MA1057: INTRODUCTION TO ABSTRACT ALGEBRA
MONOIDS AND GROUPS

LECTURER: ARUNDHATHI KRISHNAN

Notation

$\mathbb{N}$: the set of natural numbers $\{1, 2, \ldots\}$
$\mathbb{Z}$: the set of integers $\{\ldots, -1, 0, 1, \ldots\}$
$\mathbb{Q}$: the set of rational numbers
$\mathbb{R}$: the set of real numbers
$\mathbb{C}$: the set of complex numbers
$\mathbb{Q}^+$: the set of strictly positive rational numbers
$\mathbb{Q}*$: the set of non-zero rational numbers, $\mathbb{Q} \setminus \{0\}$
$\mathbb{R}^*$: the set of non-zero real numbers, $\mathbb{R} \setminus \{0\}$
$\mathbb{C}^*$: the set of non-zero complex numbers, $\mathbb{C} \setminus \{0\}$
$M_{m\times n}(\mathbb{C})$: the set of $m \times n$ matrices with complex entries
$M_n(\mathbb{C})$: the set of $n \times n$ matrices with complex entries

2. Monoids and Groups

2.1. **Binary operations.**

Definition 2.1.1. Let A be a set. A binary operation on A is a function that assigns to each ordered pair of elements of A a unique element of A.

The convention used is to denote the unique element resulting from an ordered pair (a, b) as ab. In some cases, we write $a + b$ if the binary operation is an addition.

Example 2.1.2.

(i) Addition, multiplication and subtraction on $\mathbb{Z}$ are all binary operations. What about division?
(ii) Multiplication on $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a binary operation.
(iii) Division on $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ is a binary operation.
(iv) Addition on the set of even integers is a binary operation. What about addition on the set of odd integers?
(v) Subtraction on $\mathbb{N}$ is not a binary operation.
(vi) Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. For any $x \in \mathbb{Z}$, by $x \bmod n$ we mean the unique remainder in the set $\{0, \ldots, n-1\}$ obtained on dividing x by n. Then addition and multiplication on $\mathbb{Z}_n$ are defined as follows for $a, b \in \mathbb{Z}_n$:

$$a + b := (a + b) \bmod n$$
$$ab := (ab) \bmod n.$$

Addition and multiplication on $\mathbb{Z}_n$ are binary operations.
(vii) Let S_n be the set of permutations on $\{1, \ldots, n\}$. Then the composition of permutations is a binary operation on S_n.

2.2. **Monoids.**

Definition 2.2.1. A monoid is a pair $(M, *)$, where M is a set and $*$ is a binary operation on M such that the following conditions are satisfied:

(i) Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$.
(ii) Existence of identity: There is an element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

Example 2.2.2. The following are some examples and non-examples of monoids.

(i) $(\mathbb{N} \cup \{0\}, +)$ is a monoid with the binary operation of addition and identity element 0.
(ii) $(\mathbb{N}, \cdot)$ is a monoid with the binary operation of multiplication and identity element 1.
(iii) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ are all monoids with the binary operation of multiplication and identity element 1.
(iv) $(\mathbb{Z}, -)$ is *not* a monoid because associativity does not hold. For example, $1-(2-5) = 1-(-3) = 4$, whereas $(1-2)-5 = -1-5 = -6$.
(v) Let exp be the binary operation on $\mathbb{N}$ given by $exp(a, b) = a^b$. Then $(\mathbb{N}, \exp)$ is *not* a monoid. Associativity fails as for example, $(2^3)^2 = 8^2 = 64$, whereas $2^{(3^2)} = 2^9 = 512$.
(vi) $(M_{m\times n}(\mathbb{C}), +)$ is a monoid where $+$ denotes matrix addition.
(vii) $(M_n(\mathbb{C}), \cdot)$ is a monoid where $\cdot$ denotes matrix multiplication.
(viii) For every non-empty set X, the set of functions on X given by $\{f : X \to X\}$ is a monoid with respect to the composition of functions.
(ix) The set of continuous functions on $\mathbb{R}$ given by $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\}$ is a monoid with respect to the composition of functions.
(x) If $(A, *)$ and $(B, \star)$ are monoids, then $(A \times B, \cdot)$ is a monoid with the following piece-wise operation:

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 * a_2, b_1 \star b_2).$$

(xi) $(\mathbb{R}_n)$ is a monoid with addition given by

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n).$$

2.3. **Groups.** In this section, we give the definition of a group, some examples of groups, and finally consider some basic properties of groups.

