a unique homomorphism $\overline{f} : R/\ker(f) \to S$ such that $f = \overline{f} \circ \pi$.*
2. *$R/\ker(f) \cong Im(f)$.*

Proof:

1. We define $\overline{f} : R/\ker(f) \to S$ such that $\overline{f}(r + \ker(f)) = f(r)$. We must show that 1) $\overline{f}$ is well defined, 2) $\overline{f}$ is a homomorphism, and 3) $f = \overline{f} \circ \pi$, and that $\overline{f}$ is the unique homomorphism that satisfies this property.

   To show well definition, we must show that given $r + \ker(f), r' + \ker(f) \in R/\ker(F)$, if $r + \ker(f) = r' + \ker(f)$, then $f(r) = f(r')$. Indeed, if $r + \ker(f) = r' + \ker(f)$, then $r - r' \in \ker(f)$. This implies that $f(r) - f(r') = f(r - r') = 0_S$, which implies $f(r) = f(r')$, as desired.

   We now show that $\overline{f}$ is a homomorphism. First, observe that $\overline{f}(1_R + \ker(f)) = f(1_R) = 1_S$. To see that addition and multiplication are respected, take $a + \ker(f), b + \ker(f) \in R/\ker(f)$. Indeed, we see that

$$\begin{aligned}\overline{f}(a + \ker(f)) + \overline{f}(b + \ker(f)) &= f(a) + f(b) \\ &= f(a + b) \\ &= \overline{f}(a + b + \ker(f))\end{aligned}$$

   and

$$\begin{aligned}\overline{f}(a + \ker(f))\overline{f}(b + \ker(f)) &= f(a)f(b) \\ &= f(ab) \\ &= \overline{f}(ab + \ker(f))\end{aligned}$$

   as desired.

   Finally, we note that $f = \overline{f} \circ \pi$, because $\overline{f} \circ \pi(a) = \overline{f}(pi(a)) = \overline{f}(a + \ker(f)) = f(a)$.

   To see that $\overline{f}$ is the unique map that satisfies this property, take a homomorphism $g : R/\ker(f) \to S$ such that $g \neq \overline{f}$. This means that there is $a + I$ such that $f(a + I) \neq g(a + I)$. We observe that $g \circ \pi(a) = g(\pi(a)) = g(a + \ker(f)) \neq f(a)$, which means $(g \circ \pi)(a) \neq f(a)$, so $g \circ \pi \neq f$. Therefore, $\overline{f}$ is the unique map with the property such that $f = \pi \circ \overline{f}$.

2. We will show that $Im(f)$ is the image of $\overline{f}$, and that $\overline{f}$ is injective. This implies that if we restrict the codomain of $\overline{f}$ to $Im(f)$, then $\overline{f}$ is an isomorphism.

   It is clear that $\overline{f}$ and f share the same image; because $f = \overline{f} \circ \pi$, we have $Im(f) \subseteq Im(\overline{f})$, and by construction, we have $Im(\overline{f}) \subseteq Im(f)$. We also note that $\overline{f}$ is injective: if $\overline{f}(a + \ker(I)) = 0$, then $f(a) = 0$, which implies $a \in \ker(I)$.

□

One of the neat things about the theorem above is that it tells us that a homomorphism $f : R \to S$ factor through the quotient ring $R/\ker(f)$. In fact, using the same idea, we can extend this result as follows:

Theorem 2.8 *Let $f : R \to S$ be a ring homomorphism, and suppose $I \subseteq R$ is an ideal such that $I \subseteq \ker(f)$. Then there is a unique homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \pi$.*

Proof: Homework! [Hint: the idea really is the same as the proof of the first isomorphism theorem.] □

Given a ring R and an ideal I, one may wonder how the ideals of R and R/I relate. In this setting, it makes sense to look at ideals of R that contain I, rather than any old ideal of R. The following theorem tells us how ideals of R/I corresponds with ideals of R that contain I.

Theorem 2.9 (Correspondence Theorem) *Let R be a ring, $I \subseteq R$ an ideal, and $\pi : R \to R/I$ be the canonical projection onto R/I. We abbreviate $\overline{R} = R/I$.*

1. *There is a bijective correspondence between the ideals of of R containing I and the ideals of $\overline{R}$, given by $J \mapsto \pi(J)$ and $\bar{J} \mapsto \pi^{-1}(J)$.*
2. *If an ideal $J \subseteq R$ containing I corresponds to an ideal $\overline{J} \subseteq \overline{R}$ (i.e., $\pi(J) = \overline{J}$), then $R/J \cong \overline{R}/\overline{J}$.*

Proof:

1. We must prove that given an ideal $J \subseteq R$ containing I and an ideal $\overline{J} \subseteq \overline{R}$, the set $\pi(J)$ is an ideal of $\overline{R}$ and $\pi^{-1}(\overline{J})$ is an ideal of R. We must also prove $\pi^{-1}(\pi(J)) = J$ and $\pi(\pi^{-1}(\overline{J})) = \overline{J}$.

   To see $\pi(J)$ is an ideal of $\overline{R}$, take $a+I \in \pi(J)$ and $r+I \in \overline{R}$. We observe that $(a+I)(r+I) = ar+I$, and because $ar \in J$, it follows that $ar+I \in \pi(J)$. Similarly, $(r+I)(a+I) = ra+I \in \pi(J)$.

   To see $\pi^{-1}(\overline{J})$ is an ideal of R, take $a \in \pi^{-1}(J)$ and $r \in R$. We wish to show that $ar \in \pi^{-1}(J)$. To see this, we note that $\pi(ar) = ar+I = (a+I)(r+I) \in \overline{J}$, which implies $ar \in \pi^{-1}(J)$. We can similarly show that $ra \in \pi^{-1}(J)$

   It remains to prove $\pi^{-1}(\pi(J)) = J$ and $\pi(\pi^{-1}(\overline{J})) = \overline{J}$, which will be left for homework.

