Abstract Algebra Notes

Mario L. Gutierrez Abed

Permutations, Cosets, and Direct Products

PERMUTATIONS

Definition: A permutation of a set A is a function $\phi : A \longrightarrow A$ that is bijective.

Example:
Given a set $A = \{1, 2, 3, 4, 5\}$, we apply a permutation σ given by the 1-1 correspondence

$$1 \to 4, \quad 2 \to 2, \quad 3 \to 5, \quad 4 \to 3, \quad 5 \to 1 \,,$$

which we write in the more standard notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

Then let τ be also a permutation on the set A given by

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then we apply permutation mulriplication to obtain

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}. \end{aligned}$$

• Theorem:
Let A be a nonempty set, and let S_A be the collection of all permutations on A. Then S_A is a group

under permutation multiplication.

Proof:
(See page 77, Fraleigh's) ■

Definition: Let A be the finite set $\{1, \ldots, n\}$. The group of all permutations on A is the symmetric group on n letters, and is denoted by S_n. Note that S_n has $n!$ elements.

Example:
An interesting example is the group S_3. Let the set A be $\{1, 2, 3\}$. We list all the permutations of A and assign to each a subscripted Greek letter for a name (the reasons for the choice of names will be clear later).
Let

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The multiplication table for this group is given by:

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Note that this group is not abelian. It turns out that S_3 has minimum order for any nonabelian group. That is, if G is some nonabelian group, then $|G| \geq 6$.

Remark: There is a natural correspondence between the elements of S_3 and the ways in which two copies of an equilateral triangle with vertices 1, 2, and 3 can be placed, one covering the other with vertices on top of vertices. For this reason, S_3 is also the third dihedral group, denoted by D_3, which is the group of symmetries of an equilateral triangle. Naively we use ρ_i for rotations and μ_i for mirror images in bisectors of angles.
More generally, the n^{th} dihedral group, denoted by D_n, is the group of symmetries of a regular n-gon.

Example:

Let us form the dihedral group D_4 of permutations corresponding to the ways that two copies of a square with vertices 1, 2, 3, and 4 can be placed, one covering the other with vertices on top of vertices. D_4 will be then the group of symmetries of the square, which is also called the octic group.

Note that while S_3 was equal to D_3, S_4 and D_4 are two different animals. D_4 contains a total of 8 permutations whereas S_4 has $4! = 24$ permutations.

Using ρ_i for rotations, μ_i for mirror images in perpendicular bisectors of sides, and δ_i for diagonal flips we have the following eight permutations:

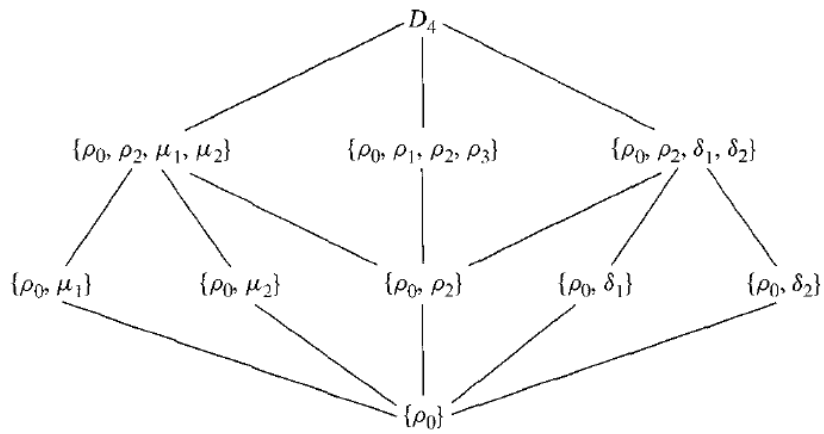
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

The multiplication table for this group is given by:

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

and its diagram:



• Lemma:
Let G and G' be groups and let $\phi : G \longrightarrow G'$ be an injective function such that $\phi(x\,y) = \phi(x)\,\phi(y)$ $\forall\, x,\ y \in G$. Then the image of G under ϕ –denoted $\phi[G]$– is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Proof:
(See page 82, Fraleigh's). ■

We are now ready to prove a classic theorem of group theory:

• Cayley's Theorem:
Every group is isomorphic to a group of permutations.

