MATH 145
Personal Notes

Marcus Chan

Taught by Nicholas Rollick

UW Math '25

Chapter 1: Fundamentals of Set Theory

*note: this assumes knowledge of MATH 147 Chap 1 & 2.

THE SIX FUNDAMENTAL AXIOMS

EXISTENCE + EXTENSIONALITY

EXISTENCE

The Axiom of Existence states that there exists a set with no elements; for this set A, A satisfies $A \& X$ for all sets X.

EXTENSIONALITY

The Axiom of Extensionality states that if two sets have the same elements, they are equal, ie if every element in X is in Y and v.v, $X = Y$.

THE UNIQUENESS OF $\emptyset$

These first 2 axioms can be used to prove the empty set, $\emptyset$, is unique.

Proof. By AoExi, $\emptyset$ exists, so we only need prove its uniqueness.

Now, suppose $\exists X_1, X_2$ such that X_1 & X_2 have no elements.

Then, every element of X_1 is in X_2 and v.v, since they both do not have any elements.

$\therefore X_1 = X_2$ by AoExt, and we are done.

COMPREHENSION

The Axiom Schema of Comprehension states that if $P(X)$ is a property of a set X ($P(X)$ is a statement), then for any set A, there exists a set B such that $X \in B$ if and only if $X \in A$, & $\forall X$ $P(X)$ is true;

ie

$$\forall P(X), A : \exists B = \{X \in A : P(X)\}.$$

*note: A, B are sets of sets!

*AoC is referred to as a "schema" as it actually is a large collection of axioms (1 for every possible $P(X)$.)

Furthermore, we can show this set B is unique.

Proof. The AoC shows B exists, so we need only prove it is unique.

Suppose $\exists B_1, B_2$ such that $B_1 = \{X \in A : P(X)\}$ and $B_2 = \{X \in A : P(X)\}$ for some $A, P(X)$.

Clearly, if $X \in B_1$, $X \in B_2$ also, and vv.

By the AoExt, this implies $B_1 = B_2$. *

PAIR, UNION & THE POWER SET

We need to define other axioms to give us sets other than $\emptyset$. (The first 3 only tell us $\emptyset$ exists!)

PAIR

The Axiom of Pair states that, given any sets A & B, there exists a set C whose elements are exactly A and B;

*again, C is a set of sets!

ie $\forall X : (X = A \lor X = B) \Rightarrow X \in C$.

We can also show C is unique, using the AoExt. Denote $\{A, B\}$ as the set containing A & B, and the shorthand $\{A\}$ for the set $\{A, A\}$.

In combination with the previous 3 axioms, we can create 2 new sets:

① Let $A = B = \emptyset$. Then, the AoP tells us $\{\emptyset, \emptyset\}$, or $\{\emptyset\}$, exists.

② Now, let $A = \emptyset$ & $B = \{\emptyset\}$. Applying AoP once again, we can also deduce $\{\emptyset, \{\emptyset\}\}$ exists.

UNION

The Axiom of Union states that, for any set S, there exists a set U such that, for any set X, $X \in U$ if and only if $X \in A$ for some set $A \in S$;

ie

$$\forall S : \exists U \ni [\forall X : X \in U \Leftrightarrow X \in A, A \in S].$$

Again, using the AoExt, we can show S is unique. Denote $\bigcup S$ to represent the union of elements in S, and $A \cup B$ as shorthand for $\bigcup\{A, B\}$.

We can use the AoP to create larger sets from smaller ones.

POWER SET

The Axiom of Power Set states for any set A, there exists a set $\mathcal{P}$ such that for any set X, $X \in \mathcal{P}$ if and only if $X \subseteq A$;

*$\mathcal{P}$ can also be written as $\mathbb{P}$.

ie

$$\forall A : \exists \mathcal{P} \ni [\forall X : X \in \mathcal{P} \Leftrightarrow X \subseteq A].$$

We can also show $\mathcal{P}(X)$ is unique from the preceding axioms. Denote $\mathcal{P}(A)$ as the power set of A.

Examples:

*note: both $\emptyset$ & A are always elements of $\mathcal{P}(A)$.

① $\mathcal{P}(\emptyset) = \emptyset$

② $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

③ $\mathcal{P}(\{x_1, x_2\}) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_1, x_2\}\}$.

OTHER SET CONSTRUCTIONS

INTERSECTION

1. We do not need any axioms to describe the intersection of two sets.

2. Given two sets A & B, we use the AoC, with $P(x)$ = "$x \in B$". We then define the output set as the intersection between A & B; ie

$$A \cap B = \{ x \in A : x \in B \}.$$

SET DIFFERENCE

Similarly, we can define $A \setminus B$ by letting $P(x)$ = "$x \notin B$" in the AoC, resulting in

$$A \setminus B = \{ x \in A \mid x \notin B \}.$$

CONSTRUCTION OF $\mathbb{N}$

1. We can use the sets we have defined to assign each natural number (and zero) to a set.

2. In particular, we would like $n \in \mathbb{N}$ to correspond to a set with n elements.

ZERO

Since $\emptyset$ is the only set with no elements, we therefore conclude that $0 = \emptyset$.

ONE

Although there are many sets with one element, we define 1 as the set $\{0\}$; ie

$$1 = \{0\} = \{\emptyset\}.$$

THE SUCCESSOR, & DEFINING SUCCESSIVE ELEMENTS

1. The "successor" of any set x is defined to be $x \cup \{x\}$.

2. We can use this to define a method to obtain the next natural number; given any $n \in \mathbb{N}$, we define

$$n+1 = n \cup \{n\}.$$

ORDERED PAIRS

1. Given any two sets X & Y, we define the ordered pair (x, y) to be $(x,y) = \{\{x\}, \{x,y\}\}$

2. We can use the AoExt to show that (x,y) is unique; ie if $x = x'$ & $y = y'$, then $(x,y) = (x', y')$, and vice versa.

Proof Case 1: $x = y$.

Then, $(x,y) = \{\{x,x\}\} = \{x\}$.

Similarly, $(x', y') = \{x'\} = \{x\}$. (proved).

Case 2: $x \neq y$.

Then, $\{x,y\} = \{x', y'\}$, as $\{x,y\} \neq \{x'\}$.

Hence, $\{x\} = \{x'\}$, so $x = x'$.

So $\{x', y'\} = \{x, y'\} = \{x, y\}$; $\therefore y = y'$. (proved).

3. We can use this definition of an ordered pair to create ordered n-tuples for any n;

$$(x_1, x_2 \cdots x_n) = ((x_1, x_2 \cdots x_{n-1}), x_n).$$

(where a 1-tuple is simply the set $\{x_1\}$.)

INDUCTIVE SETS

1. A set I is inductive if

① $0 \in I$; and

② If $n \in I$, then $S(n) = n+1 \in I$.

THE AXIOM OF INFINITY

1. The Axiom of Infinity states that an inductive set exists.

2. We can then define $\mathbb{N}$ using AoI & AoC, resulting in

$$\mathbb{N} = \{ x \in \mathcal{I} : x \in I \ \ \forall I \},$$

where $\mathcal{I}$ is the inductive set defined by AoI, and I is an inductive set.

3. We can also show $\mathbb{N}$ is unique from the AoExt.

4. Next, we can show $\mathbb{N}$ is inductive.

Proof. Since $0 \in I$, where I is an inductive set, $0 \in \mathbb{N}$ also, based on its definition.

Then, suppose $n \in \mathbb{N}$. By defn, this means $n \in I$ for all inductive sets I. For each I, $(n+1)$ must also be it (by defn).

Hence $(n+1) \in \mathbb{N}$ also.

This is enough to prove the claim. ✱

CARTESIAN PRODUCTS

Given any two sets X & Y, we define $X \times Y$ to be

$$X \times Y = \{ w \in \mathbb{P}(\mathbb{P}(X \cup Y)) : w = (x,y),\ x \in X,\ y \in Y. \}$$

Proof. We know $X \times Y = \{ w = (x,y) \in Z : x \in X, y \in Y \}$. But we need to find a set Z that contains (x,y)!

First, $(x,y) = \{\{x\}, \{x,y\}\}$.

Observe $\{x\}, \{x,y\} \subseteq (X \cup Y)$; so $\{x\}, \{x,y\} \in \mathbb{P}(X \cup Y)$.

Similarly, $\{\{x\}, \{x,y\}\} \subseteq \mathbb{P}(X \cup Y)$; hence,

$(x,y) \in \mathbb{P}(\mathbb{P}(X \cup Y))$ $\forall x \in X, y \in Y$.

So, our set $Z = \mathbb{P}(\mathbb{P}(X \cup Y))$.

METHOD OF ORDERING $\mathbb{N}$

Let $m, n \in \mathbb{N}$. We say $m < n$ (ie m is less than n) if $m \in n$.

* note: this is an "order relation" on a set.

Chapter 2: Relations & Functions

RELATIONS

1. Given two sets X & Y, a binary relation from X to Y is a subset of $X \times Y$.

2. More generally, a set R is called a relation if all the elements of R are ordered pairs.

FUNCTIONS

1. A function f is a relation such that if $(a, b_1), (a, b_2) \in f$, then $b_1 = b_2$; ie for any first coordinate in f, there is only one ordered pair with that first coordinate.

2. For any two sets A & B, f is a function from A to B if each $a \in A$ is related to exactly one element $b \in B$. We use the notation $f: A \to B$ to represent this.

TERMINOLOGY

DOMAIN OF R

The domain of a binary relation R, or $\mathrm{dom}(R)$, is the set of all x for which $(x,y) \in R$, for some y.

RANGE OF R

The range of a binary relation R, or $\mathrm{ran}(R)$, is the set of all y for which $(x,y) \in R$, for some x.

FIELD OF R

The field of a binary relation R, or $\mathrm{field}(R)$, is defined to be

$$\mathrm{field}(R) = \mathrm{dom}(R) \cup \mathrm{ran}(R).$$

IMAGE OF A SET UNDER R

The image of a set A under a binary relation R is the set

$$R(A) = \{ b \in \mathrm{ran}(R) : (a,b) \in R, \quad a \in A \}.$$

INVERSE IMAGE OF A SET UNDER R

The inverse image of a set B under a binary relation R is the set

$$R^{-1}(B) = \{ a \in \mathrm{dom}(R) : (a,b) \in R, \quad b \in B \}.$$

INVERSE OF R

The inverse relation R^{-1} of a binary relation R is defined by

$$R^{-1} = \{ z \in \mathrm{ran}(R) \times \mathrm{dom}(R) : z = (b,a), \quad (a,b) \in R \}.$$

COMPOSITION OF R_1 & R_2

Given two relations R_1 & R_2, the composition of R_1 & R_2, or $R_2 \circ R_1$, is defined by

$$R_2 \circ R_1 = \{ z \in \mathrm{dom}(R_1) \times \mathrm{ran}(R_2) : z \in (a,c), \text{ where } \exists b \ni (a,b) \in R_1 \wedge (b,c) \in R_2 \}.$$

INJECTIVITY OF f (1-1)

A function f is injective (ie 1-1) if $\forall x_1, x_2 \in \mathrm{dom}(f)$, $x_1 \neq x_2 : f(x_1) \neq f(x_2)$.

SURJECTIVITY OF f (ONTO)

A function f is surjective (ie onto) if $\mathrm{ran}(f) = B$; ie, $\forall b \in B$, $\exists a \in A \ni f(a) = b$.

BIJECTIVITY OF f (1-1 & ONTO)

A function f is bijective if it is both injective & surjective.

INVERTIBILITY OF f

1. A function f is invertible if f^{-1} exists.

2. We can prove f is injective if and only if f is invertible.

EQUIVALENCE RELATIONS

A relation R on a set A is:

① reflexive if $\forall a \in A$, aRa;

② symmetric if $\forall a, b \in A$, $aRb \Leftrightarrow bRa$;

③ transitive if $\forall a, b, c \in A$, $aRb \wedge bRc \Rightarrow aRc$.

A relation is an equivalence relation if it is reflexive, symmetric & transitive.

EQUIVALENCE CLASSES

Let E be an equivalence relation on a set A. Given an element $a \in A$, the equivalence class of a modulo E is the set

$$[a]_E = \{x \in A : aEx\}.$$

We can prove that:

1) aEb if and only if $[a] = [b]$; and

2) $\neg aEb$ if and only if $[a] \cap [b] = \emptyset$.

(Proof: MATH 147 WA1 Q2a)

PARTITIONS

Given any set A, a partition $\mathcal{P}$ of A is a collection of non-empty sets that satisfy the following:

① $P_1 \cap P_2 = \emptyset \quad \forall P_1, P_2 \in \mathcal{P}$; &

② $\bigcup \mathcal{P} = A$.

Every equivalence relation E on A gives a partition of A. (Proof from above.)

→ Denote $A/E = \{[a]_E : a \in A\}$.

We can prove A/E is a partition of A.

Proof. $[a] \neq \emptyset$ since $a \in [a]$. (as aEa).

Then $\forall a, b \in A$, $[a] \cap [b] = \emptyset$; ie they are disjoint. — ①

Next, $\forall a \in A$, $a \in [a]$. (since E is reflexive).

Hence $\bigcup (E/A) = A$. — ②

① & ② are sufficient to prove the claim. ∎

Then, let $\mathcal{P}$ be a partition on a set A. Let the relation E be such that if $\exists P \in \mathcal{P}$ such that $a_1 \in P$ & $a_2 \in P$, then $a_1 E a_2$.

We can prove E is an equivalence relation.

Proof.

① For any $a \in A$, $\exists P \in \mathcal{P}$ containing a, as $\mathcal{P}$ is a partition. Hence $aEa \ \forall a \in A$; thus E is reflexive.

② For any $a_1, a_2 \in A$ such that $a_1 E a_2$, it must be that $\exists P \in \mathcal{P} \ni a_1 \in P$ & $a_2 \in P$. Thus $a_2 \in P$ and $a_1 \in P$, implying $a_2 E a_1$ also. Hence E is symmetric.

③ Let $a_1, a_2, a_3 \in A$ such that $a_1 E a_2$ and $a_2 E a_3$. Suppose $a_1 \in P_1$ & $a_3 \in P_2$, where $P_1, P_2 \in \mathcal{P}$ & $P_1 \neq P_2$. By definition, $a_2 \in P_1$ and $a_2 \in P_2$. However, this implies $P_1 \cap P_2 \neq \emptyset$, which is a contradiction as $P_1 \neq P_2$. Thus $P_1 = P_2$, implying $a_3 \in P_1$, and so $a_1 R a_3$. Hence E is transitive.

④ As E is symmetric, transitive & reflexive, E is an equivalence relation — and so we are done. ∎

SET OF REPRESENTATIVES

Let E be an equivalence relation on a set A. A set X is a set of representatives for E if X contains exactly one element of each equivalence class;

ie $\forall [a] \in A/E$, $X \cap [a] = \{\alpha\}$ for some $\alpha \in [a]$.

ORDER RELATIONS

PARTIAL ORDERING

A relation R is "antisymmetric" if aRb & bRa implies $a = b$.

A relation "$\preceq$" on a set A is an order relation on A if it is reflexive, antisymmetric and transitive.

We also call $\preceq$ a partial ordering on A.

eg the identity relation R on A, where $R = \{(a,a) : a \in A\}$.

- R is reflexive;
- R is transitive; ($aRb, bRc \Rightarrow a=b, b=c \Rightarrow a=c \Rightarrow aRc$)
- R is antisymmetric. ($aRb, bRa \Rightarrow a=b$.)

A relation R on a set A is "asymmetric" if aRb and bRa cannot be simultaneously true.

For any partial ordering "$\preceq$" on A, we can define a strict ordering "$\prec$" from it by declaring that $\forall a, b \in A$, $a \prec b$ if $a \preceq b$ but $a \neq b$.

TOTAL / LINEAR ORDERING

For any partial ordering "$\preceq$" on A, we say $a, b \in A$ are "comparable" if either $a \preceq b$ or $b \preceq a$.

A total / linear ordering is a partial ordering in which every pair of elements are comparable.

CHAIN

For any partial ordering "$\preceq$" on A, a set $C \subseteq A$ is called a chain if every pair of elements in C are comparable.

LEAST / GREATEST ELEMENT

Let A be a set with a partial ordering "$\preceq$". Let $B \subseteq A$. Then, an element $b \in B$ is a least element of B if $b \preceq b' \ \forall b' \in B$.

Similarly, b is a greatest element of B if $b' \preceq b \ \forall b' \in B$.

MINIMAL / MAXIMAL ELEMENT

Let A be a set with partial ordering "$\preceq$". Let $B \subseteq A$. Then, an element $b \in B$ is a minimal element of B if there are no "smaller" elements of B;

ie if $b' \preceq b$ for some $b' \in B$, then $b = b'$.

Similarly, b is a maximal element of B if there are no "larger" elements of B;

ie if $b \preceq b'$ for some $b' \in B$, then $b = b'$.

Note: a least element is always minimal, but a minimal element may not be a least element.

eg for $a, b \in \mathbb{Z}^+$: let $a \preceq b$ if $\frac{b}{a} \in \mathbb{Z}^+$

Then 1 is a least element, as it divides every +ve integer.

However, $\mathbb{Z}^+ \setminus \{1\}$ no longer has a least element; there is no other integer that divides both 2 & 3.

But there are infinitely many minimal elements; every prime p is minimal, since it is not divisible by any other +ve integers other than 1 and itself.

BOUNDS ON SETS

Suppose A is a set with order relation "$\preceq$". Then, $\alpha \in A$ is a lower bound on $B \subseteq A$ if $\alpha \preceq b \ \forall b \in B$.

Similarly, $\beta \in A$ is an upper bound on B if $b \preceq \beta \ \forall b \in B$.

Then, an element $\alpha \in A$ is the greatest lower bound / infimum if it is the greatest possible lower bound.

Similarly, an element $\beta \in A$ is the lowest upper bound / supremum if it is the lowest possible upper bound.

Chapter 3: Fundamentals of Set Theory II

THE AXIOM OF CHOICE

1. Let $\mathcal{C}$ be a collection of sets, where $\mathcal{C} \neq \emptyset$. Then, the Cartesian product $\prod_{C \in \mathcal{C}} C$ is the set of functions $\alpha : \mathcal{C} \to \bigcup \mathcal{C}$, with the property that $\forall C \in \mathcal{C}$, $\alpha(C) \in C$.

   * note: this defn works for both finite and infinite collections of sets.

2. The Axiom of Choice states every Cartesian product of any non-empty collection of sets is non-empty.

ZORN'S LEMMA

1. ZL states that for any partially ordered set A, with order relation $\preceq$, if every chain in A has an upper bound in A, then A has a maximal element.

2. We can prove Zorn's Lemma is logically equivalent to the Axiom of Choice.

WELL-ORDERING THEOREM

1. A set A with order relation "$\preceq$" is well-ordered if every non-empty subset of A has a least element.

2. Then, the WOT states every non-empty set A has a well-ordering ; ie there exists an order relation $\preceq$ on A such that A is well-ordered (with respect to $\preceq$.)

3. Again, WOP is also logically equivalent to the Axiom of Choice.

CARDINALITY

$\mathbb{D}_1$ Two sets A & B have the same cardinality if there exists a bijection $f: A \to B$, and write $|A| = |B|$.

$\mathbb{D}_2$ Then:

① $|A| = |A| \quad \forall A$;
② $|A| = |B| \iff |B| = |A| \quad \forall A, B$; &
③ $|A| = |B| \wedge |B| = |C| \Rightarrow |A| = |C| \quad \forall A, B, C$.

*shown in A4 Q2.

"$\leq$" ON CARDINALITY

$\mathbb{D}_1$ We say $|A| \leq |B|$ if there is an injective function $f: A \to B$.

$\mathbb{D}_2$ Then, we can prove for any sets A_1, B, A: if $A_1 \subseteq B \subseteq A$, then $|A_1| = |A|$ implies $|B| = |A|$.

Proof. Since $|A_1| = |A|$, $f: A_1 \to A$ is a bijection. Then, let $\{A_n\}$, $\{B_n\}$ be such that $A_0 = A$ & $B_0 = B$, and $A_{n+1} = f(A_n)$ & $B_{n+1} = f(B_n)$ $\forall n \in \mathbb{N}$. We can use induction to prove $A_{n+1} \subseteq A_n$ $\forall n \in \mathbb{N}$.

Next, set $C_n = A_n \setminus B_n$ for some n. Let $C = \bigcup_{n=0}^{\infty} C_n$. Then, if $a \in f(C_n)$, then $a = f(c)$ for some $c \in C_n$. By def^{n}, $c \in A_n$ & $c \notin B_n$, implying $f(c) \in f(A_n) = A_{n+1}$. Similarly, $f(c) \notin f(B_n)$, as if $f(c) = f(b)$ for some $b \in B_n$, then necessarily $c = b$ (as f is injective) and so $c \in B_n$, which is a contradiction.

We now know $f(c) \in A_{n+1} \setminus B_{n+1} = C_{n+1}$; hence $f(C_n) \subseteq C_{n+1}$. On the other hand, if $a \in C_{n+1}$, then $a \in A_{n+1}$ & $a \notin B_{n+1}$, and so $a = f(a')$ for some $a' \in A_n$. Since $a \notin B_{n+1}$, we also know $a' \notin B_n$. Thus $a' \in C_n$, so that $a = f(a') \in f(C_n)$. Therefore $C_{n+1} \subseteq f(C_n)$, which implies $C_{n+1} = f(C_n)$.

Subsequently, if $a \in f(C)$, then $a = f(c)$ for some $c \in C$. Then $c \in C_n$ for some $n \in \mathbb{N}$, implying $a = f(c) \in f(C_n) = C_{n+1}$, proving $a \in \bigcup_{n=1}^{\infty} C_n$. Conversely, if $a \in \bigcup_{n=1}^{\infty} C_n$, then $a \in C_n$ for some $n \in \mathbb{N}$. In particular, since $C_n = f(C_{n-1})$, $a \in f(C_{n-1})$; thus $a = f(c)$ for some $c \in C_{n-1}$, implying $a \in f(C)$. Therefore, since $f(C)$ and $\bigcup_{n=1}^{\infty} C_n$ have the same elements, by extensionality $f(C) = \bigcup_{n=1}^{\infty} C_n$.

