Ring Theory Propositions

Jason Sass

May 21, 2023

Propositions/Basic Facts

Proposition 1. $(\mathbb{Z}, +, *)$ *is a commutative ring with unity* $1 \neq 0$.

Proof. Observe that $(\mathbb{Z}, +)$ is an abelian group with additive identity zero. Multiplication of integers is a binary operation on $\mathbb{Z}$ that is associative and commutative. Multiplication is left and right distributive over addition. The multiplicative identity is 1 and $1 \neq 0$. Therefore, $\mathbb{Z}$ is a commutative ring with unity $1 \neq 0$. $\square$

Proposition 2. *The product of two nonzero integers is nonzero.*

Solution. The statement means if a and b are nonzero integers, then $ab \neq 0$.

Thus, we must prove:

$(\forall a, b \in \mathbb{Z})(a \neq 0 \wedge b \neq 0 \rightarrow ab \neq 0)$. $\square$

Proof. Let a and b be arbitrary integers such that $a \neq 0$ and $b \neq 0$. Then either $a > 0$ or $a < 0$, and either $b > 0$ or $b < 0$. Thus, there are 4 cases to consider.

We consider these cases separately.

Case 1: Suppose $a > 0$ and $b > 0$.

The product of two positive integers is positive. Therefore, $ab > 0$. Hence, $ab \neq 0$.

Case 2: Suppose $a > 0$ and $b < 0$.

The product of a positive and negative integer is negative. Therefore, $ab < 0$. Hence, $ab \neq 0$.

Case 3: Suppose $a < 0$ and $b > 0$.

The product of a positive and negative integer is negative. Therefore, $ba < 0$. Since $ba = ab$, then $ab < 0$. Hence, $ab \neq 0$.

Case 4: Suppose $a < 0$ and $b < 0$.

The product of two negative integers is positive. Therefore, $ab > 0$. Hence, $ab \neq 0$.

Thus, in all cases, $ab \neq 0$. $\square$

Proposition 3. $(\mathbb{R}, +, *)$ *is a commutative ring with unity* $1 \neq 0$.

Proof. Observe that $(\mathbb{R}, +)$ is an abelian group with additive identity zero.

We must prove multiplication is a binary operation on $\mathbb{R}$ and that it is associative and commutative.

Multiplication is left and right distributive over addition. The multiplicative identity is 1 and $1 \neq 0$. Therefore, $\mathbb{Z}$ is a commutative ring with unity $1 \neq 0$. $\square$

Proposition 4. *Let $\mathbb{R}[x]$ be the set of all real polynomials in variable x.*
Then $(\mathbb{R}[x], +, *)$ is a ring.

Solution. To prove $\mathbb{R}[x]$ is a ring, we must prove:
1. $(\mathbb{R}[x], +)$ is an abelian group.
2. $(\mathbb{R}[x], *)$ is an associative binary structure.
3. Multiplication distributes over addition.

Thus, we must prove:
1. Addition of polynomials is a binary operation on $\mathbb{R}[x]$.
2. Addition of polynomials is associative and commutative.
3. There exists an additive identity in $\mathbb{R}[x]$.
4. Each polynomial has an additive inverse in $\mathbb{R}[x]$.
5. Multiplication of polynomials is a binary operation on $\mathbb{R}[x]$.
6. Multiplication of polynomials is associative.
7. Multiplication is left distributive over addition.
8. Multiplication is right distributive over addition. $\square$

Proof. We prove addition of polynomials is a binary operation on $\mathbb{R}[x]$.

Let $p(x), q(x) \in \mathbb{R}[x]$.

Since $p(x) \in \mathbb{R}[x]$, then there exists $m \in \mathbb{Z}^+$ such that $a_0, a_1, ..., a_m \in \mathbb{R}$ and $p(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$. Since $q(x) \in \mathbb{R}[x]$, then there exists $n \in \mathbb{Z}^+$ such that $b_0, b_1, ..., b_n \in \mathbb{R}$ and $q(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$. Either $m = n$ or $m \neq n$.

We consider these cases separately.

Case 1: Suppose $m = n$.

Then $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ Observe that

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0) \\ &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + ... + ((a_1 + b_1)x + (a_0 + b_0). \end{aligned}$$

The sum of two real numbers is a real number. Therefore, $a_k + b_k$ is a real number for each $k = 0, 1, ..., n$. Hence, $p(x) + q(x) \in \mathbb{R}[x]$, so $\mathbb{R}[x]$ is closed under addition. Since $p(x) + q(x)$ is a unique real polynomial, then addition is a binary operation on $\mathbb{R}[x]$.

