Informally an algorithm is a sequence of computational steps that transform the input into the output.

– Algorithm is a sequence of steps. Finite? Always correct? ....
Analysis of Algorithms, $O(\cdot)$ notation.

- Analyzing algorithms helps to predict the amount of resources a computation requires.
  
  - **Time complexity**: number of elementary steps
  - **Space complexity**: number of memory cells
Analysis of Algorithms, $O(\cdot)$ notation.

- Analysis of algorithms should tell us about the algorithm itself not about particular machine dependent implementation.
- We would like to estimate the rate of growth of the running time (number of steps) with respect to the input size.
- Constant factors are less significant in determining computational efficiency for large inputs.
- We concern with asymptotic (i.e. at the limit) efficiency of algorithms.
Analysis of Algorithms, $O(\cdot)$ notation.

– Usually algorithms have inputs. Let $I$ be the set of all possible inputs to an algorithm $A$. With every input from $I$ we associate a size value using size function

$$| \cdot | : I \rightarrow \mathbb{N}$$

– Choice of the size is crucial and should be natural for a given problem.

– What is the size of an integer $n \in \mathbb{Z}$?

- $n$
- $\log(n)$
- constant
Asymptotic Upper Bound

For a given function $g$, we denote *asymptotic upper bound* as the set of functions

$$O(g(n)) = \{ f(n) \mid \exists c > 0, N > 0 \text{ s.t. } 0 \leq f(n) \leq cg(n) \forall n \geq N \}.$$
Show that \( \frac{1}{2}n^2 - 3n \in O(n^2) \). Find \( c \) and \( N \) such that

\[
0 \leq \frac{1}{2}n^2 - 3n \leq cn^2, \forall n > N
\]

divide by \( n^2 \):

\[
0 \leq \frac{1}{2} - \frac{3}{n} \leq c, \forall n > N
\]

choose \( N = 7 \) and \( c = 1/14 \)

Show \( 6n^3 \not\in O(n^2) \). Suppose yes, then \( 6n^3 \leq cn^2 \) and \( n \leq c/6 \) which cannot hold for arbitrary large \( n \) since \( c \) is a constant.

Show \( an^2 + bn + c \in O(n^2) \). Choose \( c = 7a/4 \), \( N = 2 \max(|b|/a, \sqrt{|c|/a}) \). Check that holds

\[
0 \leq an^2 + bn + c \leq cn^2, \, n \geq N.
\]
– Hierarchy of $O(g)$:

$O(1)$ constant

$O(\log(n))$ logarithmic

$O(n)$ linear

$O(n^c)$ polynomial of degree $c$ ($c \geq 2$ is a constant)

$O(a^n)$ exponential ($a$ is a constant). We can use $O(2^n)$ since for any $a$ there exist a constant $c$ s.t. $a^n \leq ca^n$.

Easy to see

$$O(1) \subset O(\log(n)) \subset O(n) \subset O(n^c) \subset O(a^n).$$
Analysis of Algorithms, $O(\cdot)$ notation.

- Properties

  - $cf' \in O(f), \forall f' \in O(f)$
    
    $c \cdot O(f) = O(f)$ for any $c > 0$

  - $f' + g' \in O(f+g), \forall f' \in O(f), \forall g' \in O(g)$
    
    $O(f) + O(g) = O(f+g) = O(\max(f, g))$

  - $f' \cdot g' \in O(f \cdot g), \forall f' \in O(f), \forall g' \in O(g)$
    
    $O(f) \cdot O(g) = O(f \cdot g) = f \cdot O(g)$,

  - $(f')^m \in O(f^m), \forall f' \in O(f)$
    
    $O(f)^m = O(f^m)$ for any $m > 0$.

  - $f(n) \in g(n)^{O(1)} \iff f$ is bounded by a polynomial in $g$. 

Groups: Binary operation.

Definition (Binary operation)
A binary operation \( \ast : S \times S \rightarrow S \) on a set \( S \) is a rule that assigns to each ordered pair \((a, b)\), \(a, b \in S\) some element of \( S \).

Examples:
- Addition \(+\) is a binary operation on \( \mathbb{R}, \mathbb{Q}, \mathbb{Z} \)
- Addition \(+\) is not a binary operation on \( \mathbb{R}^* = \mathbb{R}/\{0\} \)
- \( \ast : a \ast b = a/b \) on \( \mathbb{Q} \) is not
- \( \ast : a \ast b = a/b \) on \( \mathbb{Q}^+ \) OK
- Matrix addition is not a binary operation on \( M(\mathbb{R}) \) - set of all matrices with real entries.
- Operation \( \ast : a \ast b = \text{min}(a, b) \) on \( \mathbb{Z}^+ = \{z \in \mathbb{Z} \mid z > 0\} \)
Groups: definition.

– Group is one of the basic algebraic structures.

Definition (Group)
A group \((G, \ast)\) is a set \(G\) closed under a binary operation \(\ast\), such that the following axioms are satisfied:

1. \(\ast\) is associative: \(\forall a, b, c \in G\) \((a \ast b) \ast c = a \ast (b \ast c)\)
2. There is identity \(e \in G\) s.t. \(\forall a \in G\) \(a \ast e = e \ast a = a\)
3. There are inverses: \(\forall a \in G\) \(\exists b \in G\), s.t. \(a \ast b = b \ast a = e\).

– \(b\) is an inverse of \(a\) with respect to \(\ast\).
Groups: Example.

– Usually we denote inverse of $a$ by $a^{-1}$.

