Math 343 - Introduction to Modern Algebra

Binary Operations and Binary Structures

ALL SETS ARE ASSUMED TO BE NONEMPTY!

Let $X$ be a set. $\ast$ is a binary operation on $X$ if $\ast$ is a function from $X \times X$ to $X$. That is, $\forall x, y \in X$, $x \ast y \in X$.

A binary operation on a set $X$ is commutative if $\forall x, y \in X$, $x \ast y = y \ast x$.

Examples:

1. Let $X = \mathbb{Z}$ (or $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) and $\ast$ be the addition operator $+$ or the multiplication operator $\cdot$. Both are commutative binary operations.

2. Let $X$ be the set of $m \times n$ matrices, denoted $M_{mn}$, and $\ast$ be matrix addition. This is a commutative operation. Note: We can distinguish between $m \times n$ matrices with real entries versus complex entries with the notations $M_{mn}(\mathbb{R})$ and $M_{mn}(\mathbb{C})$.

3. Let $X$ be the set of $n \times n$ matrices, denoted $M_{nn}$ or $M_n$, and $\ast$ be matrix multiplication. This is not a commutative operation (for $n > 1$):

$$
\begin{pmatrix}
0 & 1 \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
0 & 1 \\
0 & 0
\end{pmatrix}
\neq
\begin{pmatrix}
0 & 1 \\
0 & 0
\end{pmatrix}
\begin{pmatrix}
0 & 1 \\
0 & 1
\end{pmatrix}.
$$

4. Let $X$ be the set of functions $f : \mathbb{R} \to \mathbb{R}$ and $\ast$ be composition. This is not a commutative operation:

Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ be given by $g(x) = x - 1$. Then $f \circ g : \mathbb{R} \to \mathbb{R}$ is given by $(f \circ g)(x) = (x - 1)^2 = x^2 - 2x + 1$ and $g \circ f : \mathbb{R} \to \mathbb{R}$ is given by $(g \circ f)(x) = x^2 - 1$.

5. Let $X$ be the set of alphabet strings (finite sequences of letters) and $\ast$ be concatenation (putting two strings together in order). For example, if $\alpha = \text{race}$ and $\beta = \text{car}$ then $\alpha \ast \beta = \text{racecar}$. Clearly this binary operation is not commutative.

Let $\ast$ be a binary operation on a set $X$. Let $Y$ be a subset of $X$. $Y$ is closed under $\ast$ if $\forall x, y \in Y$, $x \ast y \in Y$.

Examples:

- Consider the interval $[0, 1] \subseteq \mathbb{R}$. Clearly addition is not closed on this subset of $\mathbb{R}$.

- Consider the set $Y$ of all $n \times n$ matrices with non-negative entries as a subset of $M_n$. Clearly matrix multiplication is closed on $Y$. 


Let $X$ be set with a binary operation $*$ on $X$. We call $(X, *)$ a binary structure and often out of laziness just refer to it as $X$.

Let $(X, *)$ and $(X', *)'$ be binary structures. A bijection $(1 - 1$ and onto) $f : X \to X'$ satisfying $f(x * y) = f(x) *' f(y)$ for all $x, y \in X$ is called a isomorphism of $X$ and $X'$ (as binary structures with respect to the binary operators) and $X$ and $X'$ are called isomorphic.

Let’s show that $(\mathbb{R}, +)$ and $(X, \cdot)$ where $X = \{x \in \mathbb{R} | x > 0\}$ are isomorphic:

Define $f : \mathbb{R} \to X$ by $f(x) = e^x$. $f$ is well-defined since $e^x \in X$ for all $x \in \mathbb{R}$ as $e^x > 0$. Let $x, y \in \mathbb{R}$ and suppose $f(x) = f(y)$. Then $e^x = e^y$. Hence $x = y$, so $f$ is $1 - 1$. Let $r \in X$. Then $\ln(r) \in \mathbb{R}$ and $e^{\ln(r)} = r$. So $f$ is onto. Finally, let $x, y \in \mathbb{R}$. $f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$.

Let $(X, *)$ be a binary structure. $e \in X$ is called an identity element (for $*$) if $\forall x \in X$, $e * x = x * e = x$.

For example, the identity matrix $I_2$ acts as the identity element in $(M_2, \cdot)$, but not in $(M_2, +)$. What acts as the identity element in $(M_2, +)$?

Not all binary structures have identity elements. Consider the interval $(1, \infty) \subseteq \mathbb{R}$ with the binary operation $\cdot$. There is no identity element in this binary structure since for all $x, y \in (1, \infty)$, $x \cdot y > \text{Max}(x, y)$, so $x \cdot y \neq x$ and $x \cdot y \neq y$.

Let $(X, *)$ be a binary structure with an identity element $e$. Suppose $e'$ is also an identity element of $(X, *)$. Then $e * e' = e$ since $e'$ is an identity element. But since $e$ is an identity element, $e * e' = e'$. Putting these together, $e' = e$. So an identity element is unique!

**Proposition 0.1:** Let $(X, *)$ be a binary structure with an identity element $e$. Suppose $(X', *')$ is an isomorphic binary structures given by the isomorphism $\phi : X \to X'$. Then $\phi(e)$ is an identity element of $(X', *')$.

**Proof:** Let $y \in X'$. It suffices to show that $\phi(e) *' y = y *' \phi(e) = y$. Since $\phi$ is onto there exists $x \in X$ such that $\phi(x) = y$. Then $\phi(e) *' y = \phi(e) *' \phi(x) = \phi(e * x) = \phi(x) = y$ and $y *' \phi(e) = \phi(x) *' \phi(e) = \phi(x * e) = \phi(x) = y \square$
Groups

A group, $G$, is a set together with a binary operation $*$ on $G$ (so a binary structure) such that the following three axioms are satisfied:

(A) For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$. We say $*$ is associative.

