A CHILD'S GARDEN OF GROUPS

Isomorphisms, Homomorphisms, and Theorems

…OH MY!

(Part 10)

by

Doc Benton

CONTENTS (PART 10)

INTRODUCTION (PART 10)

In this final part to our book, we prove some very important and often very difficult theorems, and we introduce the concept of a *homomorphism* and we indicate why it is so fundamental to the study of *groups*. In particular, we prove all three *isomorphism theorems*, *Burnside's Counting Theorem*, the *Sylow Theorems*, and the *Fundamental Theorem of Abelian Groups*. If you've made it this far, then you're almost finished!

Functions, Isomorphisms, and Homomorphisms

A *function* is essentially a rule for pairing elements from one set with elements in another set. However, there is one special condition that this rule must follow. Namely, each element in the first set can be paired with only one element in the second set. It's okay, however, if two different elements in the first set get paired with the same element in the second set. We just can't start with a single element, apply our *function*, and then suddenly wind up with more than one element. Rules which are *functions* appear everywhere in our society. For example, if you have a paying job, then there is a rule or *function* which determines how much you should receive on payday, and you certainly don't want a rule that results in two or more amounts!

In mathematics, we usually denote functions by letters such as *f* or *g*, and here are a couple of examples of *functions* as rules being evaluated at specific points:

$$f(x) = x^2$$
$$f(2) = 4$$
$$f(-2) = 4$$

$$g(x) = x + 1$$
$$g(2) = 3$$
$$g(-2) = -1$$

For each of these *functions*, we could designate that our starting set is the *real numbers*, the numbers on the *number line* that are denoted by $\mathbb{R}$, and we could also designate our receiving set as the *real numbers*, $\mathbb{R}$. When we do this, we often use the following notation:

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$g : \mathbb{R} \longrightarrow \mathbb{R}$$

or

$$\mathbb{R} \xrightarrow{f} \mathbb{R}$$
$$\mathbb{R} \xrightarrow{g} \mathbb{R}$$

Notice, too, that the *function* $f(x) = x^2$ doesn't give us back the entire set of *real numbers*, but the *function* $g(x) = x+1$ does. In the later case, we say that the *function g* is *onto*. Also, notice that different input values for *g* will always result in different output values. When this happens, we say that our *function* is *one-to-one*. Notice that *f* is not *one-to-one* since the inputs of 2 and -2 both result in an output of 4. Also, notice that a rule such as $f(x) = \pm\sqrt{x}$ is not a *function* since an input such as 4 results in two outputs, -2 and 2.

We can often follow one *function* with another *function*, such as when we have one rule for determining gross pay followed by another rule for finding net pay by deducting money for taxes and insurance, and when we follow one *function* by another, we call it a *composition of functions*. In mathematics today if we want to follow our *function g* by the *function f*, then we usually write it as $(f \circ g)(x) = f(g(x))$. For example, $(f \circ g)(2) = f(g(2)) = f(3) = 9$ and $(g \circ f)(2) = g(f(2)) = g(4) = 5$. There was also a time when some mathematicians would write *functions* as $(x)f$ or xf rather than $f(x)$, and that fits in better with our practice of applying permutations and matrices in order from left to right. It also fits in better with the following notation for $(g \circ f)(x)$ which is still very common:

$$A \xrightarrow{f} B \xrightarrow{g} C$$

However, GAP software applies *functions* in from right to left in what has now become pretty much the standard in mathematics. For example, here is how you would construct and use some *functions* in GAP.

```
gap> f:=x->x^2;
function( x ) ... end

gap> f(2);
4

gap> g:=x->x+1;
function( x ) ... end

gap> g(2);
3

gap> f(g(2));
9

gap> g(f(2));
5
```

We've used the term *"isomorphism"* before, and we pointed out that it literally means *"equal shape."* We've also said that two *groups* are *isomorphic* if they are essentially the same *group*, but with different labels for the elements. That means that there has to exist a correspondence between the two *groups* that is both *one-to-one* and *onto*, what we call a *"bijection."* Additionally, an *isomorphism* between two *groups* also means that multiplication in one *group* has to correspond to multiplication in the other group. So far we've avoided using *functions* to define *isomorphisms* in order to keep things a little simpler. However, the time has come to streamline our thinking by giving an explicit definition of a *isomorphism* purely in terms of a *function* from one *group* onto another. First, though, we will give more specific definitions for terms like *one-to-one*, *onto*, *injection*, *surjection*, and *bijection*.

<u>Definition:</u> Let $f: A \to B$ be a *function*. Then *f* is *one-to-one* if and only if whenever we have $x, y \in A$ with $x \neq y$, we also have that $f(x) \neq f(y)$. Equivalently, we can say that *f* is *one-to-one* if $f(x) = f(y)$ always implies that $x = y$. A *one-to-one function* is also known as an <u>*injection*</u> or <u>*injective function*</u>.

Definition: Let $f: A \to B$ be a *function*. Then *f* is an *onto function* if and only if whenever $y \in B$, there exists $x \in A$ such that $f(x) = y$. An *onto function* is also known as a *surjection* or *surjective function*.

Definition: Let $f: A \to B$ be a *function*. If *f* is both *one-to-one* and *onto* (both *injective* and *surjective*), then *f* is also called a *bijection* or *bijective function*.

Definition: Let $f: A \to B$ be a *bijective function* from a *group A onto* a *group B*. Then *f* is also an *isomorphism* if for all $x, y \in A$, we have that $f(x)f(y) = f(xy)$. Note that this basically says that if $xy = z$ in *A*, then $f(x)f(y) = f(xy) = f(z)$ in *B*. In other words, multiplication in *A* corresponds to multiplication in *B.*

A concept of that is more general than that of an *isomorphism* is the notion of a *"homomorphism."* The word itself means *"same shape,"* and the difference between an *isomorphism* and a *homomorphism* is that we drop the condition that our *function* be *one-to-one*. We will keep, however, the *onto* condition.

Definition: Let $f: A \to B$ be a *surjective function* from a *group A onto* a *group B*. Then *f* is also a *homomorphism* if for all $x, y \in A$ we have that $f(x)f(y) = f(xy)$. Note that this basically says that if $xy = z$ in *A*, then $f(x)f(y) = f(xy) = f(z)$ in *B*. Again, multiplication in *A* corresponds to multiplication in *B.*

An example of a *homomorphism* that is not an *isomorphism* would be the *function* that takes every *integer* in the *group* of *integers* under addition, and assigns that *integer* either to the label "even" or to the label "odd" in the usual manner. Suppose we call this latter set *E* and that we define addition in *E* according to the following table.

+	**Even**	**Odd**
Even	Even	Odd
Odd	Odd	Even

Then *E* is a *group* of order 2, and our *function* $f:\mathbb{Z}\rightarrow E$ is a *homomorphism*. Hence, using additive rather than multiplicative notation, we have, for instance, that $f(2)+f(3)=even+odd=odd=f(2+3)=f(5)$. In other words, there is a correspondence between addition in $\mathbb{Z}$ and addition in *E*.