Case 2: Suppose $m \neq n$.

Then either $m < n$ or $m > n$. Without loss of generality, we may assume $m > n$. Let $k = m - n$. Then k is a positive integer. Let $p'(x)$ be a polynomial of degree m with k terms such that $p'(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_{m-(k-2)}x^{m-(k-2)} + a_{m-(k-1)}x^{m-(k-1)}$.

Let $q'(x)$ be a zero polynomial of degree m with k terms such that $q'(x) = 0x^m + 0x^{m-1} + 0x^{m-2} + ... + 0x^{m-(k-1)}$.

Observe that

$$\begin{aligned}
x^m &= x^{n+k} \\
x^{m-1} &= x^{n+k-1} \\
x^{m-(k-2)} &= x^{n+k-(k-2)} = x^{n+2} \\
x^{m-(k-1)} &= x^{n+k-(k-1)} = x^{n+1}.
\end{aligned}$$

Thus, $q'(x) + p'(x) =$.

Then $q(x) = q'(x) + q(x) =$.

The polynomial $q(x) = q'(x) + q(x)$, where $q'(x)$ is the sum of k terms each with zero coefficient. Since

Observe that

$$\begin{aligned}
p(x) + q(x) &= (a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0) \\
&= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + ... + ((a_1 + b_1)x + (a_0 + b_0).
\end{aligned}$$

To prove $p(x) + q(x) \in \mathbb{R}[x$, we must prove there exist a positive integer k such that $\square$

Proposition 5. *The only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself.*

Proof. We prove the only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself.

Let H be an arbitrary subring of $\mathbb{Z}$. Then $H \subset \mathbb{Z}$, by definition of subring. By definition of subring, H must contain the multiplicative identity of $\mathbb{Z}$. Thus, $1 \in H$.

By definition of subring, $(H, +)$ must be an abelian subgroup of $(\mathbb{Z}, +)$. The smallest subgroup containing 1 is the cyclic group generated by 1 under addition. The cyclic group generated by 1 under addition is $\{k * 1 : k \in \mathbb{Z}\} = \{k : k \in \mathbb{Z}\} = \mathbb{Z}$. Hence, the smallest additive subgroup of $\mathbb{Z}$ containing 1 is $\mathbb{Z}$ itself. Thus, every integer must be contained in H, so $\mathbb{Z} \subset H$.

Since $H \subset \mathbb{Z}$ and $\mathbb{Z} \subset H$, then $H = \mathbb{Z}$. Since $\mathbb{Z}$ is a ring, then this implies the only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself. $\square$

Proposition 6. *The only subring of $\mathbb{Z}_n$ is $\mathbb{Z}_n$.*

Proof. We prove the only subring of $\mathbb{Z}_n$ is $\mathbb{Z}_n$ itself.

Let $n \in \mathbb{Z}^+$. Let $(H, +, *)$ be an arbitrary subring of $(\mathbb{Z}_n, +, *)$. Then $H \subset \mathbb{Z}_n$, by definition of subring. By definition of subring, H must contain the same multiplicative identity as $\mathbb{Z}_n$. Thus, $[1] \in H$.

By definition of subring, $(H, +)$ must be an abelian subgroup of $(\mathbb{Z}_n, +)$. The smallest subgroup containing [1] is the cyclic group generated by [1] under addition modulo n. The cyclic group generated by [1] under addition modulo n is $\mathbb{Z}_n$. Thus, the smallest subgroup of $\mathbb{Z}_n$ containing [1] is $\mathbb{Z}_n$ itself. Hence, every element of $\mathbb{Z}_n$ must be contained in H. Thus, $\mathbb{Z}_n \subset H$.

Since $H \subset \mathbb{Z}_n$ and $\mathbb{Z}_n \subset H$, then $H = \mathbb{Z}_n$. Since $\mathbb{Z}_n$ is a ring, then the only subring of $\mathbb{Z}_n$ is $\mathbb{Z}_n$ itself. $\square$

Proposition 7. *Let p be prime. Then $\mathbb{Z}_p$ is a field.*

Proof. For any positive integer p, $\mathbb{Z}_p$ is a commutative ring with unity $[1]$. In particular, for prime p, $\mathbb{Z}_p$ is a commutative ring with unity $[1]$.