(B) There exists an identity element $e \in G$.

(C) For all $x \in G$, there exists an element $x' \in G$ such that $x * x' = x' * x = e$. Such an element $x'$ is called an inverse of $x$.

If finite, $|G|$ is the order of the group.

Note: Formally, the group is $(G, *)$, but often when $*$ is understood by context we just write $G$ for the group. Also, the identity element is an inverse of itself.

Examples:

(1) Let $(G, *)$ consists of $G = \{e\}$ where $e * e = e$. This is the trivial group of order 1. Think $(\{1\}, \cdot)$ or $(\{0\}, +)$ or $(\{f\}, \circ)$ where $f : \mathbb{R} \to \mathbb{R}$ is the function given by $f(x) = x$.

(2) $(\mathbb{Z}, +)$ (or replace $\mathbb{Z}$ with $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$) forms a group as addition is an associative operator, 0 is the identity element, and an inverse of $x \in \mathbb{Z}$ is $-x \in \mathbb{Z}$.

(3) Let $X \subseteq \mathbb{C}$ containing the number 0. Let $X^* = X \setminus \{0\}$. $(\mathbb{Q}^*, \cdot)$ (or replace $\mathbb{Q}^*$ with $\mathbb{R}^*$ or $\mathbb{C}^*$) forms an infinite group as multiplication is an associative operator, 1 is the identity element, and an inverse of $x \in \mathbb{Q}^*$ is $1/x \in \mathbb{Q}^*$.

(4) Let $X$ be either $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$. Let $X^+ = \{x \in X | x > 0\}$. $(\mathbb{Q}^+, \cdot)$ (or replace $\mathbb{Q}^+$ with $\mathbb{R}^+$) forms an infinite group as multiplication is an associative operator, 1 is the identity element, and an inverse of $x \in \mathbb{Q}^+$ is $1/x \in \mathbb{Q}^+$.

(5) Let $n \in \mathbb{N}$. Let $\mathbb{Z}_n = \{0, 1, ..., n - 1\}$ where the closed binary operation on $\mathbb{Z}_n$ is addition modulo $n$. $\mathbb{Z}_n$ is a finite group or order $n$. Associativity is inherited from the addition operator, the identity element is 0, and an inverse of $a \in \mathbb{Z}_n$ is the element $(n - a)(\text{mod} n) \in \mathbb{Z}_n$.

(6) Let $m, n \in \mathbb{N}$. $(M_{mn}(\mathbb{R}), +)$ forms a group as matrix addition is associative, $0_{mn}$ ($m \times n$ matrix consisting of all zeros) is the identity, and an inverse of $A \in M_{mn}(\mathbb{R})$ is $-A \in M_{mn}(\mathbb{R})$. Note: This works with $\mathbb{R}$ replaced by $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{C}$ (or any other so-called ring – to be defined later).
(7) Let $n \in \mathbb{N}$. Let $GL_n(\mathbb{R}) = \{ A \in M_n | \det(A) \neq 0 \}$. With matrix multiplication as the binary operator, $GL_n(\mathbb{R})$ is called the general linear group of $n \times n$ matrices. Matrix multiplication is associative, the identity element is $I_n$ ($\det(I_n) = 1$), and an inverse of $A \in GL_n(\mathbb{R})$ is $A^{-1} \in GL_n(\mathbb{R})$ which exists since $\det(A) \neq 0$ and is in $GL_n(\mathbb{R})$ since $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$. Note: This works with $\mathbb{R}$ replaced by $\mathbb{Q}$ or $\mathbb{C}$ (or any other so-called field – to be defined later).

(8) $U = \{ z \in \mathbb{C} : |z| = 1 \}$ forms a group under multiplication. Complex number multiplication is associative, the identity element is 1, and an inverse of $z = a + bi \in U$ is $\bar{z} = a - bi \in U$ (since $1 = a^2 + b^2$). Exercise left for you (ELFY): Show that $z\bar{z} = |z| = 1$ for $z \in U$. This group is sometimes referred to as the circle group as geometrically it’s the unit circle in the complex plane.

(9) Let $n \in \mathbb{N}$. The so-called $n$th Roots of Unity, $U_n = \{ z \in \mathbb{C} | z^n = 1 \}$, form a finite group under multiplication. Associativity is inherited from complex number multiplication, $1 \in U_n$ is the identity element, and an inverse of $z \in U_n$ is $\frac{1}{z}$ (defined since $z \neq 0$) which is in $U_n$ since $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$. ELFY: Show that for $z \in U_n$, $|z| = 1$ (so $z \in U$) and $\frac{1}{z} = \bar{z}$.

Let’s have some more fun with $U_n$: Let $z \in U_n$. Since $z \in \mathbb{C}$, $z = re^{i\theta}$ where $r, \theta \in \mathbb{R}$ ($r \geq 0$). Then

$$z^n = r^n e^{in\theta} = 1$$

so $r = 1$ and $n\theta = 2k\pi$ where $k \in \{0,1,2,\ldots,n-1\}$.

Note: If $n\theta = 2k\pi$ for an integer $k$ then $\theta = \frac{2k\pi}{n}$, so by periodicity, there is no need to consider $\theta$ outside of $[0,2\pi)$ and hence there is no need to consider $k$ outside of $\{0,1,2,\ldots,n-1\}$.

So $U_n = \{ e^{i(2k\pi/n)} | k = 0,1,2,\ldots,n-1 \}$ is a finite group of order $n$. The root of unity $e^{i(2k\pi/n)}$ is primitive if the gcd($k,n$) = 1.

