

# A Few Notes on Cayley's Theorem

David Meyer

dmm@{1-4-5.net,uoregon.edu}

Last update: March 19, 2019

## 1 Introduction

Group Theory is the study of symmetry. Cayley's Theorem is a fundamental theorem in Group Theory, and the topic of these notes.

Before diving into Cayley's Theorem, a couple of notes:

- The Symmetric Group  $Sym(G)$  or sometimes  $S_n$ , where  $n = |G|$  ( $G$  is finite), is the set of all bijections from  $G$  to itself with function composition as the group operation. That is,  $Sym(G) = S_n = S_{|G|} = \{f : G \rightarrow G \mid f \text{ is an bijection}\}$ .
- We use the symbol  $\simeq$  (or sometimes  $\cong$ ) to mean that the groups  $G$  and  $H$  are *isomorphic*. That is,  $G \simeq H \implies \exists f \mid f : G \rightarrow H$  where  $f$  is a bijection and a homomorphism. See Equation 1.
- To show that  $f$  is one-to-one, show that  $f(x) = f(y) \implies x = y$ .
- To show that  $f$  is onto, pick an arbitrary  $h \in H$  and show that  $\exists g \in G \mid f(g) = h$ .

Recall also that if we have two groups  $(G, *)$  and  $(H, \cdot)$  we say that  $(G, *)$  is *isomorphic* to  $(H, \cdot)$  if there exists a bijection  $f : G \rightarrow H$  which satisfies the *homomorphism* property:

$$f(x * y) = f(x) \cdot f(y) \quad \forall x, y \in G \tag{1}$$

That is,  $f$  is a bijection (one-to-one and onto) and  $f$  is also a homomorphism.

Any bijective function  $f$  which satisfies Equation 1 is called a *group isomorphism* from  $G$  to  $H$ . The basic idea of  $(G, *)$  being isomorphic to  $(H, \cdot)$  is that  $(G, *)$  and  $(H, \cdot)$  are "algebraically equivalent". That is, there is a one-to-one correspondence between elements of  $G$  and elements of  $H$  where the outcomes of operations on elements of  $G$  are matched with the outcomes of the corresponding operations on the corresponding elements of  $H$ .

## 2 Cayley's Theorem

**Theorem 2.1. Cayley's Theorem:** If  $G$  is a group then there exists a subgroup  $H$  of  $Sym(G)$  such that  $G$  is isomorphic to  $H$ .

**Proof:** Suppose that  $G$  is a group. Then to prove Cayley's Theorem we need to find a subgroup  $H$  of  $Sym(G)$  and a bijective homomorphism  $f : G \rightarrow H$ . My roadmap for the proof looks like

1. Define  $\phi_a : G \rightarrow G$  for each  $a \in G$  and show that  $\phi_a$  is a bijection
2. Define  $H = \{\phi_a \mid a \in G\}$  and show that  $H$  is a subgroup of  $Sym(G)$
3. Define  $f : G \rightarrow H$  and show that  $f$  is both a bijection and a homomorphism

BTW, a nice thing about the proof of Cayley's theorem is that it is a *constructive* proof: the statement of the theorem is that a certain group  $H$  exists. In the course of the proof of the theorem one can actually show not only that such an  $H$  exists but also how to actually find it. We'll see an example of this below (Section 3.2).

### 2.1 Define $\phi_a : G \rightarrow G$ for each $a \in G$ and show that $\phi_a$ is a bijection

To start, for each fixed element  $a \in G$  define  $\phi_a : G \rightarrow G$  by the map  $x \mapsto ax$ . That is

$$\phi_a(x) = ax \quad \forall x \in G \tag{2}$$

Luckily it turns out that each  $\phi_a$  is a bijection. To see this we need to show that  $\phi_a$  is one-to-one and onto. First, consider that  $\phi_a$  is one-to-one since

$$\begin{aligned} \phi_a(x) &= \phi_a(y) && \# \text{ to show } \phi_a \text{ is 1-to-1 show } \phi_a(x) = \phi_a(y) \Rightarrow x = y \\ \Rightarrow ax &= ay && \# \text{ definition of } \phi_a(x) \text{ (Equation 2)} \\ \Rightarrow a^{-1}(ax) &= a^{-1}(ay) && \# \text{ multiply by } a^{-1}; a \in G \ \& \ G \text{ a group} \Rightarrow a^{-1} \in G \\ \Rightarrow (a^{-1}a)x &= (a^{-1}a)y && \# \text{ multiplication is associative} \\ \Rightarrow x &= y && \# a^{-1}a = 1 \end{aligned} \tag{3}$$

So  $\phi_a$  is one-to-one.