2. Consider the canonical projection $\phi : \overline{R} \to \overline{R}/\overline{J}$. We note that because ϕ and π are both surjective, their composition $\phi \circ \pi : R \to \overline{R}/\overline{J}$ must be as well. By the first isomorphism theorem, we see that $R/\ker(\phi \circ \pi) \cong \overline{R}/\overline{J}$. It remains to show that $\ker(\phi \circ \pi) = J$, which will be left for homework.

□

Now that we've discussed quotient rings and how they relate with their "ground" ring, let's talk about how we deal with quotients involving more than one ideal. Recall that when discussing modular arithmetics, we used the Chinese remainder theorem to relate congruence classes when considering relatively prime integers. We can extend the same idea to rings as well.

Theorem 2.10 (Chinese Remainder Theorem for rings) *Let R be a commutative ring, $a, b \in R$, and $I, J \subseteq R$ be ideals such that $I + J = R$. We can find $x \in R$ such that*

$$\begin{aligned} x &\equiv a \mod I \\ x &\equiv b \mod J\,. \end{aligned}$$

Moreover, if y also satisfies the above, then $y \equiv x \mod I \cap J$.

Proof: Because $I + J = R$, we can find $i \in I$ and $j \in J$ such that $i + j = 1$. Observe that $i \equiv 1 \mod J$ and $j \equiv 1 \mod I$.
Consider $x = bi + aj$. Because $i \equiv 1 \mod J$ and $j \equiv 1 \mod I$, we observe that

$$\begin{aligned} x &= bi + aj \\ &\equiv aj \mod I \\ &\equiv a \mod I \end{aligned}$$

and

$$\begin{aligned} x &= bi + aj \\ &\equiv bi \mod J \\ &\equiv b \mod J \end{aligned}$$

as desired.
Now, suppose y is another solution to the above. This implies $y \equiv x \mod I$ and $y \equiv x \mod J$. Therefore, $y - x \in I$ and $y - x \in J$, so $y - x \in I \cap J$ (i.e., $y \equiv x \mod I \cap J$). □
In fact, we can relate the quotient ring with respect to I, J, and $I \cap J$ in the following way:

Theorem 2.11 (Chinese Remainder Theorem: the isomorphism) *Let R be a ring, and let $I, J \subseteq R$ be ideals such that $I + J = R$. The quotient rings $(R/I) \times (R/J)$ and $R/(I \cap J)$ are isomorphic.*

Proof: Consider $f : R \to (R/I) \times (R/J)$ given by $f(r) = (r + I, r + J)$.
We first show that f is a homomorphism. Starting off, we note that $1_R \mapsto (1_R + I, 1_R + J)$. To see that addition and multiplication are preserved, we observe that given $a, b \in R$, we have:

$$\begin{aligned} f(a) + f(b) &= (a + I, a + J) + (b + I, b + J) \\ &= (a + b + I, a + b + J) \\ &= f(a + b) \end{aligned}$$

and

$$\begin{aligned} f(a)f(b) &= (a + I, a + J)(b + I, b + J) \\ &= (ab + I, ab + J) \\ &= f(ab) \end{aligned}$$

as desired.
Now, we claim that f is surjective. To see this, take $(a + I, b + J) \in (R/I) \times (R/J)$. By the chinese reminder theorem (for rings), we can find $x \in R$ such that $x + I = a + I$ and $x + J = b + J$. Therefore, it follows that $f(x) = (a + I, b + J)$.
Now, we claim that $\ker(f) = I \cap J$. To see this, suppose $f(r) = 0$. This implies $r \in I$ and $r \in J$, which implies $r \in I \cap J$. Conversely, it is clear that if $r \in I \cap J$, then $r \in I$ and $r \in J$, in which case $r + I = I$ and $r + J = J$.
By the first isomorphism theorem on f, we see that $R/I \cap J = R/\ker(f) \cong Im(f) = (R/I) \cap (R/J)$, as desired. □
Unsurprisingly, using the same ideas, we can extend the Chinese remainder theorem to having more than two ideals.

2.4 Prime and Maximal Ideals

We now discuss prime and maximal ideals, which are some of the more important families of ideals for algebraists. These ideals come up all over the place, including algebraic geometry, number theory, and K-theory.
The setting of these ideals are for commutative rings. In particular, all rings in this (sub)section are commutative.

Definition 2.17 *Let R be a commutative ring and let $I \subsetneq R$ be a proper ideal. We say that I is prime if, whenever $ab \in I$ for $a, b \in R$, we either have $a \in I$ or $b \in I$.*

This definition should, in many ways, remind us of prime numbers. In fact, the ideals generated by prime numbers are prime! We will discuss this example, along with some others:

- Consider the integers $\mathbb{Z}$, and $p \in \mathbb{Z}$ to be prime. Then the principal ideal (p) is a prime ideal. To see this, we observe that if $ab \in (p)$, the this means $p|ab$. So, we either have $p|a$ or $p|b$, which translates to either $a \in (p)$ or $b \in (p)$.

  Fact: (p) is a prime ideal if and only if $p \in \mathbb{Z}$ is prime. (Homework!)

- Let R be an integral domain. Then (0) is a prime ideal: if $ab \in (0)$, then $ab = 0$, which implies $a = 0$ or $b = 0$.

- Consider $R = \mathbb{Z}[x]$, the polynomials with integer coefficients. Let $I = (2, x)$ be the set of polynomials with even constant coefficient. To see that I is prime, we first observe that if $p(x)q(x) \in I$, then the constant term of $p(x)q(x)$ must be even. We also observe that the product of the constant terms on $p(x)$ and $q(x)$ yield the constant term on $p(x)q(x)$. Therefore, the constant term of at least one of the $p(x), q(x)$ must be even.