Proof:
Let G be a group. We show that G is isomorphic to a subgroup of S_G. By the above lemma, we need only define an injective function $\phi : G \longrightarrow S_G$ such that $\phi(x\,y) = \phi(x)\,\phi(y)$ $\forall\, x,\ y \in G$.
For $x \in G$, let $\lambda_x : G \longrightarrow G$ be defined by $\lambda_x(g) = x\,g$ $\forall\, g \in G$ (we think of λ_x as performing left multiplication by x). The equation

$$\lambda_x(x^{-1}\,c) = x(x^{-1}\,c) \quad \forall\, c \in G$$

shows that λ_x maps G onto G.
Now

$$\lambda_x(a) = \lambda_x(b) \Longrightarrow x\,a = x\,b \Longrightarrow a = b \quad \text{(by cancellation)}.$$

Thus λ_x is also injective, and it's a permutation of G.

We now define $\phi : G \longrightarrow S_G$ by defining $\phi(x) = \lambda_x$ for all $x \in G$. To show that ϕ is injective, suppose that $\phi(x) = \phi(y)$. Then $\lambda_x = \lambda_y$ as functions mapping G into G.
In particular,

$$\lambda_x(e) = \lambda_y(e) \Longrightarrow x\,e = y\,e \Longrightarrow x = y \quad \text{(by cancellation)}.$$

Thus ϕ is injective.
We only need to show that $\phi(x\,y) = \phi(x)\,\phi(y)$, that is $\lambda_{xy} = \lambda_x\,\lambda_y$. Now, for any $g \in G$, we have $\lambda_{xy}(g) = (x\,y)\,g$. Permutation multiplication is function composition, so

$$(\lambda_x\,\lambda_y)\,(g) = \lambda_x(\lambda_y(g)) = \lambda_x(y\,g) = x(y\,g) = (x\,y)\,g = \lambda_{xy}.$$

Thus we have that $\lambda_{xy} = \lambda_x\,\lambda_y$, which is the desired homomorphic property, and we have thus proven that every group is isomorphic to a group of permutations. ■

ORBITS & CYCLES

Each permutation σ of a set A determines a natural partition of A into cells with the property that $a,\ b \in A$ are in the same cell iff $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. We establish this partition using an appropriate equivalence relation:

(*) For $a,\ b \in A$, let $a \sim b$ iff $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

It is very easy to check that (*) is indeed an equivalence relation by checking that it is reflexive, symmetric, and transitive.

Definition: Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation (*) are called the orbits of σ.

Example:
Since the identity permutation ι of A leaves each element of A fixed, the orbits of ι are the one-element subsets of A.

Example:
Find the orbits of the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$ in S_8.

Solution:

‣ To find the orbit containing 1, we apply σ repeatedly:

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} \ldots.$$

Since σ^{-1} would simply reverse the directions of the arrows in this chain, we see that the orbit containing 1 is $\{1, 3, 6\}$.

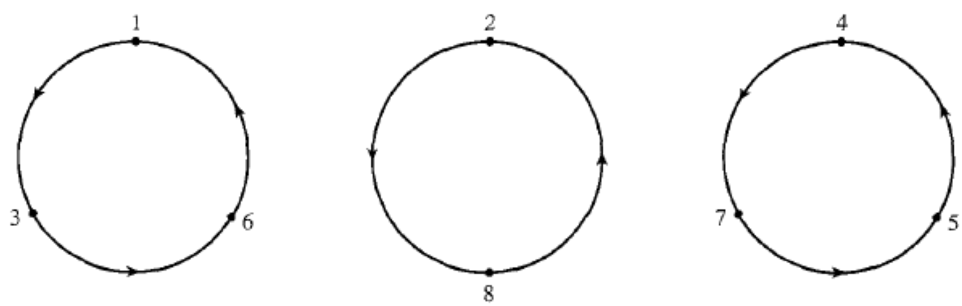
‣ We now choose an integer from 1 to 8 not in $\{1, 3, 6\}$, say 2, and using a similar procedure we find that the orbit containing 2 is $\{2, 8\}$.

‣ Finally, we find that the orbit containing 4 is $\{4, 7, 5\}$.