Definition 2.3.1. A set G together with a binary operation on G is called a group if the following hold:

(i) Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$.
(ii) Existence of identity: There is an element $e \in G$ such that $ae = ea = a$ for all $a \in G$.
(iii) Existence of inverse: For each $a \in G$, there is an element $b \in G$ such that $ab = ba = e$.

In other words, a group is a monoid with the additional condition that every element has an inverse element.

Note that the existence of an identity element implies that a group must be non-empty. In addition, if $ab = ba$ for all $a, b \in G$, then G is called *abelian* or *commutative*.

Example 2.3.2.

(i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are all abelian groups under usual addition.
(ii) $(\mathbb{Q}^+, \cdot)$ and $(\{1, -1, i, -i\}, \cdot) \subset \mathbb{C}$ are abelian groups under usual multiplication.

(iii) S_n with function composition is a group known as the symmetric group of degree n. For $n \geq 3$, S_n is non-abelian.

(iv) $M_n(\mathbb{C})$, the set of $n \times n$ matrices with complex entries, equipped with the operation of matrix addition is an abelian group.

(v) $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition mod n is an abelian group.

(vi) $GL(n, \mathbb{R})$, the set of $n \times n$ matrices with non-zero determinant, is a non-abelian (for $n > 1$) group under matrix multiplication. It is called the general linear group of degree n.

(vii) $SL(n, \mathbb{R})$, the set of $n \times n$ matrices with determinant 1, is a non-abelian (for $n > 1$) group under matrix multiplication. It is called the special linear group of degree n. Note that $SL(n, \mathbb{R}) \subset GL(n, \mathbb{R})$.

Example 2.3.3 (Quaternion Group)**.** The *quaternion group* Q is given by the set $\{1, -1, i, -i, j, -j, k, -k\}$ with multiplication table given as follows:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Remark 2.3.4. It is convenient sometimes to explicitly describe a group by its multiplication table or its Cayley table, like in the above example of the quaternion group. The rows and columns correspond to the elements of the group, and the entry on row a and column b is the element ab.

- Write the Cayley group for S_3 and for $\mathbb{Z}_4$.
- Why does each element of the group appear in each row and each column of the Cayley table?
- Why does each element appear in a row *exactly once*, and in a column *exactly once*?

2.4. Elementary Properties of Groups.

Proposition 2.4.1 (Uniqueness of identity)**.** *There exists a unique element $e \in G$ such that $ae = ea = a$ for every $a \in G$.*

Proof. The existence of an element e is guaranteed by the definition of a group. Suppose e and f are both identity elements. Then $e = ef = f$. □

Proposition 2.4.2 (Uniqueness of inverse element)**.** *For each $a \in G$, there exists a unique element $b \in G$ such that $ab = ba = e$.*

Proof. Suppose there exist $b, c \in G$ such that $ab = ba = e$ and $ac = ca = e$. Then $c = ce = c(ab) = (ca)b = eb = b$.

□

We write this unique inverse of an element $a \in G$ as a^{-1}.

Proposition 2.4.3 (Cancellative property)**.** *Let $a, b, c \in G$. Then $ba = ca \implies b = c$ and $ab = ac \implies b = c$.*

Proof. Suppose $ba = ca$. Then multiplying both sides on the right by the inverse of a gives $b = c$, so we have right cancellativity. Left cancellativity follows similarly. □

The associative property means that we can unambiguously write the product

$$\underbrace{a \cdot \cdots \cdot a}_{n \text{ times}}$$

as a^n for $n \in \mathbb{N}$. For $n < 0$, we take a^n to be the $(-n)$-fold product of a^{-1} and $a^0 := e$.