– For all $a, b \in G$

$$ (a \ast b)^{-1} = b^{-1} \ast a^{-1}. $$

– Fact: the identity element is unique in a group.

– Fact: inverses are unique in a group.
Groups: Example.

– To show that something is a group, we need to show that all 3 axioms are satisfied.

1. $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +)$.
2. $(\mathbb{R}, \times), (\mathbb{Q}, \times)$.
3. $(\mathbb{Z}, \times), (\mathbb{Z}^+, +), (\mathbb{Z}_{\geq 0}, +)$ NOT
Groups: Example.

- Let $\ast : \mathbb{Q}^+ \times \mathbb{Q}^+ \rightarrow \mathbb{Q}^+$ such that $a \ast b = \frac{ab}{2}$.

1. **Associativity:**

   $$(a \ast b) \ast c = \frac{ab}{2} \ast c = \frac{abc}{4}$$

   $$a \ast (b \ast c) = a \ast \frac{bc}{2} = \frac{abc}{4}$$

2. **Identity:** $e = 2$

   $$a \ast 2 = 2 \ast a = \frac{2a}{2} = a$$

3. **Inverse:** $a^{-1} = \frac{4}{a}$

   $$a \ast a^{-1} = a \ast \frac{4}{a} = \frac{4a}{2a} = 2 = e.$$
Let \((G, \ast)\) be a group. Set \(H \subseteq G\) is a subgroup if it is closed under multiplication \(\ast\) and inverses:

\[ \forall a, b \in H, \ a \ast b \in H, \ a^{-1}, b^{-1} \in H \]

- Denote \(H \leq G\).
- It follows that if \(H \leq G\), then \(e_G \in H\).
Groups: subgroup examples.

- Example:
  1. \((\mathbb{Z}, +) \leq (\mathbb{R}, +)\),
  2. \((\mathbb{Q}^+, \cdot) \not\leq (\mathbb{R}, +)\),
  3. \((\mathbb{Q}^+, \cdot) \leq (\mathbb{R}^+, \cdot)\)
Groups: subgroup examples.

Let $G$ a group, $a \in G$ and $H = \{a^n \mid n \in \mathbb{Z}\}$

**Theorem**

$H$ is a subgroup of $G$: $H \leq G$.

**Proof.**

1. $a^r a^s = \underbrace{a \ast a \ast \ldots \ast a}_{r + s} = a^{r+s} \in H$: closed under $\ast$

2. If $a^r \in H$ then $a^{-r} \in H$ and $a^r a^{-r} = \underbrace{a \ast a \ast \ldots \ast a}_{r} \underbrace{a^{-1} \ast a^{-1} \ast \ldots \ast a^{-1}}_{r} = e$, therefore closed under inverses.
Groups: cyclic groups examples.

1. $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

2. $\langle 3 \rangle = \{ \ldots -9, -6, -3, 0, 3, 6, 9, \ldots \} = 3\mathbb{Z}$

In general, $n\mathbb{Z} = \langle n \rangle$ denotes a cyclic group generated by $n$ and $mn\mathbb{Z} < n\mathbb{Z}$. 
Groups: cyclic groups examples.

Let \( \mathbb{Z}_4 = \{ z \mod 4 \mid z \in \mathbb{Z} \} \), then \((\mathbb{Z}_4, +) = \langle 1 \rangle = \langle 3 \rangle \)

But \((\mathbb{Z}_4, +) \neq \langle 2 \rangle \).

Note \( \mathbb{Z}_4 = \{0, 1, 2, 3\} \) and \( a^n \) corresponds to \( 3 + 3 + \ldots + 3 = n3 \)

\[
\begin{align*}
3 \mod 4 &= 3 \\
2 \cdot 3 \mod 4 &= 2 \\
3 \cdot 3 \mod 4 &= 1 \\
4 \cdot 3 \mod 4 &= 0 \\
5 \cdot 3 \mod 4 &= 3 \\
\ldots
\end{align*}
\]
Groups: commutativity.

Definition (Commutative)

A group $G$ is called commutative (Abelian) if for all $a, b \in G$

$$a \cdot b = b \cdot a$$

– In this course most of the groups are commutative
Groups: commutativity example.

Every cyclic group is abelian:

Let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ and $g_1, g_2 \in G$ then

$$g_1 g_2 = a^r a^s = \underbrace{a \ast a \ast \ldots \ast a}_{r+s} = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$$
Groups: Lagrange Theorem.

– The number of elements $|G|$ in a set $G$ is called the order of the group $(G, \cdot)$.

**Theorem (Lagrange)**

Let $G$ be a finite group and $H \subseteq G$ is a subgroup then $|H|$ divides $|G|$. 

Theorem

Let $H < G$ and let relation $\sim_L$ be defined on $G$:

$$a \sim_L b \iff a^{-1}b \in H.$$  

Then $\sim_L$ is an equivalence relation.

Proof.

– Reflexive: Let $a \in G$, then $a^{-1}a = e$ and $e \in H$, thus $a \sim_L a$.

– Symmetric: Suppose $a \sim_L b$, then $a^{-1}b \in H$ and $(a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow b \sim_L a$.

– Transitive: Let $a \sim_L b$ and $b \sim_L c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since $H$ is a subgroup $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ and therefore $a \sim_L c$. 
Groups: cosets.