Finally, let $D = A \setminus C$. Define $g: A \to B$ by
$$g(x) = \begin{cases} f(x), & x \in C \\ x, & x \in D. \end{cases}$$

If $x \in C$, then $f(x) \in C_n$ for some $n \geq 1$, implying $f(x) \in A_n$. Moreover, since $A_0 \supseteq A_1 \supseteq A_2 \cdots$, we can deduce $f(x) \in A_1$. We also know $A_1 \subseteq B$ by construction, consequently, $f(x) \in B$. Similarly, if $x \in D$, then $x \notin C$. This implies $x \notin C_0$, and hence $x \notin A \setminus B$, so $\neg x \notin B$ (ie $x \in B$.) Therefore, $\forall x \in A$: $g(x) \in B$. (So $g: A \to B$.)

Next, suppose $x_1, x_2 \in A$ such that $g(x_1) = g(x_2)$. If $x_1, x_2 \in C$, then $f(x_1) = f(x_2)$, implying $x_1 = x_2$ since f is injective. If $x_1, x_2 \in D$, then clearly $x_1 = x_2$ also. If $x_1 \in C$ & $x_2 \in D$, then $f(x_1) = x_2$; however $f(x_1) \in C$ whilst $x_2 \in D$, so this is a contradiction. A similar argument also shows $x_1 \in D$ & $x_2 \in C$ leads to a contradiction too. Therefore, $x_1 = x_2$, proving g is injective.

Similarly, let $b \in B$ be arbitrary. If $b \in f(C)$, then $\exists C$ such that $f(c) = b$, so $g(c) = f(c) = b$. If $b \notin f(C)$, then either $b \in C_0$ or $b \in D$. If $b \in D$, $g(c) = b$ trivially, and if $b \in C_0$, then $b \in A \setminus B$, contradicting the assumption that $b \in B$. Therefore $\forall b \in B$, $\exists c \in C$ such that $g(c) = b$. This is sufficient to show g is surjective.

Since g is both injective & surjective, it is also bijective. Therefore $|A| = |B|$, and we are done. ☒

$\mathbb{D}_3$ From here, we can show "$\leq$" behaves like an order relation; ie

① $\forall A, B, C$: $|A| \leq |B| \wedge |C| = |A| \Rightarrow |C| \leq |B|$;
$|A| \leq |B| \wedge |B| = |C| \Rightarrow |A| \leq |C|$;
$|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$.

ie $\leq$ is "transitive".

② (Cantor–Schröder–Bernstein Theorem)
$\forall A, B$: if $|A| \leq |B|$ & $|B| \leq |A|$, then $|A| = |B|$.

ie $\leq$ is "antisymmetric".

Proof. All the results of ① can be proved by noticing $(g \circ f)$ is injective if both f & g are injective.

We now prove ②. Suppose we have injective functions $f: A \to B$ and $g: B \to A$, for some sets A & B. Then $(g \circ f): A \to A$ is also injective. Then, let $X = g(B)$ and $Y = g(f(A))$. Clearly $X \subseteq A$, and since $f(A) \subseteq B$ we get that $Y = g(f(A)) \subseteq g(B) = X$. Additionally, since $(g \circ f)$ is injective, it is also a bijective function from A to $(g \circ f)(A) = Y$. Hence $|Y| = |A|$.

Therefore, $Y \subseteq X \subseteq A$. By the previous proof, $|Y| = |A|$ implies $|X| = |A|$. But since $X = g(B)$, and g is injective, we must have $g: B \to X$ is a bijection. So $|X| = |B|$, implying $|A| = |B|$, which we wanted to show. ☒

$\mathbb{D}_4$ We write $|A| < |B|$ to signify $|A| \leq |B|$ but $|A| \neq |B|$.

$\mathbb{D}_5$ Note that for all sets $B \neq \emptyset$, $|\emptyset| < |B|$.

Proof. Note that the empty relation from $\emptyset$ to B is both vacuously a function and injective, but not surjective (and so not bijective.) This is sufficient to prove the result. ☒

FINITE / INFINITE SETS

A set A is **finite** if it has the same cardinality as some $n \in \mathbb{N}$.
In this case, we write $|A| = n$

We can prove $\forall n \in \mathbb{N}$, there is no injective mapping from n to $X \subset n$.

Proof. Suppose such a mapping exists.
Then by WOP, there exists a least element $n \in \mathbb{N}$ which satisfies this property.
Clearly $n \neq 0$, since there are no proper subsets of 0.
Then, either $(n-1) \in X$ or $(n-1) \notin X$.
If $(n-1) \notin X$, then $X \subseteq (n-1)$.
Subsequently, if $f: n \to X$ is injective, we can define a new injective mapping $g: (n-1) \to X \setminus \{f(n-1)\}$ by $g(k) = f(k)$ $\forall k \in (n-1)$.
* g is the "restriction" of f to the set $n-1$.

Then g is injective as f is, and g maps $(n-1)$ to a proper subset of $(n-1)$, since $X \subseteq (n-1)$.
This contradicts the minimality of n.
On the other hand, if $(n-1) \in X$, we know $(n-1) = f(k)$ for some unique $k \in n$ (since f is injective.)
Then, let $g: (n-1) \to X \setminus \{n-1\}$ by

$$g(i) = \begin{cases} f(i), & i \neq k \\ f(n-1), & i = k. \end{cases}$$

Again, g is injective, and it maps $(n-1)$ to a proper subset of itself, which contradicts the minimality of n.
Thus no such n exists, proving our claim. ◻

UNIQUENESS OF CARDINALITY

For any finite set A, if $|A| = m$ & $|A| = n$, then $m = n$.

Proof. If $m \neq n$, then either $m \subsetneq n$ or $n \subsetneq m$.
However, by the above proof, both cases lead to contradiction.
Hence necessarily $m = n$. ◻

$\mathbb{N}$ IS INFINITE

We can prove $\mathbb{N}$ is infinite, ie not finite.

Proof. Consider $d: \mathbb{N} \to \mathbb{N}$ by $d(n) = 2n$.
Clearly, d is a bijection, but the set of even numbers is a proper subset of all naturals!
Hence $\mathbb{N}$ cannot be finite, as it would lead to a contradiction otherwise. ◻

SUBSETS OF A FINITE SET ARE ALSO FINITE

Let A be a finite set, and $B \subseteq A$.
Then $|B| \leq |A|$, and B is finite also.

Proof. First, let the "inclusion mapping" $\iota: B \to A$ given by $\iota(b) = b$ $\forall b \in B$.
Clearly this mapping is injective, showing $|B| \leq |A|$.
Then, let $|A| = n$ for some $n \in \mathbb{N}$.
If $n = 0$, $|B| = 0$ necessarily, implying $B = \emptyset$.
We consider what happens if $n \geq 1$.
First, let $A = \{a_0, a_1, .. a_{n-1}\}$.
Then, if $B = \emptyset$, we are done. Otherwise, there is a least index i for which $a_i \in B$.
Call this element b_0.
Again, if $B = \{b_0\}$, we are done. Otherwise, $\exists i_1 > i$ such that $a_{i_1} \in B$, and call this element b_1.
Then, if $B = \{b_0, b_1\}$, we are done.
Otherwise, we repeat this procedure until we get B.
Since A is finite, this procedure cannot go on indefinitely; thus $\exists m \in \mathbb{N}$ such that $B = \{b_0, b_1, .. b_{m-1}\}$.
This is sufficient to prove B is finite. ◻

THE IMAGE OF A FINITE SET UNDER A FUNCTION IS ALWAYS FINITE

Let A & B be sets, such that A is finite. Suppose $f: A \to B$ is a function.
Then $f(A)$ is a finite subset of B, & $|f(A)| \leq |A|$.

Proof. Assume $|A| \geq 1$, since the proof is trivial if $A = \emptyset$.
Then $A = \{a_0, a_1, .. a_{n-1}\}$. So $f(A) = \{f(a_0), f(a_1), \dots f(a_{n-1})\}$.
Subsequently, let $b_0 = f(a_0)$, and then find the least index $i_1 > 0$ for which $f(a_{i_1}) \neq f(a_0)$ (if it exists) and set $b_1 = f(a_{i_1})$.
Again, if $\{b_0, b_1\} \neq f(A)$, then we continue this process until it does, since we know $0 < i_1 < i_2 < ..$ cannot surpass $n-1$.
Hence $f(A) = \{b_0, b_1, .. b_{m-1}\}$ for some $m \in \mathbb{N}$, proving the former claim. #
Then, let the function $g: f(A) \to A$ by $g(b_0) = a_0$ & $g(b_k) = a_{i_k}$ $\forall k > 0$.
Clearly g is injective; therefore $|f(A)| \leq |A|$. ◻

THE UNION OF A FINITE COLLECTION OF SETS IS ALSO FINITE

Let A & B be finite sets. Then $|A \cup B| \leq |A| + |B|$, with $|A \cup B| = |A| + |B|$ iff $A \cap B = \emptyset$.

Proof. Let $|A| = m$ and $|B| = n$, ie $A = \{a_0, a_1, .. a_{m-1}\}$ & $B = \{b_0, b_1, .. b_{n-1}\}$.
Then $A \cup B = \{a_0, a_1, .. a_{m-1}, b_0, b_1 .. b_{n-1}\}$, implying $(A \cup B)$ has at most $m+n$ elements.
However, since some elements might be repeated, $|A \cup B|$ might be less than $(m+n)$; hence $|A \cup B| \leq (m+n) = |A| + |B|$. ◻

For any finite collection of sets S, $\bigcup S$ is also finite.

Proof. If $S = \emptyset$, $\bigcup S = \emptyset$, establishing our base case.
Then, assume for some $S = \{A_0, A_1, .. A_{n-1}\}$ the claim holds.
Subsequently, $A_n \cup (\bigcup S)$ is also finite by the above proof, implying the claim also holds for $S = \{A_0, A_1, .. A_n\}$.
By induction, this is sufficient to prove the claim. ✲

THE POWER SET OF A FINITE SET IS ALSO FINITE

For any finite set A, $\mathcal{P}(A)$ is also finite.

Proof. If $A = \emptyset$ (ie $|A| = 0$), then $\mathcal{P}(A) = \{\emptyset\}$, which is finite.
Then, assume for some set $A' = \{a_0, a_1, .. a_{n-1}\}$ for which $|\mathcal{P}(A)|$ is finite.
Subsequently, let $A = A' \cup \{a_n\}$.
Then $\mathcal{P}(A) = \mathcal{B} \cup \mathcal{C}$, where $\mathcal{B} = \{B \in \mathcal{P}(A) : a_n \in B\}$ & $\mathcal{C} = \{C \in \mathcal{P}(A) : a_n \notin C\}$. Clearly $\mathcal{B} \cap \mathcal{C} = \emptyset$.
Subsequently, observe $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{P}(A')|$.
Since $|\mathcal{P}(A')|$ is finite, necessarily $|\mathcal{B}|$ & $|\mathcal{C}|$ also are.
Thus $|\mathcal{P}(A)| = |\mathcal{B}| + |\mathcal{C}|$ is also finite.
By induction, this is sufficient to prove the claim. ◻

COUNTABLE SETS

1. A set A is "countable" if $|A| = |\mathbb{N}|$.

2. A set A is "at most countable" if $|A| \leq |\mathbb{N}|$. — this implies they are either 1) finite; or 2) countable.

3. For any countable set A, there exists a bijection $f: \mathbb{N} \to A$; ie we can write out the elements of A as an infinite sequence;

$$A = \{a_0, a_1, a_2, \dots\}$$

EVERY SUBSET OF A COUNTABLE SET IS AT MOST COUNTABLE

Let $B \subseteq A$. If A is countable, then B is either finite or countable.

Proof. If B is finite we have our conclusion, so suppose B is infinite.

Let k_0 be the smallest index k_0 such that $a_{k_0} \in B$, and set $b_0 = a_{k_0}$.

Then, let k_1 be the smallest index larger than $a_{k_1} \in B$, setting $b_1 = a_{k_1}$.

Subsequently, we continue this process for each $i \in \mathbb{N}$, as since B is infinite, $B \setminus \{b_0, b_1, \dots b_{i-1}\} \neq \emptyset$.

Hence $B = \{b_0, b_1, \dots\} = \{a_{k_0}, a_{k_1}, \dots\}$; so B is a subsequence of A, and we are done. ⁂

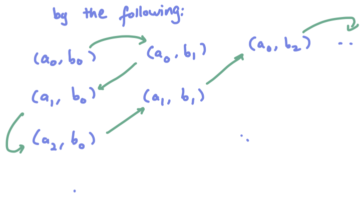
THE CARTESIAN PRODUCT OF COUNTABLE SETS IS COUNTABLE

1. Let A and B be countable sets. Then necessarily $A \times B$ is also countable.

Proof. Since $|A| = |\mathbb{N}| = |B|$, we can represent them as infinite sequences; ie $A = \{a_0, a_1, a_2, \dots\}$ and $B = \{b_0, b_1, b_2, \dots\}$

Then $(a_i, b_j) \in (A \times B)$ $\forall i, j \in \mathbb{N}$.

We can then define a bijection from $\mathbb{N}$ to $A \times B$ by the following:



Since every ordered pair only gets hit "once" in this way, this proves $A \times B$ is countable. ⁂

2. Let $A_0, A_1, \dots A_n$ be finitely many countable sets. Then $\prod_{i=0}^{n} A_i$ is also countable.

Proof. When $n=1$, this is the result above.

Suppose the claim is true for some $n = N$.

Then clearly

$$\prod_{i=0}^{N+1} A_i = \underbrace{\prod_{i=0}^{N} A_i}_{\text{countable (assumption)}} \times \underbrace{A_{N+1}}_{\text{countable}}.$$

Hence $\prod_{i=0}^{N+1} A_i$ is also countable, proving the claim for $n = N+1$.

(By induction, this is sufficient to prove the claim.) ⁂

$\mathbb{Z}$ IS COUNTABLE

We can show that $|\mathbb{Z}| = |\mathbb{N}|$.

Proof. Let $a_k = \begin{cases} -k/2, & k \text{ is even} \\ (k+1)/2, & k \text{ is odd}. \end{cases}$

Then clearly $\{a_k\} = \{0, -1, 1, -2, 2, \dots\}$ $(= \mathbb{Z})$.

So each integer is hit exactly once, so this is a bijection from $\mathbb{N}$ to $\mathbb{Z}$. ⁂

$\mathbb{Q}$ IS COUNTABLE

We can similarly show $|\mathbb{Q}| = |\mathbb{N}|$.

Proof. $\forall q \in \mathbb{Q}$, $q = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ & $b \neq 0$.

Hence every rational number can be associated to an ordered pair (a, b) of integers.

So $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$, and since $\mathbb{Z} \times \mathbb{Z}$ is countable, $\mathbb{Q}$ must be at most countable.

However $\mathbb{Z} \subseteq \mathbb{Q}$, so $|\mathbb{Z}| \leq |\mathbb{Q}|$.

Since $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$, by the Cantor-Bernstein Theorem $|\mathbb{Q}| = |\mathbb{N}|$, as required. ⊠

THE UNION OF COUNTABLE SETS IS COUNTABLE

1. Let A and B be countable sets. Then $A \cup B$ is also countable.

Proof. Again, we can write $A = \{a_0, a_1, a_2, \dots\}$ and $B = \{b_0, b_1, b_2, \dots\}$.

Then, let the sequence $\{c_n\}$ by $c_{2k} = a_k$ & $c_{2k+1} = b_k$ $\forall k \in \mathbb{N}$.

Let $C = \{c_n\}$. It follows that since $A \subseteq A \cup B$ and $A \cup B \subseteq C$ thus

$$|A| \leq |A \cup B| \leq |A| + |B|.$$

However since $|A| = |\mathbb{N}| = |A| + |B|$, by the Cantor-Bernstein-Schröder theorem we must have that $|A \cup B| = \mathbb{N}$, and we are done. ⁂

2. Let $A_0, A_1 \dots A_n$ be a finite collection of countable sets. Then $\bigcup_{i=0}^{n} A_i$ is also countable.

Proof. Again, we can use induction.

If $n=1$, this is just the above result.

Suppose the claim is true for $n = N$.

So

$$\bigcup_{i=0}^{N+1} A_i = \underbrace{\bigcup_{i=0}^{N} A_i}_{\text{countable}} \cup \underbrace{A_{N+1}}_{\text{countable}}$$

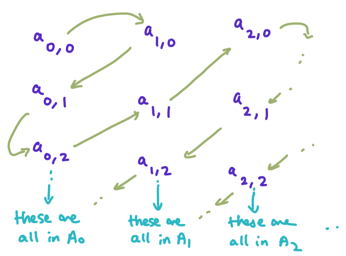
Hence $\bigcup_{i=0}^{N+1} A_i$ is also countable, and so the claim is true for $n = N+1$.

It follows by induction that the claim is true $\forall n \in \mathbb{N}$. ⁂

3. Let $A_0, A_1, A_2 \dots$ be a countable collection of countable sets. Then $\bigcup_{i=0}^{\infty} A_i$ is also countable.

Proof. Let $A_i = \{a_{i,0}, a_{i,1}, a_{i,2}, \dots\}$ for each $i \in \mathbb{N}$.

Then we can define a bijection between the elements of $\bigcup_{i=0}^{\infty} A_i$ and $\mathbb{N}$ by



Hence $\left|\bigcup_{i=0}^{\infty} A_i\right| = |\mathbb{N}|$, and we are done. ⁂

UNCOUNTABLE SETS

$\mathbb{R}$ IS UNCOUNTABLE

First, we prove that the open interval $(0,1)$ has the same cardinality as $\mathbb{R}$;
ie there exists a bijection $f:(0,1)\to\mathbb{R}$.

Proof. Let $f(x)=\frac{1-2x}{x(x-1)}$. We claim $f(x)$ is a bijection.

Suppose $f(a)=f(b)$ for some $a,b\in(0,1)$, $a\neq b$.
Then $\frac{1-2a}{a(a-1)}=\frac{1-2b}{b(b-1)}$.

$\Rightarrow\ 0=(a-b)(a+b-2ab-1)$.

Since $a\neq b$ we get that $a+b-2ab-1=0$.
This implies $ab=a+b-ab-1=-(a-1)(b-1)$.
However $ab>0$ and $-(a-1)(b-1)<0$, since $a,b\in(0,1)$;
thus this is a contradiction; hence f is injective.

Then, suppose $f(x)=r$.
This leads to $r=\frac{1-2x}{x^2-x}$.

$\Rightarrow\ rx^2+(2-r)x-1=0$.

$\therefore\ x=\frac{(r-2)\pm\sqrt{(r-2)^2-4(r)(-1)}}{2r}=\frac{(r-2)\pm\sqrt{r^2+4}}{2r}$.

We claim $0<\frac{(r-2)+\sqrt{r^2+4}}{2r}<1\quad\forall r\in\mathbb{R}\setminus\{0\}$.

Proof: if $r>0$, then $(r-2)+\sqrt{r^2+4}>0$.
Hence $\frac{r-2+\sqrt{r^2+4}}{2r}>0$.

We also can infer $(r-2)+\sqrt{r^2+4}<2r$,
so $\frac{r-2+\sqrt{r^2+4}}{2r}<1$.

There is a similar proof for when $r<0$.
Therefore for any $r\in\mathbb{R}$, there exists an $x\in(0,1)$ such that $f(x)=r$, so $f(x)$ is surjective (and hence bijective). ▨

We can now prove $\mathbb{R}$ is uncountable.

Proof. We can prove $\mathbb{R}$ is uncountable if we show $(0,1)$ is uncountable, so we will do so.

Suppose $\mathbb{R}$ is countable. Then we can write out all the real numbers in a list:

$0.\,b_{11}\,b_{12}\,b_{13}\,b_{14}\,\cdots$
$0.\,b_{21}\,b_{22}\,b_{23}\,b_{24}\,\cdots$
$0.\,b_{31}\,b_{32}\,b_{33}\,b_{34}\,\cdots$
$0.\,b_{41}\,b_{42}\,b_{43}\,b_{44}\,\cdots$

Subsequently, we take the diagonal "digits" of each number (circled in purple), and construct a number $r=0.c_1c_2c_3\ldots$ by $c_i=\begin{cases}4, & b_{ii}\neq 4\\ 5, & b_{ii}=4.\end{cases}$

Then, by definition, $r\neq r_i\ \forall i\in\mathbb{N}$, as r differs from r_i in the i^{th} decimal place.
So $|\mathbb{R}|>|\mathbb{N}|$, showing $\mathbb{R}$ is uncountable. ▨

$\mathcal{P}(\mathbb{N})$ IS ALSO UNCOUNTABLE, AND $|\mathcal{P}(\mathbb{N})|=|\mathbb{R}|$

We can also show $|\mathcal{P}(\mathbb{N})|=|\mathbb{R}|$, proving $\mathcal{P}(\mathbb{N})$ is also uncountable.

Proof. Again, we can just prove $\mathcal{P}(\mathbb{N})$ has the same cardinality as the interval $(0,1)$.
by the following:

Then, let $f:(0,1)\to\mathcal{P}(\mathbb{N})$
Given a $r\in(0,1)$, with decimal expansion $r=0.b_1b_2b_3\ldots$,
let $f(r)=\{10^{n-1}b_n:\ n\in\mathbb{N}^+\}$.

eg $r=\frac{1}{3}$. $f(r)=\{3,30,300,\ldots\}$

We claim f is injective.

Proof. Suppose $f(r)=f(s)$, for $r,s\in(0,1)$.
Let $r=0.b_1b_2b_3\ldots$ and $r=0.c_1c_2c_3\ldots$
Then for any $i\in\mathbb{N}^+$, $10^{i-1}b_i\in R$,
so $10^{i-1}b_i\in S$ also.

However:

1) if $b_i\neq 0$, then $10^{i-1}b_i$ is the unique integer between 10^{i-1} and $9\cdot 10^{i-1}$ belonging to R, and a similar statement holds for S.
$\therefore\ 10^{i-1}b_i$ must be the unique integer between 10^{i-1} & $9\cdot10^{i-1}$ as well,
proving $10^{i-1}b_i=10^{i-1}c_i$, so $b_i=c_i$.

2) if $b_i=0$, then $0\in R$, and so there is no integer between 10^{i-1} & $9\cdot10^{i-1}$ in R.
Then since $R=S$, the same holds true for S.
thus $c_i=0$ as well.

Since r and s agree in every decimal place,
$r=s$; hence f is injective.

Next, let $g:\mathcal{P}(\mathbb{N})\to(0,1)$ such that
$\forall A\subseteq\mathbb{N}.\ \ g(A)=0.a_1a_2a_3\cdots$,
where $a_i=\begin{cases}4, & i\in A\\ 5, & i\notin A\end{cases}$

Then $a_i\in(0,1)$ with an unique decimal expansion.
Suppose $A,B\subseteq\mathbb{N}$ such that $g(A)=g(B)$.