Proposition 2.4.4. *Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. The proof follows in a straightforward way by verifying that $(ab)b^{-1}a^{-1} = e = b^{-1}a^{-1}ab$. □

2.5. **Subgroups.**

Definition 2.5.1. A subset H of a group G which is itself a group under the operation of G is called a subgroup of G. This is denoted by $H \leq G$.

Suppose $H \leq G$ and $H \neq G$, then H is called a *proper* subgroup of G. G is, of course, a subgroup of itself. The subgroup $\{e\}$ is called the *trivial* subgroup of G; any subgroup H of G which is not the trivial subgroup is called a non-trivial subgroup of G.

The following theorem shows that we do not need to check all the group axioms to determine whether a subset of a group is a subgroup or not.

Proposition 2.5.2. *Let G be a group and H be a non-empty subset of G. If $ab^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of G.*

Proof. For H to be a subgroup, we need the following:

(i) The associativity of the operation is inherited from G.

(ii) As $H \neq \emptyset$, there exists some $a \in H$, so $e = aa^{-1} \in H$.

(iii) Let $a \in H$. Then $a^{-1} = ea^{-1} \in H$ by the hypothesis.

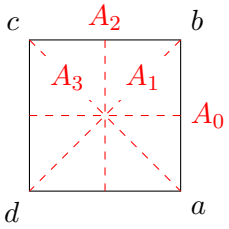
(iv) We need to show that the operation of G defines a binary operation on H, that is, H is closed under the operation. Let $x, y \in H$. Then $xy = x(y^{-1})^{-1} \in H$ by the hypothesis.

Hence H is a group in its own right, and thus a subgroup of G.

□

Example 2.5.3.

(i) The additive subgroup of even integers $(2\mathbb{Z}, +) \subset (\mathbb{Z}, +)$.
(ii) For any $d \in \mathbb{N}$, the subgroup $(d\mathbb{Z}, +) \subset (\mathbb{Z}, +)$. We will show in Proposition 2.7.1 that every subgroup of $(\mathbb{Z}, +)$ is of this form.
(iii) For $n \in \mathbb{N}$, the n-th roots of unity $(U_n, \cdot)$ form a multiplicative subgroup of $(\mathbb{C}^*, \cdot)$.
(iv) The subgroup of even permutations $(A_n, \circ) \subset (S_n, \circ)$ for $n \geq 2$.
(v) The subgroup D_4 of rotational and reflection symmetries of the square called the dihedral group (of order 8) is a subgroup of S_4.



We have $D_4 = \{r_0, r_1, r_2, r_3, s_0, s_1, s_2, s_3\}$ where r_i denotes the (counter-clockwise) rotation by $\frac{2\pi i}{4}$ and s_i denoted the reflection about the axis passing through $\frac{\pi i}{4}$. The corresponding axes are marked on the figure as A_i. The products are given by:

$$r_i r_j = r_{(i+j \mod n)}, r_i s_j = s_{(i+j \mod n)}, s_i r_j = s_{(i-j \mod n)}, s_i s_j = r_{(i-j \mod n)}.$$

In order to view D_4 as a subgroup of S_4, we can write the elements of D_4 in array form:

$$r_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = (1) = \varepsilon$$

$$r_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1\,2\,3\,4)$$

$$r_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = (1\,3)(2\,4)$$

$$r_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = (1\,4\,3\,2)$$

$$s_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (1\,2)(3\,4)$$

$$s_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = (1\,3)$$

$$s_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = (1\,4)(2\,3)$$

$$s_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} = (2\,4)$$

Exercise 2.5.4. Let G be an abelian group.

(i) $\{x \in G \mid x^2 = e\}$ is a subgroup.