**Fact**

Let $S$ be a nonempty set and $\sim$ be an equivalence relation on $S$, then $\sim$ yields a natural partition of $S$

$$\bar{a} = \{x \in S \mid x \sim a\}$$

- Therefore $\sim_L$ defines a partition on $G$.
- $a \in G$ then cell containing $a$:

$$\bar{a} = \{x \in G \mid a^{-1}x \in H\} = \{ah \mid h \in H\}$$

Denote by $aH$. 
Definition (Left coset)

Let $G$ be a group and $H \subseteq G$ a subgroup. The subset

$$aH = \{ ah \mid h \in H \} \subseteq G$$

is called the left coset of $H$ containing $a$. 
Groups: cosets example.

− Let $(3\mathbb{Z}, +) < (\mathbb{Z}, +)$

$$0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

$$0 + 3\mathbb{Z} \cup 1 + 3\mathbb{Z} \cup 2 + 3\mathbb{Z} = \mathbb{Z}$$
Lemma

Every coset of a subgroup $H$ has the same number of elements as $H$.

Proof.
Show that there exists a **one-to-one** map from $H$ and onto $gH$ for any fixed element $g \in G$.
Define map $\psi : H \rightarrow gH$.

1. $\psi$ is onto by definition: $gH = \{gh \mid h \in H\}$
2. $\psi$ is one-to-one: suppose $\psi(h_1) = \psi(h_2)$, then

$$gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2.$$
Let $G$ be a finite group and $H \subseteq G$ is a subgroup then

$$|H| \text{ divides } |G|.$$ 

Proof. 
Let $n = |G|$ and $m = |H|$. 
We know that every coset of $H$ also has $m$ elements. 
Let $r$ be the number of cells in the partition of $G$ into left cosets of $H$, then

$$n = rm \text{ or } |G| = r|H|.$$
Theorem (Lagrange)

Let \( G \) be a finite group and \( H \leq G \) is a subgroup then

\[ |H| \text{ divides } |G|. \]
– Order of an element $g \in G$ is equal to the order of the cyclic group generated by $g$.

– Fact: $ord(g) = \min_{n>0} \{g^n = e\}$, i.e. $|\langle g \rangle| = n$
The order of an element of a finite group divides the order of the group.

Proof.
Let $G$ be a finite group and $g \in G$.

Easy to see that $\langle g \rangle \leq G$ therefore by Lagrange theorem $|\langle g \rangle| \text{ divides } |G|$

Since $ord(g) = |\langle g \rangle|$ we have $ord(g)$ divides $|G|$
Every group of prime order is cyclic.

Proof
We need to show that there exists an element which generates \( G \)
Let \( G \) be a group and \( |G| = p \) - prime and \( a \in G, \ a \neq e \).

Since \( a \neq e \), \( |\langle a \rangle| \geq 2 \) and it has to divide prime \( p \), therefore
\( |\langle a \rangle| = p \) and \( \langle a \rangle = G \).

\((\mathbb{Z}_p, + \mod p)\) is cyclic since \( \mathbb{Z}_p = \{0, 1, \ldots, p - 1\} \)
Groups: generating sets.

**Finite Generating set**

A set $S = \{s_1, \ldots, s_n\}$ is called generating set of group $G$ if all elements of $G$ are precisely the finite products of elements in $S$ and their inverses:

$$G = \left\{ x_1 \ast x_2 \ast \ldots \ast x_k \mid x_i \in S^{\pm 1}, 0 < k < \infty \right\},$$

- $G = \langle S \rangle = \langle s_1, \ldots, s_n \rangle$ notation for $G$ is generated $S$.

- A group is called cyclic if there exists a generating set with just one element.
Groups: generating sets.

\[ \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \} \]

\[ \mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle = \langle 2, 3 \rangle = \langle 3, 4 \rangle \neq \langle 2, 4 \rangle \]

- \(-1 = 5; \ (-5 = 1)\)
- \(2 + 3 = 5\)
- \(3 + 4 = 1\)

Any product of 2 and 4 is even therefore \(1 \notin \langle 2, 4 \rangle\)
Groups: maps.

– A map $\varphi : A \rightarrow B$ is *injective* (one-to-one) if

$$\varphi(a_1) = \varphi(a_2) \text{ implies } a_1 = a_2, \forall a_1, a_2 \in A.$$  

– A map $\varphi : A \rightarrow B$ is *surjective* (onto) if

$$\forall b \in B, \exists a \in A \text{ s.t. } \varphi(a) = b.$$  

– A map is *bijective* if it is both surjective and injective.
Definition (Homomorphism)

Let $G$ and $G'$ be two groups. A **homomorphism** is a map

$$\varphi : G \longrightarrow G'$$

which preserves the group operation:

$$\varphi(a *_G b) = \varphi(a) *_{G'} \varphi(b),$$

where $a, b \in G$ and $\varphi(a), \varphi(b) \in G'$. 

Groups: Homomorphism.

– Homomorphism $\varphi : G \rightarrow G'$ preserves the identity, inverses and subgroups.

1. If $e$ is the identity in $G$ then $\varphi(e)$ is the identity in $G'$
2. If $g \in G$ then $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. If $H \leq G$ then $\varphi(H) \leq G'$
Groups: Homomorphism example.

– Fact (Division algorithm): If \( m \in \mathbb{Z}^+ \) and \( n \in \mathbb{Z} \) then there exist unique integers \( q \) and \( r \) such that

\[
n = mq + r, \text{ and } 0 \leq r < m.
\]

Reduction modulo \( m \):

Let \( \psi : \mathbb{Z} \rightarrow \mathbb{Z}_m \) be s.t.

\[
\psi(n) = r,
\]

where \( n = mq + r \), then \( \psi \) is a homomorphism.

Existence of such map is guaranteed by the fact above.
Groups: Homomorphism example.