$\Rightarrow\ 0.a_1a_2a_3\cdots=0.b_1b_2b_3\cdots$

Then necessarily $a_i=b_i\ \ \forall i\in\mathbb{N}$, implying that if $i\in A$, then $i\in B$, and vice versa.
Hence $A\subseteq B$ & $B\subseteq A$, proving that $A=B$,
so g is injective.

Since there exist injective functions
$f:(0,1)\to\mathcal{P}(\mathbb{N})$ and $g:\mathcal{P}(\mathbb{N})\to(0,1)$,
consequently $|(0,1)|=|\mathcal{P}(\mathbb{N})|$,
and so $|\mathbb{R}|=|\mathcal{P}(\mathbb{N})|$. ▨

Chapter 4: Algebraic Structures

BINARY OPERATION

Let S be a set. A binary operation on S is a function from $S\times S$ to S.

If $*: S\times S \to S$ is a binary operation, we write $a*b$ instead of $*(a,b)$ as the output of $*$.

Examples of binary operations:
① $+, -, \times$ on $\mathbb{Z}$ or $\mathbb{R}$ (NOT $\div$!)
② $\div$ on $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$
③ $\cup$ and $\cap$ on $P(A)$

ASSOCIATIVITY

Let $*$ be a binary operation on S.
Then $*$ is "associative" if $\forall a,b,c\in S$,
we have $(a*b)*c = a*(b*c)$.

We can show if $a_1, a_2 \cdots a_n$ are arbitrary elements in S, with $n\geq 1$, then $a_1 * a_2 * \cdots * a_n$ is well-defined, regardless of the choice of bracketing in the product.

Proof. We let the "standard product" of $a_1, a_2, \cdots, a_n$, denoted as $\langle a_1, a_2, a_3, \cdots, a_n\rangle$, to be defined recursively by $\langle a_1\rangle = a_1$, $\langle a_1, a_2\rangle = a_1 * a_2$, and $\langle a_1, a_2, \cdots, a_n\rangle = \langle a_1, a_2, \cdots, a_{n-1}\rangle * a_n$ $\forall n\geq 3$.

(So $\langle a_1, a_2, a_3\rangle = (a_1 * a_2) * a_3$;
$\langle a_1, a_2, a_3, a_4\rangle = ((a_1 * a_2) * a_3) * a_4$; etc.)

We claim every product of the n elements is equal to the standard product.

If $n=1$ or $n=2$, there is no choice of bracketing; thus the claim holds trivially in these cases.

Then, assume the claim is true for $1, 2, \cdots, n$ elements, and suppose we are given $n+1$ elements of S, eg $a_1, a_2, \cdots, a_{n+1}$.
Subsequently, any product of these elements can be expressed in the form $b*c$, where b is the product of some elements $a_1, a_2, \cdots, a_k$ with $1\leq k\leq n$, and c is the product of the remaining elements $a_{k+1}, \cdots, a_{n+1}$.

But since $b = \langle a_1, a_2, \cdots, a_k\rangle$ and $c = \langle a_{k+1}, a_{k+2}, \cdots a_n\rangle$, we can express $b*c$ by

$$\begin{aligned} b*c &= \langle a_1, a_2, \cdots, a_k\rangle * (\langle a_{k+1}, a_{k+2}, \cdots a_n\rangle * a_{n+1}) \\ &= (\langle a_1, a_2, \cdots, a_k\rangle * \langle a_{k+1}, a_{k+2}, \cdots a_n\rangle) * a_{n+1} \\ &= \langle a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_n, a_{n+1}\rangle \quad \text{(by induction hypothesis).} \end{aligned}$$

Hence the claim is also true for $n+1$.
Therefore, by induction, the claim is true $\forall n\in\mathbb{N}$. ☒

COMMUTATIVITY

Let $*$ be a binary operation on S.
Then $*$ is "commutative" if $\forall a,b\in S$,
we have $a*b = b*a$.

UNITY / IDENTITY

Let $*$ be a binary operation on S.
Then an element $e\in S$ is an "identity" for $*$ if $a*e = e*a = a$ $\forall a\in S$.

CLOSED UNDER $*$

For any binary operation $*$ on a set S, we say that S is "closed under $*$" if $\forall a,b\in S$: $a*b\in S$.

MONOID

Let S be a set with binary operation $*$.
Then S is a "monoid" if $*$ is both associative, and there exists an identity element $e\in S$ with respect to $*$.

* we use the notation "ab" $= a*b$,
and "a^n" $= \underbrace{a\times a\times\cdots\times a}_{n}$, with $a^0 = e$,
where e is the identity element wrt $*$.

We can prove the identity element of any monoid is unique.

Proof. Let S be a monoid which has two identity elements, ie e_1 and e_2.
Then $\forall a\in S$, $ae_1 = e_1a = a$ and $ae_2 = e_2a = a$.
So if $a = e_2$, then $e_2e_1 = e_1e_2 = e_2$,
and if $a = e_1$, then $e_2e_1 = e_1e_2 = e_1$.
Thus $e_1 = e_2$, proving uniqueness. ☒

UNIT & INVERSE

For any monoid S, an element $a\in S$ is called a "unit" of S if there exists some $b\in S$ for which $ab = ba = e$, where e is the identity element of S.

In this case, we call b the "inverse" of a.

* we usually use the notation "a^{-1}" or "$-a$" to denote the inverse of a,
and $a^{-m} = (a^{-1})^m$.

Once again, we can show the inverse of any unit in a monoid S is unique.

Proof. Let S be a monoid, and $a\in S$ be a unit.
Suppose b_1 & b_2 are both inverses of a,
so that $ab_1 = b_1a = e$ and $ab_2 = b_2a = e$.
Hence $b_1 = b_1e = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2$,
proving $b_1 = b_2$, giving the desired uniqueness. ☒

GROUP

$_1$ A set G is called a "group" if G is a monoid, and every element of G is a unit.

$_2$ Hence, a set G with a binary operation is called a group if:

① it is associative, ie $(ab)c = a(bc)$ $\forall a,b,c \in G$;

② there exists an identity, ie $\exists e \in G$ such that $ae = ea = e$ $\forall a \in G$; &

③ every element of G has an inverse, ie $\forall a \in G: \exists b \in G$ such that $ab = ba = e$.

ABELIAN GROUP

$_1$ A group G is further considered "abelian" if the operation $*$ on G is also commutative.

$_2$ Hence, any abelian group G satisfies the 3 properties above, in addition to:

④ it is commutative; ie $\forall a,b \in G: ab = ba$.

EXTRACTING A GROUP FROM A MONOID

Let M be a monoid, and M^* be the set of all units of M.

Then M^* is a group.

Proof. Let $a,b \in M^*$ be arbitrary.

Then by def^n, a^{-1} & b^{-1} exist such that $aa^{-1} = e$ & $bb^{-1} = e$.

Hence
$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1}\\ &= aea^{-1}\\ &= aa^{-1}\\ &= e.\end{aligned}$$

We can similarly show $(b^{-1}a^{-1})(ab) = e$ also.

This implies ab is a unit, with inverse $b^{-1}a^{-1}$.

Hence M^* is "closed" under the binary operation on M.

Subsequently, M^* is also associative & has an identity element, as M has those properties.

Furthermore, since all $a \in M^*$ has an inverse, it implies M^* is a group, and we are done. ∎

MANIPULATING EXPONENTS IN A GROUP

$_1$ Let G be a group, and $g \in G$.

Then $\forall n,m \in \mathbb{Z}$, $g^{n+m} = g^n \cdot g^m$.

Proof. If $n = 0$, $g^{n+m} = g^m$ trivially.

Assume the claim is true for some $n \in \mathbb{N}$ and all $m \in \mathbb{N}$.

Then
$$\begin{aligned}g^{n+1}\cdot g^m &= (g \cdot g^n)\cdot g^m\\ &= g\cdot(g^n \cdot g^m)\\ &= g \cdot g^{n+m}.\end{aligned}$$

If $n+m \geq 0$, then the RHS is the result of multiplying $n+m$ copies of g by one more g, which is $g^{(n+m)+1}$ by definition.

If $n+m = -1$, then the above is equal to $g \cdot g^{-1}$, which is equal to $e = g^0 = g^{(n+m)+1}$.

Lastly, if $n+m \leq -2$, then the RHS is multiplying $|n+m|$ copies of g^{-1} by one copy of g, which results in $|n+m|-1$ copies of g^{-1}, which can again be written as $g^{(n+m)+1}$.

A similar argument holds if $n \in \mathbb{Z}$ and $m \in \mathbb{N}$.

Hence the claim is true $\forall m,n \in \mathbb{Z}$. by induction, so we are done. ∎

$_2$ Similarly, for any group G, if $g \in G$, then $(g^m)^n = g^{mn}$ $\forall m,n \in \mathbb{Z}$.

Proof. If $n = 0$, then $(g^m)^n = (g^m)^0 = e = g^0$, so the claim is true.

Then, if the claim is true for some $n \in \mathbb{N}$, it implies
$$\begin{aligned}(g^m)^{n+1} &= (g^m)^n \cdot (g^m)^1\\ &= g^{mn}\cdot g^m\\ &= g^{m(n+1)},\end{aligned}$$

So the claim is true $\forall m \in \mathbb{Z}$, $n \in \mathbb{N}$.

However, if $n \in \mathbb{Z}^-$, then $(g^m)^n = (g^m)^{-\ell}$ for some $\ell \in \mathbb{N}$.

But since for any $h \in G$, $h^{-\ell} = (h^\ell)^{-1}$,

thus, $(g^m)^{-\ell} = [(g^m)^\ell]^{-1} = (g^{m\ell})^{-1} = g^{-m\ell} = g^{m(-\ell)} = g^{mn}$.

So the claim is true $\forall m,n \in \mathbb{Z}$, and we are done. ∎

$_3$ Lastly, if $g,h \in G$ commute, ie that $gh = hg$, where G is a group, then $(gh)^n = g^n h^n$ $\forall n \in \mathbb{Z}$.

Proof. If $n = 0$, then $(gh)^0 = e = ee = g^0 h^0$, so the claim is true for this value of n.

Then, assume the claim is true for some $n \in \mathbb{N}$.

It follows that
$$\begin{aligned}(gh)^{n+1} &= (gh)^n \cdot (gh)^1\\ &= (g^n h^n)\cdot gh\\ &= g^n (h^n g) h\\ &= g^n (g h^n) h\\ &= g^{n+1} h^{n+1},\end{aligned}$$

so the claim is true $\forall n \in \mathbb{N}$.

Lastly, if $n = -\ell$ for some $\ell \in \mathbb{N}$,

then $(gh)^n = (gh)^{-\ell} = [(gh)^\ell]^{-1} = (g^\ell h^\ell)^{-1} = (h^\ell)^{-1}(g^\ell)^{-1}$

$= h^{-\ell} g^{-\ell} = h^n g^n = g^n h^n$ (since g,h commute).

Hence the claim is true $\forall n \in \mathbb{Z}$, so we are done. ∎

CYCLIC GROUPS

SUBGROUP

Let G be a group, and $g \in G$ be an element. Then
$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ is a group in G,
called the "subgroup of G generated by g".

Proof. We know $\forall g^m, g^n \in \langle g \rangle$, $g^m \cdot g^n = g^{m+n} \in \langle g \rangle$,
so $\langle g \rangle$ is closed under the group operation on G.
Thus, the operation on G restricts to a binary operation on $\langle g \rangle$, and so it is associative by default.
Furthermore, $e = g^0 \in \langle g \rangle$, so an identity exists,
and for a given g^m there exists its inverse $g^{-m} \in \langle g \rangle$
as $g^m \cdot g^{-m} = g^0 = e$.
Hence $\langle g \rangle$ is a group. ▨

CYCLIC GROUP

A group G is called a "cyclic group" if $G = \langle g \rangle$ for some $g \in G$.

In this case, we say that g is a "generator" of G.

THE SET OF INTEGERS MODULO n

For any $n \in \mathbb{Z}^+$, the "set of integers modulo n", denoted by "$\mathbb{Z}/n\mathbb{Z}$", is the set of equivalence classes of $\mathbb{Z}$ under the relation "congruence modulo n", which is defined by:
$a \equiv b \pmod{n}$ if $a - b = kn$, where $k \in \mathbb{Z}$.

* this is also written as $n \mid a-b$.

We can prove that for any $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group.

Proof. Let $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$.
We can define an "addition" operation by
$[a] + [b] = [a+b]$.
why? $\rightarrow$ assume $[a] = [a']$ and $[b] = [b']$.
Then $a - a' = kn$ and $b - b' = \ell n$ for some $k, \ell \in \mathbb{Z}$.
Hence $(a+b) - (a'+b') = (k+\ell)n$,
so $a + b \equiv a' + b' \pmod{n}$.
Thus $[a+b] = [a'+b']$, so this operation is well defined.

Next, $+$ is trivially associative, with an identity $[0]$
and any element $[a] \in \mathbb{Z}/n\mathbb{Z}$ has an inverse $[-a]$.
Moreover, $+$ is commutative, so $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under this operation.

Lastly, since $[a] = a \cdot [1]$ $\forall a \in \{0, 1, \ldots, n-1\}$, $\mathbb{Z}/n\mathbb{Z}$ is cyclic, with generator $[1]$. ▨

ORDER OF AN ELEMENT

Let G be a group. Then, for any $g \in G$, the "order" of g, denoted by $o(g)$, is the smallest integer $n \geq 1$ such that $g^n = e$, if such an integer exists.

If $g^n \neq e$ $\forall n \geq 1$, then we say $o(g) = \infty$.

ORDER OF THE INVERSE OF AN ELEMENT

Let G be a group. Then, for any $g \in G$,
$o(g^{-1}) = o(g)$.

Proof. Case 1: $o(g) = \infty$.
Then $\forall k \geq 1$, $g^k \neq e$.
So $(g^{-1})^k \neq e$ also, so $o(g^{-1}) = \infty$.
Case 2: $o(g) = n$, $n \in \mathbb{N}$.
Then n is the smallest +ve integer such that $g^n = e$.
So $(g^{-1})^n = e$.
If $\exists m < n$ such that $(g^{-1})^m = e$, taking inverses of both sides implies that $g^m = e$, a contradiction.
So $o(g^{-1}) = o(g) = n$. ▨

ORDER OF ELEMENTS IN A FINITE GROUP

If G is a finite group (ie it only has finitely many elements), then every element of G has finite order.

Proof. Let G be a finite group.
Then for any $g \in G$, $g^0, g^1, g^2, \ldots$ cannot contain infinitely many elements, so $\exists m, n \in \mathbb{N}$ such that $g^m = g^n$.
This implies $g^{m-n} = e$, so g has finite order. ▨

CONNECTING ORDER TO SUBGROUPS

Let G be a group, and $g \in G$ such that $o(g) = n$, $n \in \mathbb{N}$.
Then $g^k = g^m$ iff $k \equiv m \pmod{n}$, and $g^k = e$ iff $n \mid k$.

Proof. Suppose $k \equiv m \pmod{n}$.
So $k - m = \ell n$, $\ell \in \mathbb{Z}$.
So $g^{k-m} = g^{\ell n} = (g^n)^\ell = e$, implying that $g^k = g^m$.
Then, suppose $g^k = g^m$.
So $g^{k-m} = e$.
Assume $k - m = nq + r$. This implies
$e = g^{nq+r} = e^n g^r = g^r$, forcing $r = 0$.
So $n \mid (k-m)$, implying that $k \equiv m \pmod{n}$.
If $m = 0$, then $g^k = g^0 = e$ iff $k \equiv 0$, ie iff $n \mid k$. ▨

Let G be a group, and let $g \in G$ with $o(g) = n$.
Then $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, where $e, g, g^2, \ldots, g^{n-1}$ are all distinct.

Proof. Clearly $\{e, g, g^2, \ldots, g^{n-1}\} \subseteq \langle g \rangle$.
Then, suppose $k \in \mathbb{Z}$, and $k \equiv nq + r$.
Since $g^k = g^r$, hence $g^k \in \{e, g, g^2, \ldots, g^{n-1}\}$, so $\langle g \rangle \subseteq \{e, g, g^2, \ldots, g^{n-1}\}$.
Subsequently, each element of $\{e, g, \ldots, g^{n-1}\}$ are distinct,
because if $g^k = g^m$ for some k, m where $0 \leq m < k \leq n-1$,
then $n \mid (k-m)$; this is impossible, so $k = m$,
proving the elements of this set are all distinct. ▨

SUBGROUPS

Let G be a group. Then $H \subseteq G$ is called a "subgroup" of G if H itself is a group (with respect to the binary operation defined on G.)

*note that $\{e\}$ is a subgroup of G, called the "trivial" subgroup of G.

SUBGROUP TEST

Let G be a group, and $H \subseteq G$, $H \neq \emptyset$.

Then H is a subgroup of G iff $\forall a,b \in H$, we have $ab^{-1} \in H$.

Proof. First, suppose H is a subgroup of G.
Then $\forall a,b \in H$, $b^{-1} \in H$ necessarily, and since H is closed wrt the operation on G, we get that $ab^{-1} \in H$, as desired. #

Then, suppose $\forall a,b \in H$, we have $ab^{-1} \in H$.
Since $H \neq \emptyset$, we can deduce that $\forall a \in H$, $aa^{-1} = e \in H$, so H has an identity element.
Then, taking any $b \in H$ and $a = e$, we get that $ab^{-1} = eb^{-1} = b^{-1} \in H$, so each element of H is a unit.
Lastly, since the binary operation on G is associative, necessarily the binary operation on H is also associative.
Therefore H is a group, and since $H \subseteq G$, it follows that H is a subgroup of G. ∎

CENTER

1. For any group G, the "center" of G, denoted as $Z(G)$, is defined to be the set

$$Z(G) = \{ z \in G \mid zg = gz \quad \forall g \in G \}.$$

2. We can show $Z(G)$ is an abelian subgroup of G.

Proof. Since $e \in Z(G)$, $\therefore Z(G) \neq \emptyset$.
Then, suppose $a,b \in Z(G)$. Let $g \in G$ be arbitrary.
Since $bg = gb$ (as $b \in Z(G)$), therefore
$b^{-1}(bg) = b^{-1}gb \Rightarrow g = b^{-1}gb$,
and hence $b^{-1} \in Z(G)$.
It follows that

$$(ab^{-1})g = a(b^{-1}g) = a(gb^{-1})$$
$$= (ag)b^{-1} = (ga)b^{-1} = g(ab^{-1}),$$

and so $ab^{-1} \in Z(G)$, proving $Z(G)$ is a subgroup of G.
Lastly, since $ab = ba$ $\forall a,b \in G$ (by def^{n}), $Z(G)$ is also abelian, so we are done. ∎

3. Note that $Z(G) = G$ iff G is abelian. (So $Z(G)$ is a "measure" of how commutative the group is.)

CONJUGATE

1. For any group G, the "conjugate" of H in G by some $g \in G$ to be the set

$$gHg^{-1} = \{ ghg^{-1} : h \in H \}.$$

2. Once again, we can verify that gHg^{-1} is a subgroup of G.

Proof. Since $H \neq \emptyset$, $\therefore gHg^{-1} \neq \emptyset$ also.
Then, for any $a,b \in gHg^{-1}$, by def^{n}
$a = gh_1g^{-1}$ & $b = gh_2g^{-1}$ for some $h_1,h_2 \in H$.
Hence

$$ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$$
$$= (gh_1g^{-1})(gh_2^{-1}g^{-1})$$
$$= g(h_1h_2^{-1})g^{-1},$$

and since $h_1h_2^{-1} \in H$ (by def^{n}, since H is a subgroup), therefore gHg^{-1} is also a subgroup. ∎

NORMAL

Let G be a group, and H be a subgroup of G. Then H is a "normal subgroup" if all the conjugate subgroups of H are equal to H.

SYMMETRIC GROUPS

1. For any $n \in \mathbb{N}$, the "symmetric group of degree n" is the set of all bijections $f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$, and we denote the set by S_n.

2. We can represent an element $\sigma \in S_n$ as a sort of matrix:

"input"

ie $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$ "output", where $a_i = f(i)$.

3. For any $n \in \mathbb{N}$, $|S_n| = n!$.

Proof. There are n choices for a_1,
$(n-1)$ choices for a_2 (since f is injective)
and so on, until we get that there is 1 choice for a_n.
So the number of permutations of $a_1, a_2, \dots, a_n$ is $n(n-1)\cdots(1) = n!$. ※

4. For $n \geq 3$, S_n is not abelian.

Proof. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 1 & 2 & \cdots & n \end{pmatrix}$.

Then $(\sigma \circ \tau) = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 2 & 1 & \cdots & n \end{pmatrix}$, but $(\tau \circ \sigma) = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 1 & 2 & \cdots & n \end{pmatrix}$,

so $(\sigma \circ \tau) \neq (\tau \circ \sigma)$, so S_n is not abelian. ∎

HOMOMORPHISMS

1 Let G_1 and G_2 be groups.
Then, a function $\phi: G_1 \to G_2$ is a "homomorphism"
if $\forall a, b \in G_1$, we have
$$\phi(ab) = \phi(a) \cdot \phi(b),$$
where "$\cdot$" denotes the binary operation on G_2.

2 Examples:

① The "trivial" homomorphism
$\phi(a) = e_{G_2} \quad \forall a \in G_1$

② "Reduction modulo n" map
$\phi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by
$\phi(m) = [m] \quad \forall m \in \mathbb{Z}$

③ The "exponent" map
$\phi: \mathbb{Z} \to \langle g \rangle, \quad g \in G$
$\phi(m) = g^m \quad \forall m \in \mathbb{Z}$

HOMOMORPHISMS "PRESERVE" THE IDENTITY

Let $\phi: G_1 \to G_2$ be a group homomorphism.
Then $\phi(e_{G_1}) = e_{G_2}$.

Proof. By def^{n},
$\phi(e_{G_1}) = \phi(e_{G_1} \cdot e_{G_1}) = \phi(e_{G_1}) \cdot \phi(e_{G_1})$.
Hence $[\phi(e_{G_1})]^{-1}[\phi(e_{G_1})] = [\phi(e_{G_1})]^{-1}[\phi(e_{G_1})][\phi(e_{G_1})]$
$\Rightarrow e_{G_2} = \phi(e_{G_1})$, as required. ∎

HOMOMORPHISMS "PRESERVE" INVERSES

Let $\phi: G_1 \to G_2$ be a group homomorphism.
Then $\forall g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$.

