# 1 Algebra

## Functions and Symmetries

**Definition 0.1.1 Functions**

A function $f : X \to Y$ is called

- **injective** if $f(x_1) = f(x_2) \implies x_1 = x_2$
- **surjective** if for every $y \in Y$, $\exists x \in X$ s.t. $f(x) = y$
- **bijective** if it is both injective and surjective

**Definition 1.1.3 Graph Isomorphisms**

An **isomorphism** between two graphs is a *bijection* between them that preserves all edges. More precisely, if $\Gamma_1$ and $\Gamma_2$ are graphs, with sets of vertices $V_1$ and $V_2$ respectively, then an isomorphism from $\Gamma_1$ and $\Gamma_2$ is a bijection

$$f : V_1 \to V_2$$

such that $f(v_1)$ and $f(v_2)$ are joined by an edge if and only if $v_1$ and $v_2$ are also joined by an edge. We say that $\Gamma_1$ and $\Gamma_2$ are *isomorphic* if there exists an isomorphism $f : \Gamma_1 \to \Gamma_2$

**Definition 1.1.9 Symmetry**

A **symmetry** of a graph is an *isomorphism* from the graph to itself, i.e. if the set of vertices is V, then the symmetry is a bijection $f : V \to V$ that preserves edges. That is, a symmetry is a bijection $f : V \to V$ such that $f(v_1)$ and $f(v_2)$ are joined by an edge if and only if $v_1$ and $v_2$ are joined by an edge.

## Groups

**Definition 1.2.3 Groups**

For an operation $*$, We say a non-empty set G is a **group** under $*$ if the following four axioms hold:

- **G1 - Closure:** $*$ is a binary operation on G, that is $a*b \in G$ for all $a, b \in G$.
- **G2 - Associativity:** $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$
- **G3 - Identity:** There exists an *identity* element of $G$ such that $e * g = g * e = e$ for all $g \in G$.
- **G4 - Inverse:** Every element $g \in G$ has an *inverse* $g^{-1}$ such that $g * g^{-1} = g^{-1} * g = e$

**Definition 1.2.6 Abelian Group**

The definition of a group doesn't require that $a * b = b * a$. We say that a group is **abelian** or **commutative** if $a * b = b * a$ for every $a, b \in G$. We say that $a$ *commutes* with $b$, or that $a$ and $b$ *commute*

## Subgroups

**Definition 2.1.1 Subgroups**

Let $G$ be a group. We say that a non-empty subset $H$ of $G$ is a **subgroup** of $G$ if $H$ itself is a group (under the operation from $G$). We write $H \leq G$ if $H$ is a subgroup of $G$. If $H \neq G$, we write $H < G$ and say $H$ is a proper subgroup

**Theorem 2.1.3: Subgroup Test**

$H \subseteq G$ is a subgroup of $G$ if and only if:

- **S1:** $H$ is not empty
- **S2:** If $h, k \in H$ then $h * k \in H$
- **S3:** If $h \in H$ then $h^{-1} \in H$

Alternative test for subgroups:

- $\widetilde{S1}$: $H$ is not empty.
- $\widetilde{S2}$: If $h, k \in H$ then $h * k^{-1} \in H$

**Definition 2.2.4 Order of an Element**

Let $G$ be a group and $g \in G$. Then the **order** $o(g)$ of $g$ is the *least* natural number $n$ such that

$$g^n = e$$

If no such $n$ exists, we say that $g$ has infinite order

**Definition 2.2.3 Order of a Group**

The **order** of a finite group, written $|G|$, is the number of elements in $G$. If $G$ is infinite we say that $|G| = \infty$, or the order of $G$ is infinite.

**Theorem 2.2.6: Order of a Finite Group**

In a finite group, every element has finite order.
If $g$ is an element of a finite group $G$, then there exists $k \in \mathbb{N}$ such that $g^k = g^{-1}$

**Definition 2.2.8 Generating Subset**

Let $G$ be a group and let $g \in G$ be an element. We define the subset

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$$

Note that if $G$ is finite, then by 2.2.6 $\langle g \rangle$ is finite, and we can think of $\langle g \rangle$ as

$$\langle g \rangle = \{e, g, \dots, g^{o(g)-1}\}$$

**Definition 2.2.10 Cyclic Subgroup**

A subgroup $H \leq G$ is **cyclic** if $H = \langle h \rangle$ for some $h \in H$. In this case, we say that $H$ is the *cyclic subgroup generated by* $h$. If $G = \langle g \rangle$ for some $g \in G$, then we say that the group $G$ is *cyclic*, and that $g$ is a *generator*.