Proof of $\psi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ is a homomorphism

Show that $\psi(s + t) = \psi(s) + \psi(t)$, $s, t \in \mathbb{Z}$.

Using division algorithm:

$$
\begin{align*}
    s &= q_1 n + r_1 \\
    t &= q_2 n + r_2 \\
    r_1 + r_2 &= q_3 n + r_3
\end{align*}
$$

where $0 \leq r_i < n$ Now,

$s + t = (q_1 + q_2 + q_3)n + r_3 \Rightarrow \psi(s + t) = r_3$.

and

$$
\psi(s) + \psi(t) = r_1 + r_2 \mod n = r_3
$$

Therefore,

$$
\psi(s + t) = \psi(s) + \psi(t).
$$
Groups: kernel.

**Definition (Kernel)**

Kernel $\text{ker}(\varphi)$ of the homomorphism $\varphi : G \rightarrow H$ is the set of elements that are sent to $e$:

$$\text{ker}(\varphi) = \{ g \in G \mid \varphi(g) = e_H \}$$

– Homomorphism is one-to-one if and only if $\text{ker}(\varphi) = \{ e \}$
Definition (Isomorphism)

Let $\varphi : G \longrightarrow G'$. If $\varphi$ is a bijective homomorphism then it is called *isomorphism*. We say two groups are isomorphic: $G \simeq G'$.

– From the point of view of group theory, isomorphic groups $G$ and $G'$ define the same object. We cannot distinguish between them.
Groups: isomorphism example.

Lemma

Any infinite cyclic group $G$ is isomorphic to $(\mathbb{Z},+)$. We need to show that there exists a map $\varphi : G \rightarrow \mathbb{Z}$ such that

1. $\varphi$ is one-to-one
2. $\varphi$ is onto $\mathbb{Z}$
3. $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, b \in G$. 
Groups: isomorphism example.

**Lemma**

Any infinite cyclic group $G$ is isomorphic to $(\mathbb{Z}, +)$.

**Proof.**

- Recall $G = \{ a^n \mid n \in \mathbb{Z} \}$
  
  - Define $\varphi : G \longrightarrow \mathbb{Z}$ as $\varphi(a^n) = n$ for all $a^n \in G$
  - $\varphi(a^n) = \varphi(a^m) \Rightarrow n = m \Rightarrow a^n = a^m$ : one-to-one
  - $\forall n \in \mathbb{Z}, \exists b = a^n \in G$ s.t. $\varphi(b) = \varphi(a^n) = n$ : onto
  - $\varphi(a^n a^m) = \varphi(a^{n+m}) = n + m$ and $\varphi(a^n) + \varphi(a^m) = n + m$ : $\varphi(a^n a^m) = \varphi(a^n) + \varphi(a^m)$
Groups: normal subgroup.

Definition

Let $G$ be a group and $H \leq G$. The subgroup $H$ is called normal if

$$ghg^{-1} \in H, \text{ for all } g \in G \text{ and } h \in H.$$ 

The following are all equivalent characterizations for a normal subgroup $H$:

- $ghg^{-1} \in H$, for all $g \in G$ and $h \in H$.
- $gHg^{-1} = H$, for all $g \in G$.
- $gH = Hg$, for all $g \in G$. 
Groups: normal subgroup.

Every subgroup of an abelian group is normal.

**Proof.**

Note that $gh = hg$ for all $h \in H$ and $g \in G$ therefore

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

Let $\varphi : G \longrightarrow G'$ be a homomorphism. Then $\ker(\varphi)$ is a normal subgroup of $G$.

$$h \in \ker(\varphi) \Rightarrow \varphi(h) = e$$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = e$$

Therefore $ghg^{-1} \in \ker(\varphi)$
Let $H$ be a normal subgroup. Then cosets of $H$ form a group $G/H$ with binary operation $*$ defined:

$$(aH) * (bH) = (ab)H, \quad \text{for all } aH, bH \in G/H.$$
– Recall map $\psi : \mathbb{Z} \rightarrow \mathbb{Z}_n$.

- It is a homomorphism
- $\ker(\psi) = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = n\mathbb{Z}$
- $\ker(\varphi)$ is normal and $G/\ker(\psi)$ is a factor group.

Cosets of $n\mathbb{Z}$ are the residue classes modulo $n$
Groups: factor group example.

Let $n = 3$ then the cosets of $3\mathbb{Z}$

\[
0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}
\]
\[
1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}
\]
\[
2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}
\]

form a group with 3 elements and isomorphic to $\mathbb{Z}_3$:

\[
(0 + 3\mathbb{Z}) \ast (1 + 3\mathbb{Z}) = (0 + 1) + 3\mathbb{Z} = 1 + 3\mathbb{Z}
\]
\[
(0 + 3\mathbb{Z}) \ast (2 + 3\mathbb{Z}) = (0 + 2) + 3\mathbb{Z} = 2 + 3\mathbb{Z}
\]
\[
(1 + 3\mathbb{Z}) \ast (2 + 3\mathbb{Z}) = (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\} = 0 + 3\mathbb{Z}
\]

- $0 + 3\mathbb{Z}$ is the identity
- $1 + 3\mathbb{Z}$ is the inverse of $2 + 3\mathbb{Z}$
Theorem

The map $\mu : G/\ker(\varphi) \longrightarrow \varphi(G)$ define by $\mu(aH) = \varphi(a)$ is an isomorphism and

$$G/\ker(\varphi) \cong \varphi(G)$$
Definition (Ring)

Set $R$ with two binary operations: addition $+: R \times R \rightarrow R$ and multiplication $\cdot: R \times R \rightarrow R$ is called a ring if $(R, +)$ satisfies the following conditions.