**Aside on cancellation laws:** Note that in (3) we used the fact that  $a \in H$  and that  $H$  is a group so  $a^{-1} \in H$ . Here we have  $a^{-1}a = 1$ , which essentially gives us a *cancellation*

$law^1$ ; in (3) this allows us to "cancel" the  $a$  on both sides. Now, what if we don't have access to multiplicative inverses? We might be faced with this situation if we have a ring, where we don't in general have multiplicative inverses<sup>2</sup>. So if we don't have multiplicative inverses how do we go about showing that something is one-to-one?

One approach is to factor out  $a$  and note that by assumption,  $a \neq 0$  so something else must be. For example

$$\begin{array}{lll}
 \phi_a(x) = \phi_a(y) & & \# \text{ to show } \phi_a \text{ is 1-to-1 show that } \phi_a(x) = \phi_a(y) \Rightarrow x = y \\
 \Rightarrow ax = ay & & \# \text{ definition of } \phi_a(x) \text{ (Equation 2)} \\
 \Rightarrow ax - ay = 0 & & \# \text{ subtract } ay \text{ from both sides} \\
 \Rightarrow a(x - y) = 0 & & \# \text{ factor out } a \\
 \Rightarrow x - y = 0 & & \# a \neq 0 \text{ by assumption so } x - y = 0 \\
 \Rightarrow x = y & & \# \text{ so } \phi_a \text{ is one-to-one}
 \end{array}$$

Getting back to showing that  $\phi_a$  is a bijection, we next need to show that  $\phi_a$  is onto. To do this pick an arbitrary  $y \in G$  (here  $G$  is the range). Then  $a^{-1}y \in G$  (here  $G$  is the domain) and so  $\phi_a(a^{-1}y) = a(a^{-1}y)$ . Since multiplication is associative we have  $\phi_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y$ . So  $\phi_a$  is onto and hence  $\phi_a$  is a bijection.

## 2.2 Define $H = \{\phi_a \mid a \in G\}$ and show that $H$ is a subgroup of $Sym(G)$

Now we can define  $H = \{\phi_a \mid a \in G\}$ . Since each element of  $H$  is a bijection from  $G$  to  $G$  and since  $Sym(G)$  is the set of all bijections from  $G$  to  $G$  we know that  $H \subseteq G$ . To show that  $H$  is a subgroup of  $Sym(G)$  we also need to show that  $H$  is closed under function composition and inversion.

To show closure under function composition we need to show that  $\alpha, \beta \in H \Rightarrow \alpha \circ \beta \in H$ . To see this consider  $\alpha, \beta \in H$ . Then there exists  $a \in G$  such that  $\alpha = \phi_a$ . Similarly there exists  $b \in G$  such that  $\beta = \phi_b$ . So we know that

$$\alpha \circ \beta = \phi_a \circ \phi_b \tag{4}$$

and so for any  $x \in G$  we have

---

<sup>1</sup>Note that having a cancellation law is equivalent to saying there are no *zero divisors*.

<sup>2</sup>A ring with multiplicative inverses is called a division ring (or skew field). Example: the quaternions.

$$\begin{aligned}
(\alpha \circ \beta)(x) &= (\phi_a \circ \phi_b)(x) && \# \alpha \circ \beta = \phi_a \circ \phi_b \text{ (Equation 4)} \\
&= \phi_a(\phi_b(x)) && \# \text{definition of function composition} \\
&= \phi_a(bx) && \# \phi_b(x) = bx \text{ (definition of } \phi_b) \\
&= a(bx) && \# \phi_a(x) = ax \text{ (definition of } \phi_a) \\
&= (ab)x && \# \text{multiplication is associative} \\
&= \phi_{ab}(x) && \# \phi_g(x) = gx \text{ where } g = ab
\end{aligned} \tag{5}$$

So  $\alpha \circ \beta = \phi_a \circ \phi_b = \phi_{ab}$ . Since  $ab \in G$  ( $G$  is closed under multiplication) we know that  $\phi_{ab} \in H$ . Now we have  $\phi_{ab} \in H$  and  $\alpha \circ \beta = \phi_{ab}$  which together imply that  $\alpha \circ \beta \in H$ . So  $H$  is closed under function composition.

