Math 412: Adventure sheet on groups

DEFINITION: A **group** is a nonempty set G with an operation $\star$ is associative, has an identity, and has inverses. If we want to specify the operation, we may write $(G, \star)$.

We often just write gh for $g \star h$, and g^{-1} for the inverse of g.

DEFINITION: An **abelian group** is a group $(G, \star)$ in which the operation $\star$ is commutative.

DEFINITION: A **subgroup** of a group $(G, \star)$ is a subset H which is itself a group under $\star$.

DEFINITION: An element g of a group $(G, \star)$ has **order** n if n is the smallest positive integer such that $g^n = e$. If no such n exists, we say that g has infinite order.

DEFINITION: The **order** of a group G is the number of elements in G.

DEFINITION: The **cyclic subgroup generated by an element** g in G is the subgroup

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{\dots, g^{-2} = (g^{-1})^2, g^{-1}, g^0 = e, g^1 = g, g^2, \dots\}.$$

A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$.

A. GROUPS COMING FROM RINGS: Let R be a ring with addition "$+$" and multiplication "$\times$".

(1) Show that $(R, +)$ is an abelian group. We often denote this group by R.
(2) Is $(R, \times)$ always a group?
(3) Let $R^\times \subseteq R$ be the set of units of R. Show that $(R^\times, \times)$ is a group. We often denote this group by $R^\times$.
(4) Is $R^\times$ always abelian?
(5) Show that $\mathbb{Z}_n$ is a cyclic group.
(6) How many elements are in $\mathbb{Z}_8^\times$? Is this a cyclic group?
(7) Describe the group $M_n(\mathbb{R})^\times$. What are the elements, and what is the operation? Have we seen another name for this group?

Solution.

(1) The axioms for a ring included requiring that 0 is the additive identity, that every element has an additive inverse, and that the sum is commutative.
(2) No! In fact, it is *never* a group, unless R is the ring with one element — since 0 has no inverse.
(3) The identity is 1. Given two units u and v, $(uv)^{-1} = v^{-1}u^{-1}$, so uv is invertible. By definition, every element has an inverse.
(4) No! For example, if $R = M_2(R)$, not every two invertible matrices commute.
(5) It is generated by 1.
(6) We counted the units in $\mathbb{Z}_8$ before: there are 4, and they are $1, 3, 5, 7$. All the integers between 1 and 7 that are coprime with 8.
(7) All the invertible $n \times n$ matrices with real entries. Before we called this $\mathrm{GL}_n(\mathbb{R})$.

B. SYMMETRIES OF A CUBE: Consider the group Cube whose elements are ways to pick up a cube and put it down in the same place.

(1) How many elements are there in Cube that keep the top face on top?
(2) How many elements are there in Cube?
(3) Find elements of orders $1, 2, 3$, and 4 in Cube. Could you find elements of other orders?

Solution.

(1) 4.
(2) $24 = 4 \times 6$.
(3) Order 1: the identity. Order 4: rotating clockwise by 90 degrees while keeping the top face on top. Order 2: rotating clockwise by 180 degrees while keeping the top face on top. Order 3: rotating around a corner. There are no elements of other orders!

C. ORDERS OF ELEMENTS:

(1) When we use the notation a^m for some integer $m \geqslant 2$, what axiom of groups are we implicitly using so that the notation is unambiguous?
(2) Show that if $a^m = a^n$ for some positive integers $m < n$, then the order of a is less than or equal to $n - m$.
(3) Show that if $a^n = e$, then the order of a divides n.[1]
(4) Show that if the order of a is infinite, then the powers $\{a^m \mid m \in \mathbb{Z}\}$ of a are distinct.
(5) Show that the order of an element a is equal to the order of the subgroup $\langle a \rangle \leq G$.

Solution.

(1) The notation means that we take the product of a with itself m times, and this is unambiguous because the operations is associative.
(2) If $a^m = a^n$, then multiplying by the inverse of a^m we get $a^{n-m} = e$, where e is the identity.
(3) Let k be the order of a. Clearly, $k \leqslant n$. By the division algorithm, we can write $n = kq + r$ for some positive integers k, r with $0 \leqslant r < k$. Then
$$e = a^n = a^{kq+r} = \left(a^k\right)^q a^r = a^r.$$
By definition of order, k is the smallest positive integer such that $a^k = e$. Therefore, $r = 0$.
(4) Notice that if a has infinite order, then $a^n = e$ implies that $n = 0$. By definition, $a^n = e$ does not hold for any positive n; moreover, $a^{-n} = e$ implies that $a^n = e$. If there exists $m > n$ such that $a^m = a^n$, then $a^{m-n} = e$, and since $a^k \neq e$ for any positive k by assumption, we conclude that $m = n$.
(5) We just showed that the elements $e, g, g^2, \ldots, g^{n-1}$ are all distinct, so the order of the cyclic group generated by g is at least n. Now given any integer k, by the division algorithm we can write $k = nq + r$ for $0 \leqslant r < n$, and
$$g^k = (g^n)^q \, g^r = g^r,$$
so $e, g, g^2, \ldots, g^{n-1}$ are really all the elements in the group.

