Group Theory

Alec Zabel-Mena

Text

Herstein (1965). Topics in Algebra. Blaisdel Publishing Co.

February 26, 2021

Chapter 1

Groups.

1.1 Definitions and Examples

Definition. We call a nonempty set G a **group** under a binary operation $\cdot$ if the following hold:

(1) $a, b \in G$ implies $a \cdot b \in G$.

(2) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) There is an element $e \in G$, called the **identity element** such that $a \cdot e = e \cdot a = a$, for all $a \in G$.

(4) For all $a \in G$, there is a corresponding element a^{-1}, called the **inverse element** of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

We call G **abelian** (or **commutative**) if $a \cdot b = b \cdot a$, for all $a, b \in G$. We call $|G|$ the **order** of G and denote it $\operatorname{ord} G$.

Example 1.1. (1) Let S be an n element set, and let S_n be the set of all $1-1$ mappings of S onto itself (i.e all permutations of elements of S). Then S_n forms a group over function composition $\circ$.

Indeed, whenever $f, g \in S_n$, $f \circ g \in S_n$, likewise, $f \circ (g \circ h) = (f \circ g) \circ h$. The identity map $i : S \to S$ defined by the rule $i : s \to s$ serves as the identity element; $f \circ i = i \circ f = f$. Finally since whenever $f \in G$, f is $1-1$ andd onto, f^{-1} exists and is also $1-1$ and onto; moreover $f \circ f^{-1} = f^{-1} \circ f = i$, so f^{-1} is the inverse of f. It is also easy to see that $\operatorname{ord} S_n = n!$. It is worth noting that S_n is not ingeneral commutative, as $f \circ g \neq g \circ f$.

(2) The integers $\mathbb{Z}$ form a group over $+$ (the usual addition), but not over $\cdot$ (the usual multiplication). The rationals $\mathbb{Q}$ do form a group under $\cdot$. The reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$ form abelian groups under both $+$ and $\cdot$.

(3) Let $G = \{-1, 1\}$m then $(G, \cdot)$ forms a group of order 2, where $\cdot$ is the usual multiplication.

(4) By example 1, we have that S_3 forms a group of order $3! = 6$. Now consider the maps $\phi : 1 \to 2, 2 \to 3, 3 \to 3$ and $\psi : 1 \to 3, 2 \to 3, 3 \to 1$. We can check that $\phi^2 = \psi^3 = i$, also notice that $\phi\psi : 1 \to 2, 2 \to 2, 3 \to 1$ and $\psi\phi : 1 \to 1, 2 \to 3, 3 \to 2$, so $\phi\psi \neq \psi\phi$. Likewise we also have $\psi^2 = \psi\psi : 1 \to 2, 2 \to 1, 3 \to 2$ and $\psi^{-1}\phi : 1 \to 3, 2 \to 2, 3 \to 1$. Indeed, in S_3, $\phi\psi = \psi^{-1}\phi$; it turns out that S_3 is a special case of a more general group.

(5) $\mathbb{Z}/n\mathbb{Z}$ forms an abelian group under $+$ (addition $\mod n$), and that $U(\mathbb{Z}/n\mathbb{Z})$ forms a group under $\cdot$ (multiplication $\mod n$).

(6) If we take $(G, \cdot)$ and $(H, *)$ to be groups, and consider their product $G \times H$, define the binary operation $\times$ by taking $(a, b) \times (c, d) = (a \cdot c, b * d)$, where $a, c \in G$ and $b, d \in H$, then $(g \times H, \times)$ forms a group.

Definition. We say a group G is **cyclic** if for some $g \in G$, $G = \{g^i : i \in \mathbb{Z}\}$. We call g the **generator** of G and write $G = (g)$.

Lemma 1.1.1. *If G is a group, then the following hold:*

(1) The identity element is unique.

(2) Inverses are unique.

(3) $(a^{-1})^{-1} = a$ for all $a \in G$.

(4) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. First suppose that G has an additional identity element f, that is for all $a \in G$, $af = fa = a$. Then we have that (with e the identity of G), $ae = af$, then $(a^{-1}a)e = (a^{-1}a)f$, hence $e = f$.