(10) Let $X$ be a set. Then the set $B = \{ f : X \to X | f \text{ is a bijection} \}$ forms a group under function composition $\circ$. Function composition is associative (ELFY), the identity element is $Id : X \to X$ given by $Id(x) = x$ (ELFY), and an inverse of $f \in B$ is $f^{-1} \in B$ (ELFY).
Let $X$ be the set $\{1, 2, ..., n\}$. Then $S_n = \{\sigma : X \to X|\sigma \text{ is a bijection}\}$ under function composition is called the symmetric group of permutations of $n$ (a finite group of order $n!$). We will spend a lot of time with these groups.

Notes for the symmetric group:

- Let $\sigma \in S_n$. We adopt the convention that $\sigma$ acts on the right:
  
  So if $\sigma$ sends $i \in \{1, 2, ..., n\}$ to $j \in \{1, 2, ..., n\}$ we write $(i)\sigma = j$.

- The best notation for elements of $S_n$ is cycle notation:
  
  $c \in S_n$ is a cycle if $c = (i_1 i_2 \cdots i_{\ell})$ where $\ell \in \{1, 2, ..., n\}$ is the length of the cycle and $(i_j)c = i_{(j+1)}$ for $j = 1, 2, ..., \ell - 1$ and $(i_\ell)c = i_1$, while $c$ fixes elements (sends the element to itself) in $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_{\ell}\}$.

  For example, the cycle $c = (1 2 4)$ of length 3 in $S_4$ sends 1 to 2, 2 to 4, and 4 to 1, while fixing 3. Of course this cycle can be written in three equivalent ways: $(1 2 4)$ or $(2 4 1)$ or $(4 1 2)$.

  Now let $\sigma \in S_n$. Determine $(1)\sigma, ((1)\sigma)\sigma, ..., (1)\sigma^{j_1} = 1$ until the first $j_1 \in \{1, 2, ..., n\}$ such that $(1)\sigma^{j_1} = 1$. This gives the cycle $c_1 = (1 (1)\sigma (1)\sigma^2 \cdots (1)\sigma^{j_1 - 1})$. Then pick the smallest $i \in \{1, 2, ..., n\} \setminus \{1, (1)\sigma, (1)\sigma^2, ..., (1)\sigma^{j_1 - 1}\}$ (if possible; if not, then $\sigma = c_1$) and do the same thing to get the cycle $c_2 = (i (i)\sigma (i)\sigma^2 \cdots (i)\sigma^{j_2 - 1})$ where $j_2 \in \{1, 2, ..., n\}$ is the smallest integer such that $(i)\sigma^{j_2} = i$. Note: $c_1$ and $c_2$ are disjoint cycles as they do not share any entries. Keep doing this to produce pairwise disjoint cycles $c_1, c_2, ..., c_k$ that account for all the elements of $\{1, 2, ..., n\}$. Then $\sigma = c_1c_2 \cdots c_k$ (the product can be done in any order since disjoint cycles commute: $(j)\sigma = (j)c_\ell$ where $j$ is involved in $c_\ell$). Note: Convention is to drop all cycles of length 1 and to write $Id$ for the identity permutation $(1)(2) \cdots (n)$.

  For example, let $\sigma \in S_6$ be the permutation that sends 1 to 2, 2 to 4, 3 to 5, 4 to 1, 5 to 3, and 6 to 6. Then in cycle notation $\sigma = (1 2 4)(3 5)$.

  Here are all 6 elements of $S_3$ in cycle notation: $Id, (1 2), (2 3), (1 3), (1 2 3), \text{ and } (1 3 2)$.

  Here are all 24 elements of $S_4$ in cycle notation:

  $Id, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)$.

  Note: Cycles of length two are called transpositions.
(12) Dihedral groups: Consider a regular polygon $P$ with $n \geq 3$ sides (e.g. an equilateral triangle, a square, etc...). A symmetry of $P$ is either a rotation or a reflection of $P$ such that the result looks the same (ignoring labeling of the vertices). Clearly the composition of two symmetries produces a symmetry, and each symmetry has an inverse symmetry bringing the polygon back to it’s original state (where vertices are kept track of by labels).

There are $n$ (ccw) rotations (including the trivial rotation by 0 radians) and $n$ reflections for a total of $2n$ elements in the dihedral group of order $2n$, denoted $D_{2n}$. The identity element is the trivial rotation, the inverse of a reflection is itself, and the inverse of a non-identity rotation by $\theta$ radians is the non-identity rotation by $2\pi - \theta$ radians.

For example, $D_6$ consists of the symmetries of an equilateral triangle: Let $R_0, R_1, R_2$ be the (ccw) rotations by 0, $2\pi/3$, $4\pi/3$ radians respectively and $S_0, S_1, S_2$ be the 3 reflections (as seen in the figure). Consider the product $R_1S_0$. It’s important to realize that this is the composition of $R_1$ after $S_0$. A quick check on the diagram below yields $R_1S_0 = S_1$.

Here is a multiplication table for the $D_6$ (product order is row by column):