To show that  $H$  is closed under inversion we need to show that  $\alpha \in H \Rightarrow \alpha^{-1} \in H$ . To see this consider  $\alpha \in H$ . Then there exists an  $a \in G$  such that  $\alpha = \phi_a$ . Since  $a \in G$  and since  $G$  is a group,  $a^{-1} \in G$  and so  $\phi_{a^{-1}} \in H$ . Note further that for any  $x \in G$

$$\begin{aligned}
(\phi_{a^{-1}} \circ \phi_a)(x) &= \phi_{a^{-1}}(\phi_a(x)) && \# \text{definition: } (f \circ g)(x) = f(g(x)) \\
&= \phi_{a^{-1}}(ax) && \# \phi_a(x) = ax \\
&= a^{-1}(ax) && \# \text{definition: } \phi_{a^{-1}}(x) = a^{-1}(x) \\
&= (a^{-1}a)x && \# \text{multiplication is associative} \\
&= x && \# a^{-1}a = 1
\end{aligned} \tag{6}$$

and

$$\begin{aligned}
(\phi_a \circ \phi_{a^{-1}})(x) &= \phi_a(\phi_{a^{-1}}(x)) && \# \text{definition: } (f \circ g)(x) = f(g(x)) \\
&= \phi_a(a^{-1}x) && \# \phi_{a^{-1}}(x) = a^{-1}x \\
&= a(a^{-1}x) && \# \text{definition: } \phi_a(x) = ax \\
&= (aa^{-1})x && \# \text{multiplication is associative} \\
&= x && \# aa^{-1} = 1
\end{aligned} \tag{7}$$

Recall that if a function  $f$  is a bijection we know  $(f^{-1} \circ f)(x) = (f \circ f^{-1})(x) = x$ . From (6) and (7) we see that  $\phi_{a^{-1}}$  is the inverse of  $\phi_a$ . More specifically  $\phi_{a^{-1}} = \phi_a^{-1}$ . Since  $\alpha = \phi_a$ ,  $\alpha^{-1} = \phi_a^{-1} = \phi_{a^{-1}} \in H$ . So  $H$  is closed under inversion.

### 2.3 Define $f : G \rightarrow H$ and show that $f$ is a homomorphic bijection

We still need to show a homomorphic bijection  $f$  from  $G$  to  $H$ . One way to do this is to define  $f(g) = \phi_g$  for all  $g \in G$ . Then to show that  $f$  is a bijection we need to show that  $f$  is both one-to-one and onto.

To see that  $f$  is one-to-one consider

$$\begin{array}{lll}
 f(a) = f(b) & & \# \text{ to show } f \text{ is 1-to-1 show that } f(a) = f(b) \Rightarrow a = b \\
 \Rightarrow \phi_a(x) = \phi_b(x) & & \# \text{ definition of } f(g) : f(g) = \phi_g \text{ for all } g \in G \\
 \Rightarrow \phi_a(a) = \phi_b(a) & & \# \text{ evaluate at } a \in G \\
 \Rightarrow aa = ba & & \# \text{ definition of } \phi_g : \phi_g(x) = gx \text{ for all } g \in G \\
 \Rightarrow (aa)a^{-1} = (ba)a^{-1} & & \# \text{ multiply by } a^{-1}; a \in G \text{ and } G \text{ a group } \Rightarrow a^{-1} \in G \\
 \Rightarrow a(aa^{-1}) = b(aa^{-1}) & & \# \text{ multiplication is associative} \\
 \Rightarrow a = b & & \# aa^{-1} = 1
 \end{array}$$

So  $f$  is one-to-one.

