# Math 3230 - Abstract Algebra I
# Summary of terms and theorems

## 1 Binary operations

### Definitions and Theorems

1. *Associativity* of a binary operation $\circ$ on a set $A$ means $(a \circ b) \circ c = a \circ (b \circ c)$ for **all** $a, b, c \in A$.

2. *Commutativity* of a binary operation $\circ$ on a set $A$ means $a \circ b = b \circ a$ for **all** $a, b \in A$.

3. An *identity* element for a binary operation $\circ$ on a set $A$ is an $e \in A$ such that $e \circ a = a$ and $a \circ e = a$ for **all** $a \in A$.

4. If the binary operation $\circ$ on $A$ has identity $e$, an *inverse* of $a \in A$ is $a' \in A$ such that $a \circ a' = e$ and $a' \circ a = e$. **Note**: the inverse is in $A$ and depends on the particular element. If there is no identity element, inverses make no sense.

### Examples

1. In $\mathbb{R}$, addition and multiplication are both associative and commutative, with respective identities 0 and 1: for all $a$, $b$, and $c$ in $\mathbb{R}$,

$$\begin{aligned} (a+b)+c &= a+(b+c) \qquad & (ab)c &= a(bc) \\ a+b &= b+a & ab &= ba \\ a+0 &= 0+a = a & a \cdot 1 &= 1 \cdot a = a. \end{aligned}$$

   In $\mathbb{R}$ the additive inverse of $a$ is $-a$, and for non-zero $a$ in $\mathbb{R}$ its multiplicative inverse is $1/a$ (0 has no multiplicative inverse).

2. In $\mathbb{C}$ addition and multiplication are both associative and commutative, with respective identities 0 and 1 (formulas in the previous example remain valid with real numbers replaced by complex numbers). In $\mathbb{C}$ the additive inverse of $z = x+yi$ is $-x-yi$, and for non-zero $z = x+yi$ in $\mathbb{C}$ its multiplicative inverse is $(x - yi)/(x^2 + y^2)$.

3. Matrix multiplication on $\mathrm{M}_n(\mathbb{R})$ is associative with identity $I_n$. It is **not** commutative when $n \geq 2$. A matrix in $\mathrm{M}_n(\mathbb{R})$ has an inverse for multiplication precisely when its determinant is not 0. In the $2 \times 2$ case, the inverse of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $\frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ when $ad - bc \neq 0$.

4. For any set $X$, composition of functions $X \to X$ is associative: if $f \colon X \to X$, $g \colon X \to X$, and $h \colon X \to X$ are all functions then $(f \circ g) \circ h = f \circ (g \circ h)$ as functions $X \to X$. Composition is usually not commutative: for most pairs of functions $X \to X$ the order of composition matters. The identity function $i \colon X \to X$ for composition is $i(x) = x$ for all $x \in X$. A function $f \colon X \to X$ has an inverse for composition precisely when it is a bijection (injective and surjective).

5. For any set $X$, the functions $X \to \mathbb{R}$ (not to be confused with the functions $X \to X$ in the previous example) can be added or multiplied pointwise: if $f\colon X \to \mathbb{R}$ and $g\colon X \to \mathbb{R}$ then we define $f+g\colon X \to \mathbb{R}$ and $fg\colon X \to \mathbb{R}$ by $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$ for $x \in X$. Both addition and multiplication of functions $X \to \mathbb{R}$ are commutative and associative. For functions $X \to \mathbb{R}$ the identity for addition is the constant function 0 and the identity for multiplication is the constant function 1. Every function $f\colon X \to \mathbb{R}$ has additive inverse $-f$, where $(-f)(x) = -(f(x))$ for all $x \in X$, and $f$ has a multiplicative inverse precisely when it never takes the value 0, in which case its multiplicative inverse is the function $g(x) = 1/f(x)$ for all $x \in X$.

**Non-examples**

Because associativity and commutativity are properties on all pairs in a set, to prove a binary operation is not associative or not commutative it suffices to find a single counterexample: the property might hold some of the time but it has to fail at least once.

1. Subtraction on $\mathbb{Z}$ is not associative or commutative: $1-(2-3) = 2$ while $(1-2)-3 = -4$ and $1-2 = -1$ while $2-1 = 1$. There is no identity element for subtraction: if $e \in \mathbb{Z}$ satisfies $e - a = a$ for all $a$ in $\mathbb{Z}$ then at $a = 0$ we see $e - 0 = 0$, so $e = 0$ and then $0 - a = a$ for all $a \in \mathbb{Z}$, which is false nearly all the time (indeed for every non-zero $a$).