<table>
<thead>
<tr>
<th></th>
<th>$R_0$</th>
<th>$R_1$</th>
<th>$R_2$</th>
<th>$S_0$</th>
<th>$S_1$</th>
<th>$S_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_0$</td>
<td>$R_0$</td>
<td>$R_1$</td>
<td>$R_2$</td>
<td>$S_0$</td>
<td>$S_1$</td>
<td>$S_2$</td>
</tr>
<tr>
<td>$R_1$</td>
<td>$R_1$</td>
<td>$R_2$</td>
<td>$R_0$</td>
<td>$S_1$</td>
<td>$S_2$</td>
<td>$S_0$</td>
</tr>
<tr>
<td>$R_2$</td>
<td>$R_2$</td>
<td>$R_0$</td>
<td>$R_1$</td>
<td>$S_0$</td>
<td>$S_1$</td>
<td>$S_2$</td>
</tr>
<tr>
<td>$S_0$</td>
<td>$S_0$</td>
<td>$S_2$</td>
<td>$S_1$</td>
<td>$R_0$</td>
<td>$R_2$</td>
<td>$R_1$</td>
</tr>
<tr>
<td>$S_1$</td>
<td>$S_1$</td>
<td>$S_0$</td>
<td>$S_2$</td>
<td>$R_1$</td>
<td>$R_0$</td>
<td>$R_2$</td>
</tr>
<tr>
<td>$S_2$</td>
<td>$S_2$</td>
<td>$S_1$</td>
<td>$S_0$</td>
<td>$R_2$</td>
<td>$R_1$</td>
<td>$R_0$</td>
</tr>
</tbody>
</table>

(ELFY) Verify the products in the table!
The following are binary structures that are NOT groups:

- $M_n$ where the binary operation is matrix multiplication. While matrix multiplication is associative and $I_n$ is the identity element, not every element has an inverse: In fact, for any matrix $A$ such that $\det(A) = 0$ there is no inverse.

- The set of positive integers, $\mathbb{Z}^+$ where the operation is multiplication. While the operation is associative and $1$ is the identity, for integers $n \geq 2$ there is no inverse in $\mathbb{Z}^+$.

- The set of all functions $f : \mathbb{R} \to \mathbb{R}$ where the binary operation is function composition. While the operation is associative and $f(x) = x$ is the identity, many functions have no inverse, like $f(x) = x^2$.

A group $G$ is called **abelian** if the binary operation is commutative.

(ELFY) Identify which groups among the examples are abelian, and which are not abelian. Note: This should not be hard.

**ELEMENTARY PROPERTIES OF GROUPS:**

**Proposition 1.1 (Cancellation Laws):** Let $(G, \ast)$ be a group. For all $a, b, c \in G$, $a \ast b = a \ast c$ implies $b = c$. For all $a, b, c \in G$, $b \ast a = c \ast a$ implies $b = c$.

*Proof*: Let $a, b, c \in G$ and $e$ be the identity. Assume $a \ast b = a \ast c$. Let $a'$ be an inverse of $a$. Then $a' \ast a = e$. By multiplying both sides of $a \ast b = a \ast c$ on the left by $a'$ we get $a' \ast (a \ast b) = a' \ast (a \ast c)$. By using the associative property, we get $(a' \ast a) \ast b = (a' \ast a) \ast c$. This becomes $e \ast b = e \ast c$, and thus $b = c$. Similarly, $b \ast a = c \ast a$ implies $b = c$. □

**Proposition 1.2**: Let $(G, \ast)$ be a group and $a, b \in G$. Then the equations $a \ast x = b$ and $y \ast a = b$ have unique solutions $x$ and $y$ in $G$.

*Proof*: Let $e$ be the identity. Assume $a \ast x = b$. Let $a'$ be an inverse of $a$. Then $a \ast (a' \ast b) = (a \ast a') \ast b = e \ast b = b$. So $x = a' \ast b$ is a solution to $a \ast x = b$. Suppose $x_1$ and $x_2$ are both solutions to $a \ast x = b$. Then $a \ast x_1 = a \ast x_2$. Then by the previous proposition, $x_1 = x_2$, showing that $x = a' \ast b$ is the unique solution to $a \ast x = b$. A similar argument shows that $y = b \ast a'$ is the unique solution to $y \ast a = b$. □

The last proposition justifies that **inverses are unique**:

Let $(G, \ast)$ be a group and $e$ the identity in $G$. If $a'$ is an inverse of $a$ then it is a solution to $a \ast x = e$ and $y \ast a = e$ where $e$ is the identity of $G$. Hence $a'$ is THE unique inverse of $a$, so we can finally start writing “the inverse” rather than “an inverse.” At this point we will also adopt the notations $a^{-1}$ or $-a$ as the standard for the inverse of a group element $a$. 
Proposition 1.3: Let \((G, \ast)\) be a group and \(a, b \in G\). Then the inverse of \(a \ast b\) is \((a \ast b)^{-1} = b^{-1} \ast a^{-1}\).

Proof: Let \(e\) be the identity. Then \((a \ast b) \ast (b^{-1} \ast a^{-1}) = a \ast (b \ast (b^{-1} \ast a^{-1})) = a \ast ((b \ast b^{-1}) \ast a^{-1}) = a \ast (e \ast a^{-1}) = a \ast a^{-1} = e\. Hence \(x = b^{-1} \ast a^{-1}\) is the unique solution to \((a \ast b) \ast x = e\. A similar calculation shows that \(y = b^{-1} \ast a^{-1}\) is the unique solution to \(y \ast (a \ast b) = e \).
Subgroups

Let’s begin with some conventions. If $G$ is a group and we are regarding the binary operation as a “multiplicative” operation then we write $ab$ for the product of $a \in G$ and $b \in G$ (in that order) and $a^{-1}$ for the inverse of $a \in G$. Furthermore, we write $a^2$ for $aa$, $a^3$ for $aaa = (aa)a = a(aa)$, and so it goes. $a^0$ denotes $e$. So for example, $a^2b^3a^{-1}$ is shorthand for $aabba^{-1}$.

If $G$ is a group and we are regarding the binary operation as a “additive” operation then for $a \in G$ we write $2a$ for $a + a$, $3a$ for $a + a + a = a + (a + a) = (a + a) + a$, and so it goes. 0 is the identity and $-a$ is the inverse of $a \in G$. We also write $-na$ for $n(-a)$ where $n$ is a positive integer.

Note: The use of the additive notation implies the group is abelian! So in general, the default notation for a group’s binary operation is multiplicative without assuming the group is (or isn’t) abelian.