Proof. For each $g \in G_1$, observe that
$\phi(g) \cdot \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(e_{G_1}) = e_{G_2}$.
Hence $[\phi(g)]^{-1} \cdot \phi(g) \cdot \phi(g^{-1}) = [\phi(g)]^{-1} \cdot e_{G_2}$,
or that $\phi(g^{-1}) = [\phi(g)]^{-1}$. ∎

HOMOMORPHISMS PRESERVE POWERS

Let $\phi: G_1 \to G_2$ be a group homomorphism.
Then $\forall g \in G_1, k \in \mathbb{Z}$, we have $\phi(g^k) = [\phi(g)]^k$.

Proof. We first prove this $\forall k \in \mathbb{N}$ by induction.
when $k=0$, $\phi(g^0) = \phi(e_{G_1}) = e_{G_2} = [\phi(g)]^0$,
establishing our base case.
Then assuming the claim holds for some $k \in \mathbb{N}$,
note that $\phi(g^{k+1}) = \phi(g^k \cdot g) = \phi(g^k) \cdot \phi(g)$
$= [\phi(g)]^k \cdot \phi(g) = [\phi(g)]^{k+1}$,
so the claim holds $\forall k \in \mathbb{N}$.
Subsequently, if $k = -m$ for some $m \in \mathbb{Z}^+$,
then $\phi(g^k) = \phi(g^{-m}) = \phi((g^{-1})^m)$
$= [\phi(g^{-1})]^m = [[\phi(g)]^{-1}]^m = [\phi(g)]^{-m} = [\phi(g)]^k$,
and so this is sufficient to prove the claim holds $\forall k \in \mathbb{Z}$. ∎

THE COMPOSITION OF HOMOMORPHISMS IS A HOMOMORPHISM

Let $\phi: G_1 \to G_2$ and $\psi: G_2 \to G_3$ be group homomorphisms.
Then $(\psi \circ \phi): G_1 \to G_3$ is also a group homomorphism.

Proof. By def^{n},
$\phi(a_1 \cdot_1 a_2) = \phi(a_1) \cdot_2 \phi(a_2) \quad \forall a_1, a_2 \in G_1$,
and $\psi(b_1 \cdot_2 b_2) = \psi(b_1) \cdot_3 \psi(b_2) \quad \forall b_1, b_2 \in G_2$,
where $\cdot_1, \cdot_2$ & $\cdot_3$ are the binary operations on G_1, G_2, and G_3 respectively.
Hence, if we let $b_1 = \phi(a_1)$ and $b_2 = \phi(a_2)$, then
$\psi(\phi(a_1) \cdot_2 \phi(a_2)) = \psi(\phi(a_1)) \cdot_3 \psi(\phi(a_2))$
$\Rightarrow \psi(\phi(a_1 \cdot_1 a_2)) = \psi(\phi(a_1)) \cdot_3 \psi(\phi(a_2))$
$\Rightarrow (\psi \circ \phi)(a_1 \cdot_1 a_2) = (\psi \circ \phi)(a_1) \cdot_3 (\psi \circ \phi)(a_2)$,
verifying that $(\psi \circ \phi)$ is a group homomorphism as well. ∎

KERNEL

1 Let $\phi: G_1 \to G_2$ be a group homomorphism.
Then the "kernel" of ϕ, denoted "$\ker \phi$",
is defined to be the set
$$\ker \phi = \{ g \in G_1 \mid \phi(g) = e_{G_2} \}.$$

2 We can prove that $\ker \phi$ is a subgroup of G_1.

Proof. We apply the Subgroup Test.
First, $\ker \phi$ is non-empty $\because \phi(e_{G_1}) = e_{G_2}$, so $e_{G_1} \in \ker \phi$.
Then, if $a, b \in \ker \phi$, then
$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)[\phi(b)]^{-1} = (e_{G_2})[e_{G_2}]^{-1} = e_{G_2}$,
and so $ab^{-1} \in \ker \phi$ also, verifying that $\ker \phi$ is a subgroup of G_1. ∎

3 Moreover, we can also show that ϕ is injective if and only if $\ker \phi = \{e_{G_1}\}$.

Proof. Assume ϕ is injective.
Let $g \in \ker \phi$ be arbitrary.
Then $\phi(g) = e_{G_2} = \phi(e_{G_1})$, so by injectivity of ϕ, necessarily $g = e_{G_1}$, proving $\ker \phi = \{e_{G_1}\}$.
Then, assume $\ker \phi = \{e_{G_1}\}$.
Suppose there exists $a, b \in G_1$ such that $\phi(a) = \phi(b)$.
Hence $\phi(a) \cdot \phi(b^{-1}) = \phi(b) \cdot \phi(b^{-1})$
$\Rightarrow \phi(ab^{-1}) = e_{G_2}$, implying that $ab^{-1} \in \ker \phi$.
Thus $ab^{-1} = e_{G_1}$, implying that $a = b$.
This is sufficient to prove that ϕ is injective. ∎

COSETS

1 Let G be a group, and H be a subgroup of G.
Then let the relation "$\sim$" on G be such that
$\forall a, b \in G$, we have $a \sim b$ if and only if $ab^{-1} \in H$.

2 We can prove that "$\sim$" is an equivalence relation.

Proof. Since for any $a \in G_1$, $\phi(a \cdot a^{-1}) = \phi(e_{G_1}) = e_{G_2}$,
$a \sim a$; hence $\sim$ is reflexive.
Then, for any $a, b \in G_1$, if $a \sim b$, it implies that $ab^{-1} \in H$; since H is closed under taking inverses,
we get that $(ab^{-1})^{-1} = ba^{-1} \in H$ also, saying that $b \sim a$.
So $\sim$ is also symmetric.
Lastly, if $a \sim b$ & $b \sim c$ for some $a, b, c \in G_1$, it implies that $ab^{-1} \in H$ and $bc^{-1} \in H$.
But since H is closed under multiplication,
hence $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ also, implying that $a \sim c$.
So $\sim$ is transitive (and hence an equivalence relation). ∎

3 Then, for any element $a \in G$,
the "right coset of H generated by a" is defined to be the set
$$Ha = \{ ha : h \in H \},$$
and is the equivalence class of a with respect to "$\sim$".

Proof. $[a] = \{ g \in G : g \sim a \}$
$= \{ g \in G : ga^{-1} \in H \}$
$= \{ g \in G : ga^{-1} = h \text{ for some } h \in H \}$
$= \{ g \in G : g = ha \text{ for some } h \in H \}$
$= Ha$. ∎

4 Similarly, we can define an equivalence relation $\sim_L$ on G such that $\forall a, b \in G$, we have that $a \sim b$ if and only if $b^{-1}a \in H$.
Then, the "left coset of H generated by a" for some $a \in G$ is the set
$$aH = \{ ah : h \in H \},$$
and is an equivalence class of $\sim_L$.

5 Note that if G is abelian,
then $aH = Ha$ for any $a \in G$ and subgroup H.

QUOTIENT GROUPS

NORMAL SUBGROUP

Let G be a group. Then, a subgroup $H \le G$ is called a "normal subgroup" of G if

$gHg^{-1} = \{ghg^{-1} : h \in H\} = H \quad \forall g \in G.$

We use the notation "$H \triangleleft G$" to denote that H is a normal subgroup of G.

MULTIPLICATION OF RIGHT COSETS

Let G be a group. Then, for every subgroup $H \le G$, the formula $(Ha)(Hb) = H(ab)$ gives a well-defined multiplication of right cosets if and only if $H \triangleleft G$.

Proof. First, assume $(Ha)(Hb) = Hab$ for all right cosets of H in G.

Let $g \in G$ and $h \in H$ be arbitrary.

Then clearly $Hh = He$.

So $(Hg)(Hh) = (Hg)(He)$, or $Hgh = Hge$.

By def^{n}, this implies $(gh)(ge)^{-1} = ghg^{-1} \in H \quad \forall g \in G$.

Letting $g^{-1} = g$, we see that $g^{-1}hg \in H$ also,

and hence $gHg^{-1} \le H$ and $g^{-1}Hg \le H$, or $H \le gHg^{-1}$.

Thus $H = gHg^{-1}$, implying $H \triangleleft G$. ✱

Conversely, assume $H \triangleleft G$.

Let $a, b, a_1, b_1 \in G$ be such that $Ha = Ha_1$ and $Hb = Hb_1$.

Then by definition, $aa_1^{-1} \in H$ and $bb_1^{-1} \in H$.

Next, observe that

$ab b_1^{-1} a_1^{-1} = a(bb_1^{-1})a_1^{-1} = (a(bb_1^{-1})a^{-1})(aa_1^{-1})$.

Since $aHa^{-1} = H$ and $bb_1^{-1} \in H$, so $a(bb_1^{-1})a^{-1} \in aHa^{-1} = H$.

But since we assumed $aa_1^{-1} \in H$, thus $(a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in H$

(by closure of multiplication), so $abb_1^{-1}a_1^{-1} \in H$.

But since $abb_1^{-1}a_1^{-1} = (ab)(b_1^{-1}a_1^{-1}) = (ab)(a_1b_1)^{-1} \in H$,

it follows that $(Ha)(Hb) = (Ha_1)(Hb_1)$, and so multiplication of right cosets is well-defined.

QUOTIENT GROUP

Let G be a group, and $H \triangleleft G$.

Then, the "quotient group" of G by H is the set G/H of right cosets of H under the operation $(Ha)(Hb) = Hab$.

We can verify that G/H is a group.

Proof. By the above, we know the binary operation on G/H is well-defined.

Then, notice that for any cosets Ha, Hb & Hc:

$((Ha)(Hb))(Hc) = (Hab)(Hc) = H(ab)c = Ha(bc)$

$= (Ha)(Hbc) = (Ha)((Hb)(Hc))$,

so the operation is associative.

Then the identity of G/H is the coset $H = He$,

and the inverse of the coset Ha is the coset Ha^{-1},

so G/H is indeed a group. ▩

QUOTIENT MAPPING

Let G be a group, and $H \triangleleft G$.

Then the "quotient mapping" is the function $\phi : G \to G/H$ by $\phi(g) = Hg$.

We can show ϕ is surjective, and a group homomorphism.

Proof. By def^{n}, $\phi(ab) = Hab = (Ha)(Hb) = \phi(a)\phi(b)$,

so ϕ is a homomorphism.

Then for any coset $Ha \in G/H$, $\phi(a) = Ha$,

so ϕ is also surjective. ▩

THE QUOTIENT GROUP IS ABELIAN IF THE ORIGINAL GROUP IS ABELIAN

Let G be a group, and $H \triangleleft G$.

Suppose G is abelian. Then G/H is also abelian.

Proof. If G is abelian, then $Hab = Hba$.

So $(Ha)(Hb) = Hab = Hba = (Hb)(Ha)$, implying that G/H is also abelian. ▩

THE QUOTIENT GROUP IS CYCLIC IF THE ORIGINAL GROUP IS CYCLIC

Let G be a group, and $H \triangleleft G$.

Suppose G is cyclic. Then G/H is also cyclic.

Proof. If $G = \langle g \rangle$ for some $g \in G$, then every element of G is in the form g^k for some $k \in \mathbb{Z}$.

So, given any $Ha \in G/H$, we know $a = g^k$ for some $k \in \mathbb{Z}$,

and so $Ha = Hg^k = \phi(g^k) = [\phi(g)]^k = (Hg)^k$, where ϕ is the quotient homomorphism.

Hence $G/H = \langle Hg \rangle$, so it is also cyclic. ▩

ALL SUBGROUPS OF AN ABELIAN GROUP ARE ALSO NORMAL

Let G be an abelian group.

Then all subgroups $H \le G$ are normal.

Proof. Let $g \in G$ be arbitrary.

Then $gHg^{-1} = \{ghg^{-1} : h \in H\} = \{gg^{-1}h : h \in H\} = \{h : h \in H\} = H$,

so H is normal. ▩

EXAMPLE OF A QUOTIENT GROUP: $\mathbb{Q}/\mathbb{Z}$

Consider the group $\mathbb{Q}$, with addition as its binary operation.

Then $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition, and since $\mathbb{Q}$ is abelian, $\mathbb{Z}$ is a normal group.

Hence the quotient group $\mathbb{Q}/\mathbb{Z}$ exists.

Note the elements of $\mathbb{Q}/\mathbb{Z}$ are of the form $\mathbb{Z} + q$, where $q \in \mathbb{Q}$.

In fact, we can further deduce each element of $\mathbb{Q}/\mathbb{Z}$ is uniquely represented by a coset of the form $\mathbb{Z} + \delta$, where $0 \le \delta < 1$.

TORSION

Let G be a group.

Then G is also a "torsion" if every element of G has finite order.

LAGRANGE'S THEOREM

INDEX

Let G be a group, and H be a subgroup of G.

Then, the "index" of H in G, denoted by $|G:H|$, is equal to the number of distinct left cosets of H in G.

* this can be finite or infinite.

* $|G:H|$ is also equal to the number of distinct left cosets of H.

LAGRANGE'S THEOREM

Let G be a finite group, and let H be a subgroup of G.

Then $|G:H| = \frac{|G|}{|H|}$.

Proof. Since the right cosets of H in G forms a partition of G, let $Ha_1, Ha_2, \dots, Ha_n$ denote the collection of distinct right cosets of H in G.

Then, by definition, $\bigcup_{i=1}^{n} Ha_i = G$,

and $Ha_i \cap Ha_j = \emptyset$ if $i \neq j$.

Next, since $f: H \to Ha_i$ by $f(h) = ha_i$ is a bijection, consequently $|H| = |Ha_i|$.

Hence $|Ha_1| = |Ha_2| = \dots = |Ha_n|$.

It follows that $|G| = |Ha_1| + |Ha_2| \dots + |Ha_n|$
$= n|H|$

and so $n = |G:H| = \frac{|G|}{|H|}$. ∎

o(g) DIVIDES |G|

Let G be a finite group.

Then, for any $g \in G$, $o(g)$ divides $|G|$.

Proof. Note $H = \langle g \rangle$ is a subgroup of G, and that $|H| = o(g)$.

Since $|H|$ divides $|G|$, thus $o(g)$ divides $|G|$ also. ∎

$|G| = n \Rightarrow g^n = e$

Let G be a finite group, with $|G| = n$.

Then $\forall g \in G$, we have $g^n = e$.

Proof. Let $g \in G$ be arbitrary.

Then, necessarily $o(g)$ divides n, so $n = k\ell$, where $k = o(g)$, and $\ell \in \mathbb{Z}$.

Hence $g^n = g^{k\ell} = (g^k)^\ell = e^\ell = e$, as needed. ∎

EVERY GROUP WITH A PRIME NUMBER OF ELEMENTS IS CYCLIC

Suppose G is a group with $|G| = p$, where p is a prime number.

Then for any non-identity element $g \in G$, $G = \langle g \rangle$;

ie G is cyclic.

Proof. Since $p \geq 2$, there exists a non-identity element $g \in G$.

Let $H = \langle g \rangle$. Then $|H| > 1$, since $o(g) > 1$.

But since $|H|$ must divide $|G|$ by Lagrange's Theorem, and $|G| = p$ only has 1 and p as positive divisors, it follows that $|H| = p = |G|$, so $G = H = \langle g \rangle$, showing that G is cyclic. ∎

RINGS

1 A ring is a set R equipped with two binary operations (usually denoted by addition and multiplication) that satisfy the following:

① R is an abelian group wrt the binary operation "+", with identity "0";

② R is a monoid wrt the binary operation "·", with identity "1"; and

③ Left & right distributive laws hold; ie $\forall a,b,c \in R$, $a(b+c) = ab+ac$ & $(a+b)c = ac+bc$.

$\forall a,b,c \in R$:

① $(a+b)+c = a+(b+c)$

② $\exists 0 \in R$ such that $a+0=0+a=a$

③ $\exists (-a) \in R$ such that $a+(-a) = (-a)+a = 0$

④ $a+b = b+a$.

⑤ $(ab)c = a(bc)$

⑥ $\exists 1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$

⑦ $(a+b)c = ac+bc$

⑧ $a(b+c) = ab+ac$

2 If multiplication in R is commutative, ie $ab = ba$ $\forall a,b \in R$, then we call R a "commutative ring".

PROPERTIES OF RINGS

UNIQUENESS OF IDENTITIES AND INVERSES

Let R be an arbitrary ring. Then:

① the additive and multiplicative inverses of R are unique; and

② for any $a \in R$, its additive inverse is unique, and usually denoted $-a$.

* these follow from previous theorems.

ADDITIVE IDENTITY IN MULTIPLICATION

Let R be a ring, with additive identity 0.

Then $\forall a \in R$, $a \cdot 0 = 0 \cdot a = 0$.

Proof. Since 0 is the additive identity, hence $0+0=0$.

So, by distributivity,

$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$.

Adding $-(a \cdot 0)$ to both sides yields

$0 = a \cdot 0$, as needed.

(The proof that $0 \cdot a = 0$ is similar.)

ADDITIVE INVERSES AND MULTIPLICATION

Let R be a ring, and $a,b \in R$ be arbitrary.

Then,

① $(-a)b = a(-b) = -(ab)$; and

② $(-a)(-b) = ab$.

Proof. By distributivity,

$(-a)b + ab = (-a+a)b = 0b = 0$,

and by commutativity of addition $ab + (-a)b = 0$ also.

This implies $(-a)b$ is the additive inverse of ab, and so $(-a)b = -(ab)$.

The proof that $a(-b) = -(ab)$ is similar. #

Then, note $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$,

as ab is the unique additive inverse of $-ab$. ▨

CHARACTERISTIC

Let R be a ring. Then, the "characteristic of R", denoted as "char R", is the order of the multiplicative identity 1 in the group R under addition, if this order is finite.

If it is not, we deduce char $R = 0$.

CHARACTERISTICS AND MULTIPLICATION

1 Let R be a ring with char $R \neq 0$.

Then $k \cdot r = \underbrace{r+r+\cdots+r}_{k \text{ times}} = 0$ $\forall r \in R$

if and only if $n \mid k$ (ie n divides k).

Proof. Let $k \in \mathbb{Z}$ such that $n \mid k$, and let $r \in R$ be arbitrary.

Then $k = mn$ for some $m \in \mathbb{Z}$.

Note $k \cdot r = (mn) \cdot r = (mn \cdot 1) \cdot r$ by distributivity.

Furthermore, $n \cdot 1 = 0$, so $(mn) \cdot 1 = m \cdot (n \cdot 1) = m \cdot 0 = 0$;

therefore $k \cdot r = 0 \cdot r = 0$, as needed. #

Next, suppose $k \in \mathbb{Z}$ such that $k \cdot r = 0$ $\forall r \in R$.

In particular, $k \cdot 1 = 0$, so k must be a multiple of the order of 1 in the group R under addition.

So necessarily $n \mid k$ (see the previous theorems.) ▨

2 Let R be a ring with char $R = 0$.

Then $k \cdot r = 0$ $\forall r \in R$ if and only if $k = 0$.

Proof. If $k=0$, then $k \cdot r = 0 \cdot r = 0$ $\forall r \in R$.

Conversely, if $k \cdot r = 0$ $\forall r \in R$, then $k \cdot 1 = 0$, and since 1 has infinite order, we can deduce that this occurs only when $k = 0$. ▨

ENDOMORPHISMS

1 Let G be an abelian group, with the group operation denoted by addition.

Then the "set of endomorphisms" of G, denoted by $\mathrm{End}(G)$, is the set of all group homomorphisms $\phi: G \to G$.

2 We can define an addition on $\mathrm{End}(G)$ by

$(\phi + \psi)(g) = \phi(g) + \psi(g)$ $\forall \phi, \psi \in \mathrm{End}(G)$.

3 We can also define a multiplication on $\mathrm{End}(G)$ by

$(\phi\psi)(g) = (\phi \circ \psi)(g)$ $\forall \phi, \psi \in \mathrm{End}(G)$.

SUBRINGS

1. Let R be a ring. Then a subset $S \subseteq R$ is a "subring" if the "+" and "×" operations on R restrict to binary operations on S, and if S is a ring with respect to these restricted operations from R.

2. We also insist $1_R = 1_S$; ie the multiplicative identity of the rings R and S must be the same.

Why? → they may not agree.
eg $R = \mathbb{Z}/6\mathbb{Z}$, $S = \{[0],[2],[4]\}$
$1_R = [1]$, $1_S = [4]$, $1_R \neq 1_S$.

SUBRING TEST

Let R be a ring, and $S \subseteq R$ with $S \neq \emptyset$.
Then S is a subring if and only if:

① $1_R \in S$, where 1_R is the multiplicative identity for R;
② $a-b \in S$ $\forall a,b \in S$; and
③ $ab \in S$ $\forall a,b \in S$.

Proof. First, assume $S \subseteq R$ satisfies the three conditions above.
Then by ②, S is a subgroup of R with respect to addition.
Then by ③, S is closed under multiplication, and associativity of "×" follows from the fact that it is true for R.
By ①, S has a multiplicative identity 1_R, and by the uniqueness of the identity of a monoid we know that $1_R = 1_S$.
Finally, the distributive laws hold in S because they also hold in R.
Hence S must be a ring, and so is a subring of R. ✗
Conversely, assume S is a subring of R.
Then since S is a subgroup of R wrt "+", it follows from the Subgroup Test that $a-b \in S$ $\forall a,b \in S$.
Similarly, since S is closed under the multiplication on R, we know $ab \in S$ $\forall a,b \in S$ by definition.
Finally, since by definition $1_R = 1_S \in S$, we can see all three conditions are satisfied. ☒

CENTRE OF A RING

1. Let R be a ring. Then the "centre" of R, denoted by $Z(R)$, is defined to be

$$Z(R) = \{z \in R : zr = rz \quad \forall r \in R\}.$$

2. We can prove $Z(R)$ is also a ring.

Proof. Note $Z(R) \neq \emptyset$, as $1 \in Z(R)$.
(So ① in the Subring Test is satisfied)
Then, for any $r \in R$ and $a,b \in Z(R)$:
$(a-b)r = (a+(-b))r = ar + (-b)r = ar + -(br)$
$= ra + -(rb) = ra + r(-b) = r(a-b)$,
so $(a-b) \in Z(R)$, satisfying ② in the test.
Lastly, $(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$,
so $ab \in Z(R)$ also, satisfying ③ in the test.
Hence $Z(R)$ must be a ring. ☒

3. Note if R is commutative, then $Z(R) = R$.

RING HOMOMORPHISMS

Let R and S be rings. Then, a function $\phi: R \to S$ is a "ring homomorphism" if:

① $\phi(a+b) = \phi(a) + \phi(b)$ $\forall a,b \in R$;
② $\phi(ab) = \phi(a)\phi(b)$ $\forall a,b \in R$; and
③ $\phi(1_R) = 1_S$.