(ii) $\{x^2 \mid x \in G\}$ is a subgroup.

(iii) Let H and K be two subgroups of G. Then $HK := \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

Example 2.5.5. Let $G = \mathbb{R}^*$ with multiplication and H be the set of irrational numbers. Then H is not a subgroup. (Show that there exist $a, b \in H$ such that $ab \notin H$.)

2.6. **Cyclic Groups.**

Proposition 2.6.1. *Let G be any group and $a \in G$. Let $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$. Then $\langle a \rangle$ is a subgroup of G.*

Proof. Let $a^m, a^n \in \langle a \rangle$. By Theorem 2.5.2, it suffices to show that $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$, which follows from the definition of $\langle a \rangle$. Hence $\langle a \rangle$ is a subgroup of G. □

Definition 2.6.2. $\langle a \rangle$ is called the *cyclic* subgroup of G generated by a. If $G = \langle a \rangle$, then G is called a cyclic group, and a is a called a *generator* of G.

Exercise 2.6.3. Prove that a cyclic group is abelian.

Example 2.6.4.

(i) Let $G = \mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$ with addition mod 12. Then $\langle 3 \rangle = \{3, 6, 9, 0\}$. Compute the cyclic groups generated by the other elements of G. Recall here that the operation is addition, so the symbol a^n here means taking the sum of n terms $a + a + \ldots + a$ and then going modulo 12. For example,

$$\langle 5 \rangle = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} = \mathbb{Z}_{12}.$$

(ii) The additive group $(\mathbb{Z}, +)$ is cyclic with generator 1 (or -1).

Definition 2.6.5. Let G be a group. A subset $A \subset G$ is called a set of generators of G if every element $g \in G$ can be written in terms of the elements of A and their inverses together with the binary operation.

Example 2.6.6. We saw in Exercise Sheet 2 that the permutation group $(S_n, \circ)$ is generated by several sets.

(i) $S_n = \langle \{\text{cycles}\} \rangle$.
(ii) $S_n = \langle \{\text{transpositions}\} \rangle$.
(iii) $S_n = \langle \{(1\,2), \ldots, (1\,n)\} \rangle$.
(iv) $S_n = \langle \{(1\,2), (2\,3) \ldots, (n-1\,n)\} \rangle$.
(v) $S_n = \langle \{(1\,2), (1\,2\,\ldots\,n)\} \rangle$.

2.7. Subgroups of $\mathbb{Z}$.

Proposition 2.7.1. *Let H be a subgroup of $(\mathbb{Z}, +)$. Then $H = \langle d \rangle = d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$, where d is the smallest strictly positive element of H.*

Proof. As $d \in H$, clearly $\langle d \rangle \subseteq H$. Note that

$$\langle d \rangle = \{kd \mid k \in \mathbb{Z}\},$$

where for k positive,

$$kd == \underbrace{d + \ldots + d}_{k \text{ times}},$$

for k negative,

$$kd == \underbrace{(-d) + \ldots + (-d)}_{-k \text{ times}},$$

and $0 \cdot d = 0$.

Let $n \in H$. Then by the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < d$ such that $n = dq + r$. As $n, dq \in H$ and H is a subgroup, $r = n - dq \in H$. However, as $0 \leq r < d$ and d is the smallest strictly positive element of H, we must have $r = 0$. So every element n in H is a multiple of d, that is, $H = \langle d \rangle$. □

Corollary 2.7.2. *Let $a, b \in \mathbb{Z}$ and let d be the smallest positive element of the subgroup generated by $\{a, b\}$ given by*

$$\langle a, b \rangle = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Then $d = \gcd(a, b)$.