Let $G$ be a group. If a subset $H \subseteq G$ that is closed under the binary operation of $G$ is itself a group under the same binary operation then $H$ is a subgroup of $G$. If $H \neq G$ is a subgroup of $G$ it is called a proper subgroup.

Examples:

1. Let $G$ be a group. $G$ is a subgroup of itself. Another subgroup is the trivial subgroup $\{e\}$ where $e$ is identity element in $G$.

2. Let $n \in \mathbb{N}$. $U_n$ (nth roots of unity) form a subgroup of the circle group $U$ and of $\mathbb{C}^*$ (under multiplication). The circle group $U$ is a subgroup of $\mathbb{C}^*$.

3. Let $G = \mathbb{Z}_4$. The subgroups of $G$ are the trivial subgroup, $\{0\}$, the subgroup $\{0, 2\}$, and the group $G$ itself.

4. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ (aka the Klein 4-group up to isomorphism - more on this soon!) where the operation is componentwise addition modulo 2. The subgroups of $G$ are the trivial subgroup, $\{(0,0)\}$, the subgroup $\{(0,0), (1,0)\}$, the subgroup $\{(0,0), (0,1)\}$, the subgroup $\{(0,0), (1,1)\}$, and the group $G$ itself.

Notation for a subgroup:

$H \leq G$ denotes that $H$ is a subgroup of $G$ (possibly equal to $G$). $H < G$ denotes that $H$ is a proper subgroup of $G$. 

Note:

Let $H \leq G$ and $a \in H$. The equation $ax = a$ must have a unique solution in $H$, namely the identity $e$ of $H$. But this equation would also have the same unique solution in $G$ since $H$ is a subset of $G$. This means that the identity for the group and the subgroup coincide. A similar argument shows that if $a^{-1} \in H$ is the inverse of $a \in H$ then the same element $a^{-1}$ is also the inverse of $a \in G$.

**Proposition 2.1:** Let $G$ be a group and $H \subseteq G$. $H \leq G$ iff the following three conditions hold:

1. $H$ is closed under the binary operation of $G$.
2. The identity element $e \in G$ is in $H$.
3. For all $a \in H$, $a^{-1} \in H$.

**Proof:** The fact that if $H \leq G$ then these three conditions hold follows directly from the definition of a subgroup and the remarks above.

Conversely suppose that we know that conditions 1, 2 and 3 above hold for $H \subseteq G$. Condition 1 tells us that the closed binary operation on $G$ forms a closed binary operation on $H$. Conditions 2 and 3 tell us that $H$ satisfies having an identity element and every element in $H$ has an inverse in $H$. The only thing left to check is associativity; that’s inherited from $G$ since for all $a, b, c \in H$, it follows that $a, b, c \in G$ and thusly $a(bc) = (ab)c$.

Example showing that a subset is a subgroup:

Consider $SL_n(\mathbb{R}) = \{A \in M_{nn} | \det(A) = 1\}$. Clearly $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. For all matrices $A, B \in SL_n(\mathbb{R})$, we have that $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$. So matrix multiplication is a closed binary operation on $SL_n(\mathbb{R})$. Clearly the identity $I_n \in GL_n(\mathbb{R})$ is in $SL_n(\mathbb{R})$ as $\det(I_n) = 1$. Let $A \in SL_n(\mathbb{R})$. Let $A^{-1}$ be the inverse of $A$ in $GL_n(\mathbb{R})$. Since $1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(A^{-1})$ we have that $A^{-1} \in SL_n(\mathbb{R})$. Hence by proposition 2.1, $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. This also works over other fields (to be defined later) such as $\mathbb{Q}$ and $\mathbb{C}$. $SL_n(\mathbb{R})$ is called the special linear group (subgroup of the general linear group).
Proposition 2.2 (The 1-step subgroup test): Let $G$ be a group and let $H$ be a nonempty subset of $G$. If for all $a, b \in H$, $ab^{-1} \in H$ then $H$ is a subgroup of $G$.

**Proof:** Assume for all $a, b \in H$, $ab^{-1} \in H$. Let $h \in H$. By setting $a = b = h$ we get that $ab^{-1} = hh^{-1} = e \in H$ (where $e$ is the identity in $G$). Then by setting $a = e$ and $b = h$ we get that $h^{-1} \in H$. Finally, we show that $H$ is closed under the binary operation. Let $h_1, h_2 \in H$. By setting $a = h_1$ and $b = h_2^{-1}$ we get $h_1(h_2^{-1})^{-1} = h_1h_2 \in H$. □

Let’s see this test in action! Let’s consider the group $GL_2(\mathbb{R})$.

Show that $UT_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} < GL_2(\mathbb{R})$:

First we note that $I_2 \in UT_2(\mathbb{R})$ so $UT_2(\mathbb{R}) \neq \emptyset$. Next we note that $UT_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ as for any $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in UT_2(\mathbb{R})$, $\det(A) = ad \neq 0$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \setminus UT_2(\mathbb{R})$.

Let $A, B \in UT_2(\mathbb{R})$. So $A = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ & $B = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ where $a_1, a_2, b_1, b_2, d_1, d_2 \in \mathbb{R}$, $a_1d_1 \neq 0$ and $a_2d_2 \neq 0$. Hence $a_1 \neq 0$, $a_2 \neq 0$, $d_1 \neq 0$ and $d_2 \neq 0$.