PROPERTIES OF HOMOMORPHISMS

Suppose $\phi: R_1 \to R_2$ is a ring homomorphism. Let $r \in R_1$ be arbitrary. Then:

① $\phi(0) = 0$;
② $\phi(-r) = -\phi(r)$;
③ $\phi(kr) = k\phi(r)$ $\forall k \in \mathbb{Z}$;
④ $\phi(r^n) = [\phi(r)]^n$ $\forall n \in \mathbb{N}$; and
⑤ $\phi(r^{-n}) = [\phi(r)]^{-n}$ $\forall n \in \mathbb{N}$ if r^{-1} exists.

IDEALS AND QUOTIENT RINGS

RELATIONSHIP BETWEEN $\phi: G \to G_1$ AND KER ϕ

Let $\phi: G \to G_1$ be a group homomorphism.
Then $\ker \phi$ is a normal subgroup of G.

Proof. Let $K = \ker \phi$.
Then we know K is a subgroup of G.
Let $g \in G$ be arbitrary.
Suppose $h = gkg^{-1}$ for some $k \in K$.
Observe that since
$\phi(h) = \phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1}$
$= \phi(g)\,(e)\,\phi(g)^{-1}$
$= e$,
it follows that $h \in \ker \phi = K$, and so $gKg^{-1} \subseteq K$.
If we let g^{-1} take the place of g, it shows that
$g^{-1}Kg \subseteq K$ $\forall g \in G$, so $K \subseteq gKg^{-1}$.
It follows that $K = gKg^{-1}$, and since this holds $\forall g \in G$, we thus have that K is normal in G. ∎

Let H be a normal subgroup of G.
Then there exists a group homomorphism $\phi: G \to G_1$ such that $H = \ker \phi$.

Proof. Let $G_1 = G/H$, and consider the quotient homomorphism $q: G \to G/H$ given by
$q(g) = Hg$ $\forall g \in G$.
Observe that $g \in \ker q$ if and only if $Hg = He$,
which occurs if and only if $ge^{-1} \in H$,
which occurs if and only if $g \in H$.
Hence $H = \ker q$, and we are done. ∎

KERNEL OF ABELIAN GROUPS

Let R and S be rings, and $\phi: R \to S$ be a ring homomorphism.
Then, the "kernel of ϕ", denoted by "$\ker \phi$", is defined to be the set
$$\ker \phi = \{ r \in R : \phi(r) = 0_S \}.$$

Note that by construction, $\ker \phi$ is an additive subgroup of R.

IDEAL OF A RING

Let R be a ring. Then, a subset $I \subseteq R$ is called an "ideal of R" if
1. I is a subgroup of the additive group R; and
2. I "absorbs" multiplication; ie $\forall r \in I,\ a \in R$, we have that $ar, ra \in I$.

Example: the "zero ideal" of R; $\{0\}$.
First, note $\{0\}$ is the trivial subgroup of R under addition.
Then, for any $a \in R$, certainly $a \cdot 0 = 0 \cdot a = 0 \in \{0\}$,
so $\{0\}$ absorbs multiplication as well.
So $\{0\}$ is an ideal of R.

PRINCIPAL IDEAL GENERATED BY a

Let R be a commutative ring, and $a \in R$ be arbitrary.
Then the "principal ideal generated by a" is the set
$$aR = Ra = \{ s \in R : s = ar \text{ for some } r \in R \}.$$

QUOTIENT RING

Let R be a ring, and let I be an ideal of R.
Then the set of right cosets R/I can be given the structure of a ring, with
i) addition given by $(I+a) + (I+b) = I + (a+b)$; and
ii) multiplication given by $(I+a)(I+b) = I + ab$,
for any $I+a,\ I+b \in R/I$.

Proof. First, since I is an additive subgroup of R, and R is abelian (under $+$), then by definition R/I is well defined under addition.
Then, suppose $\exists a', b' \in R$ such that $I+a = I+a'$ and $I+b = I+b'$.
This implies $a - a' \in I$ and $b - b' \in I$.
Subsequently, note that
$$ab - a'b' = ab - a'b + a'b - a'b' = (a-a')b + a'(b-b').$$
Since $a - a' \in I$, and I absorbs multiplication, necessarily $(a-a')b \in I$. Similarly, since $b - b' \in I$, we must have that $a'(b-b') \in I$.
Finally, since I is closed under addition, $(a-a')b + a'(b-b') \in I$, and so $ab - a'b' \in I$.
This shows that $I + ab = I + a'b'$, proving that multiplication is well-defined.
Certainly, $I+1$ is an identity wrt multiplication, since $(I+a)(I+1) = I + a \cdot 1 = I + a$ $\forall (I+a) \in R/I$.
Also, multiplication in R/I is associative, since
$((I+a)(I+b))(I+c) = (I+ab)(I+c) = (I + (ab)c)$
$= (I + a(bc)) = (I+a)(I+bc) = (I+a)((I+b)(I+c))$
for any $I+a,\ I+b,\ I+c \in R/I$.
We can similarly show R/I also satisfy the distributive laws.

RELATIONSHIP BETWEEN $\phi: R \to R_1$ AND KER ϕ

Let $\phi: R \to S$ be a ring homomorphism.
Then $\ker \phi$ is an ideal of R.
(Proof in previous section)

Let I be an ideal of R. Then there exists a ring homomorphism $\phi: R \to R_1$ such that $\ker \phi = I$.

Proof. Let $R_1 = R/I$, and consider the quotient mapping $q: R \to R_1$ by $q(a) = I + a$ $\forall a \in R$.
Then q is a ring homomorphism since R/I is a ring.
But since $a \in \ker q$ if and only if $q(a) = I + a = I + 0$,
which holds if and only if $a \in I$,
we must have that $I = \ker q$, and we are done. ∎

Chapter 5: Elementary Number Theory

INTEGRAL DOMAINS

ZERO DIVISOR

Let R be a commutative ring. Then, an element $a \in R$ is called a "zero divisor" if there exists a $b \in R$, $b \neq 0$ such that $ab = 0$.

INTEGRAL DOMAIN

1. Let R be a commutative ring, where $R \neq \{0\}$. Then R is an "integral domain" if 0 is the only zero divisor; ie if $ab = 0$, then either $a = 0$ or $b = 0$.
2. Example: the ring $\mathbb{Z}$.

CANCELLATION PROPERTY OF AN INTEGRAL DOMAIN

Let R be a commutative ring. Then, we can show that $R \neq \{0\}$ is an integral domain if and only if $\forall a,b,c \in R$, if $ab = ac$ and $a \neq 0$, then $b = c$.

Proof. First, suppose R is an integral domain. Let $a,b,c \in R$ such that $ab = ac$ and $a \neq 0$. Then $ab - ac = 0$, so $a(b-c) = 0$. But since R is an integral domain, and $a \neq 0$ by assumption, we must have that $b - c = 0$, and so $b = c$.

Conversely, assume the "cancellation" property holds. Let $a, b \in R$ such that $ab = 0$. If $a = 0$ the claim follows trivially, so assume $a \neq 0$. Then $ab = 0 = a \cdot 0$ and $a \neq 0$, so necessarily $b = 0$. ◼

FIELD

1. Let F be a ring. Then, F is a "field" if
   ① it is commutative; and
   ② every non-zero element of F has a multiplicative inverse in F.
2. In other words, for each $a \in F$, $\exists a^{-1} \in F$ such that $aa^{-1} = 1$.
3. Examples: $\mathbb{Q}$ and $\mathbb{R}$.

EVERY SUBRING OF A FIELD IS AN INTEGRAL DOMAIN

Let F be a field. Then every subring R of F is an integral domain of F.

* this also proves F is an integral domain!

Proof. Since multiplication is defined the same as in F, and multiplication in F is commutative, we know R is a commutative ring.

Then, suppose we have $a, b \in R$ such that $ab = 0$ in R. Necessarily, this equation also holds in F. Next, if $a \neq 0$, then a^{-1} exists in F by definition, and so $a^{-1}ab = b = a^{-1} \cdot 0 = 0$, and so $b = 0$. This proves if $ab = 0$ in R, then $a = 0$ or $b = 0$, and so R is an integral domain. ◼

GAUSSIAN INTEGERS

The ring of "Gaussian integers", denoted by $\mathbb{Z}[i]$, is defined to be the set

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

* i is such that $i^2 = -1$.

with addition given by

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

and multiplication given by

$$(a+bi)(c+di) = (ac - bd) + (ad + bc)i.$$

NORM

Let $a + bi \in \mathbb{Z}[i]$ be arbitrary. Then, the "norm" of $a + bi$, denoted by $N(a+bi)$, to be equal to

$$N(a+bi) = a^2 + b^2.$$

PROPERTIES OF INTEGRAL DOMAINS

CHAR R IS ZERO OR PRIME

Let R be an integral domain. Then either $\operatorname{char} R = 0$ or $\operatorname{char} R = p$, where p is prime.

Proof. Suppose $\operatorname{char} R \neq 0$ and $\operatorname{char} R$ is not prime. Then either $\operatorname{char} R = 1$ or $\operatorname{char} R$ is composite. If $\operatorname{char} R = 1$, then $R = \{0\}$, and so cannot be an integral domain.

If $\operatorname{char} R$ is composite, then $\operatorname{char} R = ab$, where $1 < a, b < n$. Then $r = a \cdot 1_R$ and $s = b \cdot 1_R$ are non-zero, but $rs = (ab) \cdot 1_R = 0$, which is a contradiction.

Hence necessarily if R is an integral domain, then $\operatorname{char} R = 0$ or $\operatorname{char} R$ is prime. ◼

EVERY FINITE INTEGRAL DOMAIN IS A FIELD

Let R be a finite integral domain. Then R is also a field.

Proof. Let $n = |R|$, where $n \in \mathbb{N}$. Let $a \in R$ be arbitrary, with $a \neq 0$. Let the multiplication map $\phi : R \to R$ by $\phi(r) = ar$ $\forall r \in R$.

Note ϕ is injective: if $\phi(r) = \phi(s)$, then $ar = as$, and by the cancellation property necessarily $r = s$.

Then, since R is finite, ϕ must also be surjective. By injectivity, $|\phi(R)| = n$, and since $\phi(R) \subseteq R$ and $|R| = n$, necessarily $R = \phi(R)$.

Subsequently, by surjectivity, there exists a $b \in R$ such that $\phi(b) = 1$, which says that $ab = ba = 1$. Thus each $a \in R$ has a multiplicative inverse $b \in R$, and so R must be a field. ◼

DIVISIBILITY

1. Let R be an integral domain, and let $a, b \in R$ be arbitrary. Then, we say "a divides b" if there exists a $c \in R$ such that $b = ac$, and write $a \mid b$.

* we could write $a \nmid b$ if a does not divide b.

THE DIVISIBILITY RELATION IS REFLEXIVE

Let R be an integral domain. Then $a \mid a$ $\forall a \in R$.

Proof. This follows from the fact that $a = 1 \cdot a$ $\forall a \in R$. ∎

THE DIVISIBILITY RELATION IS TRANSITIVE

Let R be an integral domain. Then $\forall a, b, c \in R$, if $a \mid b$ and $b \mid c$, necessarily $a \mid c$.

Proof. Since $a \mid b$ and $b \mid c$, thus $ak = b$ and $c = b\ell$ for some $k, \ell \in R$.

Thus
$$\begin{aligned} c &= b\ell \\ &= (ak)\ell \\ \therefore\ c &= a(k\ell). \end{aligned}$$

Since $(k\ell) \in R$, this tells us $a \mid c$, so we are done.

$a \mid b,\ b \mid c \Rightarrow a \mid (bx + cy)$

Let R be an integral domain. Then $\forall a, b, c \in R$, if $a \mid b$ and $a \mid c$, necessarily $a \mid (bx + cy)$ $\forall x, y \in R$.

Proof. Since $a \mid b$ and $a \mid c$, so $ak = b$ and $a\ell = c$ for some $k, \ell \in R$.

Thus for any $x, y \in R$,
$$\begin{aligned} bx + cy &= (ak)x + (a\ell)y \\ &= a(kx + \ell y) \end{aligned}$$

and so $a \mid (bx + cy)$, as required. ∎

ASSOCIATE

1. We can define an equivalence relation "$\sim$" on any ring R by stating that $a \sim b$ if $a \mid b$ and $b \mid a$.

why? → A4 Q3.

2. We say a and b are "associate" in R if $a \sim b$.

UNIT OF A RING

1. Let R be a ring. Then, an element $r \in R$ is called a "unit" of R if r has a multiplicative inverse in R.

2. We denote R^* to be the set of all units of R.

$a \sim b \iff a = ub$

Let R be an integral domain. Then, given any $a, b \in R$, we have $a \sim b$ if and only if $a = ub$, where $u \in R^*$.

Proof. First, suppose $a \sim b$ in R. Then $a \mid b$ and $b \mid a$, so there exists $k, \ell \in R$ such that $b = ak$ and $a = b\ell$.

Hence $b = ak = (b\ell)k = b(\ell k)$.

If $b = 0$, then $a = 0 \cdot \ell = 0$, and so $a = b = 1 \cdot b$, where $1 \in R^*$.

On the other hand, if $b \neq 0$, then $b \cdot 1 = b \cdot (\ell k)$, and by the cancellation property necessarily $\ell k = 1$.

So $\ell \in R^*$, and the proof follows.

Conversely, suppose $a = ub$ for some $u \in R^*$.

Then $b \mid a$ follows immediately.

But note $u^{-1}a = u^{-1}ub = b$, and so $a \mid b$ also.

Thus $a \sim b$, completing the proof. ∎

DIVISION WITH REMAINDER

DIVISION WITH REMAINDER IN $\mathbb{Z}$

💡1 Let $a, b \in \mathbb{Z}$ with $b > 0$.
Then there exist unique integers q and r,
with $0 \leq r < b$, such that $a = bq + r$.

Proof. First, assume $a \geqslant 0$.
Let $S = \{n \in \mathbb{N} : n = a - bq,\ q \in \mathbb{Z}\}$.
Note $S \neq \emptyset$, since $a = a - b(0)$, so $a \in S$.
Thus, by WOP, S has a least element r.
Then by construction $r = a - bq$, so $a = bq + r$.
Moreover, since both
i) $r \geqslant 0$; and
ii) $r < b$; since if $r \geqslant b$, then $r - b \geqslant 0$, and so $r - b = a - bq - b = a - b(q+1)$, implying $r - b \in S$, contradicting the minimality of r,
we get that $0 \leq r < b$, and we are done. ※

Conversely, if $a < 0$, then $-a > 0$, so by the above there exists $q_0, r_0 \in \mathbb{Z}$ such that $-a = bq_0 + r_0$, where $0 \leq r_0 < b$.
Then,
① if $r_0 = 0$, then $a = b(-q_0)$, so $q = -q_0$ and $r = 0$ satisfy the theorem's conditions; and
② if $r_0 \neq 0$, then $a = b(-q_0) - r_0 = b(-q_0 - 1) + (b - r_0)$, and so $q = -q_0 - 1$ and $r = b - r_0$ satisfy the conditions of the theorem. ※

Hence, we have shown q, r exist $\forall a \in \mathbb{Z}$, and so we only need to prove uniqueness.
Suppose $\exists q', r' \in \mathbb{Z}$ such that $a = bq' + r'$ and $0 \leq r' < b$.
Then $bq + r = bq' + r'$, and so
$r - r' = b(q - q')$.
If $q = q'$, necessarily $r = r'$, completing the uniqueness proof.
If $q \neq q'$, then by taking absolute values of both sides:
$|r' - r| = |b||q - q'| \geqslant b$.
But since $r < b$ and $r' < b$, this is impossible, so we must get that $q = q'$, and so $r = r'$, proving q and r are unique. ☒

💡2 Note that
① q is known as the "quotient" of the division; and
② r is known as the "remainder" of the division.

DIVISION WITH REMAINDER IN $\mathbb{Z}[i]$

💡1 Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$.
Then there exists $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$, with $0 \leq N(\delta) < N(\beta)$.

Proof. Let $\alpha = a + bi$ and $\beta = c + di$, for some $a, b, c, d \in \mathbb{Z}$, with $c \neq 0$ and $d \neq 0$.
Then
$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(ac+bd) + (bc-ad)i}{c^2+d^2} = r + si,$$
with $r = \frac{ac+bd}{c^2+b^2} \in \mathbb{Q}$ and $s = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$.
Subsequently, choose $m, n \in \mathbb{Z}$ such that $|m - r| \leq \frac{1}{2}$ and $|n - s| \leq \frac{1}{2}$.
Let $\gamma = m + ni \in \mathbb{Z}[i]$ and $\delta = \alpha - \beta\gamma$.
Note $\delta \in \mathbb{Z}[i]$, as "+" and "×" are closed in the ring $\mathbb{Z}[i]$.
Then, certainly $\alpha = \beta\gamma + \delta$.
Moreover, note that
$$\delta = \alpha - \beta\gamma = \beta\left(\frac{\alpha}{\beta}\right) - \beta\gamma = \beta(r + si) - \beta(m + ni) = \beta((r-m) + (s-n)i),$$
so
$$N(\delta) = |\delta|^2 = |\beta((r-m) + (s-n)i)|^2 = |\beta|^2((r-m)^2 + (s-n)^2) = N(\beta)((r-m)^2 + (s-n)^2).$$
But since $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$, consequently $(r-m)^2 \leq \frac{1}{4}$ and $(s-n)^2 \leq \frac{1}{4}$, and so $(r-m)^2 + (s-n)^2 \leq \frac{1}{2}$.
Hence $N(\delta) \leqslant N(\beta)\,\frac{1}{2} < N(\beta)$, proving the other condition of the theorem. ☒

DIVISION ALGORITHM & DIVISOR FUNCTION

💡1 Let R be an integral domain. Then, we say R has a "division algorithm" if there exists a function $d : R \setminus \{0\} \to \mathbb{N}$ such that $\forall a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$, with $d(r) < d(b)$, or $r = 0$.

💡2 In this case, we call d the "divisor function" of R.

GREATEST COMMON DIVISOR

💡1 Let R be an integral domain, and $a, b \in R$ be arbitrary, with $a \neq 0$ and $b \neq 0$.
Then, an element $d \in R$ is called a "greatest common divisor", or "gcd", of a and b if
① $d \mid a$ and $d \mid b$; and
② If $e \in R$ is another common divisor of a and b, so that $e \mid a$ and $e \mid b$, then necessarily $e \mid d$.

💡2 Note the greatest common divisor of a and b may not be unique!

RELATION BETWEEN ~ AND GCDS

💡 Let R be an integral domain, and $a, b \in R \setminus \{0\}$ be arbitrary. Then,
① If d_1 and d_2 are both greatest common divisors of a and b, then $d_1 \sim d_2$; and
② If d_1 is a greatest common divisor of a and b and $d_2 \in R$ is such that $d_2 \sim d_1$, then necessarily d_2 is a gcd of a and b.

Proof. First, suppose d_1 and d_2 are both gcds of a and b.
Then since d_1 is a common divisor of a and b, and d_2 is the greatest common divisor of a and b, necessarily $d_1 \mid d_2$.
Symmetrically, since d_1 is a gcd of a and b and d_2 is a common divisor of a and b, we must also get that $d_2 \mid d_1$.
Consequently since $d_1 \mid d_2$ and $d_2 \mid d_1$, so $d_1 \sim d_2$, proving ①.

Then, assume d_1 is a gcd of a and b, and $d_2 \sim d_1$.
So $d_2 \mid d_1$ and $d_1 \mid d_2$.
But since $d_1 \mid a$ and $d_1 \mid b$, the transitivity of divisibility tells us that $d_2 \mid a$ and $d_2 \mid b$.
So d_2 is a common divisor of a and b.
Furthermore, for any common divisor e of a and b, we know $e \mid d_1$, since d_1 is the gcd of a and b.
But since $d_1 \mid d_2$, transitivity of divisibility once again yields that $e \mid d_2$, proving that d_2 is indeed a gcd of a and b, proving ②. ☒

THE EUCLIDEAN ALGORITHM

Let R be an integral domain with a division algorithm, and $a, b \in R$ be arbitrary.

Then, we can use the Euclidean algorithm to efficiently find the gcd of a and b.

In other words, the Euclidean algorithm shows that given any $a, b \in R \setminus \{0\}$, $\gcd(a,b)$ always exists.

FUNDAMENTAL IDEA

The fundamental idea that makes the Euclidean algorithm work is as follows:

Let R be an integral domain, and suppose there exist $a, b, q, r \in R$ such that $a = bq + r$.

Then, an element $d \in R$ is a gcd of a and b if and only if it is a gcd of b and r;

ie $\gcd(a,b) \sim \gcd(b,r)$.

Proof. First, suppose d is a gcd of a and b.
This implies $d \mid a$ & $d \mid b$.
So $d \mid (a \cdot 1 + b \cdot (-q))$, telling us that $d \mid r$,
So d is a common divisor of b and r.
Then, suppose e is a common divisor of b and r.
Thus $e \mid b$ and $e \mid r$.
Hence $e \mid b \cdot q + r \cdot 1$, or $e \mid a$,
showing that e is a common divisor of a and b.
But since d is a gcd of a and b, it follows that necessarily $e \mid d$, and so d is also a gcd of b and r. ∗
A similar proof can be used to prove the backward argument. ∎

PROCEDURE

Let R be an integral domain with a division algorithm, and suppose D denotes the divisor function in this case.

Then, given some $a, b \in R$ with $a \neq 0_R$ and $b \neq 0_R$, we can calculate the gcd of a and b as follows:

1. We first carry out a division with remainder to get that
$$a = bq_0 + r_1,$$
where $q_0, r_1 \in R$ and either $r_1 = 0$ or $D(r_1) < D(b)$.

2. Then, if $r_1 = 0$, it implies $b \mid a$, and consequently that $b = \gcd(a,b)$.

3. Otherwise, if $r_1 \neq 0$, then we can use the lemma to the left to deduce that $\gcd(a,b) \sim \gcd(b, r_1)$.

4. So, we can carry out another division with remainder of b by r_1 to get that
$$b = r_1 q_1 + r_2,$$
where $q_1, r_2 \in R$ and either $r_2 = 0$ or $D(r_2) < D(r_1)$.