1. $(R, +)$ is a commutative group
2. Multiplication $\cdot$ is associative
3. Distributive: $\forall a, b, c \in R$ we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

– Examples:

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{Z}_n, +, \cdot)$
Rings.

Notations:

– 0 is the additive identity
– Addition $a + b$
– Additive inverse: $-a$

– 1 is the multiplicative identity
– Multiplication $a \cdot b$ or $ab$
– Multiplicative inverse: $a^{-1}$
Theorem

Let $R$ be a ring and $a, b \in R$ then:

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
Proof.

1. $0a = a0 = 0$

   \[ a0 + a0 = a(0 + 0) = a0 = 0 + a0 \]

   Canceling by $-a0$ on left and right we obtain $a0 = 0$

2. $a(-b) = (-a)b = -(ab)$

   Show that $a(-b) + ab = 0$.

   \[ a(-b) + ab = a(-b + b) = a0 = 0 \]

3. $(-a)(-b) = ab$

   By property 2

   \[ (-a)(-b) = -(a(-b)) = -(-(ab)) \]

   Note that $-(ab)$ is the inverse of $-(-(ab))$ and $(ab)$ is the inverse of $-((ab))$ therefore by the uniqueness property of inverses

   \[-(-ab)) = ab \Rightarrow (-a)(-b) = ab. \]
Definition (Ring homomorphism)

Let $R$ and $S$ be two rings. A map $\varphi : R \rightarrow S$ which preserves both operations of addition and multiplication is called a ring homomorphism, i.e. for all $r \in R, s \in S$

- $\varphi(r + s) = \varphi(r) + \varphi(s)$
- $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$
- $\varphi(0_R) = 0_S$ and $\varphi(1_R) = 1_S$
Show that $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ is a ring homomorphism.

- $\varphi$ is the additive group homomorphism.

- Show $\varphi(ab) = \varphi(a)\varphi(b)$:
  
  $a = q_1n + r_1$ and $b = q_2n + r_2 \Rightarrow \varphi(a) = r_1$ and $\varphi(b) = r_2$

  $ab = n(q_1q_2n + r_1q_2r_2q_1) + r_1r_2 \Rightarrow \varphi(ab) = r_1r_2$

Therefore,

$\varphi(ab) = \varphi(a)\varphi(b)$
Rings: zero dividers.

- Solve $x^2 - 5x + 6 = 0$

  Factorization gives

  $$(x - 2)(x - 3) = 0$$

  We know that the product $(x - 2)(x - 3)$ is 0 if and only if either $(x - 2) = 0$ or $(x - 3) = 0$ therefore only possible solutions are 2 and 3.

- Solve $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$

  Factorization still holds so 2 and 3 are solutions

  However there are more solutions:

  - $6 : (6 - 2)(6 - 3) = (4)(3) = 12 \mod 12 = 0$
  - $11 : (11 - 2)(11 - 3) = (9)(8) = 72 \mod 12 = 0$

  The problems is there are nonzero elements whose product gives 0!
Definition (Zero divisors)
If $a, b \in R$ are two nonzero elements of a ring $R$ such that $ab = 0$ then $a$ and $b$ are zero divisors.

Definition (Integral domain)
A nontrivial ($1 \neq 0$) commutative (with respect to addition and multiplication) ring with unity is called an integral domain if there are no nonzero zero dividers, i.e. there are no $a, b \in R$ and $a \neq 0, b \neq 0$ such that $ab = 0$. 
$\mathbb{Z}_p$ is an integral domain.

1. Show that there are no zero divisors.
   - Let $m \in \mathbb{Z}_p$, since $p$ is prime than $gcd(m, p) = 1$
   - If for some $s \in \mathbb{Z}_p$, $ms = 0$ then $p$ divides $ms$:
     \[
pk = ms
     \]
     but we know that $gcd(m, p) = 1$ therefore $p$ divides $s$ and $s = 0$ in $\mathbb{Z}_p$.

2. Commutativity and unity is an exercise.
Definition (Field)
An integral domain is called a field if there is multiplicative identity and every nonzero element of a field has multiplicative inverse.

- For any field, the nonzero elements form a group under the field multiplication.

Examples:

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ are fields.
- $\mathbb{Z}$ is not a field.
\( \mathbb{Z}_p \) is finite integral domain with unity

– Show that it has inverses.

Recall that \( \mathbb{Z}_p = \langle g \rangle \) is cyclic: every element is of the form \( g^n \) and \( g^p = 1 \)

Let \( a \in \mathbb{Z}_p \) then \( a = g^k, \ k < p \) and

\[
a^{-1} = g^{p-k}.
\]

Indeed

\[
g^k \cdot g^{p-k} = g^p = 1
\]

• Every field is an integral domain

• Every finite integral domain is a field.
Rings.
Rings:

- set $R$ closed under $+$, $\cdot$.
- $(R, +)$ - abelian group,
- $\cdot$ - associative,
- distributivity.

Integral domain: unitary commutative ring with no nonzero dividers.