And finally, if we do have a *homomorphism* $f:A\rightarrow B$, then of particular concern will be the elements in *A* that get sent or mapped to the *identity element* in *B*. The set of such elements in *A* is called the *"kernel of our homomorphism f."*

Definition: Let $f:A\rightarrow B$ be a *homomorphism* from *A onto B*. Then the *kernel of f,* denoted by $Ker(f)$, is defined by

$$Ker(f)=\left\{x\in A \mid f(x)=e \text{ where } e \text{ is the identity element in } B\right\}.$$

HOMOMORPHISMS AND IDENTITIES

Discussion: This theorem just takes care of some housekeeping details. It shows us that any *homomorphism* from one *group* to another always pairs the *identity element* in the first *group* with the *identity element* in the second I. It's not difficult to prove, but you gotta take the time to verify it anyway.

Theorem: Let *A* be a *group* and let $f: A \to B$ be a *homomorphism* from *A onto B*. Then $f(e) = e$.

Proof: Technically, we should perhaps denote the *identity element* in *A* by e_A and the *identity element* in *B* by e_B, but it is much more convenient to use *e* as the generic symbol for any *identity element*, and usually little confusion arises by using *e* to represent both *identities*. Thus, let $x \in A$. Then $f(x) = f(e \cdot x) = f(e)f(x)$. Now just multiply both sides of this equation on the right by $[f(x)]^{-1}$ to obtain $f(e) = e$.

□

HOMOMORPHISMS AND INVERSES

Discussion: This theorem takes care of another housekeeping detail. It shows us that any *homomorphism* from one *group* to another always pairs an *inverse* element in the first *group* with the corresponding *inverse* element in the second *group*. Again, it's not difficult to prove, but you gotta take the time to verify it anyway.

Theorem: Let *A* be a *group*, let $f: A \to B$ be a *homomorphism* from *A onto B*, and let $a \in A$. Then $f(a^{-1}) = \left[f(a) \right]^{-1}$. In other words, the *inverse* of *a* in *A* gets mapped to the *inverse* of $f(a)$ in *B*.

Proof: Clearly, $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ implies that $f(a^{-1}) = \left[f(a) \right]^{-1}$.

□

THE KERNEL OF A HOMOMORPHISM

Discussion: Now that we've defined a *homomorphism* as a *function* $f: A \to B$ such that for all $x, y \in A$ we have that $f(xy) = f(x)f(y)$, recall that we define the *Kernel* of our *homomorphism* to be the set of all elements in the first *group* that get sent to the *identity element* in the second *group*. Below we prove that this set, the *Kernel*, is not only a *subgroup* of our original *group*, it's also a *normal subgroup*, and that fact has major implications when it comes to investigating what *homomorphisms* from one *group* to another are even possible.

Definition: Let $f: A \to B$ be a *homomorphism* from a *group A onto B*. Then the *Kernel of f,* denoted by $Ker(f)$, is defined by

$$Ker(f) = \{x \in A \mid f(x) = e \text{ where } e \text{ is the identity element in } B\}.$$

Theorem: Let $f: A \to B$ be a *homomorphism* from a *group A onto B*. Then $Ker(f)$ is a *normal subgroup* of *A*.

Proof: First we will show that $Ker(f)$ is a *subgroup* of *A* by showing that it is *closed* under multiplication and that it contains *inverses*. Thus, let $a, b \in Ker(f)$. Then $e = f(a)f(b) = f(ab)$ implies that $ab \in Ker(f)$ and,hence, $Ker(f)$ is *closed* under multiplication.

Now we will show that the *inverse* of every element in the *Kernel* of a *homomorphism* also belongs to the *Kernel*. Thus, let $a \in Ker(f)$. Then there exists $a^{-1} \in A$. However, $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) = e \cdot f(a^{-1}) = f(a^{-1})$ implies that $a^{-1} \in Ker(f)$, and, hence, $Ker(f)$ is a *subgroup* of *A*.

To show that $Ker(f)$ is a *normal subgroup* of *A*, let $g \in A$ and let $x \in Ker(f)$. Then $f(g^{-1}xg) = f(g^{-1})f(x)f(g) = \left[f(g)\right]^{-1} \cdot e \cdot f(g) = \left[f(g)\right]^{-1} f(g) = e$ implies that $g^{-1}xg \in Ker(f)$. Therefore, $Ker(f)$ is a *normal subgroup* of *A*.

□

THE NATURAL HOMOMORPHISM

Discussion: We've talked before about *normal subgroups*, such as when *N* is a *normal subgroup* of *G*, and we've talked about the corresponding *quotient groups*, such as G/N. What we want to demonstrate now is that there is a very obvious *surjective homomorphism* from *G onto* G/N that we call the *natural homomorphism*.

Theorem: Let *G* be a *group*, and let *N* be a *normal subgroup* of *G*. Then the function $\pi : G \to G/N$ defined by $\pi(g) = Ng$ is a *homomorphism* from *G onto* G/N. This *homomorphism* is called the *natural homomorphism*.

Proof: By previous proof (Part 9, Theorem 19), we know that the *right* (left) *cosets* of *N* in *G* form a *group* under the multiplication inherited from *G*. We also know that the *function* we've defined is *onto* since if $Ng \in G/N$, then $Ng = \pi(g)$ for $g \in G$. Additionally, we know from previous proof (Part 9, Theorem 17) that if $a,b \in G$, then $Nab = NaNb$ .To show that $\pi : G \to G/N$ defined by $\pi(g) = Ng$ is a *homomorphism* is now very easy. Let $a,b \in G$, and then $\pi(ab) = Nab = NaNb = \pi(a)\pi(b)$.

□

THE CORRESPONDENCE THEOREM

<u>Discussion:</u> This important theorem basically delineates a lot of correspondences that exist between *subgroups* in a *group G* that contain a given *normal subgroup N* and *subgroups* in the corresponding *quotient group* G/N. In particular, this means that we can learn things about the structure of *G* by studying G/N.