- Consider the ring $R = \mathbb{R}[x, y]$. The ideal (x), which is generated by the variable x, is prime. However, it is not maximal, because it is properly contained in (x, y), which itself is a proper ideal.

One of the nice properties of prime ideals is that quotienting by them yield an integral domain.

Theorem 2.12 *Let R be a commutative ring, and let $I \subsetneq R$ be a proper ideal. The quotient ring R/I is an integral domain if and only if I is prime.*

Proof: Suppose that I is prime. Let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = ab + I = I$. This implies that $ab \in I$, and because I is prime, we have either $a \in I$ or $B \in I$. This implies that $a + I = I$ or $b + I = I$, which shows that R/I is an integral domain, as desired.
Suppose now that R/I is an integral domain, and suppose $ab \in I$. In particular, we observe that $(a + I)(b + I) = ab + I = I$, and because R/I is an integral domain, we must either have $a + I = I$ or $b + I = I$. This implies $a \in I$ or $b \in I$, as desired. □
We now define maximal ideals:

Definition 2.18 *Let R be a commutative ring, and let $I \subsetneq R$ be a proper ideal. We say that I is maximal if, whenever there is an ideal J such that $I \subsetneq J \subseteq R$, we must have $J = R$.*

It turns out that all maximal ideals are prime:

Theorem 2.13 *Let R be a commutative ring and $I \subseteq R$ be a maximal ideal. Then I is prime.*

Proof: Suppose I is maximal. Let $ab \in I$, and suppose $a \notin I$. We will show $b \in I$.
Because $a \notin I$, we can consider $I + (a)$. Because $I \subsetneq I + (a)$, we must have $I + (a) = R$. So, write $1 = x + ar$, for $x \in I$ and $ar \in (a)$.
We observe that $b = bx + abr$. We note that $ab \in I$ and $x \in I$, so we see that $b \in I$, as desired. $\square$
Maximal ideals also have a fun quotienting property, given as follows:

Theorem 2.14 *Let R be a commutative ring, and $I \subsetneq R$ be an ideal. I is maximal if and only if R/I is a field.*

Proof: Suppose I is maximal. Consider nonzero $a + I \in R/I$. We wish to show that $a + I$ has a multiplicative inverse.
To see this, we first note that $a \notin I$, and therefore, we have $I+(a)$ properly contains I, so $I+(a) = R$. We can therefore write $1 = x + ab$, where $x \in I$ and $ab \in (a)$. We note that $ab + I = 1 + I$. From this, we note that $(a + I)(b + I) = ab + I = 1 + I$, so $b + I$ is the multiplicative inverse of $a + I$.
Suppose now that R/I is a field. We wish to show that I is maximal. To do this, it is enough to show that, given $a \in R \setminus I$, $I + (a) = R$.
We note that $a + I$ has an inverse, as R/I is a field. Let $b + I$ be said inverse. We observe that $ab + I = 1 + I$, which implies that $ab - 1 \in I$. So, we can find $x \in I$ such that $ab - 1 = x$, or in other words, $1 = ab - x$. Because $-x \in I$ and $ab \in (a)$, we see that $1 = ab - x \in I + (a)$. This further implies that given any $r \in R$, $r = r \cdot 1 \in I + (a)$, so $I + (a) = R$, as desired.
$\square$

3 Polynomial Rings over Fields

We now shift our focus on a specific family of rings: polynomial rings over fields. Polynomial rings show up in many important contexts in algebra. They also share many similar results to integers. Throughout this section, F will be a field, and we refer to $F[x]$ as the polynomials with coefficients in F.
Recall that given $f \in F[x]$, we can (uniquely) express $f(x) = \sum_{i=0}^{n} a_i x^i$, where the leading term a_n is nonzero.

Definition 3.1 *Let $f, g \in F[x]$. We say that f is an associate of g if there is some nonzero $c \in F$ such that $g = cf$.*

3.1 Déjà vu

Definition 3.2 *Let $f \in F[x]$ be expressed as $f(x) = \sum_{i=0}^{n} a_i x^i$, where $a_n \neq 0$. We say that the degree of f is $\deg(f) = n$. We refer to a_n as the leading coefficient or leading term of f.*
We use the following convention for the zero polynomial: if $f(x) = 0$, we say $\deg(f) = -\infty$.

Proposition 3.1 *Let $f, g \in F[x]$. The following hold:*

1. $\deg(f + g) \leq \max(\deg(f), \deg(g))$.
2. $\deg(fg) = \deg(f) + \deg(g)$.

Definition 3.3 *Let $f \in F[x]$. We say that f is monic if its leading term is 1.*

Just like integers, there is a division algorithm for polynomials:

Theorem 3.1 *Let $f(x), g(x) \in F[x]$ such that $g \neq 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where $\deg(r(x)) < \deg(g(x))$.*

The proof of this theorem mirrors the proof of the division algorithm. We present a sketch of the proof.

Proof: Let $S = \{f(x) - s(x)g(x) | s(x) \in F[x]\}$. We can choose an element $f(x) - s(x)g(x)$ of smallest degree in S. We refer to this element as $r(x)$, and let $q(x) = s(x)$ be the corresponding $s(x)$. By construction, we must have $f(x) = q(x)g(x) + r(x)$.
To see $\deg(r(x)) < \deg(g(x))$, If this is NOT the case, we can find a polynomial $t(x)$ such that $r(x) - t(x)g(x)$ has degree 1 less than $r(x)$. (Why?) We observe that $r(x) - t(x)g(x) \in S$, which contradicts the fact that $r(x)$ was chosen to be of smallest degree.
To see uniqueness, suppose $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$. This implies $g(x)$ divides $r(x) - r'(x)$. (Why?) But $\deg(r - r') < g(x)$, which means we must have $r(x) = r'(x)$. This also forces $q(x) = q'(x)$. (Why?) □
In the same vain as that of the integers, we can define divisibility in the "obvious" sort of way.