To show that  $f$  is onto, choose a  $\alpha \in H$ . Then there exists an  $a \in G$  such that  $\alpha = \phi_a$ . However we know that  $f(a) = \phi_a$  and  $\phi_a = \alpha$  so we know that  $f(a) = \alpha$ . So  $f$  is onto and since we saw that  $f$  is one-to-one,  $f$  is a bijection.

Finally, to show that  $f$  is also a homomorphism we want to show that  $f(ab) = f(a) \circ f(b)$ . To see this consider that for any  $a, b \in G$  we have

$$\begin{array}{lll}
 f(ab) = \phi_{ab} & & \# \text{ definition of } f \\
 = \phi_a \circ \phi_b & & \# \text{ Equation 5} \\
 = f(a) \circ f(b) & & \# \text{ definition of } f
 \end{array}$$

So  $f$  is a homomorphism.

This completes the proof of Cayley's Theorem.

### 3 Examples

#### 3.1 $(\mathbb{Z}_4, +) \rightarrow (G, \cdot)$

Let  $(\mathbb{Z}_4, +)$  be the set  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$  with addition modulo 4 and let  $(G, \cdot)$  be the set  $G = \{1, -1, i, -i\}$  (the fourth roots of unity) with the usual multiplication on  $\mathbb{C}$ . Then  $(\mathbb{Z}_4, +) \simeq (G, \cdot)$ . To see that  $\mathbb{Z}_4$  is isomorphic to  $G$ , let  $f : \mathbb{Z}_4 \rightarrow G$  be the bijection

$$\begin{array}{ll}
 0 & \longrightarrow 1 \\
 1 & \longrightarrow i \\
 2 & \longrightarrow -1 \\
 3 & \longrightarrow -i
 \end{array}$$

|   |   |   |   |   |
|---|---|---|---|---|
| + | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Table 1:  $\mathbb{Z}_4$

|      |      |      |      |      |
|------|------|------|------|------|
| ·    | 1    | $i$  | -1   | $-i$ |
| 1    | 1    | $i$  | -1   | $-i$ |
| $i$  | $i$  | -1   | $-i$ | 1    |
| -1   | -1   | $-i$ | 1    | $i$  |
| $-i$ | $-i$ | 1    | $i$  | -1   |

Table 2:  $G$

Here are the Cayley tables for  $\mathbb{Z}_4$  and  $G$ :

To show that  $f$  is an isomorphism we need to show that  $f$  is a homomorphism, that is, that  $f(x + y) = f(x) \cdot f(y)$ . Since there are only  $n^2 = 4^2 = 16$  values for  $f(x + y)$  we can just enumerate them:

$$\begin{aligned}
 f(0+0) &= f(0) = 1 = 1 \cdot 1 = f(0) \cdot f(0) \\
 f(0+1) &= f(1) = i = 1 \cdot i = f(0) \cdot f(1) \\
 f(0+2) &= f(2) = -1 = 1 \cdot -1 = f(0) \cdot f(2) \\
 f(0+3) &= f(3) = -i = 1 \cdot -i = f(0) \cdot f(3) \\
 f(1+0) &= f(1) = i = i \cdot 1 = f(1) \cdot f(0) \\
 f(1+1) &= f(2) = -1 = i \cdot i = f(1) \cdot f(1) \\
 f(1+2) &= f(3) = -i = i \cdot -1 = f(1) \cdot f(2) \\
 f(1+3) &= f(0) = 1 = i \cdot -i = f(1) \cdot f(3) \\
 f(2+0) &= f(2) = -1 = -1 \cdot 1 = f(2) \cdot f(0) \\
 &\vdots \\
 f(3+3) &= f(2) = -1 = -i \cdot -i = f(3) \cdot f(3)
 \end{aligned}$$

So the bijection  $f : \mathbb{Z}_4 \rightarrow G$  above is a homomorphism and hence  $f$  is a group isomorphism.

### 3.2 The Klein 4-group

The Klein 4-group is the group  $K = \{e, a, b, c\}$  where  $e$  is the identity element and the group operation is defined by the Cayley table below (Table 3).