<u>The Correspondence Theorem:</u> Let *G* be a *group*, let *N* be a *normal subgroup* of *G*, and let $\pi : G \to G/N$ be the *natural homomorphism*. Then,

1. If *H* is a *subgroup* of *G* such that $N \subseteq H$, then H/N is a *subgroup* of G/N.
2. If *M* is a *subgroup* of G/N, then $H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$ is a *subgroup* of G that contains *N* ,and $H/N = M$.
3. If *H* is a *normal subgroup* of *G* such that $N \subseteq H$, then H/N is a *normal subgroup* of G/N.
4. If H/N is a *normal subgroup* of G/N, then $H = \pi^{-1}(H/N) = \{g \in G \mid \pi(g) \in H/N\}$ is a *normal subgroup* of G.
5. If *H* and *K* are *subgroups* of *G* such that $N \subseteq H \subseteq K$, then $H/N \subseteq K/N$.
6. If $H/N \subseteq K/N$, then $N \subseteq H \subseteq K$.
7. If *H* and *K* are subgroups of *G* such that $N \subseteq H \subseteq K$, then $[K:H] = [K/N : H/N]$.
8. If $N \subseteq H \subseteq K$, where *H* and *K* are *subgroups* of *G*, and if *H* is *normal* in *K*, then H/N is *normal* in K/N.
9. If $N \subseteq H \subseteq K$, where *H* and *K* are *subgroups* of *G*, and if H/N is *normal* in K/N, then *H* is *normal* in *K.*

<u>Proof:</u> (1) Let *H* be a *subgroup* of *G* such that $N \subseteq H$ where *N* is a *normal subgroup* of *G*. To show that H/N is a *subgroup* of G/N, we just need to show *closure* and existence of *inverses*. Thus, suppose $Na, Nb \in H/N$. Then $a,b \in H$. Since *H* is a *subgroup* of *G*, there exists $c \in H$ such that $c = ab$. Hence, $NaNb = Nab = Nc \in H/N$, and, thus, *closure* is satisfied.

Now suppose $Na \in H/N$. Then $a \in H$, and since *H* is a *subgroup* of *G*, there exists $a^{-1} \in H$ such that $aa^{-1} = e$. Consequently, $Na^{-1} \in H/N$ and $NaNa^{-1} = Naa^{-1} = Ne = N$, the *identity* in H/N. Therefore, *inverses* also exist in H/N, and H/N is a *subgroup* of G/N.

(2) Suppose *M* is a *subgroup* of G/N and let $H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$. Then clearly $N \subseteq H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$ since *N* is just π^{-1} applied to the *identity element* in *M*. To show that *H* is a *subgroup* of *G*, we need to verify *closure* and existence of *inverses*. Thus, suppose that $a,b \in H$. Then $Na, Nb \in M$ and $NaNb = Nab \in M$. From this it follows that $ab \in H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$, and *H* is *closed* under multiplication.

To show that *inverses* exist in *H,* suppose $a \in H$. Then $Na \in M$ and because *inverses* exist in *M*, there exists $Nb \in M$ such that $NaNb = Nab = N$. However, this means both that $b \in H$ and $ab = n$ for some $n \in N$. But this also implies that $(ab)n^{-1} = a(bn^{-1}) = e$, the *identity element* in *G*, and, thus, $bn^{-1} = a^{-1}$. We can now conclude that since $b \in H$ and $n, n^{-1} \in N \subseteq H$, that $bn^{-1} = a^{-1} \in H$, and, therefore, *H* is a *subgroup* of *G* that contains *N*.

Finally, since $H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$ and since $N \subseteq H$ and $N = Ker(\pi)$ it follows immediately that $\pi(H) = M = H/N$.

(3) Suppose that *H* is a *normal subgroup* of *G* such that $N \subseteq H$, and consider H/N, a *subgroup* of G/N. If $Ng \in G/N$ and $a \in H$, then $Ng^{-1}NaNg = Ng^{-1}ag$ since *H* being *normal* in *G* tells us that $g^{-1}ag \in H$, it follows that $N(g^{-1}ag) \in H/N$. Therefore, H/N is a *normal subgroup* of G/N.

(4) Suppose M is a *normal subgroup* of G/N and let $H = \pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$. Then by (2) above, *H* is a subgroup of *G* and $M = H/N$. Now let $Ng \in G/N$ where $g \in G$. If $Na \in H/N$, then $Ng^{-1}NaNg = Ng^{-1}ag \in H/N$ since H/N is a *normal subgroup* of G/N. But this means that $g^{-1}ag \in \pi^{-1}(Ng^{-1}ag) \subseteq H$. Therefore, *H* is a *normal subgroup* of *G.*

(5) Suppose *H* and *K* are *subgroups* of *G* such that $N \subseteq H \subseteq K$. Then H/N and K/N are both *subgroups* of G/N (by (1) above). Furthermore, if $N \subseteq H \subseteq K$, then $a \in H$ implies that $a \in K$, and this in turn means that if $Na \in H/N$, then $Na \in K/N$. Therefore, $H/N \subseteq K/N$

.

(6) Suppose $H/N \subseteq K/N$. Then $H = \pi^{-1}(H/N) = \{g \in G \mid \pi(g) \in H/N\}$ and $K = \pi^{-1}(K/N) = \{g \in G \mid \pi(g) \in K/N\}$ are *subgroups* of *G* (by (2) above). Since $N \in H/N \subseteq K/N$, it follows immediately that

$N \subseteq H = \pi^{-1}(H/N) = \{g \in G \mid \pi(g) \in H/N\} \subseteq \pi^{-1}(K/N) = \{g \in G \mid \pi(g) \in K/N\} = K$.

(7) Suppose *H* and *K* are *subgroups* of *G* such that $N \subseteq H \subseteq K$. Then *H* is also a *subgroup* of *K*, and H/N and K/N are both *subgroups* of G/N (by (1) above) with $H/N \subseteq K/N$ (by (5) above). Consequently, H/N is also a *subgroup* of K/N. Furthermore, by *Lagrange's Theorem*, $[K:H] = \dfrac{|K|}{|H|}$ and

$[K/N : H/N] = \dfrac{|K/N|}{|H/N|} = \dfrac{|K|/|N|}{|H|/|N|} = \dfrac{|K|}{|H|}$. Therefore, $[K:H] = [K/N : H/N]$.

(8) Suppose that *H* is *normal* in *K* where $N \subseteq H \subseteq K$. If $Na \in H/N$ and $Ng \in K/N$, then $g^{-1}ag \in H$ since *H* is *normal* in *K*. Thus, $Ng^{-1}NaNg = Ng^{-1}ag \in H/N$ and, therefore, H/N is *normal* in K/N.

(9) Suppose H/N is *normal* in K/N where $N \subseteq H \subseteq K$ are all *subgroups* of *G*. If we simply restrict ourselves to the *subgroup K*, then it immediately follows from (4) above that *H* is *normal* in *K*.

□

HOMORMORPHISMS AND ONE-TO-ONE FUNCTTIONS

Discussion: The theorem below give a very useful result. It shows that if we have a *homomorphism* from one *group onto* another, then another way to show that this *homomorphism* is also a *one-to-one function* is to simply verify that the only element in the *Kernel* is the *identity*.

Theorem: Let $f: A \to B$ be a *homomorphism* from a *group A* onto a *group B*. Then *f* is *one-to-one* if and only if $Ker(f) = \{e\}$.

Proof: Suppose $f: A \to B$ is a homomorphism from a *group A* onto a *group B*, and suppose that *f* is *one-to-one*. By previous proof, we know that $f(e) = e$, and if *f* is *one-to-one*, then it follows that $Ker(f)$ contains only the identity, *e*.