**Remark 2.2.12 - 16: Consequences of Cyclic groups**

- **2.2.12** If $g \in G$, then $o(g) = |\langle g \rangle|$
- **2.2.13:** If $G$ is cyclic, then $G$ is abelian.
- **2.2.14:** Let $G$ be a finite group. Then

  $$G \text{ is cyclic} \iff G \text{ has an element of order} |G|$$

- **2.2.15:** Let $G$ be a cyclic group and let $H$ be a subgroup of $G$. Then $H$ is cyclic.
- **2.2.16:** Let $m, n \in \mathbb{N}$, let $G = \langle g \rangle$ be a cyclic group of order $m$ and $H = \langle h \rangle$ be a cyclic group of order $n$. Then

  $$G \times H \text{ cyclic} \iff m \text{ and } n \text{ are coprime } (\gcd(\text{m,n}) = 1)$$

## Cosets and Lagrange

**Definition 2.3.2 Relation**

Let $X$ be a set, and $R$ a subset of $X \times X$; thus $R$ consists of some ordered pairs $(s, t)$ with $s, t \in X$. If $(s, t) \in R$ we write $s \sim t$ and say "$s$ is related to $t$". We call $\sim$ a **relation** on $X$.

**Definition 2.3.2 Equivalence Relation**

- **Reflexive:** $x \sim x$ for all $x \in X$
- **Symmetric:** $x \sim y$ implies that $y \sim x$ for all $x, y \in X$
- **Transitive:** $x \sim y$ and $y \sim z$ implies that $x \sim z$ for all $x, y, z \in X$

A relation $\sim$ is called an **equivalence relation** on X if it satisfies the following three axioms:

**Definition 2.3.4 Coset**

Let $H \leq G$ and let $g \in G$. Then a *left coset* of $H$ in $G$ is a subset of $G$ of the form $gH$, for some $g \in G$. We denote the set of left cosets of $H$ in $G$ by $G/H$

**Theorem 2.4.2: Lagrange's Theorem**

Suppose that $G$ is a finite group.

- If $H \leq G$, then $|H|$ divides $|G|$
- Let $g \in G$. Then $o(g)$ divides $|G|$
- For all $g \in G$, we have that $g^{|G|} = e$

**Theorem 2.3.8: Coset Rules**

Let $H \leq G$

- For all $h \in H$, $hH = H$. In particular $eH = H$
- For $g_1, g_2 \in G$, the following are equivalent
  - $g_1 H = g_2 H$
  - there exists $h \in H$ such that $g_2 = g_1 H$
  - $g_2 \in g_1 H$
- For $g_1$, $g_2 \in G$, define $g_1 \sim g_2$ if and only if $g_1 H = g_2 H$. Then $\sim$ defines an equivalence relation on $G$.

**Theorem 2.4.4: Index of a Subgroup**

The **index** of $H \leq G$ is defined as the number of *distinct* left cosets of $H$ in $G$, which by Lagrange's is $|G/H| = \frac{|G|}{|H|}$

**Remark 2.4.6 - 8: Consequences of Lagrange**

- **2.4.6:** Suppose that $G$ is a group with $|G| = p$, where $p$ is prime. Then $G$ is a cyclic group
- **2.4.7:** Suppose that $G$ is a group with $|G| < 6$. Then $G$ is abelian
- **2.4.8:** If $p$ is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$

## Homomorphisms and Isomorphisms

**Definition 3.1.1 Group Homomorphism**

Let $(G, *), (H, \circ)$ be groups. A map $\phi : G \to H$ is called a **homomorphism** if

$$\phi(x * y) = \phi(x) \circ \phi(y) \quad \text{for all } x, y \in G$$

Note that the product on the left is formed using $*$, while the product on the right is formed using $\circ$

**Definition 3.1.2 Group Isomorphism**

A group homomorphism $\phi : G \to H$ that is also a bijection is called an **isomorphism** of groups. In this case we say that $G$ and $H$ are *isomorphic* and we write $G \cong H$. An isomorphism $G \to G$ is called an **automorphism** of $G$.