Finally, $B^{-1} = \begin{pmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2d_2} \\ 0 & \frac{1}{d_2} \end{pmatrix}$ and thus

$$AB^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2d_2} \\ 0 & \frac{1}{d_2} \end{pmatrix} = \begin{pmatrix} \frac{a_1}{a_2} & -\frac{a_1b_2}{a_2d_2} + \frac{b_1}{d_2} \\ 0 & \frac{d_1}{d_2} \end{pmatrix} \in UT_2(\mathbb{R})$$ since $\frac{a_1d_1}{a_2d_2} \neq 0$

So the set $UT_2(\mathbb{R})$ of invertible, upper-triangular matrices is a proper subgroup of the general linear group $GL_2(\mathbb{R})$. 

Let $G$ be a group and $a \in G$. Clearly a subgroup $H \leq G$ that contains $a$ must also contain all integer powers of $a$ (these may not all be distinct!) such as the identity $a^0$, the inverse $a^{-1}$, $a^2$, $a^{-2} = (a^{-1})^2$, and so on. So if $a \in H$ and $H \leq G$ then $\{a^n | n \in \mathbb{Z}\} \subseteq H$.

**Proposition 2.3:** Let $G$ be a group and $a \in G$. Then $$< a > = \{a^n | n \in \mathbb{Z}\}$$ is the smallest subgroup of $G$ that contains $a$ (called the cyclic subgroup of $G$ generated by $a \in G$).

**Proof:** First we check that $< a >$ is closed under the binary operation: Let $x, y \in < a >$. Then there exists $r, s \in \mathbb{Z}$ such that $x = a^r$ and $y = a^s$. Then $xy = a^r a^s = a^{r+s} \in < a >$ since $r+s \in \mathbb{Z}$, so $< a >$ is closed under the binary operation. The identity element is $a^0 = e$ so the identity element of $G$ is in $< a >$. For $a^r \in < a >$, $a^{-r} \in < a >$ and $a^r a^{-r} = a^0 = e$. Finally, by the note above the proposition, if $H \leq G$ contains $a$ then $H$ contains $< a >$. So $< a >$ is the smallest subgroup of $G$ that contains $a$. 

Let $G$ be a group (maybe finite, maybe not). Let $a \in G$. If the cyclic subgroup $< a >$ is finite then the order of the element $a$ is $| < a > |$.

Let $G$ be a group. An element $a \in G$ generates $G$ (aka is a generator of $G$) if $G = < a >$. Furthermore a group $G$ is a cyclic group when there is an element $a \in G$ that generates $G$.

Note: In additive notation, $< a > = \{na | n \in \mathbb{Z}\}$.

Consider the group $Z_4$ of order 4 (integers $\{0, 1, 2, 3\}$ under addition modulo 4). $< 1 >$ contains $1, 1+1 = 2, 1+1+1 = 3, 1+1+1+1 = 0$. Similarly, $< 3 >$ contains $3, 3+3 = 2, 3+3+3 = 1$ and $3+3+3+3 = 0$. So $< 1 >= < 3 >= Z_4$. $< 2 >$ contains exactly 2 and $2+2 = 0$ ($-2 = 2$). Finally, $< 0 >$ is the trivial subgroup. Hence $Z_4$ is a cyclic subgroup of order 4 generated by 1 or 3, but not by 2 or 0.

Consider the group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$. Clearly $< (0, 0) >$ is the trivial subgroup. Let $a \in V$ be nontrivial (not $(0, 0)$). Then $a + a = 0$ so $-a = a$. Hence $< a > = \{(a, 0)\}$. So $V$ is not cyclic as there is no single generator of $V$ (all nontrivial elements are order 2).

**Proposition 2.4:** Every cyclic group is abelian.

**Proof:** Let $G$ a cyclic group generated by $a \in G$. Let $x, y \in G$. Then there exists $r, s \in \mathbb{Z}$ such that $x = a^r$ and $y = a^s$. Then $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$. 

Lemma 2.5 (Division Algorithm for \( \mathbb{Z} \)): If \( d \in \mathbb{Z}^+ \) and \( n \in \mathbb{Z} \) then there exists unique integers \( q, r \) such that \( n = qd + r \) where \( 0 \leq r \leq d - 1 \).

**Proof**: Let \( X = \{ n - dk | n - dk \geq 0, k \in \mathbb{Z} \} \). By selecting \( k \in \mathbb{Z} \) so that \( k < \frac{n}{d} \) (integers are unbounded) we have \( dk < n \) and therefore, \( n - dk \in X \). Thus \( X \) is nonempty. Let \( r \in X \) be the smallest element. In particular \( r \geq 0 \). Label by \( q \) the integer that satisfies \( n = dq + r \). Then \( n = dq + r \).

Now suppose \( r \geq d \). Then \( r - d \geq 0 \) and hence, \( n - d(q + 1) = r - d \in X \) and \( r - d < r \). But this contradicts that \( r \) is the smallest element of \( X \).

Thus \( 0 \leq r < d \).

Now for uniqueness. Suppose \( r_1, r_2, q_1, q_2 \in \mathbb{Z} \) and

\[
\begin{align*}
n &= dq_1 + r_1 \text{ and } 0 \leq r_1 < d. \\
n &= dq_2 + r_2 \text{ and } 0 \leq r_2 < d.
\end{align*}
\]

Then \( 0 = n - n = d(q_1 - q_2) + (r_1 - r_2) \) implies \( d(q_1 - q_2) = (r_2 - r_1) \). But then \( d \) divides \( r_2 - r_1 \) and since \( 0 \leq r_1, r_2 < d \),

\[
-d < r_2 - r_1 < d \text{ and so } r_1 = r_2.
\]

Then \( d(q_1 - q_2) = 0 \) implying that \( q_1 = q_2 \). □

**Proposition 2.6**: Every subgroup of a cyclic group is a cyclic group.

**Proof**: Let \( G \) a cyclic group generated by \( a \in G \). Let \( H \leq G \). Assume \( H \neq \langle e \rangle \) where \( e \) is the identity as otherwise then we are done. Let \( d \in \mathbb{Z}^+ \) be the smallest such that \( a^d \in H \).

