3. $(\mathbb{R}^3, +, 0)$ vectors in $\mathbb{R}^3$ with vector addition forms an Abelian group.

   $(x, y, z) + (x', y', z') = (x + x', y + y', z + z')$ vector addition.

   $0 = (0, 0, 0)$ is the identity. $(-x, -y, -z) = -(x, y, z)$ is the inverse of (x, y, z).

4. $(\widetilde{M}_n, *, I_n)$ $n \times n$ invertible matrices with real coefficients under matrix multiplication with I_n as the identity element forms a group, which is NOT Abelian.

5. Set $A = \mathbb{Z}$ and recall the equivalence relation $x \equiv y \bmod 3$ **i.e.** x and y have the same remainder under the division by 3. Recall that $\mathbb{Z}/\sim = \{0, 1, 2\}$, **i.e.** the set of equivalence classes under the partition determined by this equivalence relation. We denote $\mathbb{Z}/\sim = \{0, 1, 2\} = \mathbb{Z}_3$

   Consider $(\mathbb{Z}_3, \oplus_3, 0)$ where $\oplus_3$ is the operation of addition modulo 3, **i.e.** $1 + 0 = 1, 1 + 1 = 2, 1 + 2 = 3 \equiv 0 \bmod 3$.

Claim: $(\mathbb{Z}_3, \oplus_3, 0)$ is an Abelian group.

Proof of Claim: Associativity of $\oplus_3$ follows from the associativity of $+$, addition on $\mathbb{Z}$. Clearly, 0 is the identity (don't forget 0 stands for all elements with remainder 0 under division by 3, **i.e.** $\{0, 3, -3, 6, -6, ...\}$). To compute inverses recall that $a \oplus_3 a^{-1} = 0$, 0 is the inverse of 0 because $0 + 0 = 0$. 2 is the inverse of 1 because $1 + 2 = 3 \equiv 0 \bmod 3$, and 1 is the inverse of 2 because $2 + 1 = 3 \equiv 0 \bmod 3$.
More generally, consider the equivalence relation on $\mathbb{Z}$ given by $x \equiv y \bmod n$ for $n \geq 1$. $\mathbb{Z}/N = \{0, 1, ..., n - 1\} = \mathbb{Z}_n$. All possible remainders under division by n are the equivalence classes. Let $\oplus_n$ be addition mod n. By the same argument as above, $(\mathbb{Z}_n, \oplus_n, 0)$ is an Abelian group.

Q: What if we consider multiplication mod n, **i.e.** $\otimes_n$. Is $(\mathbb{Z}_n, \otimes_n, 1)$ a group?

A: No! $(\mathbb{Z}_n, \otimes_n, 1)$ is not a group because 0 is not invertible: for any $a \in \mathbb{Z}_n$, $0 \otimes_n a = a \otimes_n 0 = 0 \neq 1$.

Q: Can this be fixed?

A: Troubleshoot how to get rid of 0.
Consider $\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{0\} = \{1, 2, ..., n-1\}$ all non-zero elements in $\mathbb{Z}_n^*$. This eliminates 0 as an element, but can 0 arise any other way from the binary operation? It turns out the answer depends on n. If n is not prime, say $n = 6$, we get **zero divisors**, i.e. elements that yield 0 when multiplied. These are precisely the factors of n. For $n = 6$,

$\mathbb{Z}_6^* = \{1, 2, 3, 4, 5\}$ but $2 \otimes_6 3 = 6 \equiv 0 \bmod 6$, so 2 and 3 are zero divisors.

Claim: If n is prime, then $(\mathbb{Z}_n^*, \otimes_n, 1)$ is an Abelian group.
Used in cryptography $\to$ n is taken to be a very large prime number.
As an example, let us look at the multiplication table for $\mathbb{Z}_5^*$ to see the inverse of various elements: $\mathbb{Z}_5^* = \mathbb{Z}_5 \backslash \{0\} = \{0, 1, 2, 3, 4, \} \backslash \{0\} = \{1, 2, 3, 4\}$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1^{-1} = 1 \quad 1 \otimes_5 1 = 1$
$2^{-1} = 3 \quad 2 \otimes_5 3 = 6 \equiv 1 \bmod 5$
$3^{-1} = 2 \quad 3 \otimes_5 2 = 6 \equiv 1 \bmod 5$
$4^{-1} = 1 \quad 4 \otimes_5 4 = 16 \equiv 1 \bmod 5$

The fact that $(\mathbb{Z}_n^*, \otimes_n, 1)$ is Abelian follows from the commutativity of multiplication on $\mathbb{Z}$.

