Groups and permutations

jason hanson *

1 Abstract groups

1.1 Formal definition

Definition 1. *A* **group** *is a pair* $(G, \cdot)$ *consisting of a set* G *and a binary operation* $\cdot : G \times G \to G$ *for which the following are satisfied.*

1. *For all* $f, g, h \in G$*, the* **associative law** *holds:* $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.
2. *There exists an element* $e \in G$*, called the* **identity element** *for which* $e \cdot g = g = g \cdot e$ *for all* $g \in G$.
3. *For every* $g \in G$*, there exists an element* $g^{-1} \in G$*, called the* **inverse** *of* g*, satisfying* $g \cdot g^{-1} = e = g^{-1} \cdot g$.

For example, the integers from a group under the operation of addition. In this case, the underlying set is $\mathbb{Z}$, the set of integers (positive and negative whole numbers, along with zero), and the binary operation is addition $+$; i.e., the pair $(\mathbb{Z}, +)$ forms a group. Indeed, we know that addition of integers is associative: $(m + n) + p = m + (n + p)$; e.g., $(3 + 5) + 2 = 9 = 3 + (5 + 2)$. The identity in this case is 0, since $n + 0 = n + 0 = n$ for any integer n; e.g., $5 + 0 = 5 = 0 + 5$. And the inverse of the integer n is given by its negation $-n$: $n + (-n) = 0 = (-n) + n$; e.g., the (additive) inverse of -5 is $-(-5) = 5$, since $(-5) + 5 = 0 = 5 + (-5)$.

Exercise 1. *Show that* $(\mathbb{R}_+, \cdot)$ *is a group, where* $\mathbb{R}_+$ *denote the set of* positive *integers (not including* 0*), and* $\cdot$ *is the usual multiplication of real numbers.*

Exercise 2. *Let $G \doteq \mathbb{Z} \times \mathbb{Z}$ (the set consisting of all pairs of integers), and define the binary operation $\star$ on G by $(m,n) \star (p,q) \doteq (m + (-1)^n p, n + q)$. Show that $(G, \star)$ is a group.*

Exercise 3. *Let $(H, \sharp)$ and $(K, \flat)$ be groups. Set $G \doteq H \times K$; i.e. $g \in G$ is an ordered pair $g = (h,k)$ for some $h \in H$ and $k \in K$. Moreover, let $\cdot$ denote the binary operation*

$$(h_1, k_1) \cdot (h_2, k_2) \doteq (h_1 \sharp h_2, g_1 \flat g_2).$$

Show that $(G, \cdot)$ is a group (G is said to be the direct product *of H and K).*

In exercise 1, the binary operation $\cdot$ *commutes*; that is $x \cdot y = y \cdot x$ for all (positive) real numbers x, y. A group whose binary operation commutes is said to be an **Abelian group**. On the other hand, in exercise 2, the binary operation $\star$ does *not* commute; i.e., $(m,n) \star (p,q) \neq (p,q) \star (m,n)$, in general. For example $(1,1) \star (1,0) = (0,1)$, while $(1,0) \star (1,1) = (2,1)$. Consequently, the group $(G, \star)$ is not Abelian.

1.2 Generators and relations

When discussing a group $(G, \cdot)$ in the abstract, it is customary to drop the symbol $\cdot$ from the notation, and simply write gh instead of $g \cdot h$ — the binary operation $\cdot$ being understood. In the remainder, we will adhere to this convention.

A useful way of describing a group is in terms of a collection of *generators* and *relations*. The **generators** of a group G are simply a collection of symbols; all finite strings from these symbols, and their inverses, represent elements in the group. For example, if α, β are generators for G, then $\alpha^3 \doteq \alpha\alpha\alpha$, $\alpha\beta\alpha$, and $\beta^{-2} \doteq \beta^{-1}\beta^{-1}$ are all elements in G. The identity of G can be identified with the string of length zero (null string): $e\alpha = \alpha = \alpha e$. The **relations** for G are auxiliary conditions, or rules, for simplifying strings of generators. For example, we might have the relations $\beta\alpha = \alpha^2\beta$, $\alpha^3 = e$, and $\beta^2 = e$ in G. In this case, the string $\beta\alpha^2\beta\alpha^{-1}\beta^3\alpha$ would represent the same element in G as the string $\beta\alpha$; indeed, using the given relations we have

$$\beta\alpha^2\beta\alpha^{-1}\beta^3\alpha = \beta(\alpha^2\beta)\alpha^{-1}(\beta^2)\beta\alpha = \beta(\beta\alpha)\alpha^{-1}(e)\beta\alpha = (\beta^2)(\alpha\alpha^{-1})\beta\alpha = \beta\alpha$$

(the relations $\alpha^{-1}\alpha = e = \alpha\alpha^{-1}$ and $\beta^{-1}\beta = e = \beta\beta^{-1}$ are understood).