We want to show that \( H \) is generated by \( a^d \).

Let \( b \in H \). Then \( b = a^n \) for some \( n \in \mathbb{Z} \). Find integers \( q,r \) such that \( n = qd + r \) and \( 0 \leq r < d \). Then \( b = a^{qd+r} = (a^d)^q a^r \), so \( a^r = b(a^d)^{-q} \in H \) as \( b \in H \) and \( (a^d)^{-q} \in H \) as \( H \) contains \( \langle a^d \rangle \). Hence \( r = 0 \) as otherwise it contradicts how \( d \) was chosen. Consequently, \( a^n = (a^d)^q \) showing that \( \langle a^d \rangle \) contains \( H \), and hence is equal to \( H \). Hence \( H \) is a cyclic group generated by \( a^d \). □

**Corollary 2.7**: The subgroups of \( \mathbb{Z} \) (as a group under addition) are \( n\mathbb{Z} = \langle n \rangle = \{ kn | k \in \mathbb{Z} \} \) where \( n \in \mathbb{Z} \).

**Proof**: Since \( \mathbb{Z} = \langle 1 \rangle \) is cyclic, every subgroup must be cyclic by the previous proposition. That completes the proof. □
Let $m, n$ be positive integers. Consider $H = \{am + bn | a, b \in \mathbb{Z}\}$. ELFY: Show that $H \leq \mathbb{Z}$ (under addition).

Let $d = \gcd(m, n) \in \mathbb{Z}^+$ (greatest common divisor). We know that $H = \langle \ell \rangle = \ell \mathbb{Z}$ for some $\ell \in \mathbb{Z}$. Assume without loss of generality (WLOG) that $\ell > 0$. In particular, $m \in H$ (set $a = 1$, $b = 0$) and $n \in H$ (set $a = 0$, $b = 1$), so $m = j\ell$ and $n = k\ell$ for some $j, k \in \mathbb{Z}$. So $\ell$ must be a common divisor of $m$ and $n$ implying $\ell \leq d$. Since $\ell \in H$, there exists $a, b \in \mathbb{Z}$ such that $\ell = am + bn$. Since $d$ divides the RHS of this equation, it must divide the LHS of this equation. So $d$ divides $\ell$ and thus $\ell$ is a positive-integer multiple of $d$. From earlier we have that $\ell \leq d$. Hence it must be that $\ell = d$. So the generator of $H$ is the greatest common divisor of $m, n$.

As a consequence of this, there exists $r, s \in \mathbb{Z}$ such that $\gcd(m, n) = rm + sn$.

[The greatest common divisor of two positive integers is a linear combination of the integers!]

Let $d$ be the least positive integer such that there exists integers $k, j$ such that $d = km + jn$.

Let integers $a, b$ satisfy $d = am + bn$

Claim: $d$ is the $\gcd(m, n)$.

Let’s prove the claim. Let’s show first that $d$ divides $m$. By the division algorithm, there exists unique integers $q, r$ such that $m = qd + r$ and $0 \leq r < d$. Then it follows that $r = m - qd = m - q(am + bn) = (1 - qa)m + (-qb)n$. Since $d$ was picked to be the least positive integer such that there exists integers $k, j$ such that $d = km + jn$ we get that $r = 0$. So $d$ divides $m$. A symmetric argument shows $d$ divides $n$. So $d$ is a common divisor of $m$ and $n$.

Suppose $d' = \gcd(m, n)$. Then $d' \geq d$. Well, $d'$ divides $m$ and $n$, so it follows that $d'$ divides $d = am + bn$. Therefore $d' \leq d$. So if follows that $d = d'$, finishing the proof of the claim.

Suppose the $\gcd(m, n) = 1$ (that is, $m, n$ are relatively prime) and suppose $m$ divides $nk$ where $k \in \mathbb{Z}$. Let’s show that it must be the case that $m$ divides $k$:

First we can note that there exists integers $r, s$ such that $1 = rm + sn$.

Multiplying both sides by the integer $k$ we get $k = krm + ksn$ Since $m$ divides the RHS it divides the LHS.

We will use these results (on this page) in the next section.
Introduction to Group Isomorphisms

Let $G$ and $G'$ be groups. A bijection $(1-1$ and onto) $\phi : G \to G'$ satisfying $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$ is called a group isomorphism between $G$ and $G'$ (as groups with respect to their operations) and $G$ and $G'$ are called isomorphic groups and we use the notation $G \cong G'$.

Note: All we really require is that they are isomorphic as binary structures!

Examples:

1. Let $G = S_3 = \{Id, (1 2), (2 3), (1 3), (1 2 3), (1 3 2)\}$ (a symmetric group) and $G' = D_6 = \{R_0, R_1, R_2, S_0, S_1, S_2\}$ with the multiplication table on page 6 (a dihedral group).

   By having $\phi(Id) = R_0$, $\phi((1 2)) = S_0$, $\phi((2 3)) = S_2$, $\phi((1 3)) = S_1$, $\phi((1 2 3)) = R_2$, and $\phi((1 3 2)) = R_1$ we get an isomorphism.

   ELFY: Show that $\phi$ is indeed a group isomorphism. So $S_3 \cong D_6$.