Since these three orbits include all integers from 1 to 8, we see that the complete list of orbits of σ is

$$\{1, 3, 6\}, \qquad \{2, 8\}, \qquad \{4, 5, 7\}.$$

A nice way to visualize the structure of the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$ from the above example is by graphically representing the orbits of σ:



That is, σ acts on each integer from 1 to 8 on one of the circles by carrying it into the next integer on the circle travelling counterclockwise in the direction indicated by the arrows. For example, the leftmost circle indicates that

$$\sigma(1) = 3, \quad \sigma(3) = 6, \quad \text{and} \quad \sigma(6) = 1.$$

The important thing here is that each individual circle in the figure above also defines, by itself, a permutation in S_8.
For instance, the leftmost circle corresponds to the permutation

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$$

that acts on 1,3, and 6 just as σ does, but leaves the remaining integers fixed.
In summary, μ has one three-element orbit $\{1, 3, 6\}$ and five one-element orbits $\{2\}$, $\{4\}$, $\{5\}$, $\{7\}$, and $\{8\}$. Such a permutation, described graphically by a single circle, is called a cycle.

Definition: A permutation $\sigma \in S_n$ is called a cycle if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit.

Notation: To avoid cumbersome notation when dealing with cycles, instead of writing for instance $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$, we are going to use $\mu = (1, 3, 6)$. We understand by this notation that μ carries the first number 1 into the second number 3, the second number 3 into the next number 6, etc., until finally the last number is carried into the first one. Note that an integer not appearing in this notation for μ is understood to be left fixed by μ.

Example:
Working within S_5, we see that

$$(1, 3, 5, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

Observe that

$$(1, 3, 5, 4) = (3, 5, 4, 1) = (5, 4, 1, 3) = (4, 1, 3, 5).$$

Of course, since cycles are special types of permutations, they can be multiplied just as any two permutations. HOWEVER, the product of two cycles need not again be a cycle.
Using cyclic notation, we see that the permutation σ from the previous example can be written as a product of cycles:

$$(**) \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 7, 5).$$

These cycles are disjoint, meaning that any integer is moved by at most one of these cycles; thus no one number appears in the notations of two different cycles.

Remark: Equation (**) exhibits σ in terms of its orbits, and is a one-line description of the figure above (the one that shows the orbits of σ as three different circles). It turns out that every permutation in S_n can be expressed in a similar fashion as a product of the disjoint cycles corresponding to its orbits. We state and prove this theorem next.

• Theorem:
Every permutation σ of a finite set is a product of disjoint cycles.

Proof:
Let $B_1, \ldots, B_r$ be the orbits of σ, and let μ_i be the cycle defined by

$$\mu_i(x) = \begin{cases} \sigma(x) & \text{for } x \in B_i \\ x & \text{otherwise} \end{cases}.$$

Clearly $\sigma = \mu_1 \mu_2 \ldots \mu_r$. Since the equivalence-class orbits $B_1, \ldots, B_r$ –being distinct equivalence classes– are disjoint, the cycles $\mu_1 \mu_2 \ldots \mu_r$ are also disjoint. ■

Remark: While permutation multiplication in general is not commutative, it is readily seen that multiplication of disjoint cycles is commutative.

Example:
Write the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ as a product of disjoint cycles.

Solution:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3).$$

Multiplication of disjoint cycles is commutative, hence $(1, 6)(2, 5, 3) = (2, 5, 3)(1, 6)$.

Example:
Consider the cycles $(1, 4, 5, 6)$ and $(2, 1, 5)$ in S_6 (note that these cycles are not disjoint since 1 and 5 are in both). Multiplying them we have

$$(1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

and

$$(2, 1, 5)(1, 4, 5, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}.$$

Note that neither of these permutations is a cycle.

EVEN & ODD PERMUTATIONS

Definition: A cycle of length 2 is called a transposition.

Thus a transposition leaves all but two elements fixed, and maps each of these onto the other. A computation shows that

$$(a_1, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_3)(a_1, a_2).$$

Therefore any cycle is a product of transpositions, and the following corollary follows:

• Corollary:
Any permutation of a finite set of at least two elements is a product of transpositions.