We prove $[1]_p \neq [0]_p$. Suppose for the sake of contradiction $[1]_p = [0]_p$. Then $1 \equiv 0 \pmod{p}$, so $p|1$. Since p is an integer, then this implies either $p = 1$ or $p = -1$. Since $p > 0$, then $p \neq -1$, so $p = 1$. But p is prime, so $p > 1$. Hence, $1 > 1$, a contradiction. Therefore, $[1]_p \neq [0]_p$.

Thus, $\mathbb{Z}_p$ is a commutative ring with unity $[1] \neq [0]$.

Observe that $\mathbb{Z}_p = \{[1], [2], ..., [p-1], [p]\} = \{[a]_p : 1 \leq a \leq p, a \in \mathbb{Z}\}$. Let $[a] \in \mathbb{Z}_p$ such that $[a]_p \neq [0]_p$. Observe that $[a]_p = [0]_p$ iff $a \equiv 0 \pmod{p}$ iff $p|a$. Since $[a]_p \neq [0]_p$ and $[a]_p = [0]_p$ iff $p|a$, then $p \not| a$. Since p is prime, then either $p|a$ or $\gcd(p, a) = 1$. Since $p \not| a$, then we conclude $\gcd(p, a) = 1$, so $\gcd(a, p) = 1$. Since $[a]_p$ has a multiplicative inverse in $\mathbb{Z}_p$ iff $\gcd(a, p) = 1$, then $[a]_p$ has a multiplicative inverse in $\mathbb{Z}_p$. Hence, $[a]$ is a unit. Since $[a]$ is arbitrary, then every nonzero element of $\mathbb{Z}_p$ is a unit.

Therefore, $\mathbb{Z}_p$ is a field. □

Proposition 8. *The characteristic of $\mathbb{Z}_p$ for prime p is p.*

Proof. Let p be prime.

To prove p is the characteristic of the field $\mathbb{Z}_p$, we must prove p is the least positive integer such that $p[a] = [0]$ for all $[a] \in \mathbb{Z}_p$.

Since $(\mathbb{Z}_p, +, *)$ is a ring, then $(\mathbb{Z}_p, +)$ is an abelian group of order p. Every group of prime order is cyclic, so $(\mathbb{Z}_p, +)$ is cyclic. Since $\mathbb{Z}_p$ is a field, then there exists a nonzero element in $\mathbb{Z}_p$. Let $[a]$ be an arbitrary element of $\mathbb{Z}_p$.

Either $[a] = [0]$ or $[a] \neq [0]$.

We consider these cases separately.

Case 1: Suppose $[a] \neq [0]$.

Then $[a]$ is a generator of $\mathbb{Z}_p$. Hence, the order of $[a]$ is p. Thus, p is the least positive integer such that $p[a] = [0]$.

Case 2: Suppose $[a] = [0]$.

Then $p[a] = p[0] = [p0] = [0]$.

Thus, in all cases, p is the least positive integer such that $p[a] = [0]$ for every $[a] \in \mathbb{Z}_p$. Therefore, p is the characteristic of $\mathbb{Z}_p$. □

Lemma 9. *The ring of integers has no zero divisors.*

Solution. This statement means there does not exist an integer that is a zero divisor.

We must prove there does not exist an integer that is a zero divisor.

Our domain of discourse is the ring $\mathbb{Z}$.

Define over the set of all integers $\mathbb{Z}$ the predicate:

$p(a) : a$ is a zero divisor which means

$p(a) : a \neq 0 \wedge (\exists b \in \mathbb{Z})(b \neq 0 \wedge ab = 0)$.

We must prove $\neg(\exists a \in \mathbb{Z})(p(a))$.

Observe that

$$\begin{aligned} \neg(\exists a \in \mathbb{Z})(p(a)) &\Leftrightarrow (\forall a \in \mathbb{Z})(\neg p(a)) \\ &\Leftrightarrow (\forall a \in \mathbb{Z})(a = 0 \vee \neg(\exists b \in \mathbb{Z})(b \neq 0 \wedge ab = 0)). \end{aligned}$$

Thus, let a be arbitrary. We must prove $a = 0 \vee \neg(\exists b \in \mathbb{Z})(b \neq 0 \wedge ab = 0)$.