**Theorem 3.1.L: Cyclic Isomorphisms**

All finite cyclic groups of the same order are *isomorphic* to each other. Therefore, cyclic groups of order $n$ are isomorphic to $(\mathbb{Z}_n, +)$
All infinite cyclic groups are *isomorphic* to each other. Therefore, each cyclic group of infinite order is isomorphic to $(\mathbb{Z}, +)$

**Remark 3.1.5: Consequences of Homomorphisms**

Let $\phi : G \to H$ be a group homomorphism. Then

- $\phi(e_G) = e_H$
- $\phi(g^k) = (\phi(g))^k$ and $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$
- If $\phi$ is injective, the order of $g \in G$ equals the order of $\phi(g) \in H$.

**Definition 3.1.7 Normal Subgroup**

A subgroup $N \leq G$ is **normal** if the left and right cosets of $N$ are equal, i.e. $gN = Ng$ for all $g \in G$. If $N$ is a normal subgroup of $G$, we write $N \triangleleft G$. Kernels of homomorphisms are always normal subgroups

**Definition 3.1.6 Image and Kernel of a Group**

Let $\phi : G \to H$ be a group homomorphism.

- The **image** of $\phi$ is defined to be
$$\operatorname{im}\phi := \{h \in H \,|\, h = \phi(g) \text{ for some } g \in G\}$$
- The **kernel** of $\phi$ is defined to be
$$\ker\phi := \{g \in G \,|\, \phi(g) = e_H\}$$

Note: $\operatorname{im}\phi$ is a subgroup of $H$ and $\ker\phi$ is a subgroup of $G$

**Theorem 3.2.1: Product Isomorphisms**

Let $H, K \leq G$ be subgroups with $H \cup K = \{e\}$.

- The map $\phi : H \times K \to HK$ given by $\phi : (h, k) \to hk$ is bijective
- If every element of $H$ commutes with every element of $K$ when multiplied in $G$ (i.e. $hk = kh \quad \forall h \in H, k \in K$), then $HK$ is a subgroup of $G$, and it is isomorphic to $H \times K$ via $\phi$

**Theorem 3.2.3: Size of Product Group**

Let $H, K \leq G$ be finite subgroups of a group $G$ such that $H \cup K = \{e\}$ Then $|HK| = |H| \times |K|$.

## Group Actions

**Definition 4.1.1 Group Action**

Let $(G, *)$ be a group, and let $X$ be a nonempty set. Then a (left) **action** of $G$ on $X$ is a map

$$G \times X \to X$$

written $(g, x) \mapsto g \cdot x$, such that

$$g_1 \cdot (g_2 \cdot x) = (g * h) \cdot x \qquad \text{and} \qquad e \cdot x = x$$

for all $g_1, g_2 \in G$ and all $x \in X$.

**Definition 4.1.4 Kernel of an Action, Faithful Action**

Suppsoe that $G$ acts on $X$. Then the set

$$N := \{g \in G \mid g \cdot x = x forall x \in X\}$$

is a subgroup of $G$, and is called the **kernel** of the action. If $N = \{e\}$, then we say the action is **faithful**

**Definition 4.2.1 Orbit, Stabilizer, and Fix**

For every $x$ in $X$, the **orbit** of $x$ is defined by

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}$$

This is a subset of $X$
For every $x$ in $X$, the **stabilizer** of $x$ is defined by

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

This is a subgroup of $G$
For every $g$ in $G$, the **fix** of $g$ is defined by

$$\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$$

**Theorem 4.2.5: Orbit Equivalence**

Let $G$ act on $X$. Then

$$x \sim y \iff y = g \cdot x \text{ for some } g \in G$$

defines an equivalence relation on $X$. The equivalence classes are the orbits of $G$. Thus when $G$ acts on $X$, we obtain a partition of $X$ into orbits

**Theorem 4.3.1: Orbit-Stabilizer Theorem**

Suppose $G$ is a finite group acting on a set$X$, and let $x \in X$. Then $|\mathrm{Orb}_G(x)| \times |\mathrm{Stab}_G(x)| = |G|$, or in words:

$$\text{size of orbit } \times \text{ size of stabilizer } = \text{order of group}$$

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.