2. Division on $\mathbb{R} - \{0\}$ is not associative or commutative: $1/(2/3) = 3/2$ while $(1/2)/3 = 1/6$ and $1/2 \neq 2/1$. There is no identity element either (why?).

3. On $\mathbb{R}_{>0}$, exponentiation ($a \circ b = a^b$) is not associative or commutative. For example, $(2^1)^2 = 4$ and $2^{(1^2)} = 2$, while $2^1 = 2$ and $1^2 = 1$.

4. The cross product on $\mathbb{R}^3$ ($\mathbf{x} \circ \mathbf{y} = \mathbf{x} \times \mathbf{y}$) is not associative: find your own example of $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ in $\mathbb{R}^3$ such that $(\mathbf{x} \times \mathbf{y}) \times \mathbf{z} \neq \mathbf{x} \times (\mathbf{y} \times \mathbf{z})$. It is not commutative either: since $\mathbf{y} \times \mathbf{x} = -(\mathbf{x} \times \mathbf{y})$ for all $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{R}^3$, if $\mathbf{x} \times \mathbf{y} = \mathbf{y} \times \mathbf{x}$ then $\mathbf{x} \times \mathbf{y} = \mathbf{0}$, which (by the geometric meaning of the cross product) says $\mathbf{x}$ and $\mathbf{y}$ lie along the same line through $\mathbf{0}$. So the cross product of any pair of vectors in $\mathbb{R}^3$ not on the same line through $\mathbf{0}$ depends on the order of multiplication.

5. Addition on $\mathbb{R}_{>0}$ is associative and commutative, but there is no identity.

6. Addition on $\mathbb{R}_{\geq 0}$ is associative and commutative with identity 0, but there are no inverses for non-zero elements: if $a \in \mathbb{R}_{\geq 0}$ and $a \neq 0$, there is no $a' \in \mathbb{R}_{\geq 0}$ such that $a + a' = 0$.

## 2 Groups

### Definitions and Theorems

1. A *group* is a set $G$ with a binary operation $\circ$ on it that is associative, has an identity (in $G$!), and each element of $G$ has an inverse (in $G$!). For a general group $G$ its operation is usually written multiplicatively: $g \circ h$ is written as $gh$, $\underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$ is written as $g^n$, and the inverse of $g$ is written as $g^{-1}$.

2. When the operation on a group $G$ is commutative, the group is called *commutative* or *abelian*. In an abstract abelian group additive notation is often used: the identity is 0, the operation is $g+h$, $\underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$ is written as $ng$, and the inverse of $g$ is written as $-g$. (Do not use additive notation if a group is not abelian.)

3. Groups that are not commutative are called *non-commutative* or *non-abelian*. Non-commutativity means $gh \neq hg$ at least once, not always (*e.g.*, $ge = eg$ for all $g$ in a group).

4. A group $G$ is called *cyclic* if there is some element $g \in G$ such that (using multiplicative notation) every element of $G$ has the form $g^n$ for $n \in \mathbb{Z}$. We then write $G = \langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ and say $g$ is a *generator* of $G$. Cyclic groups must be abelian, but the converse is false (see Non-examples below).

   **Note**. For groups where the operation is written additively, we write $ng$ for $n$ copies of $g$ added together instead of $g^n$ ($n$ copies of $g$ multiplied together), so $\langle g \rangle = \{ng : n \in \mathbb{Z}\} = \{\ldots, -2g, -g, 0, g, 2g, \ldots\}$.

### Examples

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ with the operation of addition are abelian groups. Other abelian groups are the set of $n$-tuples $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, and $\mathbb{C}^n$ using componentwise addition and the set of $n \times n$ matrices $\mathrm{M}_n(\mathbb{Z})$, $\mathrm{M}_n(\mathbb{Q})$, $\mathrm{M}_n(\mathbb{R})$ and $\mathrm{M}_n(\mathbb{C})$ with matrix addition.

2. Three groups under multiplication are $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$, which are the non-zero rational numbers, non-zero real numbers, and non-zero complex numbers.

3. The set $\mathbb{Z}_m$ with the operation of addition modulo $m$ is a finite abelian group.

4. The set $\mu_m$ of $m$th roots of unity in $\mathbb{C}$ with the operation of multiplication is a finite abelian group.

5. The set $U(m)$ of integers modulo $m$ that are relatively prime to $m$, with the operation of multiplication modulo $m$, is a finite abelian group.

6. The set of $n \times n$ real matrices with non-zero determinant is a non-abelian group under multiplication. This group is denoted $\mathrm{GL}_n(\mathbb{R})$.