Definition 3.4 *Let $f, g \in F[x]$. We say that f divides g (which we write $f|g$) if there is a polynomial $s \in F[x]$ such that $f(x)s(x) = g(x)$. We say that f is a divisor of g.*

Proposition 3.2 *Let $f, g \in F[x]$, $g \neq 0$, and suppose f divides g. Then $\deg(f) \leq \deg(g)$.*

Proof: We can write $g(x) = f(x)s(x)$ for some $s \in F[x]$. From this, we observe $\deg(g) = \deg(f) + \deg(s)$, so $\deg(f) \leq \deg(g)$. □
And with divisors, we also have a notion of "greatest common divisior," which is defined similarly.

Definition 3.5 *Let $f, g \in F[x]$ be polynomials that are not both zero. The greatest common divisor of f and g is the monic polynomial of largest degree that divides f and g. That is, the greatest common divisor d of f and g is monic and satisfies the following:*

1. *$d|f$ and $d|g$.*
2. *If $a|f$ and $a|g$, then $a|d$.*

Notation 3.1 *Given $f, g \in F[x]$, We refer to the greatest common divisor h as (f, g) or $gcd(f, g)$.*

We additionally have the following familiar-looking theorem:

Theorem 3.2 *Let $f, g \in F[x]$, not both zero. We can find $m, n \in F[x]$ such that $f(x)m(x) + g(x)n(x) = d(x)$, where $d = gcd(f, g)$.*

The proof of this is remarkably similar to the proof of the integer version of this theorem. We leave this for the curious reader.

Theorem 3.3 *Let $a, b, c \in F[x]$. Suppose $a(x)|b(x)c(x)$, such that $(a, b) = 1$. Then $a|c$.*

Proof: We can find m and n such that $a(x)m(x) + b(x)n(x) = 1$. We can also find q such that $a(x)q(x) = b(x)c(x)$.
This implies

$$\begin{aligned} c(x) &= a(x)m(x)c(x) + b(x)c(x)n(x) \\ &= a(x)m(x)c(x) + a(x)q(x)n(x) \\ &= a(x)(m(x)c(x) + q(x)n(x)) \end{aligned}$$

so we see that $a|c$. □

3.1.1 Irreducibility

Just as we discussed prime numbers for integers, we now discuss irreducible polynomials.

Definition 3.6 *Let $f \in F[x]$ be nonzero and nonconstant. We say that f is irreducible if its only factors are units and its associates. Otherwise, f is reducible.*

Remark 3.1 *Another way to say that f is reducible is if we can find polynomials $a, b \in F[x]$ of lower degree such that $a(x)b(x) = f(x)$.*

Theorem 3.4 *Let $p \in F[x]$. The following are equivalent:*

1. *$p(x)$ is irreducible.*
2. *If $p|ab$, then $p|a$ or $p|b$.*
3. *If $p = ab$, then either a or b is a unit.*

Proof: To see (1) implies (2), suppose $p \not| b$. Then $(p, b) = 1$, which implies $p|c$.
To see (2) implies (3), suppose $p = ab$. Note that we have $\deg(a), \deg(b) \leq \deg(p)$ Because $p|ab$, we must have $p|ab$ have $p|a$ or $p|b$. Without loss of generality, suppose $p|a$. This implies $\deg(p) \leq \deg(a)$. So, we have $\deg(p) = \deg(a)$, and because we also have $p|a$ and $a|p$, we must have $a(x) = cq(x)$ for $c \in F$ (why?). This implies that b must be a unit, because $p(x) = a(x)b(x) = ab(x)p(x)$.
(3) implies (1) is left as homework. □

Corollary 3.1 *Let $p \in F[x]$ be irreducible. If $p|a_1 \cdots a_n$, then $p|a_i$ for some i.*

In the same way that integers can be uniquely written as a product of primes, polynomials can be uniquely written as a product of irreducibles.

Theorem 3.5 *Let $f \in F[x]$ be nonzero and a non-constant. f can be written as a product of irreducible polynomials. Moreover, if $f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ are two irreducible factorizations, then $n = m$ and there is a permutation σ on $\{1, \cdots, n\}$ such that p_i and $q_{\sigma(i)}$ are associates.*

Proof: [Sketch] To show that all nonzero polynomials, we can, seeking a contradiction, take the set S of all nonzero non-constant polynomials that cannot be written as a product of primes, and suppose it is nonempty. Choose an $f \in S$ of smallest degree. Note: f cannot be irreducible, so we can write $f = ab$, where $\deg(a), \deg(b) < \deg(f)$. But a and b both <u>can</u> be written as a product of irreducibles, so $f = ab$ can as well, a contradiction.
Now, suppose $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$. Without loss of generality, suppose $n \leq m$. We note $p_1 | q_1 q_2 \cdots q_m$, so without loss of generality, let $p_1 | q_1$. Note that p_1 and q_1 are associates as they are both irreducible. (Why?) So, we have $q_1 = c_1 p_1$ where c_1 is a unit, so we have $p_2 \cdots p_n = c_1 q_2 \cdots q_m$. We can continue this process, from which, without loss of generality, we have p_i and q_i being associates. We must then have $n = m$, as otherwise, we have a product of irreducibles resulting in a unit (why is this not possible?). □

3.2 Roots!

Now that we've discussed a bunch of stuff that should look weirdly familiar, we now discuss properties of polynomial rings that don't quite have analogs to integers.

