Section I.5. Subgroups

Note. Just as a vector space can have a subspace, as you see in linear algebra, a group can have a subgroup. As with vector spaces, this would be a sub<u>set</u> with all the structure of a <u>group</u>.

Definition 5.3. If G is a group, then the *order* $|G|$ of G is the number of elements in G.

Note. We will primarily study finite groups where the above definition is clear. However, we will occasionally study infinite groups (such as $\langle \mathbb{R}, + \rangle$).

Definition 5.4. If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a *subgroup* of G. We denote this as $H \leq G$ or $G \geq H$. If H is a subgroup of G and $H \neq G$, we write $H < G$ or $G > H$.

Example. $\langle \mathbb{Z}, + \rangle < \langle \mathbb{Q}, + \rangle < \langle \mathbb{R}, + \rangle < \langle \mathbb{C}, + \rangle$.

Example From Linear Algebra. $\langle \text{span}\{\hat{\imath}, \hat{\jmath}\}, + \rangle < \langle \text{span}\{\hat{\imath}, \hat{\jmath}, \hat{k}\}, + \rangle$.

Example 5.8. The nth roots of unity in $\mathbb{C}$ form a subgroup U_n of the group $\langle \mathbb{C}^*, \cdot \rangle$ (recall that $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$).

Definition 5.5. If G is a group, then G itself is a subgroup of G called the *improper subgroup* of G; all other subgroups are *proper subgroups*. The subgroup $\{e\}$ is the *trivial subgroup*; all other subgroups are *nontrivial subgroups.*

Example 5.9. There are two (nonisomorphic) groups of order 4. One is $\langle \mathbb{Z}_4, +_4 \rangle = \mathbb{Z}_4$:

$$\mathbb{Z}_4 : \quad \begin{array}{c|cccc} +_4 & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$$

Then $\mathbb{Z}_4$ has three subgroups:

1. the trivial group $\{0\}$,
2. the nontrivial, proper subgroup $\{0, 2\}$, and
3. the improper subgroup $\mathbb{Z}_4$.

The other group of order 4 is the *Klein 4-group*, denoted V ("V" for the German *vier* for four):

$$V : \quad \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

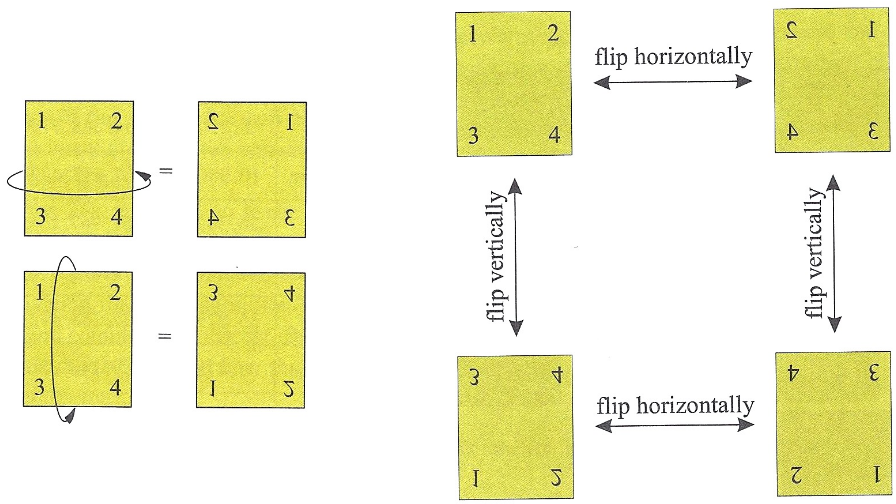
Notice that every element of V is its own inverse and this is not the case with $\mathbb{Z}_4$, so the two groups are <u>not</u> isomorphic. V has five subgroups:

1. the trivial group $\{e\}$,
2. the nontrivial, proper subgroup $\{e, a\}$,
3. the nontrivial, proper subgroup $\{e, b\}$,
4. the nontrivial, proper subgroup $\{e, c\}$, and
5. the improper subgroup V.