Proof. By Theorem 2.7.1, $\langle a, b\rangle = d\mathbb{Z}$, so d is a common divisor of a and b. On the other hand, suppose f is any common divisor of a and b. Then $a = fp$ and $b = fq$ for some $p, q \in \mathbb{Z}$. As $d = ax + by$ for some $x, y \in \mathbb{Z}$, we get

$$d = fpx + fqy = f(px + qy),$$

so $f|d$ and hence $f \leq d$. Hence $d = \gcd(a, b)$. □

Remark 2.7.3. The above corollary shows that if $d = \gcd(a, b)$, then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. We can find $x, y \in \mathbb{Z}$ by using the following lemma and Euclid's algorithm.

Lemma 2.7.4. *Let $a, b, n \in \mathbb{Z}$ and $c = a - nb$. Then*

$$\gcd(a, b) = \gcd(b, c).$$

Proof. We have $c = a - nb$ (equivalently, $a = c + nb$). Hence $c \in \langle a, b\rangle$ and $a \in \langle b, c\rangle$. This means that $b, c \in \langle a, b\rangle$ and $a, b \in \langle b, c\rangle$, so that $\langle a, b\rangle = \langle b, c\rangle$. By Corollary 2.7.2, $\gcd(a, b) = \gcd(b, c)$.

□

Example 2.7.5. We will find the generator of the subgroup $\langle 100, 15\rangle$ of $(\mathbb{Z}, +)$. We know that

$$\begin{aligned} 100 &= 6 \times 15 + 10 \text{ so } \gcd(100, 15) = \gcd(15, 10) \\ 15 &= 1 \times 10 + 5 \text{ so } \gcd(15, 10) = \gcd(10, 5) \\ 10 &= 2 \times 5 + 0 \text{ so } \gcd(10, 5) = \gcd(5, 0) = 5. \end{aligned}$$

Hence $\gcd(100, 15) = 5$. Tracing backwards also gives us

$$\begin{aligned} 5 &= 15 - 1 \times 10 \\ &= 15 - 1 \times (100 - 6 \times 15) \\ &= 7 \times 15 + (-1) \times 100. \end{aligned}$$

The algorithm followed in the example above to find the greatest common divisor uses Lemma 2.7.4 and is known as **Euclid's Algorithm** for finding $gcd(a, b)$. The algorithm terminates when the remainder is 0, and the last non-zero remainder is the required gcd.

Exercise 2.7.6. Find the generator of $\langle 24, 9\rangle$ by finding the greatest common divisor $\gcd(24, 9)$. Also find $x, y \in \mathbb{Z}$ such that

$$\gcd(24, 9) = 24x + 9y.$$

2.8. **Modular Arithmetic.** We earlier defined the additive group $(\mathbb{Z}_n, +)$ as the set $\mathbb{Z}_n = \{0, \ldots, n-1\}$ and the binary operation given by addition modulo n, for $n \geq 2$. We will rewrite $\mathbb{Z}_n$ slightly as being a group consisting of n equivalence classes as follows:

$$\mathbb{Z}_n := \{[0], \ldots, [n-1]\},$$

where

$$[0] = n\mathbb{Z} = \{\cdots, -2n, -n, 0, n, 2n, \cdots\}$$

and for $k = 1, \ldots, n$ each equivalence class $[k]$ is given by

$$[k] = n\mathbb{Z} + k = \{nz + k \mid z \in \mathbb{Z}\}.$$

For example in $\mathbb{Z}_3 = \{[0], [1], [2]\}$:

$$[0] = 3\mathbb{Z} = \{\cdots, -6, -3, -0, 3, 6, \cdots\}$$
$$[1] = 3\mathbb{Z} + 1 = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$$
$$[2] = 3\mathbb{Z} + 2 = \{\cdots, -4, -1, 2, 5, 8, \cdots\}.$$

Note that $\mathbb{Z} = [0] \cup [1] \cup [2]$.

In general,

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1], n \geq 2.$$

Why do we call the elements of $\mathbb{Z}_n$ equivalence classes? Consider the relation given by congruence modulo n:

$$a \equiv b \bmod n \text{ if } n|(a-b).$$

Exercise 2.8.1. Show that

(i) $a \equiv a \bmod n$ (reflexivity).
(ii) $a \equiv b \bmod n$ implies that $b \equiv a \bmod n$ (symmetry).
(iii) $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply that $a \equiv c \bmod n$ (transitivity).