Field: integral domain with division
(has multiplicative inverses. $(F - \{0\}, \cdot)$ is a group.)
Definition (Ring homomorphism)

Let $R$ and $S$ be two rings. A map $\varphi : R \rightarrow S$ which preserves both operations of addition and multiplication is called a ring homomorphism. For all $r \in R, s \in S$

- $\varphi(r + s) = \varphi(r) + \varphi(s)$
- $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$
- $\varphi(0_R) = 0_S$ and $\varphi(1_R) = 1_S$
Definition

Let $\varphi : R \rightarrow S$ be a ring homomorphism. Define kernel of $\varphi$

$$\ker(\varphi) = \{ a \in R \mid \varphi(a) = 0 \}$$

- If $c \in \ker(\varphi)$, then $c + \ker(\varphi) = \ker(\varphi)$
  Show set equivalence.
  Note $\varphi(x) = 0$ and $c + \ker(\varphi) = \{ c + b \mid \varphi(b) = 0 \}$
  - Show $c + \ker(\varphi) \subseteq \ker(\varphi)$: pick $a \in c + \ker(\varphi)$ then
    $\varphi(a) = \varphi(c + b) = \varphi(c) + \varphi(b) = 0 \Rightarrow a \in \ker(\varphi)$
  - Show $\ker(\varphi) \subseteq c + \ker(\varphi)$: Since $c \in \ker(\varphi)$ then $-c \in \ker(\varphi)$.
    Pick $a \in \ker(\varphi)$ then $-a \in \ker(\varphi)$ and $(a - c) \in \ker(\varphi)$. Now,
    $c + (a - c) \in \{ c + b \mid \varphi(b) = 0 \} \Rightarrow a \in \{ c + b \mid \varphi(b) = 0 \} = c + \ker(\varphi)$

- $\varphi^{-1}(\varphi(a)) = a + \ker(\varphi) = \{ a + b \mid \varphi(b) = 0 \}$
  Indeed:
  $\varphi(a + b) = \varphi(a) + \varphi(b) = \varphi(a) + 0 = \varphi(a)$
Consider quotient

\[ R/\ker(\varphi) = \{ a + \ker(\varphi) \mid a \in R \} \]

Define operation

- \((a + \ker(\varphi)) + (a + \ker(\varphi)) = (a + b + \ker(\varphi))\)
- \((a + \ker(\varphi)) \cdot (a + \ker(\varphi)) = (ab + \ker(\varphi))\)
Rings: factor rings.

Show that operations are well defined. We need to show that they do not depend on the choice of \( a \) and \( b \)

Suppose

\[
a + \ker(\varphi) = a' + \ker(\varphi) \Rightarrow a' = a + x
\]

\[
b + \ker(\varphi) = b' + \ker(\varphi) \Rightarrow b' = b + y
\]

where \( x, y \in \ker(\varphi) \). Note that \( x + y \in \ker(\varphi) \)

Addition:

\[
(a' + \ker(\varphi)) + (b' + \ker(\varphi)) = a' + b' + \ker(\varphi)
\]

\[
= (a + x + b + y) + \ker(\varphi)
\]

\[
= (a + b) + (x + y) + \ker(\varphi)
\]

\[
= a + b + \ker(\varphi)
\]
Rings: factor rings.

Multiplication:

\[(a' + \ker(\varphi)) \cdot (b' + \ker(\varphi)) = a'b' + \ker(\varphi)\]

\[= (a+x)(b+y) + \ker(\varphi)\]

\[= ab + ay + xb + xy + \ker(\varphi)\]

\[= ab + \ker(\varphi)\]

\[\varphi(ay + xb + xy) = \varphi(a)\varphi(y) + \varphi(x)\varphi(b) + \varphi(x)\varphi(y) = 0\varphi(a) + 0\varphi(b) + 0 \Rightarrow ay + xb + xy \in \ker(\varphi)\]
Theorem

Let \( R \) be a ring and \( \varphi : R \rightarrow S \) be a homomorphism. Then the quotient \( R/\ker(\varphi) \) is a ring.

Proof.

\[ + : (R/\ker(\varphi), +) \text{ is an additive group. It follows from the result for groups since } \varphi \text{ is a group homomorphism.} \]

\[ + \text{ is commutative in } R/\ker(\varphi). \text{ It follows from the commutativity of } + \text{ is commutative in } R \]

\[ \cdot : \text{ Associativity.} \]

\[
[(a + \ker(\varphi))(b + \ker(\varphi))](c + \ker(\varphi)) \\
= (ab + \ker(\varphi))(c + \ker(\varphi)) \\
= abc + \ker(\varphi) \\
= (a + \ker(\varphi))(bc + \ker(\varphi)) \\
= (a + \ker(\varphi))[(b + \ker(\varphi))(c + \ker(\varphi))] \\
\]

Distributivity is similar.
Rings: factor rings.

Let \( \mu : R/\ker(\varphi) \rightarrow S \) be defined as

\[
\mu(a + \ker(\varphi)) = \varphi(a) \in S.
\]

Then \( \mu \) is a homomorphism

\[
\begin{align*}
+ & : \\
\mu((a + \ker(\varphi)) + (b + \ker(\varphi))) &= \mu((a + b) + \ker(\varphi)) \\
&= \varphi(a + b) \\
&= \varphi(a) + \varphi(b) \\
&= \mu(a + \ker(\varphi)) + \mu(b + \ker(\varphi))
\end{align*}
\]
Rings: factor rings.

Proof.

\[
\mu((a + \ker(\varphi))(b + \ker(\varphi))) = \mu(ab + \ker(\varphi)) = \varphi(ab + \ker(\varphi)) = \varphi(a) \varphi(b) = \mu(a + \ker(\varphi)) \mu(b + \ker(\varphi))
\]
\[ \mu(R/\ker(\varphi)) \longrightarrow \varphi(R) \] is an isomorphism, i.e.

\[ R/\ker(\varphi) \simeq \varphi(R) \]

**Proof**

- \( \mu \) is a homomorphism.
- \( \mu \) is one-to-one by construction
- Show that it is onto.
Rings: factor rings.