7. Some finite non-abelian groups include $S_n$ (all permutations of $\{1, 2, \ldots, n\}$) for $n \geq 3$ and $D_n$ (all rigid motions of a regular $n$-gon) for $n \geq 3$, both under the operation of composition. In $S_n$ every pair of disjoint permutations commute, but non-disjoint permutations may or may not commute: in $S_3$, (12) and (13) don't commute while (123) and (132) do commute (they are inverses).

8. The group $\mathbb{Z}$ is cyclic, with generator 1 or $-1$.

9. The group $\mathbb{Z}_m$ is cyclic, with generator 1 mod $m$ or more generally $a$ mod $m$ when $(a, m) = 1$. For instance, additive generators of $\mathbb{Z}_8$ are 1, 3, 5, or 7 mod 8.

10. The group $\mu_m$ is cyclic, with a generator $\cos(2\pi/m) + i\sin(2\pi/m)$.

**Non-examples**

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_m$ under multiplication are not groups since 0 has no inverse.

2. The non-zero integers $\mathbb{Z} - \{0\}$ under multiplication are not a group since most integers (in fact all of them except $\pm 1$) have no inverse for multiplication in $\mathbb{Z} - \{0\}$.

3. The set of $2 \times 2$ *integer* matrices with non-zero determinant is not a group under multiplication because some (in fact most) such matrices don't have a matrix inverse with integer entries.

4. The group $\mathbb{Q}$ under addition is not cyclic: no fraction has all its (additive) multiples equal to all of $\mathbb{Q}$.

5. Every cyclic group is abelian but many abelian groups are not cyclic. For instance, all $U(m)$ are abelian and many are not cyclic; the first three non-cyclic $U(m)$ are $U(8)$, $U(12)$, and $U(15)$.

# 3 Subgroups

**Definitions and Theorems**

1. A *subgroup* of a group $G$ is a subset $H$ of $G$ that is a group using the same operation that $G$ has. (Associativity on a subset is automatic, and if $G$ is an abelian group then commutativity of the operation on a subset is automatic. The identity element and inverses in a subgroup have to be the same as in $G$.)

2. A *cyclic subgroup* $H$ is a subgroup that is a cyclic group in its own right: $H = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ for some $a \in H$.

3. An *abelian subgroup* $H$ is a subgroup that is an abelian group in its own right: $hk = kh$ for all $h, k \in H$.

4. The *center* $Z(G)$ of a group $G$ is all elements of $G$ that commute with everything in $G$: $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$.

5. **Theorem**. *Every subgroup of an abelian group is abelian and every subgroup of a cyclic group is cyclic.* The first result only relies on some very simple reasoning (and knowing what the words mean), but the second result requires a clever idea (using division algorithm in $\mathbb{Z}$).

**Examples**

1. In $S_4$, (12) and (34) commute and $H = \{(1), (12), (34), (12)(34)\}$ is an abelian subgroup of $S_4$ that is not cyclic (every element squares to (1)).

2. In $S_4$ let $g = (1234)$. Then $g^2 = (13)(24)$, $g^3 = (1432) = (4321)$, and $g^4 = (1)$, so $\langle g \rangle = \{(1), (1234), (13)(24), (4321)\}$.

3. Subgroups of $\mathbb{Z}$ include the even integers $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$, and more generally $a\mathbb{Z} = \{am : m \in \mathbb{Z}\}$ for $a \in \mathbb{Z}$. (In fact it is a theorem that every subgroup of $\mathbb{Z}$ is $a\mathbb{Z}$ for some integer $a$.)

4. In $\mathbb{R}^\times$, the subset $\mathbb{R}_{>0}$ of positive numbers is a subgroup.

5. In $\mathbb{R}^\times$, the subset $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\} = \{\ldots, 1/4, 1/2, 1, 2, 4, \ldots\}$ is a subgroup.

6. In $\mathbb{C}^\times$, the subset $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is a subgroup.

7. In $\mathrm{GL}_2(\mathbb{R})$, one cyclic subgroup is $\{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\} = \{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n : n \in \mathbb{Z}\} = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$.

8. Subgroups of $\mathrm{GL}_2(\mathbb{R})$ include $\mathrm{Aff}(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{R}^\times, b \in \mathbb{R}\}$ and $\mathrm{SL}_2(\mathbb{R}) =$ the $2 \times 2$ matrices with determinant 1. These are both non-abelian, but the subgroup of diagonal matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ where $a, b \in \mathbb{R}^\times$ is an abelian subgroup.

9. The alternating group $A_n$, which is all *even* permutations in $S_n$, is a subgroup of $S_n$.

10. Every group $G$ has the subgroups $G$ and $\{e\}$. If a subgroup contains $a$ then it must at least contain $\langle a \rangle$, but could be larger.

11. The group $S_n$ is not cyclic for $n \geq 3$ since it is non-abelian for $n \geq 3$. While $S_n$ for $n \geq 3$ does not have a single generator, it is generated by all the transpositions $(ij)$.