2. Let $n \in \mathbb{N}$. The $n$th roots of unity $U_n = \{e^{i(2k\pi/n)}|k = 0, 1, 2, ..., n-1\}$ (with complex number multiplication) is isomorphic to the cyclic group $\mathbb{Z}_n$ (modulo $n$ addition):

   Let $\phi : U_n \to \mathbb{Z}_n$ be given by $\phi \left(e^{i(2k\pi/n)}\right) = k$ for $k = 0, 1, ..., n-1$. By explicit construction this is a bijection from $U_n$ to $\mathbb{Z}_n$. We just require that the “morphism” property is satisfied:

   Let $z_1, z_2 \in U_n$. Then there exists $a, b \in \{0, 1, ..., n-1\}$ such that $z_1 = e^{i(2a\pi/n)}$ and $z_2 = e^{i(2b\pi/n)}$. Then

   $\phi(z_1z_2) = \phi \left(e^{i(2a\pi/n)}e^{i(2b\pi/n)}\right) = \phi \left(e^{i(2(a+b)\pi/n)}\right) = (a + b) \mod n = (\phi(z_1) + \phi(z_2)) \mod n$.

   So $U_n \cong \mathbb{Z}_n$.

Proposition 3.1: Let $G$ and $G'$ be isomorphic groups and $\phi : G \to G'$ be an isomorphism. Let $e$ and $e'$ be the identities in $G$ and $G'$ respectively. The following hold true:

1. $\phi(e) = e'$.  
2. For all $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$.

Proof: Let $g \in G$. $\phi(g) = \phi(ge) = \phi(g)\phi(e)$. By left-cancelation by $\phi(g)$ we get that $e' = \phi(e)$ proving 1. Now consider that we have $e' = \phi(e) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$ and $e' = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. So using either one $\phi(g)^{-1} = \phi(g^{-1})$ $\square$
**Proposition 3.2:** Let $G$ be a cyclic group with generator $a \in G$. If $G$ is infinite then $G \cong \mathbb{Z}$ (under addition). If $G$ is finite with $|G| = n$ then $G \cong \mathbb{Z}_n$ (under addition modulo $n$).

**Proof:** Let $e = a^0$ be the identity. Two cases: Either $a$ is of order $m \in \mathbb{N}$ or not (meaning $a^m \neq e$ for all $m \in \mathbb{N}$).

Let’s start with the latter. Define $\phi : G \to \mathbb{Z}$ by $\phi(a^n) = n$ for $n \in \mathbb{Z}$. First we show this is a well-defined function. $a^n \neq a^m$ for all distinct integers $m, n$ because otherwise, $a$ would be of order $|m - n| \in \mathbb{N}$. So every input is unique and hence we don’t have one input going to multiple outputs. This makes $\phi$ a well-defined function. By construction $\phi$ is $1 - 1$ and onto. So $\phi$ bijection. Finally, for $a^m, a^n \in G$, $\phi(a^m a^n) = \phi(a^{m+n}) = m + n = \phi(a^m) + \phi(a^n)$. So $\phi$ is an isomorphism showing $G \cong \mathbb{Z}$.

Now let’s assume $a$ is of order $m$. Let $n$ be the smallest positive integer such that $a^n = e$. Let $s \in \mathbb{Z}$. Then $s = qn + r$ for unique integers $q, r$ such that $0 \leq r < n$. Then $a^s = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$. So for all $a^s \in G$ there exists $r \in \{0, 1, 2, ..., n - 1\}$ such that $a^s = a^r$. This means that $G = \{a^i | i = 0, 1, ..., n - 1\}$. Suppose $0 \leq i < j < n$ and $a^i = a^j$. Then $a^{j-i} = a^0$ for $0 < j - i < n$ contradicting that the order of $a$ is $n$. Thus the elements $a^0, a^1, ..., a^{n-1}$ are all distinct (so $G = \langle a \rangle$ is of order $m = n$). Thus the map given by $\phi(a^i) = i$ for $i \in \{0, 1, ..., n - 1\}$ is well-defined, $1 - 1$ and onto. Finally, for $i, j \in \mathbb{Z}$, $\phi(a^{i+j}) = \phi(a^{(i+j) \mod n}) = (i + j) \mod n = (\phi(a^i) + \phi(a^j)) \mod n$. So $\phi$ is an isomorphism proving that $G \cong \mathbb{Z}_n$. □

**Proposition 3.3:** Let $G$ be a cyclic group of order $n$ generated by $a$. Let $b = a^s \in G$ and $H = \langle b \rangle$. Then $H$ is of order $n/d$ where $d = \gcd(n, s)$.

**Proof:** Let $e$ be the identity of $G$. As we have seen in the proof of the previous proposition, the order of $H$ is the smallest positive integer $m$ where $b^m = e$. Then $e = (a^s)^m = a^{sm}$. $a^{sm} = e$ iff $n$ divides $sm$. So $n$ divides $sm$ and $m$ is the smallest positive integer such that $n$ divides $sm$. That is, there exists an integer $k$ such that $nk = sm$. Let $d = \gcd(s, n)$. Then there exists integers $u, v$ such that $d = un + vs$. Then $1 = u(n/d) + v(s/d)$ where $n/d, s/d \in \mathbb{Z}$. So $n/d$ and $s/d$ are relatively prime as their greatest common divisor is 1.

So we want to find the smallest positive integer $m$ such that $\frac{sm}{n}$ is an integer.

This is equivalent to finding the smallest positive integer $m$ such that $\frac{(s/d)m}{(n/d)}$ is an integer.

That is, find the smallest positive integer $m$ such that $n/d$ divides $(s/d)m$.

Since $n/d$ and $s/d$ are relatively prime, $m$ would need to be the smallest positive integer such that $n/d$ divides $m$. Thus $m = n/d$. □

**Corollary 3.4:** Let $G$ be a cyclic group of order $n$ generated by $a$. Let $b = a^s \in G$ where $\gcd(s, n) = 1$. Then $b$ generates $G$.

**Proof:** Simply apply the last theorem to see that the order of $H = \langle b \rangle$ is $n$, so it must contain all $n$ elements of $G$, making $H = G$. Hence $b$ generates $G$. □