Now suppose that $Ker(f) = \{e\}$, and suppose that *f* is not *one-to-one*. Then there exists $a, b \in A$ with $a \neq b$ such that $f(a) = f(b)$. But this means that $e = f(a)\left[f(b)\right]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ where $ab^{-1} \neq e$. This contradicts our assumption that $Ker(f) = \{e\}$. Therefore, *f* is *one-to-one*.

□

THE FIRST ISOMORPHISM THEOREM

Theorem: Let $f: A \to B$ be a *homomorphism* from a *group A onto* a *group B*, and let $N = Ker(f)$. Then $A/Ker(f) = A/N \cong B$.

Proof: Recall that $\pi : A \to A/N$ defined by $\pi(a) = Na$ is called the *natural homomorphism*. Now define a function *i* from A/N to *B* by $i(Na) = f(a)$. What we want to do now is to verify that *i* is an *isomorphism* from A/N to *B*. First, we will show that this function is *onto*. Thus, if $b \in B$, then there exists $a \in A$ such that $f(a) = b$ since *f* is *onto*. Hence, $i(\pi(a)) = i(Na) = f(a) = b$ shows that *i* is also *onto*.

To show that *i* is *one-to-one*, let $Nx, Ny \in A/N$ and suppose that $Nx \neq Ny$. Then, in particular, Nx and Ny have no elements in common because if they did, then we would have $n_1 x = n_2 y \Rightarrow x = n_1^{-1} n_2 y \Rightarrow x \in Ny \Rightarrow Nx = Ny$. Furthermore, $f(x) \neq f(y)$ because if $f(x) = f(y)$, then $e = f(x)\left[f(y)\right]^{-1} = f(x) f(y^{-1}) = f(xy^{-1})$ implies that $xy^{-1} \in N = Ker(f)$ which implies that $xy^{-1} = n \in N \Rightarrow x = ny \Rightarrow Nx = Ny$. But this contradicts our assumption that $Nx \neq Ny$, and, hence, $Nx \neq Ny \Rightarrow f(x) \neq f(y) \Rightarrow i(Nx) \neq i(Ny)$, and so $i : A/N \to B$ is *onto-to-one*.

Before we show that $i : A/N \to B$ is a *homomorphism*, notice that it doesn't matter what representative we use from a coset such as *Na*. In other words, since $N = Ker(f)$, if $a, b \in Na$, then $a = nb$ and $f(a) = f(nb) = f(n) f(b) = e \cdot f(b) = f(b)$. Hence, it is also true that $i(a) = i(b)$. Now let $Nx, Ny \in A/N$. Then $i(NxNy) = i(Nxy) = f(xy) = f(x) f(y) = i(Nx) i(Ny)$. Therefore, $i : A/N \to B$ is an *isomorphism*, and $A/Ker(f) = A/N \cong B$.

□

THE SECOND ISOMORPHISM THEOREM

Discussion: In Theorem 29 of Part 9 we proved that if *H* is a *subgroup* of a *group* *G* and if *N* is a *normal subgroup* of *G*, then the right (left) cosets corresponding to elements of *H* form a *subgroup* of G/N. The theorem below, known as the *Second Isomorphism Theorem*, give us much sharper detail on the structure of this *subgroup* of G/N.

The Second Isomorphism Theorem: If *H* and *N* are *subgroups* of a *group G* with *N normal* in *G*, then $H/H \cap N \cong HN/N$.

Proof: Recall that earlier we proved (Part 9, Theorem 29) that if *H* is a *subgroup* of *G*, then there will exist a corresponding *subgroup* of G/N that is obtained by looking at the *cosets Nh* where $h \in H$. This theorem, the *Second Isomorphism Theorem*, sharpens and clarifies the result. To prove it, though, we first need to show that $H \cap N$ is a *normal subgroup* of *H* and that *HN* is a *subgroup* of *G* that contains *N*. So let's begin!

To show that $H \cap N$ is a *normal subgroup* of *H*, we first need to show that it is at least a *subgroup* by verifying properties of *closure* and existence of *inverses*. Thus, let $n_1, n_2 \in H \cap N$. Since $n_1, n_2 \in H$, a *subgroup* of *G*, it follows that $n_1 n_2 \in H$. But by the same token, $n_1, n_2 \in N$ implies that $n_1 n_2 \in N$. Hence, $n_1 n_2 \in H \cap N$, and *closure* is satisfied.

Now suppose that $n \in H \cap N$. Then an *inverse* to *n* exists in both *H* and in *N*. In other words, $n^{-1} \in H$ and $n^{-1} \in N$ implies that $n^{-1} \in H \cap N$. Thus, existence of *inverses* is satisfied, and $H \cap N$ is a *subgroup* of *H*.

To show that $H \cap N$ is a *normal subgroup* of *H*, let $h \in H$ and let $n \in H \cap N$. Then $h^{-1}nh \in H$ since all three elements belong to *H*. But on the other hand, $h^{-1}nh \in N$ since *N* is a *normal subgroup* of *G*. Hence, $h^{-1}nh \in H \cap N$, and so $H \cap N$ is a *normal subgroup* of *H*.

Now let's show that *HN* is a *subgroup* of *G*. Thus, to show *closure*, let $h_1n_1, h_2n_2 \in HN$, and consider the product $h_1n_1h_2n_2$. Since *N* is a *normal subgroup* of *G*, every *left coset* of *N* is equal to the corresponding *right coset*, and that means that $h_2N = Nh_2 = Nh_2 = (Nn_1)h_2 = Nn_1h_2$. Hence, there exists $n_3 \in N$ such that $h_2n_3 = n_1h_2$. Thus, $h_1n_1h_2n_2 = h_1(n_1h_2)n_2 = h_1(h_2n_3)n_2 = h_1h_2n_3n_2 \in HN$, and *closure* is satisfied. To show the existence of *inverses* in *HN*, let $hn \in HN$ where $h \in H$ and $n \in N$. Then it's *inverse* is $n^{-1}h^{-1}$. However, again since *N* is *normal* in *G*, there exist $n^{-1}, n_4 \in N$ such that $hn^{-1}h^{-1} = n_4 \Rightarrow n^{-1}h^{-1} = h^{-1}n_4 \in HN$. Therefore, *inverses* exist in *HN*, and *HN* is a subgroup of *G*. Furthermore, $N \subseteq HN$ since every element of *N* can be written as $e \cdot n$ where $e \in H$ and $n \in N$.