This statement has the form $Q \vee \neg R$, a disjunction, where the statements are

$Q : a = 0$ and

$R : (\exists b \in \mathbb{Z})(b \neq 0 \wedge ab = 0)$.

From logic we know that

$$\begin{aligned} Q \vee \neg R &\Leftrightarrow \neg\neg Q \vee \neg R \\ &\Leftrightarrow \neg Q \rightarrow \neg R. \end{aligned}$$

Thus, to prove $Q \vee \neg R$ we may prove $\neg Q \rightarrow \neg R$. Hence, assume $\neg Q$, that is assume $a \neq 0$.

We must prove $\neg R$.

Thus, we must prove $\neg(\exists b \in \mathbb{Z})(b \neq 0 \wedge ab = 0)$.

We observe that the product of two nonzero integers is nonzero because we already proved that fact.

Thus, $(\forall x, y \in \mathbb{Z})(x \neq 0 \wedge y \neq 0 \rightarrow xy \neq 0)$.

Thus, assume b is an arbitrary integer such that $b \neq 0$. Then $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$. Since $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. Thus, we have $b \neq 0$ and $ab \neq 0$. Hence, this implies the statement $b \neq 0$ and $ab = 0$ is false. Therefore, there does not exist $b \in \mathbb{Z}$ such that $b \neq 0$ and $ab = 0$. Thus, a is not a zero divisor, by definition of zero divisor. Since a is arbitrary, then a is not a zero divisor for all $a \in \mathbb{Z}$, by universal generalization. Therefore, every integer is not a zero divisor. Hence, there does not exist an integer that is a zero divisor. Thus, $\mathbb{Z}$ has no zero divisors. □

Proof. Observe that $\mathbb{Z}$ is a commutative ring. Let a and b be arbitrary nonzero integers. Then $a \neq 0$ and $b \neq 0$. The product of two nonzero integers is nonzero. Thus, $ab \neq 0$. Since $b \neq 0$ and $ab \neq 0$, then there does not exist an integer b such that $b \neq 0$ and $ab = 0$. Therefore, a is not a zero divisor. Since a is arbitrary, then every nonzero integer is not a zero divisor. Hence, there does not exist a nonzero integer that is a zero divisor. Therefore, $\mathbb{Z}$ has no zero divisors. □

Integral Domains

Proposition 10. *The ring of integers is an integral domain.*

Proof. Let $(\mathbb{Z}, +, *)$ be the ring of integers under addition and multiplication. Observe that multiplication of integers is commutative. Observe that the unity of $\mathbb{Z}$ is $1 \neq 0$. Observe that $\mathbb{Z}$ has no zero divisors. Therefore, $\mathbb{Z}$ is an integral domain. □

Lemma 11. *The product of two nonzero rational numbers is nonzero.*

Proof. Let a and b be arbitrary nonzero rational numbers. Then there exist integers m, n, p, q such that $a = \frac{m}{n}$ and $b = \frac{p}{q}$ and $n \neq 0$ and $q \neq 0$. A rational number is zero if and only if its numerator is zero. Since a and b are nonzero rational numbers, then this implies $m \neq 0$ and $p \neq 0$. Observe that $ab = \frac{m}{n}\frac{p}{q} = \frac{mp}{nq}$. The product of two nonzero integers is non zero. Hence, $mp \neq 0$. Therefore, $ab \neq 0$. ☐

Proposition 12. *The ring of rational numbers is an integral domain.*

Proof. Let $(\mathbb{Q}, +, *)$ be the ring of rational numbers. Then $\mathbb{Q}$ is a commutative ring with unity $1 \neq 0$.

To prove $\mathbb{Q}$ is an integral domain we need only show that $\mathbb{Q}$ has no zero divisors.

Let a and b be arbitrary nonzero rational numbers. Then $a \neq 0$ and $b \neq 0$. The product of two nonzero rational numbers is nonzero. Thus, $ab \neq 0$. Since $b \neq 0$ and $ab \neq 0$, then there does not exist a rational number b such that $b \neq 0$ and $ab = 0$. Therefore, a is not a zero divisor. Since a is arbitrary, then every nonzero rational number is not a zero divisor. Hence, there does not exist a nonzero rational number that is a zero divisor. Therefore, $\mathbb{Q}$ has no zero divisors.