Example:
Following the remarks prior to the corollary, we see that $(1, 6)(2, 5, 3)$ is the product $(1, 6)(2, 3)(2, 5)$ of transpositions.

Example:
In S_n for $n \geq 2$, the identity permutation is the product $(1, 2)(1, 2)$ of transpositions.

Remark: We have seen that every permutation of a finite set with at least two elements is a product of transpositions. The transpositions may not be disjoint, and a representation of the permutation in this way is not unique. For example, we can always insert at the beginning of the transposition $(1, 2)$ twice because $(1, 2)(1, 2)$ is the identity permutation. What is true is that the number of transpositions used to represent a given permutation must either always be odd or always be even. This is a very important fact that's stated in the following theorem:

• Theorem:
No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof:
(See pg 91, Fraleigh's). ■

Definition: A permutation of a finite set is even or odd according to whether it can be expressed as a product of an even number of transpositions or a product of an odd number of transpositions, respectively.

Example:

- The identity permutation ι in S_n is an even permutation since we have $\iota = (1,\ 2)(1,\ 2)$. If $n = 1$ so that we cannot form this product, we define ι to be even.

- The permutation $(1,\ 4,\ 5,\ 6)(2,\ 1,\ 5)$ in S_6 can be written as

$$(1,\ 4,\ 5,\ 6)(2,\ 1,\ 5) = (1,\ 6)(1,\ 5)(1,\ 4)(2,\ 5)(2,\ 1)\,,$$

which has five transpositions, so this is an odd permutation.

ALTERNATING GROUPS

• Theorem:

If $n \geq 2$, then the collection of all even permutations of $\{1,\ \ldots,\ n\}$ forms a subgroup of order $n!\,/\,2$ of the symmetric group S_n.

Definition: The subgroup of S_n consisting of the even permutations of n letters is called the alternating group A_n on n letters.

Remark: Both S_n and A_n are very important groups. Cayley's theorem shows that every finite group G is structurally identical to some subgroup of S_n for $n = |G|$. It can be shown that there are no formulas involving just radicals for solution of polynomial equations of degree $n \geq 5$. This fact is actually due to the stucture of A_n, surprising as that may seem!

COSETS & THE THEOREM OF LAGRANGE

• Theorem:

Let H be a subgroup of G.

Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \quad \text{iff} \quad a^{-1}\, b \in H.$$

Let the relation $\sim_R$ be defined on G by

$$a \sim_R b \quad \text{iff} \quad a\, b^{-1} \in H.$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations.

Proof:
First we show that $\sim_L$ is an equivalence relation.
‣ Let $a \in G$. Then $a^{-1}\, a = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_L a$. (Reflexive)
‣ Suppose $a \sim_L b$. Then $a^{-1}\, b \in H$. Since H is a subgroup, $(a^{-1}\, b)^{-1} = b^{-1}\, a$ is in H.
This shows that $b \sim_L a$. (Symmetric)
‣ Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}\, b \in H$ and $b^{-1}\, c \in H$. Since H is a subgroup, $(a^{-1}\, b)\,(b^{-1}\, c) = a^{-1}\, c$ is in H, hence $a \sim_L c$. (Transitive) ✓

Now we show that $\sim_R$ is an equivalence relation.
‣ Let $a \in G$. Then $a\, a^{-1} = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_R a$. (Reflexive)
‣ Suppose $a \sim_R b$. Then $a\, b^{-1} \in H$. Since H is a subgroup, $(a\, b^{-1})^{-1} = b\, a^{-1}$ is in H.
This shows that $b \sim_R a$. (Symmetric)
‣ Let $a \sim_R b$ and $b \sim_R c$. Then $a\, b^{-1} \in H$ and $b\, c^{-1} \in H$. Since H is a subgroup, $(a\, b^{-1})\,(b\, c^{-1}) = a\, c^{-1}$ is in H, hence $a \sim_R c$. (Transitive) ✓ ■

These equivalence relations $\sim_L$ and $\sim_R$ partition a group into its left and right cosets, respectively:

Definition: Let H be a subgroup of a group G. The subset $aH = \{ah : h \in H\}$ of G is the left coset of H containing a, while the subset $Ha = \{ha : h \in H\}$ is the right coset of H containing a.