And finally, we need to state and prove our *isomorphism* from $H/H \cap N$ to HN/N. In this case, define $f : H/H \cap N \to HN/N$ by $f[(H \cap N)h] = Nh$. To show that *f* is a *homomorphism*, observe that

$f[(H \cap N)h_1] \cdot f[(H \cap N)h_2] = Nh_1 \cdot Nh_2 = N(h_1h_2) = f[(H \cap N)h_1h_2]$ Notice, too, that elements in $H/H \cap N$ look like $\{H \cap N, (H \cap N)h_1, (H \cap N)h_2, (H \cap N)h_3, \ldots\}$ where $h_1, h_2, h_3, \ldots \notin H \cap N$, and the corresponding elements in HN/N look like $\{N, Nh_1, Nh_2, Nh_3, \ldots\}$. From this it should be clear that $Ker(f) = H \cap N$, the *identity* in $H/H \cap N$, because if $h \notin H \cap N$, then it gets mapped to $Nh \neq N$, where *N* is the *identity* in HN/N. Thus, from previous proof on *homomorphisms* and *one-to-one functions*, it follows that *f* is *one-to-one*. And finally, to show that *f* is *onto*, suppose that $Nhn \in HN/N$, where $h \in H$ and $n \in N$. Then since *N* is a *normal subgroup*, we can rewrite *hn* as n_1h for some $n_1 \in N$. Hence, $Nhn = Nn_1h = Nh = f[(H \cap N)h]$, and therefore, *f* is *onto* and $H/H \cap N \cong HN/N$. □

THE THIRD ISOMORPHISM THEOREM

Discussion: This *Third Isomorphism Theorem* is in some ways a continuation of our *Correspondence Theorem* in that it establishes an *isomorphism* between a *quotient group* and a particular *quotient* of another *quotient group*.

The Third Isomorphism Theorem: Let *G* be a *group*, let *N* and *H* be *normal subgroups* of *G*, and suppose that $N \subseteq H \subseteq G$. Then H/N is a *normal subgroup* of G/N, and $(G/N)/(H/N) \cong G/H$.

Proof: It follows immediately from (3) of the *Correspondence Theorem* that H/N is a *normal* subgroup of G/N. Now let $i: G \to G/N$ be the *natural homomorphism*, and let $j: G/N \to (G/N)/(H/N)$ be another *natural homomorphism*. Then $j \circ i$ is a *homomorphism* from *G onto* $(G/N)/(H/N)$.

$$G \xrightarrow{i} G/N \xrightarrow{j} (G/N)/(H/N)$$

Hence, our *First Isomorphism Theorem* tells us that $(G/N)/(H/N)$ is *isomorphic* to $G/Ker(j \circ i)$. Thus, we just need to figure out what is contained in $Ker(j \circ i)$. Hence, let $h \in H \subseteq G$. Then $Nh \in H/N \subseteq G/N$ tells us that $h \in Ker(j \circ i)$. On the other hand, if $g \in G$, but $g \notin H$, then $Ng \notin H/N$, and, thus, $g \notin Ker(j \circ i)$. Therefore, $Ker(j \circ i) = H$, and by the *First Isomorphism Theorem*, G/H is *isomorphic* to $(G/N)/(H/N)$.

□

AN APPLICATION

Discussion: Recall that in a *permutation group*, every permutation can be classified as even or odd and it can easily be shown that the *even permutations* form a *normal subgroup* of any *permutation group*. In particular, if S_n is the group of all *permutations* that can be made of *n* objects, then the *normal subgroup* of all *even permutations* is called the *alternating group of degree n*, A_n, and in the theorem below we show that for $n \geq 2$, the number of elements in A_n is $|A_n| = \frac{n!}{2}$.

Definition: If S_n is the group of all permutations that can be made of *n* objects (known as the *symmetric group of degree n*), then the *alternating group of degree n*, A_n, is the *subgroup* of all *even permutations* in S_n. Also, since the *identity* is counted as an *even permutation*, this *subgroup* of S_n always exists.

Theorem: If S_n is the *symmetric group of degree n* for $n \geq 2$, then $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Proof: We can define a *surjective* (*onto*) *homomorphism* $f : S_n \to \mathbb{Z}_2$ by
$$f(p) = \begin{cases} 0 & \text{if } p \text{ is an even permutation} \\ 1 & \text{if } p \text{ is an odd permutation} \end{cases}.$$

For S_n with $n \geq 2$, it should be clear that S_n will contain both *even* and *odd permutations*. For example, it contains the *identity* which is an *even permutation*, and it contains *transpositions* of two elements which are *odd permutations*. Thus, $S_n \neq A_n$. However, A_n is the *Kernel of f*, and, thus, $\mathbb{Z}_2 \cong S_n / Ker(f) = S_n / A_n$. From this it immediately follows that $2 = |\mathbb{Z}_2| = |S_n / A_n| = |S_n| / |A_n| = \frac{n!}{|A_2|} \Rightarrow |A_n| = \frac{n!}{2}$. □

ANOTHER APPLICATION

Discussion: Frankly, I found this result rather interesting!

Theorem: A *group* of permutations of odd order consists of only *even permutations*.

Proof: Let *G* be a *group* of permutations such that $|G|$ is odd. If $|G|=1$, then the only permutation in *G* is the *identity* which is even. If $|G|=3$, then *G* is the cyclic group of order 3 (since up to *isomorphism* there exists only one group of order 3), and we can represent the permutations as $\{(\ ),(1,2,3),(1,3,2)\}$, and each of these permutations is even. Thus, assume that $|G|$ is odd and greater than three. Then *G* has more than two elements which are not the identity. Also, as before, define $f:G\to\mathbb{Z}_2$ by $f(p)=\begin{cases}0 & \text{if } p \text{ is an even permutation}\\ 1 & \text{if } p \text{ is an odd permutation}\end{cases}$.

If $Ker(f)=G$, then every permutation in *G* is even, and we are done. Thus, assume that not every permutation in *G* is even, i.e. that some are odd. In this case, $f:G\to\mathbb{Z}_2$ will be an onto function, and we have that $2=|\mathbb{Z}_2|=|G/Ker(f)|=|G|/|Ker(f)|\Rightarrow|G|=2\cdot Ker(f)$. But this contradicts our assumption that $|G|$ is odd, and therefore, a *group* of permutations of odd order consists of only *even permutations*.

□

A THIRD APPLICATION

<u>Discussion:</u> Below, we define an *isomorphism* from a *group onto* itself as an *automorphism*, and we show that the operation of conjugation that we introduced back in Part 2 results in a very important *automorphism* that we call an *inner automorphism*.

<u>Definition:</u> An *isomorphism* from a *group G* onto itself is called an <u>*automorphism*</u>.

<u>Theorem:</u> Let *G* be a *group*, let $g \in G$, and defined a function $f_g : G \to G$ by $f_g(a) = g^{-1}ag$ for every $a \in G$. Then f_g is an *automorphism*.

<u>Proof:</u> Let *G* be a *group*, let $g \in G$, and define a function $f_g : G \to G$ by $f_g(a) = g^{-1}ag$ for every $a \in G$. To show that f_g is an *automorphism*, we need to show that it is a *homomorphism*, it's *onto*, and it's *one-to-one*. To show that it's a *homomorphism*, let $a, b \in G$. Then $f_g(a) f_g(b) = g^{-1}ag \cdot g^{-1}bg = g^{-1}a \cdot e \cdot bg = g^{-1}(ab)g = f_g(ab)$. To show that it's *onto*, let $a \in G$. Then gag^{-1} is also an element of *G*, and $f_g(gag^{-1}) = g^{-1}(gag^{-1})g = e \cdot a \cdot e = a$. And finally, to show that $f_g : G \to G$ is *one-to-one*, suppose $a \in Ker(f_g)$. Then $f_g(a) = e \Rightarrow g^{-1}ag = e \Rightarrow a = geg^{-1} = e$. Hence, $Ker(f_g)$ consists only of *e*, and the *homomorphism* is *one-to-one* as well as *onto*. Therefore, $f_g : G \to G$ defined by $f_g(a) = g^{-1}ag$ is an *automorphism*. Furthermore, this particular type of *automorphism* is called an <u>*inner automorphism*</u>.