Definition 3.7 *Let $f \in F[x]$. We say that $a \in F$ is a <u>root</u> of f if $f(a) = 0$.*

The existence of roots gives us insight into when polynomials have factors:

Lemma 3.1 *Let $f \in F[x]$, and let $a \in F$ be a root of f. The remainder of $f(x)$ divided by $x - a$ is $f(a)$.*

Proof: We can express $f(x) = (x - a)q(x) + r(x)$, where $\deg(r) < \deg(x - a) = 1$. Therefore, r must be constant.
By plugging in a, we see $f(a) = (a - a)q(a) + r$, so the remainder $r = f(a)$. □

Theorem 3.6 *Let $f \in F[x]$ and $a \in F$. a is a root of f if and only if $x - a$ is a factor of f.*

Proof: Suppose a is a root of f. By the lemma we just proved, remainder of f divide by $x - a$ is $f(a) = 0$, which implies $x - a$ divides f.
Suppose $x - a$ is a factor of f. Then $f(x) = (x - a)q(x)$; plugging in a into f clearly yields 0. □

Corollary 3.2 *Let $f \in F[x]$ such that $\deg(f) = n$. f has at most n roots.*

Proof: Homework! □

3.3 Quotienting by an irreducible

We end our excursion on polynomials with the following results related to the quotienting by an irreducible polynomial.

Proof: Let $p \in F[x]$ be a nonzero non-constant polynomial. The following are equivalent:

1. p is irreducible.
2. (p) is maximal.
3. (p) is prime.

□

Proof: First, we show (1) implies (2). Suppose p is irreducible. Take $a \in F[x] \setminus (p)$. We show that $(p) + (a) = F[x]$. If a is a unit, then this is clear. Otherwise, we note that $(p, a) = 1$. Thus, we can find $c, d \in F[x]$ such that $pc + ad = 1$, which implies $1 \in (p) + (a)$. This would necessitate $(p) + (a) = F[x]$. Thus, there is no intermediate ideal between (p) and $F[x]$, so (p) is maximal.
To see (2) implies (3), note that if (p) is maximal, then it is prime.
To see (3) implies (1), suppose (p) prime, To show that p is irreducible, we show that if $p|ab$, then $p|a$ or $p|b$. If $p|ab$, then $ab \in (p)$, and by primality of (p), we must have $a \in (p)$ or $b \in (p)$. Therefore, $p|a$ or $p|b$. □
Another way of viewing the above theorem is as follows:

Corollary 3.3 *Let $p \in F[x]$ be a nonzero non-constant polynomial. The following are equivalent:*

1. *p is irreducible.*
2. *$F[x]/(p)$ is a field.*
3. *$F[x]/(p)$ is prime.*

Remark 3.2 *Let $p \in F[x]$ be an irreducible with $p(x) = a_0 + a_1x + \cdots + a_nx^n$ ($a_n \neq 0$). The field $F[x]/(p)$ has elements can be expressed in the form $c_0 + c_1x + \cdots + c_nx^n + (p)$, where $c_i \in F$. Moreover, we have $a_0 + a_1x + \cdots + a_nx^n + (p)$ is the zero element. Thus, $F[x]/(p)$ is basically F, but we include a root of p (represented by $x + (p)$).*

4 Integral Domains

We now focus out gaze at a specific family of (commutative) rings: integral domains. In particular, we will study subclasses of integral domains, including Euclidean domains (integral domains with a "division"), principal ideal domains (PIDs; in which all ideals are generated by a singular element), and unique factorization domains (UFD; description somewhat self-explanatory).
We recall that a commutative ring R is an integral domain if, whenever $ab = 0$ for $a, b \in R$, we either have $a = 0$ or $b = 0$.
Before getting started, we make a few definitions.

Definition 4.1 *Let R be an integral domain, and let $a, b \in R$. We say that a and b are associates if there exists a unit c such that $a = bc$.*

Remark 4.1 *The relation that two elements are associates is an equivalence relation. (Homework!)*

We also extend the term "divides" to this more general setting.

Definition 4.2 *Let R be an integral domain, and let $a, b \in R$. We say that a divides b (written as $a|b$) if we can find $q \in R$ such that $aq = b$.*

Definition 4.3 *Let R be an integral domain, and let $p \in R$ be a non-unit. We say p is irreducible if the only divisors of p are units and associates of p.*

Here is another way to think about irreducible elements:

Remark 4.2 *If p is irreducible, this is the same as saying $p = bc$ implies b or c is a unit. This will be for homework.*

We also have a notion called "prime," which, in general, is DIFFERENT (!!) than being irreducible.

Definition 4.4 *Let R be an integral domain, and let $p \in R$ be a non-unit. We say p is prime if, whenever $p|ab$, we either have $p|a$ or $p|b$.*

The natural question now is how do the two notions relate. The following theorem tells us:

Theorem 4.1 *Let R be an integral domain, and let $p \in R$ be prime. Then p is irreducible.*

Proof: Suppose p is prime, and suppose $p = ab$. Naturally, we have $p|ab$, and because p is prime, we either have $p|a$ or $p|b$. Without loss of generality, suppose $p|a$, in which case, we can write $a = pc$ for $c \in R$. This implies $p = ab = pcb$. Cancelling p yields $cb = 1$, so b is a unit, as desired. □
An important thing to note is that, as we will see in the (near) future, irreducible elements MAY NOT BE PRIME!
Consider the following example. Let $R = \mathbb{Z}[\sqrt{-5}]$. It shouldn't be surprising that 2 and 3 are irreducible. However, they are not prime! This is because $3 \cdot 2 = 6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, and $1 \pm \sqrt{5}$ is divisible by neither 2 or 3.
Another question that one may wonder is whether prime elements relate with prime ideals. The question, of course, is yes.

Theorem 4.2 *Let R be an integral domain, and let $p \in R$. Then the principal ideal (p) is a prime ideal if and only if p is prime.*

Proof: Homework! □

Before going into specific integral domains, we discuss an important property that integral domains have — namely, they can be "embedded" into a field.