5. Again, if $r_2 = 0$, then $r_1 = \gcd(b, r_1)$, implying that $r_1 = \gcd(a,b)$ as well.

6. Otherwise, we can infer $\gcd(b, r_1) \sim \gcd(r_1, r_2)$, and so we are reduced to calculate a gcd of r_1 and r_2.

7. We can continue this process to obtain a succession of divisions with remainder:
$$\begin{aligned} a &= bq_0 + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0, \end{aligned}$$
where r_n is the last non-zero remainder obtained.
Then, since $D(b) > D(r_1) > \cdots$, we must eventually get a remainder of 0, as this is a strictly decreasing sequence of natural numbers.

8. But since $\gcd(a,b) \sim \gcd(b, r_1) \sim \cdots \sim \gcd(r_{n-1}, r_n)$, and $r_n \mid r_{n-1}$, we can consequently infer $r_n = \gcd(r_n, r_{n-1})$, and so $r_n = \gcd(a,b)$ also.

EXAMPLE: gcd(1009, 33)

We can use the Euclidean algorithm to find the gcd of 1009 and 33.

First, we perform divisions with remainder:
$$\begin{aligned} 1009 &= 33 \cdot 30 + 19 \\ 33 &= 19 \cdot 1 + 14 \\ 19 &= 14 \cdot 1 + 5 \\ 14 &= 5 \cdot 2 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

So the last non-zero remainder is 1, implying $1 = \gcd(1009, 33)$.

THE EXTENDED EUCLIDEAN ALGORITHM

The Euclidean algorithm can be used to find elements $x, y \in R$ such that $ax + by = d$, where $d = \gcd(a, b)$.

PROCEDURE

We can accomplish the above by the following:

① Suppose after running the Euclidean algorithm on a and b, we generate divisions with remainder

$$a = bq_0 + r_1$$
$$b = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

* we leave out the last step.

② We now reverse the order of the equations, and isolate the remainder in each one:

$$r_n = r_{n-2} - r_{n-1} q_{n-1}$$
$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$$
$$\vdots$$
$$r_2 = b - r_1 q_1$$
$$r_1 = a - bq_0.$$

③ Then, we can "back-substitute" the below equations into the above one, which will eventually terminate when we have expressed $\gcd(a, b) = r_n = ax + by$ for some $x, y \in R$, which is what we wanted to do.

EXAMPLE: $1009x + 33y = 1$

We can use the Extended Euclidean algorithm to find integer solutions to the equation $1009x + 33y = 1$

First, we reverse and solve for each non-zero remainder the equations we obtained when applying the Euclidean Algorithm:

$$1 = 5 - 4 \cdot 1 \quad \text{—— ①}$$
$$4 = 14 - 5 \cdot 2 \quad \text{—— ②}$$
$$5 = 19 - 14 \cdot 1 \quad \text{—— ③}$$
$$14 = 33 - 19 \cdot 1 \quad \text{—— ④}$$
$$19 = 1009 - 33 \cdot 30 \quad \text{—— ⑤}.$$

Then, observe if we substitute ② into ①, we get that

$$1 = 5 - (14 - 5 \cdot 2) \cdot 1 = 5 \cdot 3 - 14 \cdot 1.$$

If we substitute ③ into this new equation, we subsequently get that

$$1 = 5 \cdot 3 - 14 \cdot 1 = (19 - 14 \cdot 1) \cdot 3 - 14 \cdot 1 = 19 \cdot 3 - 14 \cdot 4.$$

We can keep "back-substituting" like this, eventually arriving at the conclusion that

$$1 = 1009 \cdot 7 - 33 \cdot 214,$$

and so $1009x + 33y = 1$ has a solution $x = 7$ and $y = -214$ over $\mathbb{Z}$.

LINEAR DIOPHANTINE EQUATIONS

Suppose R is an integral domain with a division algorithm. Then, a linear Diophantine equation (in 2 variables) is any equation of the form

$$ax+by+c,$$

where $a,b,c \in R$ and x,y are the solutions to the equation.

IF A LINEAR DIOPHANTINE EQUATION HAS A SOLUTION, THEN $\gcd(a,b) \mid c$

Let R be an integral domain with a division algorithm, and let $a,b,c \in R$ be arbitrary. Then, if there exists a solution to the equation $ax+by=c$, with $x,y \in R$, then $\gcd(a,b) \mid c$.

Proof. Let $d=\gcd(a,b)$. Then $d \mid a$ and $d \mid b$, implying that $d \mid (ax+by)=c$. So $d \mid c$, and we are done. ■

IF $\gcd(a,b) \mid c$, $ax+by=c$ HAS A SOLUTION

Let R be an integral domain with a division algorithm, and $a,b,c \in R$ be arbitrary, with $a \neq 0$ and $b \neq 0$. Then, if $\gcd(a,b) \mid c$, the equation $ax+by=c$ has a solution with $x,y \in R$.

Proof. Let $d=\gcd(a,b)$. Then, the Euclidean algorithm tells us that $\exists x_0,y_0 \in R$ such that $ax_0+by_0=d$. Since $d \mid c$, it follows that $\exists k \in \mathbb{Z}$ such that $c=kd$, and so

$$c=kd=k(ax_0+by_0)=a(kx_0)+b(ky_0).$$

so that $ax+by=c$ has a solution $x=kx_0$ and $y=ky_0$. ■

$a \mid bc$ & $1 \sim \gcd(a,b) \Rightarrow a \mid c$

Suppose R is an integral domain with a division algorithm, and let $a,b,c \in R$ be arbitrary. Then, if both $a \mid bc$ and $1 \sim \gcd(a,b)$, necessarily $a \mid c$.

Proof. Since $a \mid bc$, there must exist a $k \in R$ such that $ak=bc$. Moreover, since 1 is a gcd of a and b, we know there must exist $x,y \in R$ such that

$$ax+by=1.$$

Thus, if we multiply both sides by c, we get

$$acx+bcy=c$$

But since $bc=ak$, so

$$acx+aky=c$$
$$\Rightarrow a(cx+ky)=c,$$

proving $a \mid c$, as required. ■

$d=\gcd(a,b) \Rightarrow a=da_0,\ b=db_0 \Rightarrow \gcd(a_0,b_0) \sim 1$

Let R be an integral domain with a division algorithm, and let $a,b \in R \setminus \{0\}$ be arbitrary. Suppose $d=\gcd(a,b)$, so that $a=da_0$ and $b=db_0$ for some $a_0,b_0 \in R$. Then $\gcd(a_0,b_0) \sim 1$ necessarily.

Proof. First, we know that $\exists x,y \in R$ such that

$$ax+by=d.$$

So $(da_0x)+(db_0y)=d$ and cancelling out the $d \neq 0$ yields that $a_0x+b_0y=1$, which shows that $\gcd(a_0,b_0) \mid 1$, and so $\gcd(a_0,b_0) \sim 1$ (as $1 \mid \gcd(a_0,b_0)$ holds trivially.) ■

THE GENERAL SOLUTION OF A LINEAR DIOPHANTINE EQUATION

Let R be an integral domain with a division algorithm, and $a,b,c \in R$ be such that $a \neq 0$ & $b \neq 0$.

Let $d=\gcd(a,b)$ be such that $d \mid c$, and write $a=da_0$ and $b=db_0$ for some $a_0,b_0 \in R$.

Then, the complete set of solutions to the equation

$$ax+by=c \quad , \quad \text{where } x,y \in R,$$

is given by

$$(x,y)=(x_0+kb_0,\ y_0-ka_0),$$

where $k \in R$ is arbitrary, and (x_0,y_0) is a particular solution to $ax+by=c$.

Proof. By assumption, (x_0,y_0) is a solution to $ax+by=c$, implying that $ax_0+by_0=c$. —①

Let (x_1,y_1) be another solution to the equation, so that $ax_1+by_1=c$. —②

Subtracting ① from ② yields that

$$a(x_1-x_0)+b(y_1-y_0)=0,$$

and making the substⁿs $a=da_0$ and $b=db_0$ gives us

$$(da_0)(x_1-x_0)+(db_0)(y_1-y_0)=0.$$

Rearranging this gets us that $a_0(x_1-x_0)=-b_0(y_1-y_0)$.

Hence $b_0 \mid a_0(x_1-x_0)$. But since $\gcd(a_0,b_0) \sim 1$, we can infer that $b_0 \mid (x_1-x_0)$, and so $x_1-x_0=kb_0$ for some $k \in R$. (This implies $x_1=x_0+kb_0$).

So $a_0(kb_0)=-b_0(y_1-y_0)$,

and thus $ka_0=-(y_1-y_0)$; then, if we solve for y_1, we get that $y_1=y_0-ka_0$.

Thus if (x_1,y_1) is a solution to the equation, then $(x_1,y_1)=(x_0+kb_0,\ y_0-ka_0)$. ※

Conversely, note if $x_1=x_0+kb_0$ and $y_1=y_0-ka_0$, then

$$\begin{aligned} ax_1+by_1 &= a(x_0+kb_0)+b(y_0-ka_0) \\ &= (ax_0+by_0)+k(ab_0-ba_0) \\ &= c+k((da_0)b_0-(db_0)a_0) \\ &= c+0 \\ &= c, \end{aligned}$$

and so (x_1,y_1) is a solution to the equation. ■

EXAMPLE: FINDING THE GENERAL SOLUTION TO $1009x+33y=5$

We can use the formula given above to find all the solutions to $1009x+33y=5$ (in $\mathbb{Z}$).

First, by running the Euclidean algorithm on the eqⁿ, we get that $\gcd(1009,33)=1$ and that

$$1009(7)+33(-214)=1.$$

Then, since $\gcd(1009,33) \mid 5$, the above eqⁿ has a solution. Subsequently, multiplying both sides by 5 yields that

$$1009(35)+33(-1070)=5,$$

and so our equation has the particular solution $(x_0,y_0)=(35,-1070)$.

To get the general solution, note $a_0=a=1009$ & $b_0=b=33$, because the gcd is 1 in this case, and so the general solution of this eqⁿ is

$$(x,y)=(35+33k,\ -1070-1009k),$$

where $k \in \mathbb{Z}$ is arbitrary.

MULTIPLICATIVE INVERSES IN $\mathbb{Z}/n\mathbb{Z}$

1. We can use linear Diophantine equations to calculate the multiplicative inverse of an element in $\mathbb{Z}/n\mathbb{Z}$, if it exists.

2. In particular, we can show $[a] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if $ax+ny=1$ has a solution.

   <u>Proof</u>. Observe $[a]$ has a multiplicative inverse if and only if there exists a $[x] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][x]=[1]$. This is equivalent to the assertion that $[ax]=[1]$, or that $ax \equiv 1 \pmod{n}$. In turn, this is the same as saying $n \mid (ax-1)$, ie $ny = 1-ax$ for some $y \in \mathbb{Z}$, or in other words whether $ax+ny=1$ has a solution. $\blacksquare$

3. Hence, this is only possible if $\gcd(a,n)=1$.

4. Note if $n=p$, where p is prime, then $\gcd(a,p)=1 \ \forall [a] \in (\mathbb{Z}/p\mathbb{Z}) \setminus [0]$, and so $\mathbb{Z}/p\mathbb{Z}$ is a field.

POLYNOMIALS OVER A FIELD

Let F be a field. Then, we define the set of "polynomials with coefficients in F", denoted by $F[x]$, by

$$F[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : n \geqslant 0, \ a_i \in F \ \forall i \}.$$

We can turn $F[x]$ into a commutative ring; given a $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{i=0}^{n} b_i x^i$, we can define an addition and multiplication by

$$f+g = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x_i$$

and

$$fg = \sum_{i=0}^{m+n} c_i x^i, \quad \text{with} \quad c_i = \sum_{j=0}^{i} a_j b_{i-j} \text{ for each } i.$$

DEGREE

Let $F[x]$ be a set of polynomials with coefficients in some field F.
Let $f \in F[x]$ be arbitrary.
Then, the "degree" of f, denoted by $\deg(f)$, is the largest index i such that $a_i \neq 0$.

$\deg(f+g) \leqslant \max(\deg(f), \deg(g))$

Let F be an arbitrary field, and $f, g \in F[x]$ be arbitrary. Then, if $\deg(f+g) \neq 0$, then $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$.

Proof. By definition, $f+g = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$.
So all coefficients of powers of x after $\max(m,n)$ are equal to 0, so if $f+g \neq 0$, then $\deg(f+g) \leqslant \max(m,n) = \max(\deg(f), \deg(g))$.

$\deg(fg) = \deg(f) + \deg(g)$

Let F be an arbitrary field, and $f, g \in F[x]$ be arbitrary.
Then $\deg(fg) = \deg(f) + \deg(g)$.

Proof. By defn, $fg = \sum_{i=0}^{m+n} c_i x^i$; hence all coefficients of powers of x after $m+n$ are equal to 0, implying $\deg(fg) \leqslant \deg(f) + \deg(g)$.

Next, observe that

$$c_{m+n} = \sum_{j=0}^{m+n} a_j b_{m+n-j} = a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_m b_n + \cdots + a_{m+n} b_0.$$

Then, since $a_j = 0 \ \forall j > m$, so all terms after $a_m b_n$ in the sum above are equal to 0.
Likewise, since $b_{m+n-j} = 0$ when $j < m$, all terms before $a_m b_n$ in the sum above are equal to 0.
Hence $c_{m+n} = a_m b_n$, and since $a_m \neq 0$ & $b_n \neq 0$, the fact that F is an integral domain tells us that $a_m b_n = c_{m+n} \neq 0$.

This is sufficient to prove that $\deg(fg) = m+n = \deg(f) + \deg(g)$. ☐

$F[x]$ IS AN INTEGRAL DOMAIN

Let F be an arbitrary field. We can show that $F[x]$ must be an integral domain.

Proof. Observe if $f, g \in F[x] \setminus \{0\}$, then $\deg(f)$ and $\deg(g)$ exist, and by the above $\deg(fg) = \deg(f) + \deg(g)$.
So $fg \neq 0$; combined with the fact that $F[x]$ is a commutative ring, this is sufficient to show that $F[x]$ is an integral domain. ■

$F[x]$ HAS A DIVISION ALGORITHM

Let F be an arbitrary field. Then, the integral domain $F[x]$ admits a division algorithm with divisor function $\deg(\cdot)$;
ie for any polynomials $f, g \in F[x]$ with $g \neq 0$, there exist $q, r \in F[x]$ such that $f = gq + r$, and either $r = 0$ or $\deg(r) < \deg(g)$.

Proof. Let $S = \{ f - gq : q \in F[x] \}$.
If $0 \in S$, then there exists a $q \in F[x]$ such that $f = gq$, and we are done.
Otherwise, let $r \in S \setminus \{0\}$ be arbitrary.
By construction, $r = f - gq$ for some $q \in F[x]$, and so $f = gq + r$ as needed. ✱

Next, suppose $\deg(r) \geqslant \deg(g)$, and let $r = a_n x^n + a_{n-1} x^{n-1} + \cdots$ and $g = b_m x^m + b_{m-1} x^{m-1} + \cdots$, where $b_m \neq 0$ since $g \neq 0$, and $n \geqslant m$.
Then, since $b_m \neq 0$ and F is a field, b_m^{-1} must exist.
Let

$$\begin{aligned} r_1 &= r - a_n b_m^{-1} x^{n-m} g \\ &= (a_n x^n + a_{n-1} x^{n-1} + \cdots) - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots) \\ &= (a_{n-1} - a_n b_m^{-1} b_{m-1}) x^{n-1} + \cdots, \end{aligned}$$

so that $\deg(r_1) < \deg(r)$.
However, $r_1 = r - a_n b_m^{-1} x^{n-m} g = (f - gq) - a_n b_m^{-1} x^{n-m} g = f - (q + a_n b_m^{-1} x^{n-m}) g$, so $r_1 \in S$, contradicting our choice of r as an element of S of smallest degree.
Therefore $\deg(r) < \deg(g)$ after all, verifying that a decomposition $f = gq + r$ where $r = 0$ or $\deg(r) < \deg(g)$ does exist.

EVALUATION

Let F be an arbitrary field, and $f \in F[x]$ be arbitrary.
Then, the "evaluation of f" at c, where $c \in F$, is defined to be

$$f(c) = a_n c^n + a_{n-1} c^{n-1} \cdots + a_0.$$

ROOT

Let F be an arbitrary field, and $f \in F[x]$ be arbitrary.
Then a $c \in F$ is a "root of f" if $f(c) = 0$.

EVALUATION HOMOMORPHISM

Let F be a field. Then, the "evaluation homomorphism" of F at some $c \in R$ is defined to be the mapping $\phi_c : F[x] \to F$ given by $\phi_c(f) = f(c) \ \forall f \in F$.

Note that ϕ_c is a ring homomorphism.

THE FACTOR THEOREM

Let F be a field, and $c \in F$ be arbitrary.
Then c is a root of f if and only if
$(x-c) \mid f$ in $F[x]$; ie $\ker \phi_c = F[x](x-c)$.

Proof. First, assume $(x-c) \mid f$.
Then, by definition, there exists some $q \in F[x]$ such that $f = (x-c)q$.
Note $\phi_c(x-c) = c - c = 0$; thus,
$f(c) = \phi_c(f) = \phi_c(x-c)\phi_c(q) = 0 \cdot \phi_c(q) = 0$, showing that c is a root of f.

Conversely, suppose c is a root of f.
Applying division with remainder of f by $(x-c)$, we know there necessarily exists $q, r \in F[x]$ such that
$$f = (x-c)q + r,$$
where $r = 0$ or $\deg(r) < \deg(x-c) = 1$.
Either way, this guarantees r is a constant polynomial, in the form $r = r_0$ for some $r_0 \in F$.
So, applying ϕ_c to the eq^n yields that
$$0 = f(c) = \phi_c(f) = \phi_c((x-c)q + r)$$
$$= \phi_c(q)\phi_c(x-c) + r_0$$
$$= 0 \cdot \phi_c(x-c) + r_0$$
$$\therefore 0 = r_0,$$
showing that $f = (x-c)q$, so $(x-c) \mid f$.

Thus $f(c) = 0$ exactly when f is multiple of $(x-c)$, implying that $\ker \phi_c = F[x](x-c)$. ☒

f HAS AT MOST DEG(f) DISTINCT ROOTS IN F (IF $f \neq 0$)

Let F be a field. Then, any polynomial $f \in F[x] \setminus \{0\}$ has at most $\deg(f)$ distinct roots in F.

Proof. We prove this by induction.
First, if $\deg(f) = 0$, then $f = f_0$, where $f_0 \in F \setminus \{0\}$.
Hence $f_0 \neq 0$ $\forall c \in F$, showing f has no roots in F, establishing our first base case.
Similarly, if $\deg(f) = 1$, then $f = ax + b$ for some $a, b \in F$, with $a \neq 0$.
Then note $f(c) = 0$ iff $ac + b$, iff $ac = -b$, iff $c = -a^{-1}b$;
so f has exactly one root in F, establishing our second base case.
Next, suppose $\deg(f) = n+1$ for some $n \geqslant 1$, $n \in \mathbb{Z}^+$, and assume all polynomials of degree $k < n+1$ have at most k roots in F.
If f has no roots in F the result is trivially true, so assume $c \in F$ is a root of f.
By the Factor Theorem, thus $f = (x-c)f_n$ for some $f_n \in F$.
Taking degrees of both sides yields that $\deg(f_n) = n$.
Then, note $\forall a \in F$, $f(a) = 0$ if and only if $(a-c)f_n(a) = 0$,
which holds if and only if $a = c$ or $f_n(a) = 0$.
But $f_n(a) = 0$ has at most n distinct values for at most n distinct values of $a \in F$;
hence, $f(a) = 0$ for at most $n+1$ distinct values of a.
The claim follows by induction. ☒

PRIMITIVE ROOTS MODULO P

$g \in G$, $o(g)$ IS MAXIMAL $\Rightarrow h^{o(g)}$ $\forall h \in G$

Let G be a finite abelian group, and suppose $g \in G$ is such that $o(g)$ is maximal.
Then, if $o(g) = k$, then $h^k = e$ $\forall h \in G$.
(Proof in A9)

F^* IS CYCLIC (F IS A FINITE FIELD)

Let F be a finite field. Then the group F^* of units of F is cyclic.

Proof. Since F^* is a finite abelian group, we can choose an element $c \in F^*$ that has maximal order.
Let this order be k.
Then by the above lemma, $a^k = 1$ $\forall a \in F^*$.
In particular, the polynomial $x^k - 1 \in F[x]$ has at least $|F^*|$ distinct roots, so $|F^*| \leqslant k$.
But we also know $x^k - 1$ can only contain at most $|F^*|$ distinct roots, so $k \leqslant |F^*|$.
Thus $k = |F^*|$, and so there exists an element of F^* having order $|F^*|$.
Hence $|F^*|$ is cyclic, which we wanted to prove. ☒

$(\mathbb{Z}/p\mathbb{Z})^*$ IS CYCLIC (p IS A PRIME)

For any prime p, we can show that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Proof. Note for any prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field.
So, by the above theorem, necessarily we must get that $\mathbb{Z}/p\mathbb{Z}$ is cyclic. ☒

CHINESE REMAINDER THEOREM

COPRIME / RELATIVELY PRIME

Let $a, b \in \mathbb{Z}$ be arbitrary.
Then, we say a and b are "coprime"
if $\gcd(a, b) = 1$.

PAIRWISE COPRIME

Let $m_1, m_2, \ldots, m_k$ be a list of integers.
We say this list is "pairwise coprime" if
every pair of distinct elements is coprime;
ie $\gcd(m_i, m_j) = 1$ if $i \neq j$.

CHINESE REMAINDER THEOREM FOR $\mathbb{Z}$

Let $a_1, a_2, \ldots, a_k$ denote arbitrary integers,
and let $m_1, m_2, \ldots, m_k$ be a list of
pairwise coprime integers.

Then, the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a solution $x \in \mathbb{Z}$, and this
solution is also unique in modulo $m_1 m_2 \cdots m_k$;
ie if $y \in \mathbb{Z}$ is a solution to the system above,
then $x \equiv y \pmod{m_1 m_2 \cdots m_k}$.