□

A FOURTH RESULT

Discussion: We introduced the notion of a *commutator* back in our section on beginning *group theory*, and in Theorem 21 of Part 9 we proved that the *subgroup* generated by forming all finite products of the *commutators* in our *group* is a *normal subgroup* of our *group*. In the theorem below, we show that the *quotient group* of our *group* by the c*ommutator subgroup* is always *abelian*. Furthermore, it could even be shown that the *Kernel* of any *quotient group* that is *abelian* must contain this *commutator* subgroup. However, this last part we leave for you to ponder.

Theorem: Let *G* be a *group*, and let G' be the *derived* or *commutator subgroup*, the *subgroup* generated by all products in *G* of the form $a^{-1}b^{-1}ab$. Then G/G' is *abelian*.

Proof: Let $\pi : G \to G/G'$ be the *natural homomorphism* where $\pi(g) = G'g$. To show that G/G' is *abelian*, we need to show that if $G'a, G'b \in G/G'$, then $G'aG'b = G'bG'a$. Another way to express this equation is as $\left[G'a\right]^{-1}\left[G'b\right]^{-1}G'aG'b = G'$, the *identity* in G/G'. However, this is easy to verify since $\left[G'a\right]^{-1}\left[G'b\right]^{-1}G'aG'b = (G'a^{-1})(G'b^{-1})G'aG'b = G'(a^{-1}b^{-1}ab)$. Hence, since $a^{-1}b^{-1}ab$ is a *commutator*, it follows that $G'(a^{-1}b^{-1}ab) = G'$, the *identity* in G/G'. Therefore, $\left[G'a\right]^{-1}\left[G'b\right]^{-1}G'aG'b = G'(a^{-1}b^{-1}ab) = G'$, the *identity* in G/G', implies that $G'aG'b = G'bG'a$ and G/G' is *abelian*.

□

QUOTIENTS OF QUOTIENTS OF QUOTIENTS

We are now going to examine not only some *quotient groups*, but also *quotients of quotients* and *quotients of quotients of quotients* in order to get a feel for what they are really like. Thus, let's start with the *group* $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The order of *G* is $|G| = 16$, and the elements of *G*, expressed as coordinates (not permutations) are,

$$G = \left\{ \begin{matrix} (0,0,0,0),\ (0,1,0,0),\ (0,0,1,0),\ (0,0,0,1),\ (0,1,1,0),\ (0,1,0,1),\ (0,0,1,1),\ (0,1,1,1), \\ (1,0,0,0),\ (1,1,0,0),\ (1,0,1,0),\ (1,0,0,0),\ (1,1,1,0),\ (1,1,0,1),\ (1,0,1,1),\ (1,1,1,1) \end{matrix} \right\}$$

Since these elements are expressed as coordinates *modulo* 2, when we "multiply" them we actually just <u>add</u> them together coordinatewise using the rule that 1 + 1 = 0. For example, $(1,0,1,0) + (0,1,1,1) = (1+0, 0+1, 1+1, 0+1) = (1,1,0,1)$. Also, this group is *abelian*, and so all of its *subgroups* are *normal*. In particular, let's consider the following *subgroups*:

$$N_1 = \{(0,0,0,0),\ (1,0,0,0)\} = \left\{ \begin{matrix} (0,0,0,0) \\ (1,0,0,0) \end{matrix} \right\}$$

$$N_2 = \{(0,0,0,0),\ (1,0,0,0),\ (0,1,0,0),\ (1,1,0,0)\} = \left\{ \begin{matrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{matrix} \right\}$$

$$N_3 = \{(0,0,0,0),\ (1,0,0,0),\ (0,1,0,0),\ (1,1,0,0),\ (0,0,1,0),\ (1,0,1,0),\ (0,1,1,0),\ (1,1,1,0)\}$$

$$= \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \\ (0,0,1,0) \\ (1,0,1,0) \\ (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix}$$

Notice that $N_1 \subset N_2 \subset N_3$. Furthermore, $|G/N_1| = 8$, and the *cosets* in G/N_1 are,

$$G/N_1 = \left\{ \begin{matrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,1,0,0), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,0,1,0), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,0,0,1), \\ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,1,1,0), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,1,0,1), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,0,1,1), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,1,1,1) \end{matrix} \right\}$$

$$= \left\{ \begin{matrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,0) \\ (1,0,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \end{Bmatrix}, \\ \begin{Bmatrix} (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,1,0,1) \\ (1,1,0,1) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,1) \\ (1,0,1,1) \end{Bmatrix}, \begin{Bmatrix} (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \end{matrix} \right\}$$

We want to now look at G/N_2 which by our 3rd *isomorphism theorem* is *isomorphic* to $(G/N_1)/(N_2/N_1)$. Thus, we'll first write down the *cosets* for G/N_2 and then compare this to the *cosets* in $(G/N_1)/(N_2/N_1)$ and in the process our construction will show that we can always find *quotients of quotients* by multiplying the *subgroup* we are *factoring* out by an appropriate element of our original *group G*. In particular, $|G/N_2| = 4$, and the *cosets* in G/N_2 are,

$$G/N_2 = \left\{ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}(0,0,1,0), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}(0,0,0,1), \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}(0,0,1,1) \right\}$$

$$= \left\{ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,0) \\ (1,0,1,0) \\ (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \\ (0,1,0,1) \\ (1,1,0,1) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,1) \\ (1,0,1,1) \\ (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \right\}$$

Now we want to compare this to the *cosets* in $(G/N_1)/(N_2/N_1)$, so let's first write down N_2/N_1.

$$N_2/N_1 = \left\{ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}(0,1,0,0) \right\} = \left\{ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix} \right\}$$

$$= \left\{ \begin{matrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix} \\ \begin{Bmatrix} (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix} \end{matrix} \right\}$$

Since,

$$G/N_1 = \left\{ \begin{matrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,0) \\ (1,0,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \end{Bmatrix}, \\ \begin{Bmatrix} (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,1,0,1) \\ (1,1,0,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,1,1) \\ (1,0,1,1) \end{Bmatrix}, \begin{Bmatrix} (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \end{matrix} \right\},$$

