Reminder about groups

On this page, $\circ$ will denote a general binary operation on a (nonempty) set G.

Recall that a binary operation takes two inputs (in a specific order) from G and produces an output which must also be in G. In other words, the expression "binary operation" will, in this class, automatically include the so-called **closure** condition:

$$(\forall g, h \in G)\, g \circ h \in G.$$

Definition. *Let G be a (nonempty) set, and let $\circ$ be a binary operation on G. We say that $(G, \circ)$ is a* **group** *if the following three conditions are satisfied.*

(i) **(associativity)** $(g \circ h) \circ k = g \circ (h \circ k)$ *for all* $g, h, k \in G$.

(ii) **(existence of identity)** *There is an $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.*
[it is easy to see that this e is unique]

(iii) **(existence of inverse)** *For every $g \in G$ there is an $h \in G$ such that $g \circ h = h \circ g = e$.*

The number of elements in G (cardinality of G) is called the **order** *of the group: $o(G) = |G|$.*

If the group satisfies the additional property $(\forall g, h \in G)\, g \circ h = h \circ g$, then it is said to be **commutative** *or* **Abelian**.

Remarks. When $(G, \circ)$ is a group, we often say that G is a group under (or with respect to) the operation $\circ$, or simply say that G is a group.

Typically, a multiplicative notation is used by writing "$\cdot$" for the operation $\circ$. In this case we sometimes write 1 for the identity e, and g^{-1} for the inverse of g. We also often drop the symbol $\cdot$ altogether, and simply write gh for $g \cdot h$, and g^2, g^3, etc, for repeated "multiplications."

With an additive notation $(G, +)$ (typically used for Abelian groups), we usually write 0 for the identity, $-g$ for the inverse of g, and $2g$, $3g$, etc, for repeated "additions."

Here are some **essential properties** of groups (using the multiplicative notation):

For arbitrary fixed $a, b \in G$, the equations $ax = b$ and $xa = b$ have unique solutions. (The two solutions $x = a^{-1}b$ and $x = ba^{-1}$ may be different!)

Cancellation rules: $ac = bc$ implies $a = b$, and $ca = cb$ implies $a = b$.

Inverse of products: $(ab)^{-1} = b^{-1}a^{-1}$
(or in an "additive group": $-(a + b) = (-b) + (-a)$; not $(-a) + (-b)$!)

Examples. (Using the notations $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.)

Here are a few standard Abelian groups:
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, and $(\mathbb{Z}_n, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$.

The set of all $k \times k$ non-singular real matrices forms a non-Abelian group with respect to matrix-multiplication.

The set of all symmetries of an equilateral triangle forms a non-Abelian group under composition. So does, in general, the set of all isometries of $\mathbb{R}^d$ which map a certain fixed set of points $S \subseteq \mathbb{R}^d$ into itself.

Subgroups

Definition. *Let $(G, \circ)$ be a group. A subset H of G is a subgroup if H itself is a group with respect to the same operation $\circ$. We write $(H, \circ) \leq (G, \circ)$, or simply write $H \leq G$ when it is clear what the operation is. $H < G$ means $H \leq G$ and $H \neq G$ (proper subgroup).*

Lemma. *Let G be a group (with respect to the operation $\cdot$). Let $e = e_G$ denote the identity in G, and let H be a subgroup of G. Then, $e \in H$, that is, $e_H = e_G$. Also, for every $a \in H$, the inverse a^{-1} (within the group G) is also an element of H, and hence it is the inverse of the element a within the group H also.*

Proof. Since H itself is a group, it has an identity $i = e_H$. We need to show that $i = e$. Indeed, $i \cdot i = i$ (by the definition of i), and since $i \in G$ also, so $i \cdot e = i$ holds as well (by the definition of e). Using cancellation (within G) in the equality $i \cdot i = i \cdot e$, we get $i = e$.

Notice how we repeatedly used the fact that the two groups have the same operation!

Now let $a \in H$ be given, and let b be the element of H for which $a \cdot b = i$. Since $a \cdot a^{-1} = e$ and $e = i$, we get, by cancellation (in G) again, that $b = a^{-1}$ (and hence $a^{-1} \in H$). $\square$

The following test easily follows from the above lemma.

Theorem (Subgroup Test). *Let $(G, \circ)$ be a group with identity e, and let H be a subset of G. Then, H is a subgroup with respect to the same operation $\circ$ if and only if H is nonempty, H is closed under $\circ$, and H is closed under taking inverse (within the group $(G, \circ)$):*

(a) $H \neq \emptyset$,

(b) $(\forall a, b \in H)\, a \circ b \in H$,

(c) $(\forall a \in H)\, a^{-1} \in H$.

It is easy to see that condition (a) can be replaced with the alternative condition

(a') $e \in H$.

(Here is an exercise you may want to think about, or may wait until cyclic groups are discussed: Let G be a (multiplicative) group, and let H be a *finite* nonempty subset of G closed under multiplication. Prove that H is a subgroup of G. In other words, when H is finite, then we need not check that H is also closed under taking inverse, it's automatic.)

The following test provides a more compact form:

Theorem. *Let $(G, \circ)$ be a group and let $H \subseteq G$ be nonempty. Then $(H, \circ)$ is a group if and only if $a^{-1} \circ b \in H$ for all $a, b \in H$.*

Examples:

$$(\{0\}, +) < (6\mathbb{Z}, +) < (2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$$

and

$$(\{1\}, \cdot) < (\{1, -1\}, \cdot) < (\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$$

Given $a \in G$, the group $<a> := \{a^k : k \in \mathbb{Z}\}$ is called the cyclic subgroup generated by a. The order of $<a>$ is called the order of the element a and is denoted by $o(a)$.

Theorem. *The only subgroups of* $(\mathbb{Z}, +)$ *are the sets* $d\mathbb{Z} := \{dn : n \in \mathbb{Z}\}$, $d = 0, 1, 2, \ldots$

[Hint for a proof: let $I \leq \mathbb{Z}$ and start with the smallest positive element of I (if any).]

Corollary. *Let* $(G, \cdot)$ *be a group with identity* e*, and let* $a \in G$ *be arbitrary. The set* $\{k \in \mathbb{Z} : a^k = e\}$ *is clearly a subgroup of* $\mathbb{Z}$*, and hence it is of the form* $d\mathbb{Z}$ *for some nonnegative integer* d*. When this* d *is positive (so it's the smallest positive integer* d *such that* $a^d = e$*), then it's easily seen to be equal to the order* $o(a)$ *of* a*.*

Theorem (Lagrange). *Let* G *be a* finite *group of order* n *with identity* e*. Then,* $a^n = e$ *for all* $a \in G$*. In fact,*

$$\{m \in \mathbb{Z} : g^m = e\} = o(g)\mathbb{Z} := \{o(g)\ell : \ell \in \mathbb{Z}\}.$$

More generally, if H *is a subgroup of* G*, then* $o(H)|o(G)$ *(*$|$ *denotes "divides"). Hence, the order of any element of* G *is a divisor of* n*. Even more generally, the order of any subgroup of* G *divides* n*.*

Remark. One can get an easy proof for commutative groups by using the following lemma. (For non-commutative groups, the proof will use the notion of cosets.)

Lemma. *Let* $(G, \circ)$ *be a group and let* $a \in G$ *be arbitrary. The map* $f_a : G \to G : x \mapsto a \circ x$ *is a bijection.*

Proof of Lagrange's theorem in the commutative case: Let $a \in G$. By the previous lemma,

$$\prod_{g \in G} g = \prod_{g \in G} (ag) = a^{|G|} \prod_{g \in G} g$$

and the claim follows.