6. Let $(A, *, e)$ be any group, and let $a \in A$.
Consider $A' = \{a^m \mid m \in \mathbb{Z}\}$ all powers of a. It turns out $(A', *, e)$ is a group called the cyclic group determined by a. $(A', *, e)$ is Abelian regardless of whether the original group was Abelian or not because of the theorem we proved on powers of a: $\forall m, n \in \mathbb{Z}\ a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m$.
Cyclic groups come in two flavours: finite (A' is a finite set) and infinite (A' is an infinite set).
For example, let $(A, *, e) = (\mathbb{Q}^*, \times, 1)$
If $a = -1$ $\quad A' = \{(-1)^m \mid m \in \mathbb{Z}\} = \{-1, 1\}$ is finite.
If $a = 2$ $\quad A' = \{2^m \mid m \in \mathbb{Z}\} = \{1, 2, \frac{1}{2}, 4, \frac{1}{4}, ...\}$ is infinite.

7.7 Homomorphisms and Isomorphisms

Task: Understand the most natural functions between objects in abstract algebra such as semigroups, monoids or groups.

Definition: Let $(A, *)$ and $(B, *)$ both be semigroups, monoids or groups. A function $f : A \to B$ is called a homomorphism if

$$f(x * y) = f(x) * f(y)\ \forall x, y \in A.$$

In other words, if f is a function that respects (behaves well with respect to) the binary operation.

Examples:

1. Consider $(\mathbb{Z}, +, 0)$ and $(\mathbb{R}^*, \times, 1)$.
Pick $a \in \mathbb{R}^*$, then $f(n) = a^n$ is a homomorphism between $(\mathbb{Z}, +, 0)$ and $(\mathbb{R}^*, \times, 1)$ because $(\mathbb{R}^*, \times, 1)$ is a group, and we proved for groups that $a^{m+n} = f(m + n) = a^m * a^n = f(m) * f(n)\ \forall m, n \in \mathbb{Z}$.

2. More generally, $\forall a \in A$ invertible, where $(A, *)$ is a monoid with identity element e, $f(m) = a^m$ gives a homomorphism between $(\mathbb{Z}, +, 0)$ and $(A', *, e)$, where as before $A' = \{a^m \mid m \in \mathbb{Z}\} \subset A$.
   We get even better behaviour if we require $f : A \to B$ to be bijective.

Definition: Let $(A, *)$ and $(B, *)$ both be semigroups, monoids or groups. A function $f : A \to B$ is called an isomorphism if $f : A \to B$ is both bijective AND a homomorphism.

Examples:

1. Let $A' = \{2^m \mid m \in \mathbb{Z}\} = \{1, 2, \frac{1}{2}, 4, \frac{1}{4}, ...\}$
   $f(m) = 2^m$ from $(\mathbb{Z}, +, 0)$ to $(A', \times, 1)$ is an isomorphism since $2^m \neq 2^n$ if $m \neq n$.
2. Let $A' = \{(-1)^m \mid m \in \mathbb{Z}\} = \{-1, 1\}$
   $f(m) = (-1)^m$ from $(\mathbb{Z}, +, 0)$ to $(A', \times, 1)$ is NOT an isomorphism since it's not injective $(-1)^2 = (-1)^4 = 1$.

Theorem: Let $(A, *)$ and $(B, *)$ both be semigroups, monoids or groups. The inverse $f^{-1} : B \to A$ of any isomorphism $f : A \to B$ from A to B is itself an isomorphism.

Proof: If $f : A \to B$ is an isomorphism $\Rightarrow f : A \to B$ is bijective $\Rightarrow f^{-1} : B \to A$ is bijective (proven when we discussed functions).

To show $f^{-1} : B \to A$ is a homomorphism, let $u, v \in B$. $\exists x, y \in A$ s.t. $x = f^{-1}(u)$ and $y = f^{-1}(v)$, but then $u = f(x)$ and $v = f(y)$.

Since $f : A \to B$ is a homomorphism, $f(x * y) = f(x) * f(y) = u * v$. Then $f^{-1}(u * v) = f^{-1}(f(x * y)) = x * y = f^{-1}(u) * f^{-1}(v)$ as needed.

qed

Definition: Let $(A, *)$ and $(B, *)$ both be semigroups, monoids or groups. If $\exists f : A \to B$ an isomorphism betwen A and B, then $(A, *)$ and $(B, *)$ are said to be isomorphic.

Remark: "Isomorphic" comes from "iso" same and "morph$\overline{e}$ " form: the same abstract algebra structure on both $(A, *)$ and $(B, *)$ given to you in two different guises. As the French would say: "Même Marie, autre chapeau" same Mary, different hat.

8 Formal Languages

Task: Use what we learned about structues in abstract algebra in order to make sense of formal languages and grammars.
Let A be a finite set. When studying formal languages, we call A an alphabet and the elements of A letters.

Examples:

1. $A = \{0, 1\}$ binary digits
2. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ decimal digits
3. $A =$ letters of the English alphabet

Definition: $\forall n \in \mathbb{N}^*$, we define a <u>word</u> of length n in the alphabet A as being any string of the form $a_1, a_2, ..., a_n$ $s.t.$ $a_i \in A \quad \forall i, 1 \leq i \leq n$. Let A^n be the set of all words of length n over the alphabet A.