We have that,

$$\left(G/N_1\right)/\left(N_2/N_1\right)$$

$$=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\}(0,0,1,0),\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\}(0,0,0,1),\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\}(0,0,1,1)\right\}$$

$$=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}(0,0,1,0)\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}(0,0,1,0)\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}(0,0,0,1)\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}(0,0,0,1)\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}(0,0,1,1)\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}(0,0,1,1)\end{matrix}\right\}\right\}$$

$$=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,0,1)\\(1,1,0,1)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,1,1)\\(1,0,1,1)\end{matrix}\right\}\\\left\{\begin{matrix}(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\end{matrix}\right\}\right\}$$

Notice now the structural similarity between $\left(G/N_1\right)/\left(N_2/N_1\right)$ and G/N_2.

$$G/N_2=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\\(0,1,0,1)\\(1,1,0,1)\end{matrix}\right\},\left\{\begin{matrix}(0,0,1,1)\\(1,0,1,1)\\(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\right\}$$

And now we'll move on to G/N_3 which is *isomorphic* to both $\left(G/N_2\right)/\left(N_3/N_2\right)$ and $\left[\left(G/N_1\right)/\left(N_2/N_1\right)\right]/\left[\left(N_3/N_1\right)/\left(N_2/N_1\right)\right]$. As before, we'll start with the simplest *quotient group*, G/N_3, and we'll methodically construct the other *quotient groups* so that we can observe the similarities. Thus, $\left|G/N_3\right|=2$, and the *cosets* in G/N_3 are,

$$G/N_3=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\\(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\\(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}(0,0,0,1)\right\}=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\\(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\\(0,1,0,1)\\(1,1,0,1)\\(0,0,1,1)\\(1,0,1,1)\\(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\right\}$$

To construct $(G/N_2)/(N_3/N_2)$, we must first write down N_3/N_2.

$$N_3/N_2=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}(0,0,1,0)\right\}=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\right\}$$

$$=\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\}$$

And since,

$$G/N_2=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\\(0,1,0,1)\\(1,1,0,1)\end{matrix}\right\},\left\{\begin{matrix}(0,0,1,1)\\(1,0,1,1)\\(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\right\},$$

we have that,

$$\left(G/N_2\right)/\left(N_3/N_2\right)=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\}(0,0,0,1)\right\}$$

$$=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}(0,0,0,1)\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}(0,0,0,1)\end{matrix}\right\}\right\}=\left\{\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\}\end{matrix}\right\},\left\{\begin{matrix}\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\\(0,1,0,1)\\(1,1,0,1)\end{matrix}\right\}\\\left\{\begin{matrix}(0,0,1,1)\\(1,0,1,1)\\(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\end{matrix}\right\}\right\}$$

Again, notice the structural similarity between this and G/N_3.

$$G/N_3=\left\{\left\{\begin{matrix}(0,0,0,0)\\(1,0,0,0)\\(0,1,0,0)\\(1,1,0,0)\\(0,0,1,0)\\(1,0,1,0)\\(0,1,1,0)\\(1,1,1,0)\end{matrix}\right\},\left\{\begin{matrix}(0,0,0,1)\\(1,0,0,1)\\(0,1,0,1)\\(1,1,0,1)\\(0,0,1,1)\\(1,0,1,1)\\(0,1,1,1)\\(1,1,1,1)\end{matrix}\right\}\right\}$$

And finally, we want to construct the *cosets* for $\left[\left(G/N_1\right)/\left(N_2/N_1\right)\right]/\left[\left(N_3/N_1\right)/\left(N_2/N_1\right)\right]$. We'll start first with N_2/N_1, then N_3/N_1 followed by $\left(N_3/N_1\right)/\left(N_2/N_1\right)$.

$$N_2/N_1=\left\{\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix},\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,1,0,0)\right\}=\left\{\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix},\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\right\}$$

$$=\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\}$$

$$N_3/N_1=\left\{\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix},\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,1,0,0),\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,0,1,0),\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,1,1,0)\right\}$$

$$=\left\{\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix},\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix},\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix},\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\right\}$$

$$\left(N_3/N_1\right)/\left(N_2/N_1\right)=\left\{\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\}(0,0,1,0)\right\}$$

$$=\left\{\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,0,1,0)\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}(0,0,1,0)\end{matrix}\right\}\right\}.$$

$$=\left\{\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{matrix}\right\}\right\}$$

We previously found the following *cosets* for $\left(G/N_1\right)/\left(N_2/N_1\right)$.

$$\left(G/N_1\right)/\left(N_2/N_1\right)=\left\{\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,0,0)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,0,1)\\(1,0,0,1)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,1)\\(1,1,0,1)\end{Bmatrix}\end{matrix}\right\},\left\{\begin{matrix}\begin{Bmatrix}(0,0,1,1)\\(1,0,1,1)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,1)\\(1,1,1,1)\end{Bmatrix}\end{matrix}\right\}\right\}$$

Hence, we can now write down the *cosets* for

$\left[(G/N_1)/(N_2/N_1)\right]/\left[(N_3/N_1)/(N_2/N_1)\right]$ as follows,

$$\left[(G/N_1)/(N_2/N_1)\right]/\left[(N_3/N_1)/(N_2/N_1)\right]=\left\{\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix},\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix}(0,0,0,1)\right\}$$

$$=\left\{\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix},\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}(0,0,0,1)\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}(0,0,0,1)\end{Bmatrix}\right\}=\left\{\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix},\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}(0,0,0,1)\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}(0,0,0,1)\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}(0,0,0,1)\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}(0,0,0,1)\end{Bmatrix}\end{Bmatrix}\right\}$$

$$=\left\{\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,0)\\(1,0,0,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,0)\\(1,1,0,0)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,0)\\(1,0,1,0)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,0)\\(1,1,1,0)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix},\begin{Bmatrix}\begin{Bmatrix}\begin{Bmatrix}(0,0,0,1)\\(1,0,0,1)\end{Bmatrix}\\\begin{Bmatrix}(0,1,0,1)\\(1,1,0,1)\end{Bmatrix}\end{Bmatrix}\\\begin{Bmatrix}\begin{Bmatrix}(0,0,1,1)\\(1,0,1,1)\end{Bmatrix}\\\begin{Bmatrix}(0,1,1,1)\\(1,1,1,1)\end{Bmatrix}\end{Bmatrix}\end{Bmatrix}\right\}$$

Again, we want to notice the structural similarities between the three *isomorphic groups*.

$$G/N_3 = \left\{ \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \\ (0,0,1,0) \\ (1,0,1,0) \\ (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix}, \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \\ (0,1,0,1) \\ (1,1,0,1) \\ (0,0,1,1) \\ (1,0,1,1) \\ (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \right\}$$