We need to show that \( \ker(\mu) = \{0\} \)

\[
\ker(\mu) = \{ x \in R/\ker(\varphi) \mid \mu(x) = 0 \}
= \{ a + \ker(\varphi) \mid \mu(a + \ker(\varphi)) = 0, a \in R \}
= \{ a + \ker(\varphi) \mid \varphi(a) = 0 \} \text{ by definition}
\]

Therefore, \( a \in \ker(\varphi) \) which means that

\[
a + \ker(\varphi) = \ker(\varphi) \text{ and } \ker(\mu) = \ker(\varphi)
\]

\( \ker(\varphi) = \{0\} \in R/\ker(\varphi) \) by definition.

– Similar to factor groups,
Factor rings a nontrivial way to construct new rings.
Polynomials.

Definition (Polynomial)

Let $R$ be a ring. A polynomial $f(x)$ with coefficients in $R$ is an infinite sum

$$
\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,
$$

where $a_i$ in $R$ and $a_i = 0$ for all but a finite number of $i$.

- $a_i$ - coefficients
- $\text{deg}(f)$ - degree of $f$ is the largest $i$ such that $a_i \neq 0$
- We agree to denote a polynomial with $a_i = 0$ for all $i > n$ by

$$
f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.
$$
- $R[x]$ is the set of all polynomials in $x$ with coefficients in $R$

Two polynomials $f, g \in R[x]$

\[
f(x) = a_0 + a_1x + \ldots + a_nx^n
\]

\[
g(x) = b_0 + b_1x + \ldots + b_mx^m
\]

are equal if and only if

\[n = m, \ a_i = b_i\]
Polynomials: operations.

Let

\[ f(x) = a_0 + a_1 x + \ldots + a_n x^n \ldots \]
\[ g(x) = b_0 + b_1 x + \ldots + b_n x^n \ldots \]

then

- \( f(x) + g(x) = c_0 + c_1 x + \ldots + c_n x^n + \ldots, \quad c_n = a_n + b_n \)
- \( f(x) \cdot g(x) = d_0 + d_1 x + \ldots + d_n x^n + \ldots, \quad d_n = \sum_{i=0}^{n} a_i b_{n-i} \)
Polynomials.

The set $R[x]$ of all polynomials in $x$ with coefficients in a ring $R$ is a ring under polynomial addition and multiplication.

- If $R$ is an integral domain then so is $R[x]$
- If $F$ is a field then $F[x]$ is an integral domain, NOT FIELD!
Prove that if $R$ is a ring then $R[x]$ is also a ring.

- Easy to see that $< R[x], + >$ is an abelian group:
  
  $f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i)x^i$, since $a_i + b_i \in R$, then $f(x) + g(x) \in R[x]$  
  
  $0 \in R[x]$, $0 + f(x) = f(x) + 0 = f(x)$  
  
  For all $a \in R$, $-a \in R$
  
  For $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ define $-f(x) = \sum_{i=0}^{\infty} -a_i x^i \in R[x]$, then

$$f(x) - f(x) = \sum_{i=0}^{\infty} (a_i - a_i)x^i = 0$$
Prove that if $R$ is a ring then $R[x]$ is also a ring.

- Show associativity of multiplication by using formal definitions of polynomials and applying ring axioms to $a_i, b_j, c_k \in R$
- Distributivity proved similarly.
Polynomials.

- Since $R[x]$ is a ring, then
  - $(R[x])[y]$ is a ring with coefficients in $R[x]$
  - $((R[x])[y])[z]$ is a ring with coefficients in $(R[x])[y]$
  - ...

- In general we denote $R[x_1, \ldots, x_n]$ the ring of polynomials in $n$ variables and coefficients in $R$
Definition (Evaluation homomorphism)

Let $F$ be a field and $u \in F$. An evaluation homomorphism is a map $\epsilon_u : F[x] \rightarrow F$ such that

$$\epsilon_u(f) = f(u) \in F, \ f \in F[x], \ u \in F.$$ 

Example: $f(x) = x^3 + 3x - 2$

$$\epsilon_2(f) = f(2) = 2^3 + 2 \cdot 2 - 2 = 12$$
Polynomials: evaluation homomorphism.

– Easy to see that $\epsilon_u$ is a homomorphism:

Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$

– Addition:

$$\epsilon_u(f(x) + g(x)) = \epsilon_u \left( \sum_{i=0}^{\infty} (a_i + b_i) x^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) u^i$$

$$\epsilon_u(f(x)) + \epsilon_u(g(x)) = \sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j = \sum_{i=0}^{\infty} (a_i + b_i) u^i$$
Polynomials: evaluation homomorphism.

Let \( f(x) = \sum_{i=0}^{\infty} a_i x^i \) and \( g(x) = \sum_{j=0}^{\infty} b_j x^j \)

\[ \epsilon_u(f(x) \cdot g(x)) = \epsilon_u \left( \sum_{i=0}^{\infty} d_i x^i \right) = \sum_{i=0}^{\infty} d_i u^i, \]

\[ \epsilon_u(f(x)) \cdot \epsilon_u(g(x)) = \left( \sum_{i=0}^{\infty} a_i u^i \right) \cdot \left( \sum_{j=0}^{\infty} b_j u^j \right) = \sum_{k=0}^{\infty} d_k u^k, \]

where

\[ d_n = \sum_{i=0}^{n} a_i b_{n-i} \]
Polynomials: zero of polynomial.