Hence congruence modulo n is an equivalence relation on $\mathbb{Z}$ with equivalence classes given by $[k] = n\mathbb{Z} + k$. An element x belong to the equivalence class $[k]$ if and only if $n|x-k$, that is if and only if $x = nz + k$ for some $z \in \mathbb{Z}$.

Proposition 2.8.2. *Addition and multiplication are compatible with congruence modulo n. That is, if $x \in [a]$ and $y \in [b]$, then*

(i) $x + y \in [a + b]$.
(ii) $xy \in [ab]$.

Proof.

(i) $x \in [a]$ means that $n|x-a$ and $y \in [b]$ means that $n|y-b$. Hence $n|(x-a)+(y-b)$, that is $n|(x+y)-(a+b)$, so that $x + y \in [a + b]$.
(ii) $x \in [a]$ means that $x = nz_1 + a$ and $y \in [b]$ means that $y = nz_2 + b$ for $z_1, z_2 \in \mathbb{Z}$. Hence $xy = n^2 z_1 z_2 + naz_2 + nbz_1 + ab$, so

$$xy = n(nz_1 z_2 + az_2 + bz_1) + ab.$$

Hence $xy \in [ab]$.

□

We often drop the square brackets and simply write elements of $\mathbb{Z}_n$ (as we did right at the beginning of these notes) as $0, 1, \ldots, n-1$ with addition given by $a + b \bmod n$. Recall that $x \bmod n$ denotes the unique remainder obtained in $\{0, \ldots, n-1\}$ on dividing x by n.

Proposition 2.8.3. $(\mathbb{Z}_n, +)$ *is a group.*

Proof. Clearly addition is a binary operation as $a + b \bmod n \in \mathbb{Z}_n$. The identity element is 0, the inverse of 0 is 0 and for $k \neq 0$, the inverse of k is $n - k$. Prove associativity! □

Exercise 2.8.4. Write the Cayley tables for $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ and $\mathbb{Z}_5$.

In general, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is a monoid but not a group. The product is a binary operation; associativity holds; and 1 is the multiplicative inverse. However, some elements may not have

multiplicative inverses. For example, in $\mathbb{Z}_4 \setminus \{0\}$:

$$2 \times 1 = 2$$
$$2 \times 2 = 0$$
$$2 \times 3 = 2.$$

So 2 has no multiplicative inverse in $\mathbb{Z}_4 \setminus \{0\}$. However, you will find that in $\mathbb{Z}_5$, every non-zero element has a multiplicative inverse.

Definition 2.8.5. Let $n \in \mathbb{N}$ be a composite number with $n = ab$, $a \neq 1, b \neq 1$. Then in $(\mathbb{Z}_n, \cdot)$ we have $[a][b] = [0]$, even though neither $[a]$ nor $[b]$ is $[0]$. We say that $[a]$ and $[b]$ are zero divisors of $\mathbb{Z}_n$.

We will end with a proposition that tells us precisely for what values of n the monoid $(\mathbb{Z}_N \setminus \{0\}, \cdot)$ is a group.

Proposition 2.8.6. *The monoid $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is a group if and only if n is a prime.*

Proof. n is a prime if and only if the only factors of n are 1 and n. This is true

$$\iff \gcd(a, n) = 1 \ \forall a \not\equiv 0 \bmod n$$
$$\iff ax + ny = 1 \text{ for some } x, y \in \mathbb{Z}$$
$$\iff ax \equiv 1 \bmod n$$
$$\iff [ax] = 1 \text{ (that is, x is the multiplicative inverse of a in } \mathbb{Z}_n).$$

□

References

[1] Course notes of Anca Mustata, Lecturer, University College Cork.
[2] Chapters 2, 3 and 4. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.