[1] Hint: Division algorithm.

DEFINITION: Given two groups G and G, their product is the group with underlying set

$$G \times H = \{(g,h) : g \in G, h \in H\}$$

and with the operation defined by

$$(g,h)(a,b) = (ga, hb).$$

D. PRODUCTS OF GROUPS:

(1) Show that the product of two groups is indeed a group. What is the identity of the group $G \times H$? What are the inverses of each element?
(2) Show that if G and H are abelian groups, then so is $G \times H$.
(3) If G is a nonabelian group and H is some group, can we say anything about whether $G \times H$ is an abelian group?
(4) Are $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ isomorphic groups?

Solution.

(1) The identity is (e_G, e_H), and $(g,h)^{-1} = (g^{-1}, h^{-1})$, so every element is invertible.
(2) $(g,h)(g',h') = (gg', hh') = (g'g, h'h) = (g',h')(g,h)$.
(3) It isn't: if $gg' \neq g'g$, then $(g,e)(g',e) \neq (g',e)(g,e)$.
(4) No: one has an element of order 4 and the other doesn't.

DEFINITION: Given elements $g_1, \dots, g_n$ of a group G, the subgroup generated by $g_1, \dots, g_n$, which we write $\langle g_1, \dots, g_n \rangle$, is the set of all the finite products of the elements $g_1, \dots, g_n, g_1^{-1}, \dots, g_n^{-1}$, in any order, with any number of repetitions.

Given a group G, we say that $g_1, \dots, g_n \in G$ are generators of G if $\langle g_1, \dots, g_n \rangle = G$.

E. GENERATORS AND SUBGROUPS:

(1) Explain why $\langle g_1, \dots, g_n \rangle$, is the smallest subgroup of G containing $g_1, \dots, g_n$.
(2) Find a set of 2 generators for D_3. Are there other sets of two generators for D_3? Is D_3 cyclic?
(3) Find a finite set of generators for $\mathbb{Z}^k$, where the operation is addition term-by-term.
(4) Show that every subgroup of a cyclic group is cyclic.
(5) Show that if G and H are both cyclic groups of order n, then G and H are isomorphic.[2]

Solution.

(1) It is a subgroup containing these elements. If H is a subgroup that contains all of these elements, it must contain all of their inverses, and all of the products of these elements and the inverses, so $\langle g_1, \dots, g_n \rangle \subseteq H$. This means that $\langle g_1, \dots, g_n \rangle$ is the smallest subgroup containing the elements.
(2) A rotation and a flip generate: if we look at all of the subgroups of D_3, no proper subgroup contains a flip and a rotation. Any such pair suffices. It is not cyclic, since there is no element of order 6.
(3) $(1, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$,$\dots$, $(0, 0, \dots, 0, 1)$.

[2]Sometimes we abuse notation and talk about *the* cyclic group of order n. What group is this?

(4) Let $G = \langle g \rangle$ be cyclic, and $H \leq G$. If $H = \{e\}$, it is a boring cyclic group. Otherwise, note that there exists some $g^n \in H$ with $n > 0$: there is some nonzero power of H, and if we have a negative power, the inverse is a positive power. Let n be the smallest positive integer such that $g^n \in H$; we can do this by the well-ordering principle. We claim that $H = \langle g^n \rangle$. Let $g^m \in H$, and write $m = qn + r$ with $0 \leq r < n$. Then $g^r = g^m (g^n)^{-q} \in H$, and by choice of r, we find that $r = 0$. Thus, $m = qr$, so $g^m \in \langle g^n \rangle$, as required.

(5) If $G = \langle g \rangle$ and $H = \langle h \rangle$, then mapping $g^n \mapsto h^n$ is an isomorphism.

F. BIJECTIONS OF A SET: Let X be any set. Let G be the set of all BIJECTIONS from X to itself.

(1) Prove that G is a group under composition.

(2) If X is a finite set of three objects, what is the book's word for a *bijection* from X to X? What is the book's notation in 7.1 for a bijection in this case? What is the book's notation for G in this case?

(3) Let X be an arbitrary set. Let $x \in X$. Let $H = \{g \in G \mid g(x) = x\}$. Prove that H is a subgroup of G.

Solution.

(1) Composition of functions is associative; bijections have inverses; the identity map is the identity.

(2) Permutation; S_3.

(3) This subset is closed under composition and inverses.