Now suppose that for some $a \in G$, that a has an additional inverse element x, then $ax = xa = e$, firthermore, since a^{-1} is the inverse of a, we have $aa^{-1} = ax$, applying inverses again we get $(a^{-1}a)a^{-1} = (a^{-1}a)x$, hence $a^{-1} = x$.

We have that $aa^{-1} = e$, and there exists a unique inverse element $(a^{-1})^{-1}$ of a^{-1}, hence $a(a^{-1}(a^{-1})^{-1}) = (a^{-1})^{-1}$, hence we get that $a = (a^{-1})^{-1}$.

Finally, we have that $ab(ab)^{-1} = e$, then $(a^{-1}a)b(ab)^{-1} = a^{-1}$, and so $b^{-1}b(ab)^{-1} = (ab)^{-1} = b^{-1}a^{-1}$. ■

Lemma 1.1.2 (The Cancelation laws)**.** *Let G be a group with $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solutions. Moreover for $u, w \in G$, $au = aw$ implies $u = w$ and $ua = wa$ implies $u = w$.*

Proof. We have that $x = a^{-1}b$ and $y = ba^{-1}$ are the unique solutions to the equations. Now for $u, w \in G$, we have that $au = aw$ has as solution $u = (a^{-1}a)w = w$, the same holds for $ua = wa$. ■

Definition. Let G be a group, for $x \in G$, we define the **order** of x to be the smallest positive integer n such that $x^n = e$, and denote it $\operatorname{ord} x = n$. If no such n exists, then we say that x has infinite order and write $\operatorname{ord} x = \infty$.

1.2 The Dihedral Group.

As we noted in a previous example, the group S_3 is a special case of a more broad group of permutations. We can recall that $\phi^2 = \psi^3 = i$, and that $\phi\psi = \psi^{-1}\phi$, and indeed $\operatorname{ord} S_3 = 6 = 3! = 2(3)$. We would like to generalize this group structure further.

Theorem 1.2.1. *Let $n \in \mathbb{Z}^+$ and let D_{2n} be the set of all symmetries of a regular n-gon; that is the set of all permutation of points of the n-gon, defined by two maps $\tau : A \to -A$ which is a transposition of opposite vertices, and $\rho : A \to A+1$ which is a rotation of the vertices about an angle of $\frac{2\pi}{n}$. Then D_{2n} forms a group under function composition.*

Proof. Let S be a regular n-gon with vertices $0, 1, \ldots, n$. Notice that $\tau, \rho \in S_n$, so they are $1-1$ maps of the n-gon onto itself. By our definitions of τ and ρ, we have that $\tau : i \to n-1$ and $\rho : i \to i+1$. Hence $\tau\rho : i \to n-i \to n-i+1$, which must coinide with some given vertex of S, hence $\tau\rho \in D_{2n}$; moreover, D_{2n} inherits associativity from function composition.

Now let $\iota : i \to i$ be the symmetry that leaves points unchange in S, clearly ι is the identity map, and so $\tau\rho = \iota\tau\rho = \tau\rho$.

Now how do we find the inverses? Notice that $\tau : n-i \to i$, hence $\tau^2 : i \to n-i \to i$, that is $\tau^2 = \iota$, and also notice that $\rho^n : i \to i+1 \to i+2 \to \cdots \to i+n = i$, so $\rho^n = \iota$. This shows that $\tau = \tau^{-1}$ and $\rho^{n-1} = \rho^{-1}$. Then if $y \in D_{2n}$ such that $\tau\rho y = \iota$, then $\rho y = \tau$, and $y = \tau\rho^{n-1}$. Checking we get that $\tau\rho(\tau\rho^{n-1}) = (\tau\rho^{n-1})\tau\rho = \iota$. Therefore D_{2n} is a group under $\circ$. ∎

Corollary. $D_{2n} = 2n$.