Thus, $\mathbb{Q}$ is an integral domain. ☐

Lemma 13. *The product of two nonzero real numbers is nonzero.*

Solution. This statement means: if a is a nonzero real number and b is a nonzero real number, then ab is nonzero.

A basic fact about real numbers is that the product of two real number is zero iff either real number is zero. Thus, $(\forall a, b \in \mathbb{R})(ab = 0 \Leftrightarrow a = 0 \vee b = 0)$. Observe that

$$\begin{aligned} ab = 0 \Leftrightarrow a = 0 \vee b = 0 \quad &\Leftrightarrow \quad ab \neq 0 \Leftrightarrow \neg(a = 0 \vee b = 0) \\ &\Leftrightarrow \quad ab \neq 0 \Leftrightarrow (a \neq 0 \wedge b \neq 0). \end{aligned}$$

☐

Proof. Observe that the product of two real numbers is zero iff either real number is zero. Therefore, for every real number a and b, $ab = 0$ iff either $a = 0$ or $b = 0$. Hence, for every real number a and b, $ab \neq 0$ iff $a \neq 0$ and $b \neq 0$. Thus, for every real number a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. Therefore, the product of two nonzero real numbers is nonzero. ☐

Proposition 14. *The ring of real numbers is an integral domain.*

Proof. Let $(\mathbb{R}, +, *)$ be the ring of rational numbers. Then $\mathbb{R}$ is a commutative ring with unity $1 \neq 0$.

To prove $\mathbb{R}$ is an integral domain we need only show that $\mathbb{R}$ has no zero divisors.

Let a and b be arbitrary nonzero real numbers. Then $a \neq 0$ and $b \neq 0$. The product of two nonzero real numbers is nonzero. Thus, $ab \neq 0$. Since $b \neq 0$ and $ab \neq 0$, then there does not exist a real number b such that $b \neq 0$ and $ab = 0$. Therefore, a is not a zero divisor. Since a is arbitrary, then every nonzero real number is not a zero divisor. Hence, there does not exist a nonzero real number that is a zero divisor. Therefore, $\mathbb{R}$ has no zero divisors.

Thus, $\mathbb{R}$ is an integral domain. $\square$

Proposition 15. *Let $n \in \mathbb{Z}^+$. Then $(n\mathbb{Z}, +, *)$ has a multiplicative identity iff $n = 1$.*

Solution. We must prove: 1. if $n = 1$, then $n\mathbb{Z}$ has a multiplicative identity 2. if $n\mathbb{Z}$ has a multiplicative identity, then $n = 1$. $\square$

Proof. Let $n \in \mathbb{Z}^+$.

Suppose $n = 1$. Then $n\mathbb{Z} = 1\mathbb{Z} = \{1k : k \in \mathbb{Z}\} = \{k : k \in \mathbb{Z}\} = \mathbb{Z}$. Since $\mathbb{Z}$ is a ring with unity 1, then 1 is multiplicative identity of $\mathbb{Z}$. Therefore, 1 is multiplicative identity of $n\mathbb{Z}$, so $n\mathbb{Z}$ has a multiplicative identity.

Conversely, suppose $n\mathbb{Z}$ has a multiplicative identity. Then there exists $e \in n\mathbb{Z}$ such that $ae = a$ for all $a \in n\mathbb{Z}$.

Let $a \in n\mathbb{Z}$. Then there exists $e \in n\mathbb{Z}$ such that $ae = a$.

Since $n \in \mathbb{Z}^+$, then either $n = 1$ or $n > 1$.

Suppose $n > 1$. Then $n \neq 1$. Since $ae = a$, then $0 = ae - a = a(e-1)$. Since $e, a \in n\mathbb{Z}$ and $n\mathbb{Z} \subset \mathbb{Z}$, then $e, a \in \mathbb{Z}$.

The product of two nonzero integers is nonzero. Therefore, for every $x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $xy \neq 0$. Thus, for every $x, y \in \mathbb{Z}$, if $xy = 0$, then either $x = 0$ or $y = 0$. Hence, in particular, if $a(e-1) = 0$, then either $a = 0$ or $e - 1 = 0$. Thus, since $a \in \mathbb{Z}$ and $e - 1 \in \mathbb{Z}$, then either $a = 0$ or $e - 1 = 0$.

Therefore, either $a = 0$ or $e = 1$.

We consider these cases separately.

Case 1: Suppose $e = 1$.