Notation 4.1 *Let R be an integral domain. We denote R^* as the nonzero elements of R.*

Recall that in order to get $\mathbb{Q}$ from $\mathbb{Z}$, we consider fractions $\frac{a}{b}$ such that $a, b \in \mathbb{Z}$ with $b \neq 0$, and $\frac{a}{b} = \frac{a'}{b'}$ if $ab' = a'b$. We can do the same thing for any integral domain!

Lemma 4.1 *Let R be an integral domain. We denote $S(R) = \{(a, b) | a, b \in R; b \neq 0\}$. The relation $(a, b) \sim (a', b')$ if and only if $ab' = a'b$ forms an equivalence relation.*

Proof: Homework! □

It turns out that we can define addition and multiplication on the equivalence classes as addition and multiplication of representatives. To do this, we first need to make sure addition and multiplication are well defined.

Definition 4.5 *We define addition and multiplication in $S(R)$ by $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b)(c, d) = (ab, cd)$.*

In fact, we can extend these operations to equivalence classes!

Lemma 4.2 *Suppose R is an integral domain. Suppose $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, where $(a, b), (a', b'), (c, d), (c', d') \in S(R)$. Then $(ad, bc) \sim (a'd', b'c')$ and $(ad + bc, bd) \sim (a'd' + b'c', b'd')$.*

Proof: This is a routine computation; We will do it for multiplication and leave addition for homework.

To show $(ad, bc) \sim (a'd', b'c')$, we need to show $adb'c' = a'd'bc$. Indeed, this is true because $ad = bc$ and $a'd' = b'c'$. □

Definition 4.6 *Let R be an integral domain. We note the field of fractions for R to be $Frac(R) = S(R)/\sim$, equipped with addition and multiplication given by $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$ and $[(a, b)][(c, d)] = [(ab, cd)]$, respectively.*

Notation 4.2 *We will refer to $[(a, b)]$ as $\frac{a}{b}$.*

Theorem 4.3 *Let R be an integral domain. $Frac(R)$ forms a field, and R can be viewed as a subring.*

Proof: The ring axioms of $Frac(R)$ are readily checked and will be omitted.

To see that $Frac(R)$ forms a field, observe that given nonzero $\frac{a}{b}$, its multiplicative inverse is $\frac{b}{a}$ (note that $a \neq 0$, as otherwise, $\frac{a}{b} = 0$).

To see that R can be viewed as a subring, consider the homomorphism $f : R \to Frac(R)$ with $r \mapsto \frac{r}{1}$. It is readily checked that f is an injective homomorphism. □

As a sanity check, we should check that given a field F, we have $Frac(F) \cong F$. This will be for homework.

4.1 Euclidean Domains

We now discuss Euclidean domains, which are integral domains that have some sort of "size" function, which we refer to as a norm. This size function provides us context for having a remainder when performing division.

Definition 4.7 *Let R be an integral domain. A norm is a non-negative function $N : R \to \mathbb{Z}$ such that (1) $N(0_R) = 0$, and (2) given $a, b \in R$ with $b \neq 0$, there exists q such that $a = bq + r$ where $r = 0$ or $N(r) < N(b)$.*

Definition 4.8 *We say an integral domain R is a Euclidean domain if there is a norm function $N : R \to \mathbb{Z}$.*

Remark 4.3 *Some authors require norm functions to also satisfy $N(a) \leq N(ab)$ for a, b nonzero. This is not required, because if N does not satisfy this condition, we can construct another norm N', defined by $N'(a) = \min_{r \neq 0} N(ar)$, that does satisfy that property. (Homework!)*

Examples:

- Let F be a field, and consider $N : F \to \mathbb{Z}$ defined by $N(a) = 0$ for all $a \in F$. This gives a norm on F. Note that given $a, b \in F$ and $b \neq 0$, we have $a = b(b^{-1}a)$.
- Let $R = \mathbb{Z}$. The norm $N(a) = |a|$ forms a norm,
- Let F be a field and $R = F[x]$. Consider $N(f) = \begin{cases} \deg(f) & f \neq 0 \\ 0 & f = 0 \end{cases}$. This gives a norm.

One of the important properties of Euclidean domains are as follows:

Theorem 4.4 *Let R be a Euclidean domain, and let $I \subseteq R$ be an ideal. The I is principal.*

Proof: If $I = \{0\}$, then $I = (0)$. Suppose now that I is nonzero. Let d be a nonzero element of I with the smallest nonzero norm. We wish to show that $(d) = I$.
Clearly, we have $(d) \subseteq I$. To see the other inclusion, take $a \in I$. Because d is nonzero, we can find q and r such that $a = qd + r$. Because $a, qd \in R$, we must have $r \in I$. If r is nonzero, then we must have $N(r) < N(d)$. However, this is not possible, because d was chosen to be of smallest norm. Therefore, $a = dq$, so $a \in (d)$, as desired. □
This characterization also gives non-examples of Euclidean domains. Consider the following:

- Let F be a field, and consider the polynomial ring $R = F[x, y]$. R is not a Euclidean domain, because the ideal (x, y) is not principal.

Other non-examples are a bit harder to define. We will see a few later on.
An important property that general Euclidean domains share with the integers is that there is a notion of "greatest common divisor." While this can be defined for general (commutative) rings, they always exist for Euclidean domains.

Definition 4.9 *Let R be a commutative ring, and let $a, b \in R$, with $b \neq 0$. A greatest common divisor of a and b is an element $d \in R$ such that (1) $d|a$ and $d|b$, and (2) whenever there is another $c \in R$ such that $c|a$ and $c|b$, we have $c|d$.*

The reason for why greatest common divisors exist is because all ideals are principal.