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
|     | $e$ | $a$ | $b$ | $c$ |
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

Table 3: The Klein 4-group Operation

Here  $K$  is *not* isomorphic to  $\mathbb{Z}_4$ . To see this notice that there are 24 bijections from  $\mathbb{Z}_4$  and  $K$ :  $|K| = |\mathbb{Z}_4| = 4$  so there are  $n! = 4! = 24$  possible bijections from  $\mathbb{Z}_4$  to  $K$ . Since we need  $f(0) = e$  that leaves  $3! = 6$  bijections that could be homomorphisms. For example, consider the bijection

$$\begin{array}{lcl} 0 & \longrightarrow & e \\ 1 & \longrightarrow & a \\ 2 & \longrightarrow & c \\ 3 & \longrightarrow & b \end{array}$$

This bijection is not a homomorphism since  $f(1+3) = f(4) = f(0) = e$  while  $f(1) \cdot f(3) = ab = c$ , so  $f(1+3) \neq f(1) \cdot f(3)$ .

One way to see that  $\mathbb{Z}_4$  is not isomorphic to  $K$  is to recognize that every element of  $K$  satisfies the equation  $x \cdot x = e$  (a key property of the Klein 4-group). However not every element of  $\mathbb{Z}_4$  satisfies the equation  $x + x = 0$ .

This gives a clue as to how to prove, by contradiction, that  $\mathbb{Z}_4$  is not isomorphic to  $K$ . Specifically, suppose that  $\mathbb{Z}_4$  is isomorphic to  $K$ . Then there exists a bijection  $f : \mathbb{Z}_4 \rightarrow K$  such that  $f(x+y) = f(x) \cdot f(y)$  for all  $x, y \in \mathbb{Z}_4$ . Well, we know by definition that  $f(0) = e$  and since  $f$  is one-to-one we also know that  $f(1) \neq e$ . Since  $f$  is a homomorphism we also know that

$$f(1+1) = f(1) \cdot f(1)$$

However, since  $f(1) \in K$  and all elements of  $K$  satisfy  $x \cdot x = e$  we can conclude that  $f(1) \cdot f(1) = e$ , so  $f(1+1) = f(2) = e$ . Now we have  $f(0) = e$  and  $f(2) = e$  which is a contradiction since we assumed that  $f$  was one-to-one. So the original assumption that  $\mathbb{Z}_4$  is isomorphic to  $K$  is false.

Ok, but Cayley's Theorem says there is a subgroup  $H$  of  $S_4$  which is isomorphic to  $K$ . How to find  $H$ ? Since as noted above Cayley's Theorem is constructive, we should be able to follow the approach used in the proof to find  $H$ . Here we let  $H = \{\phi_e, \phi_a, \phi_b, \phi_c\}$  where, for all  $x \in K$

$$\begin{array}{ll} \phi_e(x) = ex & \# \phi_e(x) = x \\ \phi_a(x) = ax & \\ \phi_b(x) = bx & \\ \phi_c(x) = cx & \end{array}$$

Now we can rewrite the Cayley table for the Klein 4-group (Table 3) as

$$\begin{aligned}\phi_e &= \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} \\ \phi_a &= \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} \\ \phi_b &= \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} \\ \phi_c &= \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}\end{aligned}$$

Now, if we relabel  $K$  by the bijection

$$\begin{array}{cccc} e & a & b & c \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{array}$$

we can represent  $K$  in cyclic notation:

$$\begin{aligned}\phi_e &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) \\ \phi_a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) \\ \phi_b &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24) \\ \phi_c &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)\end{aligned}$$

Now we can see that  $K \simeq H$  where  $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ . That is,  $f : K \rightarrow H$  is the bijection

$$\begin{array}{cccc} f : & 1 & 2 & 3 & 4 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ & (1) & (12)(34) & (13)(24) & (14)(23) \end{array}$$

The Klein 4-group  $K$  has many other interesting properties, including

- $K$  is the smallest non-cyclic group
- $K$  is the underlying group of the four-element field



- $K$  is the symmetry group of a non-square rectangle
- $K$  is the group of bitwise exclusive or operations on two-bit binary values
- $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ , the direct product of two copies of the cyclic group of order 2

## 4 Acknowledgements

# References