Section I.4. Groups

Note. The text gives an argument on pages 36 and 37 to motivate the idea that "groups" are really related to what we classically call "algebra."

Definition 4.1. A *group* $\langle G, *\rangle$ is a set G and a binary operation on G such that G is closed under $*$ and

$\mathcal{G}_1$ For all $a, b, c \in G$, $*$ is *associative*:

$$(a * b) * c = a * (b * c).$$

$\mathcal{G}_2$ There is $e \in G$ called the *identity* such that for all $x \in G$:

$$e * x = x * e = x.$$

$\mathcal{G}_3$ For all $a \in G$, there is an *inverse* $a' \in G$ such that:

$$a * a' = a' * a = e.$$

Example. Some familiar infinite groups include $\langle \mathbb{R}, +\rangle$, $\langle \mathbb{Z}, +\rangle$, $\langle \mathbb{Q}, +\rangle$, and $\langle \mathbb{C}, +\rangle$. Another infinite group is the set of all $n \times n$ invertible matrices under matrix multiplication. This is denoted $GL(n, \mathbb{R})$, called the *general linear group of order n*.

Example. The text also mentions the infinite group of complex numbers of the form $e^{i\theta}$ where $\theta \in \mathbb{R}$ under multiplication, denoted $\langle U, \cdot\rangle$.

Example. The finite group of integers modulo n under addition, $\langle \mathbb{Z}_n, +_n \rangle$, is a group. The nth roots of unity in the complex plane, $\langle U_n, \cdot \rangle$, form a finite group under multiplication. In fact, these are isomorphic binary structures (and hence, isomorphic groups).

Definition 4.3. A group $\langle G, * \rangle$ (or just "G" for short) is *abelian* if its binary operation is commutative.

Note. The groups $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, and $\langle \mathbb{C}, + \rangle$, $\langle U, \cdot \rangle$, $\langle \mathbb{Z}_n, +_n \rangle$, and $\langle U_n, \cdot \rangle$ are all abelian groups. The group of invertible $n \times n$ matrices under matrix multiplication is a nonabelian group.

Example 4.8. The sets $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ of nonzero numbers under multiplication are abelian groups.

Exercise 4.8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4(7) + 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.

Exercise 4.18. Consider the set of all $n \times n$ matrices with determinant either 1 or -1 under matrix multiplication. Does this form a group? Recall that for $n \times n$ matrices A and B, we have $\det(AB) = \det(A)\det(B)$, $\det(I_n) = 1$, and that A is invertible if and only if $\det(A) \neq 0$.

Note. At this stage, the only things we know about groups are the things given in the definition. We'll prove other properties now—you should not assume additional properties that the above examples have as properties of all groups. Without proofs, we have nothing but the definition.

Theorem 4.15. If $\langle G, * \rangle$ is a group, then

1. $a * b = a * c$ implies $b = c$, and
2. $b * a = c * a$ implies $b = c$

for all $a, b, c \in G$. These properties are called the *left and right cancellation laws*, respectively.

Note. The following result shows that the equations of the form $a * x = b$ and $y * a = b$ have unique solutions for all $a, b \in G$. This implies that the table for a group must have every element of the group in each row and each column of the group.

Theorem 4.16. If $\langle G, * \rangle$ is a group, then the equations $a * x = b$ and $y * a = b$ have unique solutions x and y for all $a, b \in G$.

Theorem 4.17a. In group $\langle G, * \rangle$, there is only one element $e \in G$ such that $e * x = x * e = x$ for all $x \in G$.

Theorem 4.17b. In a group $\langle G, * \rangle$, for given $a \in G$ there is only one element $a' \in G$ such that $a' * a = a * a' = e$. That is, inverses are unique.

Corollary 4.18. Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$.

Theorem. Suppose $*$ is a binary operation on a set G. Then $\langle G, * \rangle$ is a *group* if

1. $*$ is associative,
2. there exists $e_\ell \in G$ such that for all $x \in G$, $e_\ell * x = x$ (e_ℓ is called a *left identity*), and
3. for each $a \in G$, there exists $a' \in G$ such that $a' * a = e_\ell$ (a' is a *left inverse* of a).

Proof. (Exercise 4.38). We need to establish $\mathcal{G}_1$ (which is **1**), $\mathcal{G}_2$ and $\mathcal{G}_3$. For $\mathcal{G}_2$ let $x \in G$ and consider $x * e_\ell$. For x' the left inverse of x, we have

$$\begin{aligned} x' * (x * e_\ell) &= (x' * x) * e_\ell \text{ by } \mathbf{1} \\ &= e_\ell * e_\ell \text{ since } x' \text{ is a left inverse of } x \\ &= e_\ell \text{ since } e_\ell \text{ is a left identity.} \end{aligned}$$

So x' is a left inverse of x and also a left inverse of $x * e_\ell$. However, left cancellation holds and $x' * x = x' * (x * e_\ell)$ implies that $x = x * e_\ell$. Therefore e_ℓ is a left and a right inverse.

For $\mathcal{G}_3$, suppose $a' * a = e_\ell$ and consider $a * a'$. We have

$$\begin{aligned} a' * (a * a') &= (a' * a) * a' \text{ by } \mathbf{1} \\ &= e_\ell * a' = a' \\ &= a' * e_\ell \text{ by the above result.} \end{aligned}$$

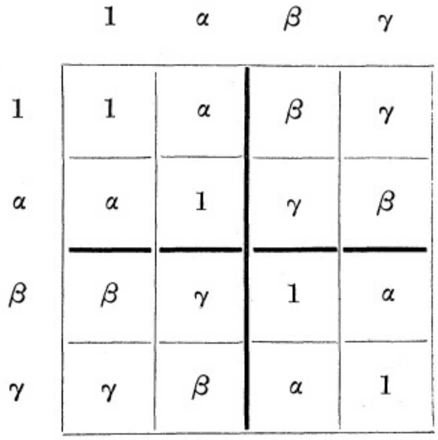
However, left cancellation holds and $a' * (a * a') = a' * e_\ell$ implies $a * a' = e_\ell$. Therefore a' is also a right inverse of a. ∎

Note. Of course, the previous result holds with "left" replaced with "right." The benefit of a result like the previous one is that a binary structure can be shown to be a group by showing (1) associativity, (2) a left identity, and (3) a left inverse for each element. We know that we are then guaranteed the right hand identity and inverses.

Note. For finite groups, we can draw a table illustrating the binary operation, as before. Since the equations $a * x = b$ and $y * a = b$ have solutions x and y for all a, b (Theorem 4.16), then each element of the group must appear in each row and each column of the table.

Note. On pages 43–45, Fraleigh argues that there is only one group with one element, only one group with two elements, and only one group with three elements. Technically, all groups of these given sizes are isomorphic.

Historical Note. The "multiplication table" for a group is sometimes called a *Cayley table* for the group. This is due to the fact that Arthur Cayley first introduced the idea of a group in his 1854 paper "On The Theory of Groups, As Depending on the Symbolic Equation $\theta^n = 1$," *Philosophical Magazine*, **7** (1854), 40-47. This work is available in *The Collected Mathematical Works* of Arthur Cayley (pages 123–130) which can be found in Google books (and can be downloaded in PDF). An example of one of the tables is the following:



	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

You will encounter this group in the next section as the Klein-4 group.

Revised: 7/7/2023