12. The center of a group is a subgroup of $G$. If $G$ is abelian then $Z(G) = G$, and conversely. Having $Z(G)$ be a "small" subgroup of $G$ is a measure of $G$ being highly non-abelian.

13. The center of $\mathrm{GL}_2(\mathbb{R})$ is the scalar diagonal matrices $\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{R}^\times\}$.

**Non-examples**

1. In $\mathbb{Z}$, while the even integers $2\mathbb{Z}$ are a subgroup, the odd integers $1 + 2\mathbb{Z}$ are not a subgroup (no identity, not closed under addition).

2. In $\mathbb{R}^\times$, while the positive numbers $\mathbb{R}_{>0}$ are a subgroup, the negative numbers $\mathbb{R}_{<0}$ are not a subgroup (no identity, not closed under multiplication).

3. Even though $\mathbb{R}^\times$ is a subset of $\mathbb{R}$ and each is a group under a suitable operation (addition for $\mathbb{R}$, multiplication for $\mathbb{R}^\times$), we do not consider $\mathbb{R}^\times$ to be a subgroup of $\mathbb{R}$ since the operations are not the same.

4. In the group $\mathbb{R}$, the subset of positive real numbers is closed under addition but is not a subgroup of $\mathbb{R}$ since there is no additive identity. The subset $\mathbb{R}_{\geq 0}$ of non-negative numbers is not a group (under addition) even though it has an identity since additive inverses generally fail to exist in $\mathbb{R}_{\geq 0}$.

# 4 Order

**Definitions and Theorems**

1. The *order* of a subgroup $H \subset G$ is the size of $H$ and is denoted $|H|$. When $H$ is infinite, often we write $|H| = \infty$.

2. The *order* of an element $g \in G$ is the size of $\langle g \rangle$ and is denoted $|g|$, so $|g| = |\langle g \rangle|$.

3. **Theorem**. *If $|g| < \infty$ then $|g|$ is the smallest $n \geq 1$ such that $g^n = e$. If $|g| = \infty$ there is no $n \geq 1$ such that $g^n = e$.*

4. **Theorem**. *If $|g| = n$ is finite then $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ and $g^i = g^j \iff i \equiv j \bmod n$. We have $|g^k| = n$ when $(k, n) = 1$ and $|g^d| = n/d$ if $d \mid n$.*

**Examples**

1. We have $|\mathbb{Z}_m| = m$, $|S_n| = n!$, $|A_n| = n!/2$, and $|D_n| = 2n$. The order of $U(m)$ is denoted $\varphi(m)$, so $\varphi(4) = |\{1, 3 \bmod 4\}| = 2$ and $\varphi(5) = |\{1, 2, 3, 4 \bmod 5\}| = 4$.

2. In $\mathbb{Z}$, every integer besides 0 has infinite order under addition, while 0 has order 1.

3. In the group $\mathbb{R}^\times$, 1 has order 1, $-1$ has order 2 (because $(-1)^2 = 1$ while $(-1)^1 \neq 1$), and every non-zero real number besides $\pm 1$ has infinite order.

4. In $\mathbb{C}^\times$, $-1$ has order 2 and $i$ has order 4. The complex number $\cos(2\pi/n) + i \sin(2\pi/n)$ has order $n$. Most non-zero complex numbers, like most non-zero real numbers, have infinite multiplicative order.

5. In $S_4$, $|(1234)| = 4$: $(1234)^2 = (13)(24)$, $(1234)^3 = (1432) = (4321)$, and $(1234)^4 = (1)$. More generally, in $S_n$ a $k$-cycle $(i_1 i_2 \ldots i_k)$ has order $k$.

6. In a finite group every element has finite order. In $\mathbb{Z}_m$ the order of $a \bmod m$ is $m/(a, m)$. In $U(m)$ there is no simple formula for the order of an element (other than $\pm 1 \bmod m$).

**Non-examples**

1. If $g^n = e$ in a group, this does **not** imply $|g| = n$. Consider $(-1)^4 = 1$ in $\mathbb{R}^\times$ and $-1$ has order 2, not 4. What $g^n = e$ implies is that $|g| \leq n$. In fact, $g^n = e \iff |g| \mid n$.

2. In $S_3$, $|(12)| = |(23)| = 2$ and $|(12)(23)| = |(123)| = 3$, so $|(12)(23)| \neq |(12)||(23)|$.

3. In $\mathrm{GL}_2(\mathbb{R})$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ both have order 2, but their product $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order (for $n \in \mathbb{Z}$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$), so in some groups two non-commuting (!) elements with finite order can have a product with infinite order.