Proposition 4.1 *Let R be a Euclidean domain, and let $a, b \in R$, such that $b \neq 0$, and let d be a greatest common divisor of a and b. Then $d' \in R$ is also a greatest common divisor of a and b if and only if d' is an associate of d.*

Proof: Homework! □

Theorem 4.5 *Let R be a Euclidean domain, and let $a, b \in R$ such that $b \neq 0$. Suppose d is such that $(d) = (a, c)$. Then d is a greatest common divisor of a and b.*

Proof: Suppose $(d) = (a, c)$. Because $a, c \in (d)$, we can have that $d|a$ and $d|b$, as desired.
Now, suppose $c|a$ and $c|b$. Because $(d) = (a, c)$, we have $d \in (a, c)$, so we can write $d = ax + by$.
Let c be any divisor of both a and b. Because $c|a$ and $c|b$, we must have $c|d$. □
It turns out that Euclidean domains also have unique factorizations! We will see this fairly shortly, in the next (and bigger) subclass of integral domains.

4.2 Principal Ideal Domains

Definition 4.10 *Let R be an integral domain. We say that R is a principal ideal domain (PID) if every ideal of R is principal. That is, given an ideal $I \subseteq R$, we can find $a \in R$ such that $I = (a)$.*

Remark 4.4 *Recall that all ideals in a Euclidean are principal. Thus, all Euclidean domains are PIDs.*

While not all PIDs are Euclidean domains, it turns out the class of PIDs hold many of the same properties as Euclidean domains.

Theorem 4.6 *Let R be a PID, and let $a, b \in R$, with $b \neq 0$. Let $d \in R$ be such that $(d) = (a, b)$. Then d is a greatest common divisor of R. Moreover, $d' \in R$ is a greatest common divisor of a and b if and only if d' is an associate of d.*

Remark 4.5 *The proof of the above theorem is IDENTICAL to the one given for Euclidean domains. Indeed, the proof for Euclidean domains did not, at all, use anything about norms.*

Let us now discuss some other facts about PIDs.

Proposition 4.2 *Let R be a PID, and let $P \subseteq R$ be a nonzero prime ideal. Then P is maximal.*

Proof: Suppose $P = (p)$ be an ideal, and suppose $P = (p) \subseteq M = (m)$, where M is another ideal. We wish to show that either $M = P$ or $M = R$.
Because $p \in M = (m)$, we have that $p = mr$ for $r \in R$. Because P is prime, we either have $m \in P$ or $r \in P$. If $m \in P$, then we are done, as this would result in $M = (m) \subseteq P$. If $r \in P$, then we can write $r = pt$ for $t \in R$. Therefore, we have $p = mr = mpt$; cancelling out p yields $1 = mt$. This shows m is a unit, so $(m) = R$. □
One important corollary of this result is the following:

Corollary 4.1 *Let R be a commutative ring, and suppose the polynomial ring $R[x]$ is a PID. Then R must be a field.*

Proof: Homework! (Think about the principal ideal (x).) □
Another important thing about PIDs is that, in this setting, we have irreducibles and primes being the same thing!

Proposition 4.3 *Let R be a PID, and let $p \in R$ be irreducible. Then p is prime.*

Proof: Suppose p is irreducible, and consider (p). We wil show that (p) is maximal, and therefore prime.
Suppose $(p) \subseteq I = (a)$. Then because $p \in (a)$, we can write $p = ab$ for some b. This implies a or b is a unit.
If a is a unit, then $I = (a) = R$. On the other hand, if b is a unit, then b and a are associates, and therefore, generate the same ideal. This implies that either $I = R$ or $I = (p)$, so (p) is maximal. □
We now show an important property of PIDs, that we will later use to show unique factorization of elements of a PID.

Definition 4.11 *Let R be an integral domain. We say that R satisfies the ascending chain condition on principal ideals if, whenever we have a chain of inclusions of ideals given by*

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

where each $a_i \in R$, there exists a positive integer n such that for all $m \geq n$, we have $(a_m) = (a_n)$.

Lemma 4.3 *Let R be an integral domain, and let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideal in R. Then their union $\bigcup_j I_j$ is also an ideal.*

Proof: Homework! □

Theorem 4.7 *A PID satisfies the ascending chain condition on principal ideals.*

Proof: Suppose we have an ascending chain of ideals given by

$$(a_1) \subseteq (a_2) \subseteq \cdots .$$

Consider their union, $I = \bigcup_j (a_j)$. We observe that because $I \subseteq R$ is principal, we can represent it as $I = (a)$ for $a \in R$.
Because $a \in R$, we must have $a \in (a_n)$ for some positive n. This further implies $(a) \in (a_m)$ for $m \geq n$.
On one hand, because $a \in (a_m)$, we have $(a) \subseteq (a_m)$. On the other hand, we have $(a_m) \subseteq I = (a)$, because I is constructed as a union of our chain of ideals. Therefore, we have that $(a_m) = (a)$ for every $m \geq n$. In particular, this implies $(a_m) = (a_n)$ for every $m \geq n$. □
In some sense, the ascending chain condition tells us that we can't get ideals that are "arbitrarily big" but not the whole ring.
In more concrete terms, the asceneding chain condition gives us prime factorizations in a PID.