When defining a group in terms of generators and relations, it is common to write $\langle \textit{generators} \mid \textit{relations} \rangle$ to mean the group with the specified generators and relations. E.g., the group G in the previous paragraph would be written as

$$G = \langle \alpha, \beta \mid \beta\alpha = \alpha^2\beta, \alpha^3 = e, \beta^2 = e \rangle. \tag{1}$$

Observe that the group G thus defined is non–Abelian, since $\beta\alpha = \alpha^2\beta \neq \alpha\beta$.

A simple but important group is C_n, the **cyclic group** of order n: the group with a single generator, say γ, and the single relation $\gamma^n = e$. That is, $C_n \doteq \langle \gamma \mid \gamma^n = e \rangle$. For instance, the cyclic group of order 3 has only the elements $C_3 = \{e, \gamma, \gamma^2\}$. The group C_n is necessarily Abelian.

Exercise 4. *Let G be the group in equation* (1)*. Show that as a set, $G = \{e, \alpha, \beta, \alpha\beta, \alpha^2, \alpha^2\beta\}$; i.e., every string in α, α^{-1}, β, and β^{-1} can be reduced to one of these 6 forms.*

Exercise 5. *Show that the group $G \doteq \langle \alpha, \beta \mid \alpha\beta = \beta\alpha, \alpha^2 = e, \beta^3 = e \rangle$ is* isomorphic *to the direct product group $C_2 \times C_3$; that is, there is a map $\eta : G \to C_2 \times C_3$ that is one–to–one and onto and preserves binary operations: $\eta(g_1 g_2) = \eta(g_1)\eta(g_2)$.*

2 Permutation groups

2.1 Permutations

Recall that a *permutation* of a sequence is a rearrangement of its terms. For example, $[2, 3, 1]$ is a permutation of the sequence $[1, 2, 3]$. Alternatively, we may think of the permutation $[2, 3, 1]$ as the *map* $p : \{1, 2, 3\} \to \{1, 2, 3\}$, where $p(1) \doteq 2$, $p(2) \doteq 3$, and $p(3) \doteq 1$. Not all maps on $\{1, 2, 3\}$ yield permutations: only those maps which are *bijective* will be permutations; that is, they must be *one–to–one* and *onto*. E.g., the map $q : \{1, 2, 3\} \to \{1, 2, 3\}$, given by $q(1) \doteq 1$, $q(2) \doteq 1$, $q(3) \doteq 2$, is not a permutation, since q is neither one–to–one (since $q(1) = q(2)$) nor onto (as 3 has no preimage under q); equivalently, the sequence $[1, 1, 2]$ is not a permutation of $[1, 2, 3]$.

Definition 2. *A* **permutation on n letters** *(or simply a* **permutation** *when n is understood) is a bijection $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. The set of all permutations on n letters is denoted by S_n.*

The reader will recall the notion of the *composition* of two functions: if A, B, C are sets and $f : B \to C$ and $g : A \to B$ are two functions, then the composition of f and g is the function $f \circ g : A \to C$ given by $(f \circ g)(a) \doteq f(g(a))$. For example, if $g : \mathbb{R} \to \mathbb{R}$ denotes the function $g(x) \doteq 2x + 3$, and if $f : \mathbb{R} \to \mathbb{R}$ denotes the function $f(x) \doteq x^2$, then $f \circ g : \mathbb{R} \to \mathbb{R}$ is the function $(f \circ g)(x) = (2x + 3)^2$.

Exercise 6. *Show that $(S_n, \circ)$ is a group.*

Exercise 7. *We say that $(H, \cdot)$ is a* subgroup *of a group $(G, \cdot)$ if H is a subset of G and $(H, \cdot)$ is a group (where $\cdot : H \times H \to H$ is given by restricting the binary operation $\cdot : G \times G \to G$). Show that if $m \leq n$, then $(S_m, \circ)$ is a subgroup of $(S_n, \circ)$.*

Exercise 8. *Prove: if G is a finite group containing n elements, then there exists an* injective *(one–to–one) map $i : G \to S_n$ such that for all $g, h \in G$, we have $i(gh) = i(g) \circ i(h)$.*

In other words, every finite group is equivalent (isomorphic) to a subgroup of a permutation group. For example, consider the cyclic group of order three, $C_3 = \langle \gamma \mid \gamma^3 = e \rangle$. Let $p \in S_3$ be the map $p(1) \doteq 2$, $p(2) \doteq 3$, $p(3) \doteq 1$. If we define $p^2 \doteq p \circ p$, or more generally, $p^m \doteq p \circ p \circ \cdots \circ p$ (p composed with itself m times), then we find that

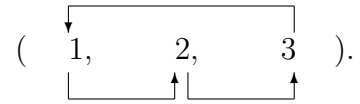
$$p^2(1) = 3,\ p^2(2) = 1,\ p^2(3) = 2, \quad \text{and} \quad p^3(1) = 1,\ p^3(2) = 2,\ p^3(3) = 3.$$

For example, $p^2(1) = p(p(1)) = p(2) = 3$, and $p^3(2) = p(p(p(2))) = p(p(3)) = p(1) = 2$. In particular, p^3 is the *identity* map id, where $id(k) \doteq k$ for $k = 1, 2, 3$. We see then that $\{id, p, p^2\}$ forms a subgroup of S_3. Moreover, the map $i : C_3 \to S_3$, given by $i(e) \doteq id$, $i(\gamma) \doteq p$, and $i(\gamma^2) \doteq p^2$ respects the group operations; e.g., $i(\gamma\gamma) = i(\gamma) \circ i(\gamma)$, since $i(\gamma^2) = p^2 = p \circ p$. And in particular, i respects the relation $\gamma^3 = e$ in C_2: $i(\gamma)^3 = id$, since $p^3 = id$. Thus the group C_3 and the subgroup $\{id, p, p^2\} \subseteq S_3$ are essentially the same: they are isomorphic.