Definition

Let $F$ be a field, $f(x) \in F[x]$ and $\varphi_u : F[x] \rightarrow F$ be an evaluation polynomial. Then $\alpha$ is a zero of $f(x)$ if

$$\varphi_\alpha(f(x)) = 0.$$ 

– Now we can reformulate the problem of finding roots of a polynomial $f(x)$:

Find all $\alpha \in F$, s.t. $\varphi_\alpha(f(x)) = 0$.
Let $F$ be a field and $f(x), g(x) \in F[x]$ s.t. $\deg(f) > 0$. Then there exist \textit{unique} polynomials $q(x), r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

and $\deg(g) > \deg(r)$.

– This theorem holds for other rings, called Euclidean ring.
Proof.

- Existence by Euclidean algorithm.
- Uniqueness: Suppose not i.e.

$$f = gq_1 + r_1$$ and $$f = gq_2 + r_2$$

$$(gq_1 + r_1) - (gq_2 + r_2) = 0 \Rightarrow g(q_1 - q_2) = r_2 - r_1 \quad (1.1)$$

But since $$\text{deg}(g) > \text{deg}(r_1)$$ and $$\text{deg}(g) > \text{deg}(r_2)$$ we have

$$\text{deg}(g(q_1 - q_2)) > \text{deg}(r_2 - r_1)$$ unless $$q_1 = q_2$$

So (1.1) is true if $$r_1 = r_2$$. 
Let \( f(x) \in F[x], a \in F \) then

\[ f(a) = 0 \iff f(x) = (x - a)h(x) \]

for some \( h(x) \in F[x] \).

**Proof.**

Let \( g(x) = (x - a) \). By the division algorithm

\[
\begin{align*}
f(x) &= g(x)q(x) + r(x) \\
f(x) &= (x - a)q(x) + r(x) \\
f(x) &= (x - a)q(x) + b, \ b \in F \\
f(a) &= (a - a)q(a) + b \\
f(a) &= 0q(a) + b = b
\end{align*}
\]

\[ f(a) = 0 \iff b = 0 \iff f(x) = (x - a)q(x). \]
Let $f(x) \in F[x]$. $f(x)$ has at most $n = \text{deg}(f(x))$ roots (zeros of $f(x)$).

**Proof.**

Let $a_1$ be a root of $f$ then

$$f(x) = (x - a_1)h_1(x), \deg(h) < \deg(f)$$

Now let $a_2 \neq a_1$ be a root of $f$ then

$$0 = f(a_2) = (a_2 - a_1)h_1(a_2) \Rightarrow h_1(a_2) = 0$$
Polynomials: corollaries of the division algorithm.

**Proof.**

– Continue to apply this steps to $h_2$, then to $h_3$ and so on. Since we decrease polynomial degree on each step by 1 then we should stop in $n$ steps:

\[
\begin{align*}
  f(x) & = (x - a_1)h_1(x) \\
  & = (x - a_1)(x - a_2)h_2(x) \\
  & = \ldots \\
  & = (x - a_1)(x - a_2)\ldots(x - a_n)h_n, \ h_n \in F
\end{align*}
\]

– Inverses are unique and no zero dividers
A polynomial $p(x) \in F[x]$ is called irreducible over $F$ if

$$p(x) = g(x)h(x), \text{ then } \deg(g) = 0 \text{ or } \deg(h) = 0.$$ 

- $p(x)$ is reducible otherwise.
Polynomials: irreducible examples.

• $x^2 - 2$ is irreducible over $\mathbb{Q}$
  Suppose not, then $(x^2 - 2) = (x - a)(x - b)$, then $a, b$ are roots,
  but $a = \pm \sqrt{2} \not\in \mathbb{Q}$ so it cannot be decomposed into some
  polynomial of $\deg > 0$

• $x^2 + 1$ is irreducible over $\mathbb{R}$

• $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$
  $x^3 + 3x + 2 = (x - a)(x^2 + bx + c)$ since $\mathbb{Z}_5$ is finite we can
  try all possibilities for

  $$f(a) = 0, a = 0, 1, 2, 3, 4$$

No roots therefore $f(x)$ cannot be decomposed - irreducible.
Theorem (Fermat’s little theorem)

If \(a \in \mathbb{Z}\) and \(p\) is a prime not dividing \(a\) then

\[a^{p-1} \equiv 1 \pmod{p}, \text{ for } a \not\equiv 0 \pmod{p}\]
Fermat’s little theorem.

Proof.

– Recall that $\mathbb{Z}_p$ is a field and $(\mathbb{Z}_p - \{0\}, \cdot \mod p)$ is a group, i.e. 
$$\{1, 2, 3, \ldots, p - 1\}$$
form a group of order $p - 1$ under multiplication modulo $p$.

– By Lagrange theorem, order of any element divides order of the group, then for $b \in \mathbb{Z}_p$, $b \neq 0$ we have

$$ord(b) \cdot k = p - 1 \Rightarrow b^{ord(b)\cdot k} = b^{p-1} \Rightarrow 1^k = b^{p-1} \Rightarrow b^{p-1} = 1.$$ 

– Recall $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ is a homomorphism. $\ker(\varphi) = p\mathbb{Z}$, therefore 
$\mathbb{Z}/\ker(\varphi) = \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$,

– Pick $a \in \mathbb{Z}$ s.t. $a \notin (0 + p\mathbb{Z}) \in \mathbb{Z}/p\mathbb{Z}$.
Then $p$ does not divide $a$ and $a \neq 0$ therefore

$$a^{p-1} \equiv 1 \pmod{p}.$$