Theorem 4.8 *Let R be an integral domain that satisfies the ascending chain condition on principal ideals. Let $r \in R$ be nonzero and not a unit. We can express r as a product of irreducible elements.*

Proof: If r is irreducible, then we are done.
Suppose r is not irreducible. Seeking a contradiction, suppose r cannot be written as a product of irreducibles. Because r is not irreducible, we can express $r = r_1^1 r_2^1$ such that neither r_1^1 nor r_2^1 are a unit. One of r_1^1 or r_2^1 cannot be a product of irreducibles, because otherwise, r is a product of irreducibles. Suppose it is r_1^1, in which case, we can express $r_1^1 = r_1^2 r_2^2$, where neither r_1, r_2 are units. In turn one of the factors r_1^2 or r_2^2 cannot be a product of irreducibles; suppose it's r_1^2.
We continue this process, from which we have $r_1^1, r_1^2, \ldots$ such that r_1^{i+1} is a proper factor of r_1^i for each i. This yields a chain of principal ideals given by $(r_1^1) \subsetneq (r_1^2) \subsetneq \cdots$. This contradicts the ascending chain condition, which R was assumed to satisfy. □

Corollary 4.2 *Because PIDs satisfy the ascending chain condition on principal ideals, every non-zero and non-unit decomposes as a product of irreducibles. Furthermore, because irreducibles are primes in a PID, every non-zero and non-unit decomposes as a product of primes.*

Theorem 4.9 *Let R be a PID, and let $r \in R$. Then r has a unique prime factorization. That is, if $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ are both prime factorizations of r, then $n = m$, and there is a permutation σ on $1, \ldots, n$ such that for every i, we have that p_i and $q_{\sigma(i)}$ are associates.*

Proof: This is literally the same proof as the uniqueness of prime factorization for integers and polynomials over a field. □

4.3 Unique Factorization Domain

We now discuss unique factorization domains, which are a superset of what the integral domains that we discussed previously.

Definition 4.12 *Let R be an integral domain. We say that R is a unique factorization domain (UFD) if, given a nonzero non-unit $r \in R$, the following hold:*

1. *r can be factored as a product of irreducibles. That is, we can express $r = p_1 p_2 \cdots p_n$, where each p_i is irreducible.*
2. *the factorization of r is unique. That is, if $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ are both prime factorizations of r, then $n = m$, and there is a permutation σ on $1, \ldots, n$ such that for every i, we have that p_i and $q_{\sigma(i)}$ are associates.*

Remark 4.6 *As discussed previously, any PID is a UFD. This is because, as showed above, any nonzero non-unit in a PID can be expressed as a product of primes (which are irreducible).*

The following are examples of UFDs that are not PIDs. We will not prove that they are UFDs right now, but we will see that this is the case later on.

1. Let F be a field. $F[x_1, \cdots, x_n]$ is a UFD. It is not a PID: the ideal (x_1, x_2) is not principal.
2. The ring $\mathbb{Z}[x]$ is a UFD but not a PID. The ideal $(2, x)$ is not principal.
3. Let R be any UFD. It turns out that $R[x]$ is a UFD as well.

It turns out that we also have that in a UFD, every irreducible element is prime.

Theorem 4.10 *Let R be a UFD, and let $r \in R$. The element $r \in R$ is prime if and only if it's irreducible.*

Proof: We know that in any integral domain, all primes are irreducible. It remains to show that that all irreducibles are prime.
Suppose r is irreducible, and suppose $r|ab$. We wish to show that $r|a$ or $r|b$. Because $r|ab$, we can write $ab = rc$ for $c \in R$.
If a is a unit, it is readily checked that $r|b$, because we would then have $rca^{-1} = b$. Similarly, if b is a unit, then $r|a$.
Suppose now that neither a or b are units. We now write $a = p_1 p_2 \cdots p_n$ and $b = q_1 q_2 \cdots q_m$ as factorizations by irreducibles. We note that c is not a unit, as otherwise, we have $r = c^{-1}ab$, which in turn implies r is reducible. So, we also write $c = t_1 \cdots t_s$ as a product of irreducibles. Note that both $p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m$ and $r t_1 \cdots t_s$ are factorizations of ab. Therefore, r (which is irreducible) must be associates with one of the p_i or q_j. If r is associated with some p_i, then $r|a$, and similarly, if r is associated with some q_j, then $r|b$. □

Remark 4.7 *Because (1) UFDs have unique factorization into irreducibles and (2) primes and irreducibles are equivalent in a UFD, we have unique prime factorizations in a UFD.*

Using prime factorizations, one can show that greatest common divisors exist in a UFD.

Theorem 4.11 *Let R be a UFD, and suppose $a, b \in R$. Let $a = up_1^{e_1} \cdots p_n^{e_n}$ and $a = vp_1^{f_1} \cdots p_n^{f_n}$ be prime factorizations, where u and v are units and each p_i is a distinct prime (i.e., the p_i are not associates of each other). For each n, let $m_i = \min(e_i, f_i)$. Then $d = up_1^{m_1} \cdots p_n^{m_n}$ is a greatest common divisor of a and b.*

Proof: It is clear, by construction, that $d|a$ and $d|b$ (because $m_i \leq e_i, f_i$).
Suppose $c|a$ and $c|b$; we wish to show $c|d$. Let $c = wq_1^{g_1} \cdots q_r^{g_r}$ be a prime factorization, where w is a unit and q_i are distinct primes. Because $q_i|c$, we must also have $q_i|a$ and $q_i|b$; this implies that each q_i must divide one of the p_j. Because each p_j is prime, each q_i must be associates with precisely one of the p_j. Without loss of generality, we can assume that $q_i = p_i$ (why?). This implies that we must have $g_i \leq \min(e_i, f_i) = d_i$ for each i, which in turn implies that $c|d$. □
Recall that in order to show that a PID is a UFD, we used (1) the ascending chain condition on principal ideals to show factorizations exist, and (2) the fact that irreducible elements are prime to show uniqueness of factorization. In fact, it turns out that these are the precise conditions needed to show an integral domain in a UFD.

Theorem 4.12 *Let R be an integral domain. R is a UFD if and only if R satisfies the ascending chain condition on principal ideals and irreducible elements of R are prime.*

Proof: Homework! (some of the pieces have already been proven; feel free to cite them.) □

4.4 Gauss's Lemma