Note. We can make a subgroup diagram (sometimes called a *Hasse diagram*) for $\mathbb{Z}_4$ and V as follows:

$$\begin{tikzcd}
\mathbb{Z}_4 \arrow[d, dash] \\
\{0,2\} \arrow[d, dash] \\
\{0\}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
& V \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{e,a\} \arrow[dr, dash] & \{e,b\} \arrow[d, dash] & \{e,c\} \arrow[dl, dash] \\
& \{e\} &
\end{tikzcd}$$

Note. We will see in Section II.8 that every group is a group of "permutations." This gives us the opportunity to visualize groups in terms of how they act on various items. For example, suppose we have a rectangle (not a square) with numbered corners. We want to see how many ways we can pick up the rectangle, rotate of flip it around, and place it back in its original position. Different configurations can be determined from the different arrangements of the labeled corners. The figure below shows that there are four configurations of the rectangle. These configurations can be generated by the two movements labeled "flip horizontally" and "flip vertically." The group of order 4 which describes these "symmetries" of a rectangle is isomorphic to the Klein 4-group.



Figures from *Visual Group Theory* by Nathan Carter, New York: Mathematical Association of America, 2009.

Note. We now state a result which allows us to check a group for nontrivial, proper subgroups. We also start using multiplicative notation to represent inverses: $a' = a^{-1}$.

Theorem 5.14. A subset H of a group G is a subgroup of G if and only if:

1. H is closed under the binary operation of G,

2. the identity element e of G is in H, and

3. for all $a \in H$ we have $a' = a^{-1} \in H$.

Exercise 5.10. Is the set of upper triangular $n \times n$ matrices with no zeros on the diagonal a subgroup of $GL(n, \mathbb{R})$? **Answer.** Yes.

Exercise 5.16. Let F be the set of all real-valued functions with domain $\mathbb{R}$ and let $\tilde{F}$ be the subset of F consisting of those functions that have a nonzero value at every point in $\mathbb{R}$. Is the subset of all $f \in \tilde{F}$ such that $f(1) = 1$ a subgroup of F

(a) under addition? **Answer.** No; not closed.

(b) under multiplication? **Answer.** Yes; identity is $f(x) \equiv 1$ and g^{-1} is $1/g(x)$.

Theorem 5.17. Let G be a multiplicative group and let $a \in G$. Then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the "smallest" subgroup of G that contains a (that is, every subgroup of G which contains a contains all the elements of H).

Note. In Theorem 5.17, by a^0 we mean the identity e: $a^0 = e$. By a^{-n} where $n \in \mathbb{N}$, we mean $(a^{-1})^n$: $a^{-n} = (a')^n = (a^{-1})^n$.

Definition 5.18. Let G be a group and let $a \in G$. Then the subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ of G (of Theorem 5.17) is the *cyclic subgroup of G generated by a*, denoted $\langle a \rangle$.

Definition 5.19. An element a of a group G *generates* G if $\langle a \rangle = G$. A group is *cyclic* if there is $a \in G$ such that $\langle a \rangle = G$.

Example 5.20. $\mathbb{Z}_4$ is cyclic since $\langle 1 \rangle = \mathbb{Z}_4$. Also, $\langle 3 \rangle = \mathbb{Z}_4$. In fact, $\mathbb{Z}_n$ is cyclic since $\mathbb{Z}_n = \langle 1 \rangle$. Are there other generators of $\mathbb{Z}_n$?

Note. The notation in Definition 5.18 is that of a multiplicative group, but Example 5.20 is based on an additive group. In an additive group, $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ (where $0a = 0$ and $-1a = -a$ by definition).

Example 5.12. $\langle \mathbb{Z}, + \rangle$ is a cyclic group with generators 1 and -1.

Notation. We can generate subgroups of $\langle \mathbb{Z}, + \rangle$ simply by considering $\langle n \rangle$ for any $n \in \mathbb{Z}$. We denote $\langle n \rangle$ as $n\mathbb{Z}$. For example, $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots,\}$ Notice $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$.

Exercise 5.24. Describe the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$.

Answer. Elements are of the form $\begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix}$ where $n \in \mathbb{Z}$.

Revised: 7/7/2023