Proof. First, assume there exists integers
$b_1, b_2, \ldots, b_k$ such that

$$\begin{cases} b_1 \equiv 1 \pmod{m_1} \\ b_2 \equiv 0 \pmod{m_2} \\ \quad \vdots \\ b_k \equiv 0 \pmod{m_k} \end{cases}, \quad \begin{cases} b_2 \equiv 0 \pmod{m_1} \\ b_2 \equiv 1 \pmod{m_2} \\ \quad \vdots \\ b_k \equiv 0 \pmod{m_k} \end{cases} \quad \cdots \quad \begin{cases} b_k \equiv 0 \pmod{m_1} \\ b_k \equiv 0 \pmod{m_2} \\ \quad \vdots \\ b_k \equiv 1 \pmod{m_k} \end{cases}.$$

Then, note that

$$\sum_{i=1}^{k} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_k b_k$$
$$\equiv a_1(1) + a_2(0) + \cdots + a_k(0) \pmod{m_1}$$
$$\equiv a_1 \pmod{m_1},$$

so that $\sum_{i=1}^{k} a_i b_i \equiv a_1 \pmod{m_1}$.
Similar computations show $\sum_{i=1}^{k} a_i b_i \equiv a_j \pmod{m_j}$ $\forall j \in \{1, 2, \ldots, k\}$,
so that $x = \sum_{i=1}^{k} a_i b_i$ is a solution to the system of equations.

We now show why b_1 exists.
Since $b_1 \equiv 0 \pmod{m_i}$ $\forall i \in \{2, 3, \ldots, k\}$, it follows
that $b_1 \mid m_j$ $\forall j \in \{2, 3, \ldots, k\}$.

Let $M_1 = m_2 m_3 \cdots m_k$.
Then if $b_1 = c_1 M_1$ for some $c_1 \in \mathbb{Z}$, then b_1 automatically
satisfies $b_1 \equiv 0 \pmod{m_i}$ for $2 \leq i \leq k$.

Next, if b_1 satisfies the first congruence, we need
to find a $c_1 \in \mathbb{Z}$ such that $c_1 M_1 \equiv 1 \pmod{m_1}$.
We know this can only happen if $[c_1] = [M_1]^{-1}$ in $\mathbb{Z}/m_1\mathbb{Z}$,
which in turn can only occur iff $\gcd(M_1, m_1) = 1$.

But observe if $\gcd(M_1, m_1) \neq 1$, it implies M_1 & m_1 share
a prime factor.
By def$^{\underline{n}}$, this factor would divide both m_1 and one of
the other integers in $M_1 = m_2 m_3 \cdots m_k$, implying this
prime is a common factor of m_1 and some m_i for $i \neq 1$.
This is a contradiction, as $m_1, m_2, m_3, \ldots, m_k$ is pairwise
coprime by assumption!

Thus M_1 necessarily has a multiplicative inverse in $\mathbb{Z}/m_1\mathbb{Z}$,
implying $\exists c_1 \in \mathbb{Z}$ such that $c_1 M_1 \equiv 1 \pmod{m_1}$.
So letting $b_1 = c_1 M_1$ gives us the integer we want.
A similar proof can be used to show why $b_2, b_3, \ldots, b_k$
exist as well, (we can set $b_j = c_j M_j$, where $c_j \in \mathbb{Z}$ and $M_j = \prod_{j \neq i} m_j$)
and this is sufficient to show a solution exists. ※

Now, we can show why this solution is unique.
Suppose $x, y \in \mathbb{Z}$ both satisfy the system of congruences.
Then, in particular, $x \equiv y \pmod{m_i}$ $\forall i \in \{1, 2, \ldots, k\}$,
implying $m_i \mid (x - y)$ $\forall i$.

So, by A9 Q4, since $m_1, m_2, \ldots, m_k$ are pairwise coprime,
it follows that $(m_1 m_2 \cdots m_k) \mid (x - y)$,
implying $[x] = [y]$ in $\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z}$. ∎

EXAMPLE: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

We can use the Chinese Remainder Theorem to find the solutions $x \in \mathbb{Z}$ to the system

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

To start, let $M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$ and $M_3 = 3 \cdot 5 = 15$, using the notation from the proof.

Then c_1, c_2, c_3 are determined by solving

① $35c_1 \equiv 1 \pmod 3$;

$\Rightarrow 35c_1 - 36c_1 \equiv 1 - 36c_1 \pmod 3$

$\Rightarrow -c_1 \equiv 1 \pmod 3$ $\quad \because 36c_1 \mid 3$

$\therefore c_1 = 2$;

② $21c_2 \equiv 1 \pmod 5$; and

$\Rightarrow 21c_2 - 20c_2 \equiv 1 - 20c_2 \pmod 5$

$\Rightarrow c_2 \equiv 1 \pmod 5$ $\quad \because 20c_2 \mid 5$

$\therefore c_2 = 1$;

③ $15c_3 \equiv 1 \pmod 7$.

$\Rightarrow 15c_3 - 14c_3 \equiv 1 - 14c_3 \pmod 7$

$\Rightarrow c_3 \equiv 1 \pmod 7$ $\quad \because 14c_3 \mid 7$

$\therefore c_3 = 1$.

So, we get that $c_1 = -1$, $c_2 = 1$ and $c_3 = 1$.

Hence $b_1 = c_1 M_1 = -1(35) = -35$;

$b_2 = c_2 M_2 = 1(21) = 21$; and

$b_3 = c_3 M_3 = 1(15) = 15$,

so our solution to our system is

$$x = a_1 b_1 + a_2 b_2 + a_3 b_3 = 2(-35) + 3(21) + 2(15)$$

$$\Rightarrow x = 23.$$

This solution is unique modulo $3 \cdot 5 \cdot 7 = 105$, so that if $y \in \mathbb{Z}$ is another integer solution to the system, then $y \equiv 23 \pmod{105}$.

ISOMORPHISM

1. Let $\phi: R \to S$ be a ring homomorphism. Then, ϕ is an "isomorphism" if ϕ is also a bijection.

* a similar definition exists for homomorphisms between groups.

2. Alternatively, ϕ is also an isomorphism if there exists a ring homomorphism $\psi: S \to R$ such that $\psi \circ \phi = id_R$ and $\phi \circ \psi = id_S$, where id_R and id_S are the identity maps on R and S respectively.

3. If an isomorphism exists between rings R and S, then we say R and S are "isomorphic", and write $R \cong S$.

4. Note the relation "$\cong$" on rings is an equivalence relation.

$(\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z})(\mathbb{Z}/m_2\mathbb{Z}) \cdots (\mathbb{Z}/m_k\mathbb{Z})$

Suppose $m_1, m_2, \ldots, m_k$ are pairwise coprime positive integers. Then we must have that

$$(\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z})(\mathbb{Z}/m_2\mathbb{Z}) \cdots (\mathbb{Z}/m_k\mathbb{Z}).$$

Proof. First, let $[x]_n = n\mathbb{Z} + x$ for any $n \in \mathbb{Z}^+$, $x \in \mathbb{Z}$.

Then, let the homomorphism between rings $\phi: (\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z}) \to (\mathbb{Z}/m_1\mathbb{Z})(\mathbb{Z}/m_2\mathbb{Z}) \cdots (\mathbb{Z}/m_k\mathbb{Z})$ be defined by

$$\phi([x]_{m_1 m_2 \cdots m_k}) = ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_k}) \quad \forall [x]_{m_1 m_2 \cdots m_k} \in \mathbb{Z}/m_1 m_2 \cdots m_k.$$

First, we show this map is well-defined.

If $[x]_{m_1 m_2 \cdots m_k} = [y]_{m_1 m_2 \cdots m_k}$, then $(m_1 m_2 \cdots m_k) \mid (x-y)$.

In particular, we have that $m_1 \mid (x-y)$, $m_2 \mid (x-y)$ $\cdots$, $m_k \mid (x-y)$,

so $[x]_{m_i} = [y]_{m_i}$ for each $1 \le i \le k$.

Hence $\phi([x]_{m_1 m_2 \cdots m_k}) = \phi([y]_{m_1 m_2 \cdots m_k})$, showing this map is well-defined.

Then, we can similarly check ϕ preserves addition, multiplication and the unity.

To show ϕ is injective, we show $\ker \phi = \{0\}$.

Suppose we have a coset $[x]_{m_1 m_2 \cdots m_k}$ such that

$\phi([x]_{m_1 m_2 \cdots m_k}) = ([0]_{m_1}, [0]_{m_2}, \ldots [0]_{m_k})$.

Then x satisfies the system of congruences

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k}. \end{cases}$$

Clearly $x = 0$ is a solution to the system, and by the uniqueness of solutions in the CRT we can deduce that $x \equiv 0 \pmod{m_1 m_2 \cdots m_k}$, so $[0]_{m_1 m_2 \cdots m_k} = [x]_{m_1 m_2 \cdots m_k}$.

So $\ker \phi$ is the zero ideal, proving that ϕ is injective. #

Next, to show ϕ is surjective, suppose we are given an arbitrary element

$$([a_1]_{m_1}, [a_2]_{m_2}, \ldots, [a_k]_{m_k}) \in \prod_{i=1}^{k} (\mathbb{Z}/m_i\mathbb{Z}).$$

By CRT, $\exists x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

and since

$$\phi([x]_{m_1 m_2 \cdots m_k}) = ([a_1]_{m_1}, [a_2]_{m_2}, \ldots, [a_k]_{m_k}),$$

it follows that ϕ is surjective.

So, since ϕ is both injective & surjective, it follows that ϕ is bijective, and so ϕ is an isomorphism from $\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z}$ to $(\mathbb{Z}/m_1\mathbb{Z})(\mathbb{Z}/m_2\mathbb{Z}) \cdots (\mathbb{Z}/m_k\mathbb{Z})$. ∎

FIELD OF FRACTIONS OF AN INTEGRAL DOMAIN

THE "FRACTION" EQUIVALENCE RELATION

Let R be an integral domain.
Let the relation $\sim$ on $R \times (R\setminus\{0\})$ be such that $(a,b) \sim (c,d)$ if $ad = bc$.
Then $\sim$ is an equivalence relation.

Proof. First, since $ab = ba$, it follows that $(a,b) \sim (a,b)$, showing $\sim$ is reflexive.

Then, if $(a,b) \sim (c,d)$, then necessarily $ad = bc$; thus $cb = da$, so that $(c,d) \sim (a,b)$.

Lastly, suppose we are given $(a,b), (c,d), (e,f) \in R\times(R\setminus\{0\})$ such that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.
By def$^{\underline{n}}$, this implies $ad = bc$ and $cf = de$.
Multiplying the former eq$^{\underline{n}}$ by f yields

$$adf = bcf$$
$$\Rightarrow adf = b(de)$$
$$\Rightarrow af(d) = be(d).$$

Then, since R is an integral domain and $d \neq 0$, we can use the cancellation property to conclude that $af = be$, so that $(a,b) \sim (e,f)$, and thus that $\sim$ is transitive. ∎

We denote the set of equivalence classes of $\sim$ by $Q(R)$.

Example: $\mathbb{Q}$
$[(a,b)]$ "stands for" $\frac{a}{b}$.

FIELD OF FRACTIONS

Let R be an integral domain.
Then, we can define an addition operation on $Q(R)$ by

$$[(a,b)] + [(c,d)] = [(ad+bc),\ bd)]$$

and a multiplication operation by

$$[(a,b)] \times [(c,d)] = [(ac,\ bd)].$$

We can show that $Q(R)$ is a field with respect to these two operations, called the "field of fractions" of R.

*for notational ease, we write $\frac{a}{b}$ to represent the equivalence class $[(a,b)]$ in $Q(R)$.

Proof. First, suppose $[(a_1,b_1)] = [(a_2,b_2)]$ and $[(c_1,d_1)] = [(c_2,d_2)]$.
Then, this implies $a_1b_2 = b_1a_2$ & $c_1d_2 = d_1c_2$.
Subsequently, note that

$$(a_1d_1 + b_1c_1)(b_2d_2) = (a_1b_2)d_1d_2 + (c_1d_2)b_1b_2$$
$$= (b_1a_2)d_1d_2 + (d_1c_2)b_1b_2$$
$$= (a_2d_2 + b_2c_2)(b_1d_1),$$

and thus $[(a_1d_1+b_1c_1),\ b_1d_1] = [(a_2d_2+b_2c_2,\ b_2d_2)]$,
so $[(a_1,b_1)] + [(c_1,d_1)] = [(a_2,b_2)] + [(c_2,d_2)]$,
showing $+$ is well defined.
A similar proof shows $\times$ is also well defined.

Next, we claim $[(0,b)] \in Q(R)$ is the additive identity, where $b \in R\setminus\{0\}$ is arbitrary.
Indeed, note for any $[(c,d)] \in Q(R)$, we have that

$$[(0,b)] + [(c,d)] = [(0\cdot d + bc,\ bd)] = [(bc, bd)] = [(c,d)]$$

(the last equality holds since $bcd = bdc$.)
A similar check shows that $[(c,d)] + [(0,b)] = [(c,d)]$, so that $[(0,b)]$ is the additive identity.

A similar proof shows $[(1,1)]$ is the multiplicative identity of $Q(R)$.

Subsequently, we claim for any $[(a,b)] \in Q(R)$ with $[(a,b)] \neq [(0,c)]$ for any $c \in R\setminus\{0\}$, $[(b,a)] = [(a,b)]^{-1}$.
First, note $a \neq 0$, since $[(a,b)] \neq [(0,c)]$ implies $ac \neq 0$, and so $a \neq 0$ as $c \neq 0$.
Thus $[(b,a)] \in Q(R)$, and

$$[(b,a)] \cdot [(a,b)] = [(ba, ab)] = [(1,1)],$$

with a similar proof showing that $[(a,b)] \cdot [(b,a)] = [(1,1)]$, so that $[(a,b)] = [(b,a)]^{-1}$.

We can use similar lines of reasoning to show $Q(R)$ obeys the other conditions of a field. ∎

$R \cong \{\frac{r}{1} : r \in R\}$

Let R be an integral domain. Then R is isomorphic to the subring $\{\frac{r}{1} : r \in R\} \subseteq Q(R)$.

Proof. We first verify $R_0 = \{\frac{r}{1} : r \in R\}$ is a subring of $Q(R)$.
Clearly since $\frac{1}{1} \in R_0$, so that R_0 has the unity of $Q(R)$.
Then, given $\frac{a}{1}, \frac{b}{1} \in R_0$, notice that

$$\frac{a}{1} - \frac{b}{1} = \frac{a\cdot 1 - b\cdot 1}{1\cdot 1} = \frac{a-b}{1} \in R_0$$

and

$$\frac{a}{1}\cdot\frac{b}{1} = \frac{ab}{1\cdot 1} = \frac{ab}{1} \in R_0,$$

so by the Subring Test R_0 is a subring of R.

Subsequently, let the function $\sigma : R \to R_0$ by $\sigma(r) = \frac{r}{1}$ $\forall r \in R$.
We claim σ is a ring homomorphism.
Indeed, for any $r, s \in R$, we have that

① $\sigma(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \sigma(r) + \sigma(s)$;

② $\sigma(rs) = \frac{rs}{1} = \frac{rs}{1\cdot 1} = \frac{r}{1}\cdot\frac{s}{1} = \sigma(r) + \sigma(s)$; and

③ $\sigma(1) = \frac{1}{1}$,

so that σ is a ring homomorphism.
Moreover, σ is clearly surjective, and the fact that $\ker\sigma = \{0\}$ (since $\sigma(r) = \frac{0}{1}$ implies $r = 0$) tells us σ is also injective.
Thus σ is bijective, and hence must also be an isomorphism, proving the claim. ∎

EVERY ELEMENT OF R HAS AN INVERSE IN Q(R)

Let R be an integral domain. Then for every element $a \in R$, there exists an $a^{-1} \in Q(R)$ such that $a \cdot a^{-1} = 1$.

Proof. Note since $Q(R)$ is a field, every non-zero element of R_0 has an inverse in $Q(R)$.
But since $R_0 \cong R$, the claim follows from here.

EVERY ELEMENT OF Q(R) CAN BE WRITTEN AS ab^{-1}; $a \in R$, $b \in R$

Let R be an integral domain. Then for any element $q \in Q(R)$, we can show there must exist some $a \in R$, $b \in R$ such that $q = ab^{-1}$.

Proof. This follows from the fact that

$$\frac{a}{b} = \frac{a}{1}\cdot\frac{1}{b} = \left(\frac{a}{1}\right)\cdot\left(\frac{b}{1}\right)^{-1} = ab^{-1}$$

(and that $\frac{a}{b} \in Q(R)$). ∎

LOCALISATION

MULTIPLICATIVE SET

Let R be an integral domain.
Then, a subset $S \subseteq R$, where $S \neq \emptyset$, is called a "multiplicative set" if $1 \in S$ and S is closed under multiplication; ie if $a \in S$ and $b \in S$, then $ab \in S$.

LOCALISATION

1. Let R be an integral domain, and S be a multiplicative set S in R.
Then the "localisation of R at S", denoted as $S^{-1}R$, is defined to be the set of equivalence classes of ordered pairs in $R \times S$, with the equivalence relation being that $(a,b) \sim (c,d)$ if $ad = bc$ in R.

2. The addition and multiplication operations are the same in $S^{-1}R$ as they are in $Q(R)$.

3. Also, R is isomorphic to a similar subring of $S^{-1}R$ (ie with denominator 1) and every element of S has a multiplicative inverse in $S^{-1}R$.

COMPLEX NUMBERS

1. The set of complex numbers, or $\mathbb{C}$, is given to be the set of ordered pairs $(a,b) \in \mathbb{R} \times \mathbb{R}$, where we represent each ordered pair (a,b) by $a+bi$, where $i^2 = -1$.

2. Moreover, we define an addition on $\mathbb{C}$ by
$$(a+bi) + (c+di) = (a+c) + (b+d)i$$
and a multiplication on $\mathbb{C}$ by
$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i.$$

$\mathbb{C}$ IS A FIELD

With respect to the two operations defined above, we can show $\mathbb{C}$ is a field.

Proof. Since $+$ agrees with the ordinary additive structure on $\mathbb{R} \times \mathbb{R}$, we can deduce $\mathbb{C}$ is an abelian group under addition.

Then, note that
$$\begin{aligned}((a+bi)(c+di))(e+fi) &= ((ac-bd) + (ad+bc)i)(e+fi) \\ &= ((ac-bd)e - (ad+bc)f) + ((ad+bc)e + (ac-bd)f) \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i\end{aligned}$$
and
$$\begin{aligned}(a+bi)((c+di)(e+fi)) &= (a+bi)((ce-df) + (de+cf)i) \\ &= (a(ce-df) - b(de+cf)) + (b(ce-df) + a(de+cf))i \\ &= (ace - adf - bde - bcf) + (bce - bdf + ade + acf)i \\ &= ((a+bi)(c+di))(e+fi),\end{aligned}$$
showing multiplication in $\mathbb{C}$ is associative.

Moreover, $1 \in \mathbb{C}$ is a multiplicative identity, and note that
$$\begin{aligned}(a+bi)(c+di) &= (ac-bd) + (bc+ad)i \\ &= (ca-db) + (cb+da)i \\ &= (c+di)(a+bi),\end{aligned}$$
showing multiplication is commutative in $\mathbb{C}$.

Next, observe that for any $a+bi \in \mathbb{C}$, we have that
$$\begin{aligned}(a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) &= \left(\frac{a^2}{a^2+b^2} - \left(\frac{-b^2}{a^2+b^2}\right)\right) + \left(\frac{ab}{a^2+b^2} - \frac{ab}{a^2+b^2}\right)i \\ &= 1 + 0i \\ &= 1,\end{aligned}$$
so that every $a+bi \in \mathbb{C}$ has a multiplicative inverse $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$ in $\mathbb{C}$.

We could also show the distributive laws hold in $\mathbb{C}$; this would be sufficient to show $\mathbb{C}$ is a field. $\blacksquare$

TERMINOLOGY

STANDARD FORM

Let $z \in \mathbb{C}$. Then, the form $z = a+bi$, where $a,b \in \mathbb{R}$, is called the "standard form" for z.

REAL PART

Let $z \in \mathbb{C}$, and suppose $z = a+bi$, where $a,b \in \mathbb{R}$.
Then we say $a \in \mathbb{R}$ is the "real part" of z, denoted by $\operatorname{Re}(z)$.

IMAGINARY PART

Let $z \in \mathbb{C}$, and suppose $z = a+bi$, where $a,b \in \mathbb{R}$.
Then, we say $b \in \mathbb{R}$ is the "imaginary part" of z, denoted by $\operatorname{Im}(z)$.

COMPLEX CONJUGATE

Let $z \in \mathbb{C}$, and suppose $z = a+bi$, where $a,b \in \mathbb{R}$.
Then the "complex conjugate" of z, denoted by $\bar{z}$, is defined to be the complex number
$$\bar{z} = a - bi.$$

MODULUS

Let $z \in \mathbb{C}$, and suppose $z = a+bi$, where $a,b \in \mathbb{R}$.
Then, the "modulus" of z, denoted by $|z|$, is defined to be
$$|z| = \sqrt{a^2+b^2}.$$

PROPERTIES OF COMPLEX NUMBERS

$\overline{z+w} = \overline{z} + \overline{w}$

Let $z, w \in \mathbb{C}$ be arbitrary.
Then $\overline{z+w} = \overline{z} + \overline{w}$.

Proof. Write $z = a+bi$ and $w = c+di$, where $a, b, c, d \in \mathbb{R}$.
Then $z+w = (a+c) + (b+d)i$.
Thus
$$\begin{aligned} \overline{z+w} &= (a+c) - (b+d)i \\ &= a+c - bi - di \\ &= (a-bi) + (c-di) \\ &= \overline{z} + \overline{w}, \end{aligned}$$
as needed. $\blacksquare$

$\overline{zw} = \overline{z} \cdot \overline{w}$

Let $z, w \in \mathbb{C}$ be arbitrary.
Then $\overline{zw} = \overline{z} \cdot \overline{w}$.

Proof. Again, write $z = a+bi$ and $w = c+di$, where $a, b, c, d \in \mathbb{R}$.
Then $zw = (ac-bd) + (ad+bc)i$;
thus,
$$\overline{zw} = (ac-bd) - (ad+bc)i.$$
But
$$\begin{aligned} \overline{z} \cdot \overline{w} &= (a-bi)(c-di) \\ &= (ac-(-b)(-d)) + (-bc-ad)i \\ &= (ac+bd) - (ad+bc)i \\ &= \overline{zw}, \end{aligned}$$
completing the proof. $\blacksquare$

$\overline{z^{-1}} = \overline{z}^{-1}$

Let $z \in \mathbb{C}$. Then $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$.