Example:
Exhibit the left cosets and right cosets of the subgroup $3\,\mathbb{Z}$ of $\mathbb{Z}$.

Solution:
Our notation here is additive, so the left coset of $3\,\mathbb{Z}$ containing m is $m + 3\,\mathbb{Z}$.
Taking $m = 0$, we see that

$$3\,\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

is itself one of its left cosets, the coset containing 0.
To find another left coset, we select an element of $\mathbb{Z}$ not in $3\,\mathbb{Z}$, say 1, and find the left coset containing it. We have

$$1 + 3\,\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

These two left cosets, $3\,\mathbb{Z}$ and $1 + 3\,\mathbb{Z}$, do not yet exhaust $\mathbb{Z}$. For example, 2 is neither of them. The left coset containing 2 is

$$2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \quad .$$

It is clear that these three left cosets that we've found do exhaust $\mathbb{Z}$, so they constitute the partition of $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$.
Since $\mathbb{Z}$ is abelian, the left coset $m + 3\mathbb{Z}$ and the right coset $3\mathbb{Z} + m$ are the same, so the partition of $\mathbb{Z}$ into right cosets is the same.

Remark: For a subgroup H of an abelian group G, the partition of G into left cosets of H and the partition into its right cosets are the same.

Remark: The equivalence relation $\sim_R$ for the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is the same as the relation of congruence modulo n. Recall that $h \equiv k \pmod{n}$ in $\mathbb{Z}$ if $h - k$ is divisible by n. this is the same as saying that $h + (-k)$ is in $n\mathbb{Z}$, which is the relation $\sim_R$ in additive notation. Thus the partition of $\mathbb{Z}$ into cosets of $n\mathbb{Z}$ is the partition of $\mathbb{Z}$ into residue classes modulo n. For that reason, we often refer to the cells of this partition as cosets modulo $n\mathbb{Z}$. (Note that we don't have to specify left or right cosets since they are the same for this abelian group $\mathbb{Z}$).

Example:
The group $\mathbb{Z}_6$ is abelian. Find the partition of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0, 3\}$.

Solution:
One coset is $\{0, 3\}$ itself. The coset containing 1 is $1 + \{0, 3\} = \{1, 4\}$. The coset containing 2 is $2 + \{0, 3\} = \{2, 5\}$. Since $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$ exhaust all of $\mathbb{Z}_6$, these are all the cosets.

Remark: Every coset (left or right) of a subgroup H of a group G has the same number of elements as H. We can easily show this by choosing a bijection $\phi : H \longrightarrow g H$ (or $\phi : H \longrightarrow H g$), where $\phi(h) = g h$ (or $\phi(h) = h g$) for each $h \in H$.

• Lagrange's Theorem:
Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof:
Let n be the order of G, and let H have order m. The remark preceding this theorem shows that every coset of H also has m elements. Let r be the number of cells in the partition of G into left cosets of H. Then $n = r m$, so m is indeed a divisor of n. ■

Remark: The converse of Lagrange's theorem holds if G is abelian. That is, if G is an abelian group of order n, and there exists an m that divides n, then we are guaranteed the existence of a subgroup of G of order m.

• Corollary:
Every group of prime order is cyclic.

Proof:
Let G be of prime order p, and let a be an element of G other than the identity. Then the cyclic subgroup $\langle a \rangle$ of G generated by a has at least two elements, a and e. But by Lagrange's theorem, the order $m \geq 2$ of a must divide the prime p. Thus we must have $m = p$ and $\langle a \rangle = G$, so G is cyclic. ■

Definition: Let H be a subgroup of a group G. The number of left cosets of H in G is the index of H in G, denoted by $(G:H)$.

Remark: The index $(G:H)$ just defined may be finite or infinite. If G is finite, then obviously $(G:H)$ is finite and we have that

$$(G:H) = \frac{|G|}{|H|},$$

since every coset of H contains $|H|$ elements. By the way, it can be shown that the index $(G:H)$ could be equally defined as the number of right cosets of H in G.

• Theorem:
Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose $(H:K)$ and $(G:H)$ are both finite. Then $(G:K)$ is finite, and $(G:K) = (G:H)\,(H:K)$.