Proof. We have that there are n possible vertices to which i can mapped to via ρ, so already there are n possible ρ. Now we also have that $\tau : i \to n-1$, which means that i under τ can only be mapped to $n-1$. Since the elements of D_{2n} are obviously of the form $\tau\rho^j$, for $1 \leq j \leq n$, we see there are n possible $\tau\rho^j$. Therefore, there are $2n$ total symmetries of the n-gon. ∎

Remark. Now since D_{2n} is obviously finite, ($\operatorname{ord} D_{2n}$ need not be known), then we can simply enumerate all the elements of D_{2n}, which are $D_{2n} = \{\iota, \tau, \rho, \rho^2, \ldots \rho^{n-1}, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$. It is also worth noting that if $\tau\rho^i = \tau\rho^j$, then $\rho^i = \rho^j$, hence $i = j$, that is the elements of R_{2n} are well defined.

Corollary. $\rho\tau = \tau\rho^{-1}$.

Proof. By direct computation, notice that $\rho\tau : i \to n-1 \to n-i+1$ and $\tau\rho^{-1} : i \to i-1 \to n-(i-1) = n-i+1$ (We can consider ρ^{-1} also to be a rotation about the angle of $-\frac{2\pi}{n}$, hence it takes any vertex i to $i-1$). Hence $\rho\tau = \tau\rho^{-1}$. ∎

Remark. This also shows that $\tau\rho \neq \rho\tau$, hence D_{2n} is not commutative.

Corollary. *For $i \in \mathbb{Z}^+$ with $1 \leq i \leq n$, $\rho^i\tau = \tau\rho^{-i}$.*

Proof. Bu induction, the previous corollary gives $\rho^1\tau = \tau\rho^{-1}$. Now suppose that for all $1 \leq i \leq n$, that $\rho^i\tau = \tau\rho^{-i}$, and consider ρ^{i+1}. If $i+1 = n$, then we are done, so take $i+1 < n$. Then $\rho^{i+1}\tau = \rho(\rho^i\tau) = (\rho\tau)\rho^{-i} = \tau(\rho^{-1}\rho^{-i}) = \tau\rho^{-i-1}$. ∎

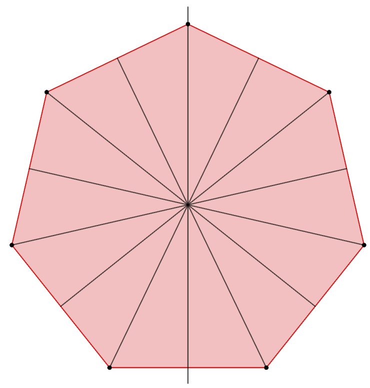

Figure 1.1: The dihedral group D_{14} on 7 points.

Definition. We call the group D_{2n} of symmetries of the regular n-gon the **dihedral group** of order $2n$.

Now we see that both τ and ρ generate D_{2n}, furthermore, we have the relations $\tau^2 = \iota$ and $\rho^n = \iota$ and $\rho\tau = \tau\rho^{-1}$. This motivates the idea of "generators" of arbitrary groups.

Definition. Let G be a group with $S \subseteq G$. We call S a set of **generators** of G if every element in G can be written as a finite product of elements of S and their inverses. We say that S **generates** G and write $G = (s)$. We call a **relation** of the group any equation satisfied by the generators of G.

Example 1.2. (1) If G is any group, and S is the set of generators of G with $|S| = 1$, then G is a cyclic group.

(2) In $(\mathbb{Z}, +)$, $\{1\}$ generates $\mathbb{Z}$, so $\mathbb{Z} = \{1\}$.

(3) In D_{2n}, we have that $\{\tau, \rho\}$ generate all of D_{2n}, so $D_{2n} = (\tau, \rho)$. and D_{2n} has the relations $\tau^2 = \iota$, $\rho^n = \iota$ and $\rho\tau = \tau\rho^{-1}$.

We can also write G in terms of just its generators and relations as $G = \{S : R_1, \ldots, R_m\}$, where R_i is a relation of the generators for $1 \leq i \leq m$. Then for the dihedral group, we have $D_{2n} = \{\tau, \rho : \tau^2 = \rho^n = \iota,\ \rho\tau = \tau\rho^{-1}\}$

1.3 Symmetric Groups.