Proof. Write $z = a+bi$, where $a, b \in \mathbb{R}$.
Then $\frac{1}{z} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, implying that
$$\overline{\left(\frac{1}{z}\right)} = \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2}i.$$
But notice that
$$\begin{aligned} \frac{1}{\overline{z}} &= \frac{1}{a-bi} = \frac{1}{a-bi} \cdot \frac{a+bi}{a+bi} \\ &= \frac{a+bi}{a^2+b^2} \\ &= \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2}i \\ &= \overline{\left(\frac{1}{z}\right)}, \end{aligned}$$
completing the proof. $\blacksquare$

$\overline{\overline{z}} = z$

Let $z \in \mathbb{C}$. Then $\overline{(\overline{z})} = z$.
(Trivial proof.)

$z + \overline{z} = 2\mathrm{Re}(z)$

Let $z \in \mathbb{C}$.
Then $z + \overline{z} = 2\mathrm{Re}(z)$.
(Trivial proof.)

$z - \overline{z} = 2i\,\mathrm{Im}(z)$

Let $z \in \mathbb{C}$.
Then $z - \overline{z} = 2i\,\mathrm{Im}(z)$.
(Trivial proof.)

$z \cdot \overline{z} = |z|^2$

Let $z \in \mathbb{C}$.
Then $z \cdot \overline{z} = |z|^2$.

Proof. Let $z = a+bi$, where $a, b \in \mathbb{R}$.
Then
$$\begin{aligned} z \cdot \overline{z} &= (a+bi)(a-bi) \\ &= a^2+b^2 \\ &= \left(\sqrt{a^2+b^2}\right)^2 \\ &= |z|^2, \end{aligned}$$
as needed. $\blacksquare$

$\mathrm{Re}(z) \leq |\mathrm{Re}(z)| \leq |z|$

Let $z \in \mathbb{C}$.
Then $\mathrm{Re}(z) \leq |\mathrm{Re}(z)| \leq |z|$.

Proof. Let $z = a+bi$, where $a, b \in \mathbb{R}$.
Then clearly $a \leq |a|$, establishing the first inequality.
Next, note
$$\begin{aligned} |\mathrm{Re}(z)|^2 &= a^2 \\ &\leq a^2+b^2 \quad \because b^2 \geq 0 \\ &= |z|^2, \end{aligned}$$
so that $|\mathrm{Re}(z)| \leq |z|$, establishing the second inequality. $\blacksquare$

$\mathrm{Im}(z) \leq |\mathrm{Im}(z)| \leq |z|$

Let $z \in \mathbb{C}$.
Then $\mathrm{Im}(z) \leq |\mathrm{Im}(z)| \leq |z|$.
(Similar proof to the "Re" section.)

$|zw| = |z||w|$

Let $z, w \in \mathbb{C}$.
Then $|zw| = |z||w|$.

Proof. Write $z = a+bi$ and $w = c+di$, for some $a, b, c, d \in \mathbb{R}$.
Then $zw = (a+bi)(c+di)$
$\therefore zw = (ac-bd) + (bc+ad)i$,
so that
$$\begin{aligned} |zw|^2 &= (ac-bd)^2 + (bc+ad)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + b^2c^2 + 2adbc + a^2d^2 \\ &= a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= |z|^2|w|^2, \end{aligned}$$
implying that $|zw| = |z||w|$, as required. $\blacksquare$

$|\overline{z}| = |z|$

Let $z \in \mathbb{C}$.
Then $|\overline{z}| = |z|$.
(Proof is trivial.)

TRIANGLE INEQUALITY FOR $\mathbb{C}$

Let $z, w \in \mathbb{C}$ be arbitrary.
Then necessarily $|z+w| \leq |z| + |w|$.

Proof. First, note that
$$\begin{aligned} |z+w|^2 &= (z+w)\overline{(z+w)} \\ &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + w\overline{z} + z\overline{w} + w\overline{w} \\ &= |z|^2 + |w^2| + (z\overline{w} + \overline{(z\overline{w})}) \\ &= |z|^2 + |w^2| + 2\mathrm{Re}(z\overline{w}). \end{aligned}$$
Then, since $\mathrm{Re}(z\overline{w}) \leq |z\overline{w}| = |z| \cdot |\overline{w}| = |z||w|$, it follows that
$$\begin{aligned} |z+w|^2 &= |z|^2 + |w|^2 + 2\mathrm{Re}(z\overline{w}) \\ &\leq |z^2| + |w^2| + 2|z||w| \end{aligned}$$
$$\therefore |z+w|^2 = (|z|+|w|)^2,$$
and taking the square root of both sides yields
$$|z+w| \leq |z| + |w|,$$
which we wanted to show. $\blacksquare$

POLAR FORM

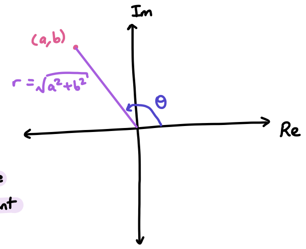
$e^{i\theta}$

1. Let the angle $\theta \in \mathbb{R}$ (in radians) be arbitrary.
Then, we define the complex exponential function at θ, denoted by $e^{i\theta}$, by
$$e^{i\theta} = \cos\theta + i\sin\theta.$$

2. Note that regardless of θ,
$$|e^{i\theta}| = \sqrt{\cos^2\theta + \sin^2\theta} = \sqrt{1} = 1.$$

POLAR FORM

Let $z \in \mathbb{C}$ be arbitrary.
Then the "polar" form of z is given by
$$z = re^{i\theta},$$
where $r = |z|$ and θ is the angle from the positive x-axis to the line segment from (a,b) to the origin.



ARGUMENT

Let $z \in \mathbb{C}$ be arbitrary, and write $z = re^{i\theta}$, with $r, \theta \in \mathbb{R}$.
Then θ is called the "argument" of z.

MULTIPLICATION IN POLAR FORM

Suppose $z_1, z_2 \in \mathbb{C}$ are given in polar form, with $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, for some $r_1, r_2 \in \mathbb{R}^+$ and $\theta_1, \theta_2 \in \mathbb{R}$.
Then $z_1 z_2 = (r_1 r_2)\, e^{i(\theta_1+\theta_2)}$.

Proof. By definition,
$$z_1 = r_1 e^{i\theta_1} = r_1(\cos\theta_1 + i\sin\theta_1)$$
and $$z_2 = r_2 e^{i\theta_2} = r_2(\cos\theta_2 + i\sin\theta_2).$$

Thus
$$\begin{aligned} z_1 z_2 &= (r_1(\cos\theta_1 + i\sin\theta_1))(r_2(\cos\theta_2 + i\sin\theta_2)) \\ &= r_1 r_2 (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2 [(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + (\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)i] \\ &= r_1 r_2 [(\cos(\theta_1+\theta_2)) + (\sin(\theta_1+\theta_2))i] \end{aligned}$$
$\therefore z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$, which we wanted to show. ☒

DE MOIVRE'S THEOREM

Let $z \in \mathbb{C}\setminus\{0\}$ be arbitrary, and suppose $z = re^{i\theta}$, where $r \in \mathbb{R}^+$ and $\theta \in \mathbb{R}$.
Then, for any $n \in \mathbb{Z}$, we have that
$$z^n = r^n e^{i(n\theta)}.$$

Proof. First, if $n=0$, then $z^0 = 1 = r^0 e^{i(0)\theta} = 1$, proving the base case.

Then, assume the result is true for some $n \in \mathbb{N}$.
This implies $z^n = r^n e^{i(n\theta)}$.
So,
$$\begin{aligned} z^{n+1} = z^n \cdot z &= (r^n e^{i(n\theta)})(re^{i\theta}) \\ &= r^{n+1} e^{i(n\theta+\theta)} \\ \therefore z^{n+1} &= r^{n+1} e^{i(n+1)\theta}, \end{aligned}$$
proving the claim holds for $n+1$ as well.
It follows by induction that the claim is true $\forall n \in \mathbb{N}$.

Moreover, observe for any $n \in \mathbb{N}$,
$$(r^{-n} e^{i(-n\theta)})(r^n e^{i(n\theta)}) = 1.$$
But since $r^n e^{i(n\theta)} = (re^{i\theta})^n$,
it follows that $(r^{-n} e^{i(-n\theta)}) = (re^{i\theta})^{-n}$,
which exists by uniqueness of inverses.
Therefore the claim is true $\forall n \in \mathbb{Z}$, and we are done. ☒

THE FUNDAMENTAL THEOREM OF ALGEBRA

The Fundamental Theorem of Algebra states that any non-constant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$; ie there always exists a $c \in \mathbb{C}$ such that $f(c) = 0$.

ALGEBRAICALLY CLOSED

1. Let F be a field. Then, we say F is "algebraically closed" if every non-constant polynomial $f \in F[x]$ has a root in F.

2. Alternatively, F is algebraically closed if and only if every non-constant polynomial $f \in F[x]$ can be factored as a product of linear polynomials
$$f = c(x-a_1)(x-a_2)\cdots(x-a_n),$$
where $c, a_1, \ldots, a_n \in F$ and $n = \deg(f)$.

Proof. First, suppose F is algebraically closed.
Then, if $n=1$, $f = ax+b$ for some $a, b \in F$ with $a \neq 0$, so that $f = a(x + a^{-1}b)$ gives the required factorisation of f in the required form.
Now, assume the claim is true for all polynomials of degree n in $F[x]$, where $n \geq 1$.
Let $f \in F[x]$ has degree $n+1$.
Then, since F is algebraically closed, f must have a root in F.
Let this root be a_{n+1}.
So, by the Factor Theorem, $f = g(x - a_{n+1})$, where $g \in F[x]$.
In particular, $\deg(g) = n$, so that by the induction hypothesis, we have that
$$g = c(x-a_1)(x-a_2)\cdots(x-a_n)$$
so that
$$f = g(x-a_{n+1}) = c(x-a_1)(x-a_2)\cdots(x-a_n)(x-a_{n+1}),$$
proving the claim is true for $n+1$ also.
By induction, it follows that the claim is true $\forall n \in \mathbb{N}$. ✳

Conversely, assume F is a field for which every non-constant polynomial in $F[x]$ factors as a product of linear polynomials.
This implies for any $f \in F[x]$ which is non-constant, we can write
$$f = c(x-a_1)(x-a_2)\cdots(x-a_n),$$
where $n = \deg(f) \geq 1$.
Indeed, as $a_1, a_2, \ldots, a_n$ are roots of f, it follows that F is algebraically closed, proving the backward argument. ☒

SOLVING EQUATIONS IN $\mathbb{C}$

SOLVING $z^n = a$ IN $\mathbb{C}$

Let $a \in \mathbb{C}$ and $n \in \mathbb{Z}^+$ be arbitrary.
Write a in polar form, so that $a = re^{i\theta}$
for some $r \in \mathbb{R}^+$ and $\theta \in \mathbb{R}$.
Then there are exactly n distinct solutions
z to the equation $z^n = a$, given by

$$z = \sqrt[n]{r} \cdot e^{i\left(\frac{\theta + 2k\pi}{n}\right)},$$

where $k \in \{0, 1, \dots, n-1\}$.

Proof. First, assume z is a solution to the eqn (which we know exists due to the fundamental theorem of algebra), and write $z = se^{i\phi}$, where $s > 0$ and $\phi \in \mathbb{R}$. This implies that

$$z^n = (se^{i\phi})^n = s^n e^{ni\phi} = a = re^{i\theta}.$$

Then, since $|s^n e^{ni\phi}| = |re^{i\theta}|$ it follows that $r = s^n$, so that $s = \sqrt[n]{r}$.

Additionally, $n\phi = \theta + 2k\pi$ for some $k \in \mathbb{Z}$, so that $\phi = \frac{\theta}{n} + \frac{2k\pi}{n}$.

But note that only taking $k = 0, 1, \dots, n-1$ yields distinct values for the argument of z, so that there are exactly n possible nth roots.

Finally, we can verify these are indeed roots of the equation:

$$\left(\sqrt[n]{r} \cdot e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)}\right)^n = re^{i(\theta + 2k\pi)} = re^{i\theta} = a. \quad \blacksquare$$

EXAMPLE: $z^4 = (1+i)$

We can use the method described above to find the solutions in $\mathbb{C}$ of the equation $z^4 = (1+i)$.

First, note $r = \sqrt{1^2 + 1^2} = \sqrt{2}$, and that $\theta = \tan^{-1}\left(\frac{1}{1}\right) = \frac{\pi}{4}$, so that

$$1 + i = \sqrt{2}\, e^{i\frac{\pi}{4}}.$$

It follows that

$$z = (\sqrt{2})^{\frac{1}{4}} e^{i\left(\frac{(\frac{\pi}{4})}{4} + \frac{2k\pi}{4}\right)}, \quad k \in \{0, 1, 2, 3\}$$

$$\Rightarrow z = 2^{\frac{1}{8}} e^{i\left(\frac{\pi}{16} + \frac{k\pi}{2}\right)}, \quad k \in \{0, 1, 2, 3\}.$$

QUADRATIC FORMULA FOR A FIELD

Let F be a field with $\operatorname{char} F \neq 2$, and suppose we are given $a, b, c \in F$ with $a \neq 0$.
Suppose further there exists a $y \in F$ such that $y^2 = b^2 - 4ac$.
Then the quadratic equation

$$ax^2 + bx + c = 0$$

has solutions given exactly by

$$x = (-b \pm y)(2a)^{-1}.$$

Proof. First, notice that

$$a\left((-b \pm y)(2a)^{-1}\right)^2 + b(-b \pm y)(2a^{-1}) + c = (4a)^{-1}(b^2 \mp 2by + y^2) + (2a)^{-1}(-b \pm by) + c$$
$$= (4a^{-1})(b^2 \mp 2by + b^2 - 4ac - 2b^2 \pm 2by + 4ac)$$
$$= 0,$$

so that both values of x given above are solutions to the quadratic equation. $*$

Conversely, suppose that $x \in F$ satisfies $ax^2 + bx + c = 0$.

Then, $a(x^2 + a^{-1}bx) + c = 0$

$$\Rightarrow a(x^2 + a^{-1}bx + (2a)^{-2}b^2) - (4a)^{-1}b^2 + c = 0$$
$$a(x + (2a)^{-1}b)^2 + (4a)^{-1}(4ac - b^2) = 0$$
$$\Rightarrow a(x + (2a)^{-1}b)^2 = (b^2 - 4ac)(4a)^{-1}$$
$$\therefore (x + (2a)^{-1}b)^2 = (b^2 - 4ac)(2a)^{-2}.$$

From here, note the two square roots of the RHS are $y \cdot (2a)^{-1}$ and $-y \cdot (2a)^{-1}$, since $y^2 = b^2 - 4ac$.

Thus $x + (2a)^{-1}b = \pm y \cdot (2a)^{-1}$

and so

$$x = -(2a)^{-1}b \pm y(2a)^{-1},$$

$$\therefore x = (-b \pm y) \cdot (2a)^{-1},$$

proving the theorem. $\blacksquare$

IRREDUCIBLE POLYNOMIALS

Let F be a field, and $f \in F[x]$ a non-constant polynomial.

Then we say that f is "reducible" if f admits a proper factorisation $f = gh$, where $g, h \in F[x]$ and $\deg(g), \deg(h) \geq 1$.

Otherwise, we say f is "irreducible".

In other words, f is irreducible if whenever we have a factorisation $f = gh$ with $g, h \in F[x]$, necessarily either g or h must be constant.

$\deg f \geq 2$, f IS IRREDUCIBLE $\Rightarrow$ f HAS NO ROOTS IN F

Let F be an arbitrary field, and $f \in F[x]$ be a polynomial with $\deg(f) \geq 2$.

Suppose f is irreducible.

Then f has no roots in F.

Proof. Suppose f has a root $c \in F$.

Then, by the Factor Theorem, this implies we can write $f = (x-c)h$ for some $h \in F[x]$.

But since $\deg(x-c) = 1$ and $\deg(h) = \deg(f) - 1 \geq 1$, this is a contradiction to our assumption that f is irreducible.

Thus f cannot have any roots in F, proving the claim. ∎

$\deg(f) = 2$ or 3, f HAS NO ROOTS IN F $\Rightarrow$ F IS IRREDUCIBLE

Let F be an arbitrary field, and $f \in F[x]$ be a polynomial such that $\deg(f) = 2$ or $\deg(f) = 3$.

Suppose f has no roots in F.

Then f is irreducible.

Proof. Suppose f is reducible.

Then we can write $f = gh$, where $g, h \in F[x]$ are non-constant polynomials.

It follows that $\deg(f) = \deg(g) + \deg(h)$, and so (since $\deg(f) = 2$ or $\deg(f) = 3$) it forces $\deg(g) = 1$ or $\deg(h) = 1$.

Either way, this means f has a linear factor, and this linear factor necessarily has a root in F.

In turn, this implies f has a root in F, which is a contradiction.

Thus f is irreducible after all, which we wanted to prove. ∎

f IS IRREDUCIBLE $\Leftrightarrow$ $\deg(f) = 1$ (f IS A NON-CONSTANT POLYNOMIAL IN AN ALGEBRAICALLY CLOSED FIELD)

Let F be an algebraically closed field.

Then a non-constant polynomial $f \in F[x]$ is irreducible if and only if $\deg(f) = 1$.

Proof. Clearly, a linear polynomial over any field is irreducible.

Conversely, if $f \in F[x]$ is irreducible and $\deg(f) > 1$, then f has no roots in F.

But this is impossible since F is algebraically closed, so that there are no irreducible polynomials of degree larger than 1 in $F[x]$. ∎

IRREDUCIBLE POLYNOMIALS IN $\mathbb{R}[x]$

$f(c) = 0 \Rightarrow f(\bar{c}) = 0$

Suppose $f \in \mathbb{R}[x]$ is such that $f(c) = 0$, where $c \in \mathbb{C}$.

Then necessarily $f(\bar{c}) = 0$ also.

Proof. First, write

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n \in \mathbb{R}$ and $a_n \neq 0$.

Then, since $f(c) = 0$, it follows that

$$0 = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0.$$

Taking conjugates of both sides yields that

$$\bar{0} = 0 = \overline{a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0}$$

$$= \overline{a_n}\,\overline{c^n} + \overline{a_{n-1}}\,\overline{c^{n-1}} + \cdots + \overline{a_1}\,\overline{c} + \overline{a_0}$$

$$= a_n \bar{c}^n + a_{n-1}\bar{c}^{n-1} + \cdots + a_1 \bar{c} + a_0,$$

so that $f(\bar{c}) = 0$, completing the proof. ∎

f IS IRREDUCIBLE IN $\mathbb{R}[x]$ $\Leftrightarrow$ $\deg(f) = 1$ OR $\deg(f) = 2$ AND f HAS NO REAL ROOTS

Let $f \in \mathbb{R}[x]$ be a non-constant polynomial.

Then f is irreducible in $\mathbb{R}[x]$ if and only if $\deg(f) = 1$, or $\deg(f) = 2$ and f has no real roots.

Proof. First, if $\deg(f) = 1$ or $\deg(f) = 2$ and f has no real roots, then the work in the previous sections tell us that f is irreducible.

Conversely, suppose $f \in \mathbb{R}[x]$ is an irreducible, non-constant polynomial.

Since $\mathbb{R} \subseteq \mathbb{C}$, it follows that $f \in \mathbb{C}[x]$ also.

Then, by the Fundamental Theorem of Algebra, f has a complex root $c \in \mathbb{C}$.

If $c \in \mathbb{R}$, then f has a real root, and the irreducibility of f forces $\deg(f) = 1$.

Otherwise, $c \notin \mathbb{R}$, so that $\bar{c} \neq c$ and so $\bar{c}$ is also a root of f.

Then, applying the Factor Theorem, we get that $f = (x-c)(x-\bar{c})h$ for some other polynomial $h \in \mathbb{C}[x]$.

Note that $g = (x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + c\bar{c} = x^2 - (2\operatorname{Re} c)x + |c|^2 \in \mathbb{R}[x]$.

Thus, if we carry out division with remainder of f by g in $\mathbb{R}[x]$, we get that $f = gh' + r$, where $h', r \in \mathbb{R}[x]$ and $\deg(r) < 2$.

But if we do the same division with remainder over $\mathbb{C}[x]$, we know we get that $f = gh + 0$.

Since the remainders are unique, it follows that $r = 0$, so that $h = h'$.

Consequently, $f = gh$ in $\mathbb{R}[x]$, where $\deg(g) = 2$.

By the irreducibility of f, h must be a constant polynomial.

This implies $f = kg$, where k is constant, so that f is also of degree 2 with no real roots. ∎

IRREDUCIBLE POLYNOMIALS IN $\mathbb{Q}[x]$

RATIONAL ROOTS THEOREM

Let $f \in \mathbb{Q}[x]$ be a non-constant polynomial, and suppose $r \in \mathbb{Q}$ is a root of f. Suppose further that

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $a_n \neq 0$.

Then, if $r = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $\gcd(p,q) = 1$, we must have that $q \mid a_n$ and $p \mid a_0$ in $\mathbb{Z}$.

Proof. Since $f(\frac{p}{q}) = 0$, it follows that

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 1.$$

Multiplying both sides by q^n and re-arranging gives us that

$$\begin{aligned} a_0 q^n &= -(a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1}) \\ &= -p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}), \end{aligned}$$

showing that $p \mid a_0 q^n$.

Then since $\gcd(p, q^n) = 1$, it follows that $p \mid a_0$.

Similarly, if we isolate for $a_n p^n$ instead of $a_0 q^n$, we deduce that $q \mid a_n p^n$, and since $\gcd(q, p^n) = 1$, we get that $q \mid a_n$, completing the proof. $\boxtimes$

SHOWING NUMBERS ARE IRRATIONAL

1. We can use the Rational Roots Theorem to evaluate whether a given $\gamma \in \mathbb{R}$ is irrational.

2. Example: we can show that $\sqrt{2} + \sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$.

First, let $\alpha = \sqrt{2} + \sqrt{3}$.

Then note that

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{6} + 3 \\ &= 5 + 2\sqrt{6} \end{aligned}$$

so that

$$\alpha^2 - 5 = 2\sqrt{6}$$

and hence

$$\begin{aligned} (\alpha^2 - 5)^2 &= (2\sqrt{6})^2 \\ &= 24 \end{aligned}$$

$$\Rightarrow \alpha^4 - 10\alpha^2 + 25 = 24$$

and so α is a solution to the polynomial

$$f = x^4 - 10x^2 + 1.$$

Then, by the Rational Roots Theorem, the only candidate rational roots of f are 1 and -1; but since $f(1) = f(-1) = -8 \neq 0$, this implies that α, being a root of f, cannot be rational!