2.2 Cycle notation

When working with permutation groups, it is convenient to use a special notation, the so–called *cycle notation*. Consider the permutation p representing $\gamma \in C_3$ above: $p(1) = 2$, $p(2) = 3$, and $p(3) = 1$. In cycle notation, we would

write p as the *cycle* $(1, 2, 3)$. The meaning is that 1 is mapped to 2 under the permutation p, 2 is mapped to 3, and 3 is mapped back around to 1:



Note that the cycles $(2, 3, 1)$ and $(3, 1, 2)$ are also representations of the permutation p. The permutation with $1 \mapsto 3$, $2 \mapsto 2$, and $3 \mapsto 1$ becomes $(1, 3)$ in cycle notation; the convention is that if an index does not occur, it is mapped to itself. In general, the cycle $(n_1, n_2, \ldots, n_k)$ would represent the permutation with $n_1 \mapsto n_2$, $n_2 \mapsto n_3$, $\ldots$, $n_{k-1} \mapsto n_k$, and $n_k \mapsto n_1$; all indices not in the list $n_1, \ldots, n_k$ map to themselves. The identity permutation is represented by the *trivial cycle* $()$.

Not every permutation can be represented by a single cycle; to represent any permutation, we must consider products of cycles. The product of two cycles is simply the composition of two permutations. Thus

$$(1, 2, 3, 4)(1, 2) = (1, 3, 4).$$

Indeed, if p is the permutation $p(1) \doteq 2$, $p(2) \doteq 3$, $p(3) \doteq 4$, $p(4) \doteq 1$, and if q is the permutation $q(1) \doteq 3$, $q(2) \doteq 1$, $q(3) \doteq 3$, $q(4) \doteq 4$, then $p \circ q$ is the permutation $(p \circ q)(1) = p(q(1)) = p(2) = 3$, $(p \circ q)(2) = p(q(2)) = p(1) = 2$, $(p \circ q)(3) = p(q(3)) = p(3) =$, and $(p \circ q)(4) = p(q(4)) = p(4) = 1$; which is represented by the cycle $(1, 3, 4)$.

Every permutation can be represented by a product of cycles. For example, consider the permutation sending the sequence $[1, 2, 3, 4, 5, 6]$ to the sequence $[3, 2, 1, 6, 4, 5]$; i.e., $1 \mapsto 3$, $2 \mapsto 2$, et cetera. Since $1 \mapsto 3 \mapsto 1$, one of the factors is the cycle $(1, 3)$. Another factor is $(4, 6, 5)$, since $4 \mapsto 6 \mapsto 5 \mapsto 4$. There are no other factors, as the only other index not used is 2, which is mapped to itself. Thus the given permutation is represented by the product of cycles $(1, 3)(4, 6, 5)$. Observe that the two cycles contain no indices in common, and so commute: $(1, 3)(4, 6, 5) = (4, 6, 5)(1, 3)$; both give equivalent representations of our permutation.

Exercise 9. *Show that* $(n_1, n_2 \ldots, n_k)^{-1} = (n_k, n_{k-1}, \ldots, n_1)$.

Exercise 10. *Show that* $(n_1, n_2, \ldots, n_k) = (n_1, n_k)(n_1, n_{k-1}) \cdots (n_1, n_2)$. *As a consequence, conclude that every permutation can be written as a product of* 2–cycles*: cycles of the form* (m, n).

Exercise 11. *Show that if the permutation p can be written as the product of an even (odd) number of 2–cycles, then every other representation of p as a product of 2–cycles must also have an even (odd) number of factors.*

Thus we may define a permutation to be **even** if it can be written as a product of an even number of 2–cycles; similarly, it is **odd** if it can be written as a product of an odd number of 2–cycles. For example, the permutation $(1,3)(4,6,5)$ is odd, since $(1,3)(4,6,5) = (1,3)(4,5)(4,6)$ — the product of an odd number of cycles.

Exercise 12. *Let A_n denote the set of all even permutations in S_n. Show that A_n is a (sub)group. A_n is called the* alternating group *on n letters.*

3 References

- *Contemporary abstract algebra*, sixth edition, by Joseph A. Gallian; published by Houghton Mifflin Company, 2005; ISBN: 0618514716.
- *Basic algebra I*, second edition, by Nathan Jacobson; published by W. H. Freeman and Company, 1985; ISBN: 0716714809.