Since $e \in n\mathbb{Z}$, then there exists $k \in \mathbb{Z}$ such that $e = nk$. Thus, $1 = e = nk$. Since there exists $k \in \mathbb{Z}$ such that $1 = nk$, then $n|1$. The only integers that divide 1 are 1 and -1. Since n is a positive integer, then this implies $n = 1$. Thus we have $n \neq 1$ and $n = 1$, a contradiction.

Case 2: Suppose $a = 0$.

Since a is arbitrary, then every $a \in n\mathbb{Z}$ is equal to zero. Since $n = n * 1$, then $n \in n\mathbb{Z}$. Hence, in particular, $n = 0$. Since $n > 1$, then $0 > 1$, a contradiction.

Therefore, in all cases a contradiction occurs if $n > 1$. Thus, n cannot be greater than 1.

Hence, $n = 1$, as desired. $\square$

Proposition 16. *Let $n \in \mathbb{Z}^+$. Then $(n\mathbb{Z}, +, *)$ is an integral domain iff $n = 1$.*

Solution. We must prove: 1. if $n = 1$, then $(n\mathbb{Z}, +, *)$ is an integral domain
2. if $(n\mathbb{Z}, +, *)$ is an integral domain, then $n = 1$. $\square$

Proof. Suppose $n = 1$. Then $n\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, then $n\mathbb{Z}$ is an integral domain.

Conversely, suppose $n\mathbb{Z}$ is an integral domain. Then $n\mathbb{Z}$ is a commutative ring with unity. Thus, $n\mathbb{Z}$ has a multiplicative identity. The ring $n\mathbb{Z}$ has a multiplicative identity iff $n = 1$. Hence, $n = 1$. $\square$

Ideals

Proposition 17. *$(n\mathbb{Z}, +, *)$ is an ideal of $\mathbb{Z}$.*

Proof. Let $n \in \mathbb{Z}^+$. Observe that $(n\mathbb{Z}, +)$ is an abelian subgroup of $(\mathbb{Z}, +)$.

Let $I = n\mathbb{Z}$.

Let $x \in I$. Then $x = nk$ for some $k \in \mathbb{Z}$.

Let $a \in \mathbb{Z}x$. Then $a = rx$ for some $r \in \mathbb{Z}$. Thus, $a = r(nk) = (nk)r = n(kr)$. Since $kr \in \mathbb{Z}$, then $a \in I$, by definition of I. Hence, $a \in \mathbb{Z}x$ implies $a \in I$, so $\mathbb{Z}x \subset I$.

Let $b \in x\mathbb{Z}$. Then $b = xr$ for some $r \in \mathbb{Z}$. Thus, $b = (nk)r = n(kr)$. Since $kr \in \mathbb{Z}$, then $b \in I$, by definition of I. Hence, $b \in x\mathbb{Z}$ implies $b \in I$, so $x\mathbb{Z} \subset I$.

Thus, $\mathbb{Z}I \subset I$ and $I\mathbb{Z} \subset I$.

Therefore, $(I, +)$ is an abelian subgroup of $(\mathbb{Z}, +)$ and $\mathbb{Z}I \subset I$ and $I\mathbb{Z} \subset I$, so I is an ideal of $\mathbb{Z}$. Hence, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. $\square$

Quotient Rings

Proposition 18. *Let I be an ideal in a ring R. Let $a, b \in R$. Then $a - b \in I$ iff $a + I = b + I$.*

Proof. Suppose $a - b \in I$. Then $a \equiv b \pmod{I}$. Since congruence modulo I is an equivalence relation over R, then every element of R is contained in exactly one congruence class. Observe that $a \in a + I$ and $b \in b + I$. Since a and b are congruent, then a and b are in the same congruence class, by definition of equivalence class. Hence, $a + I = b + I$.

Conversely, suppose $a + I = b + I$. Since $b \in b + I$ and $b + I = a + I$, then $b \in a + I$. Hence, $b = a + i$ for some $i \in I$. Thus, $i = -a + b = b - a$, so $b - a \in I$. Therefore, $b \equiv a \pmod{I}$. Since congruence modulo I is an equivalence relation, then $\equiv$ is symmetric. Hence, $b \equiv a \pmod{I}$ implies $a \equiv b \pmod{I}$, so $a \equiv b \pmod{I}$. Thus, $a - b \in I$. $\square$

Fields