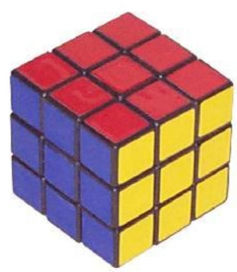
$$(G/N_2)/(N_3/N_2) = \left\{ \begin{Bmatrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \\ (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix} \\ \begin{Bmatrix} (0,0,1,0) \\ (1,0,1,0) \\ (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix} \end{Bmatrix}, \begin{Bmatrix} \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \\ (0,1,0,1) \\ (1,1,0,1) \end{Bmatrix} \\ \begin{Bmatrix} (0,0,1,1) \\ (1,0,1,1) \\ (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \end{Bmatrix} \right\}$$

$$\left[(G/N_1)/(N_2/N_1)\right]/\left[(N_3/N_1)/(N_2/N_1)\right] = \left\{ \begin{Bmatrix} \begin{Bmatrix} \begin{Bmatrix} (0,0,0,0) \\ (1,0,0,0) \end{Bmatrix} \\ \begin{Bmatrix} (0,1,0,0) \\ (1,1,0,0) \end{Bmatrix} \end{Bmatrix} \\ \begin{Bmatrix} \begin{Bmatrix} (0,0,1,0) \\ (1,0,1,0) \end{Bmatrix} \\ \begin{Bmatrix} (0,1,1,0) \\ (1,1,1,0) \end{Bmatrix} \end{Bmatrix} \end{Bmatrix}, \begin{Bmatrix} \begin{Bmatrix} \begin{Bmatrix} (0,0,0,1) \\ (1,0,0,1) \end{Bmatrix} \\ \begin{Bmatrix} (0,1,0,1) \\ (1,1,0,1) \end{Bmatrix} \end{Bmatrix} \\ \begin{Bmatrix} \begin{Bmatrix} (0,0,1,1) \\ (1,0,1,1) \end{Bmatrix} \\ \begin{Bmatrix} (0,1,1,1) \\ (1,1,1,1) \end{Bmatrix} \end{Bmatrix} \end{Bmatrix} \right\}$$

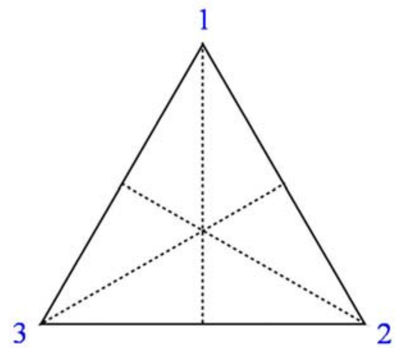
Among other things, this hopefully illustrates that as we continue to take *quotients of quotients*, every *coset* in the resulting *quotient group* can still be written as an element of *G* times the *identity* in that particular *quotient of quotients*. Divide and conquer!

ORBITS, STABILIZERS, FIXERS, AND BURNSIDE'S COUNTING THEOREM

Consider this situation. You have just solved Rubik's cube, but you also instinctively know that if you rotated the cube 90° in any of six directions, then you would still consider the cube to still be in the same solved configuration. Thus, certain movements of the cube don't really result in what we consider a different configuration. And now our problem is this. Suppose we color the faces of the cube with six different colors and that we are also allowed to rotate the cube as described above. Then how many truly different color configurations are possible when we allow for rotations of the cube? This is the type of question we'll learn to answer in this chapter with the help of what we call *orbits*, *stabilizers*, *fixers*, and *Burnside's Counting Theorem*.



Remember: There are a few definitions and theorems you might want to recall before you wade any further into this section. First, when we say that G is a group that acts on a set of objects X, that means that each element of G corresponds to a permutation of the elements of X. For example, consider the equilateral triangle below with vertices labeled by 1, 2, or 3.



We can let $X=\{1,2,3\}$ and our *group G* can correspond to the permutations of these numbers created by either rotating the above triangle clockwise through angles that are *integer* multiples of $120°$ or by flipping the triangle about one of the indicated axes of symmetry or by some combination of these moves. By doing so, we can identify six distinct permutations which can be represented as follows.

$$\begin{aligned}
&g_1 = \text{ the identity } = e = (\ )\\
&g_2 = (1,2,3) \ \ [\text{Recall that this permutation means } 1 \to 2,\ 2 \to 3,\ \&\ 3 \to 1]\\
&g_3 = (1,3,2)\\
&g_4 = (2,3)\\
&g_5 = (1,3)\\
&g_6 = (1,2)
\end{aligned}$$

We will use this example down below, so remember it. Also, recall that we denote the number of elements in a set or *group* by putting absolute value signs around the symbol for that set or *group*. Hence, for the *group G* above, we have $|G|=6$.

And finally, recall that if *H* is a *subgroup* of a *finite group G*, then the ***left coset*** of *H* in *G* created by $a \in G$ is $aH=\{ah \mid h \in H\}$. Additionally, by *Lagrange's Theorem*, the number of *left cosets* of *H* in *G* is a divisor of *G* and is denoted by $[G:H]=\dfrac{|G|}{|H|}$.

Notice that even though in the past we have generally examined *right cosets*, for the proofs that follow it will be easier this time to deal with *left cosets*.

Definition: Let *G* be a *group* that acts on a set *X*, and let $x \in X$. The *orbit of x by G* is the set $Orbit_G(x) = \{g(x) | g \in G\}$. In other words, the *orbit of x* consists of all elements of *X* that *x* can be changed into by the various elements of *G*.

Theorem: Let *G* be a *group* that acts on a set *X*, and let $\equiv$ be a relation on *X* defined by $x \equiv y$ if and only if $y = g(x)$ for some $g \in G$. Then $\equiv$ is an *equivalence relation*.

Proof: Recall that we need to show that this relationship is *reflexive*, *symmetric*, and *transitive*. Let's begin!

1. (*reflexive*) Let $e \in G$ be the *identity element* in *G*. Then, by definition, *e* leaves every element of *X* fixed so that $e(x) = x$. Hence, $x \equiv x$ and $\equiv$ is *reflexive*.

2. (*symmetric*) Suppose $x \equiv y$. Then there exists $g \in G$ such that $g(x) = y$. However, this implies that $g^{-1}(y) = x$ and that $y \equiv x$. Thus, $\equiv$ is *symmetric*.

3. (*transitive*) Suppose there exist $x, y, z \in X$ such that $x \equiv y$ and $y \equiv z$. Then there exist functions $g_1, g_2 \in G$ such that $g_1(x) = y$ and $g_2(y) = z$. Now let $g_3 = g_2 \circ g_1 \in G$. Then $g_3(x) = (g_2 \circ g_1)(x) = g_2(g_1(x)) = g_2(y) = z$. Therefore, $x \equiv z$ and $\equiv$ is *transitive*.

It now follows that $\equiv$ is an *equivalence relation* on *X*, and, hence, it partitions *X* into a series of disjoint subsets whose union is *X*. Also, it should be clear that each subset of this partition represents a single *orbit* created by the permutations in *G* when applied to the elements in the set *X*.

□

Corollary: If *x* and *y* belong to the same orbit, then $Orbit_G(x) = Orbit_G(y)$ and, consequently, $|Orbit_G(x)| = |Orbit_G(y)|$. (Recall that $|Orbit_G(x)|$ means the number of elements in $Orbit_G(x)$.)

Definition: Let *G* be a *group* that acts upon a set *X*, and let $x \in X$. Then the *stabilizer of x by G* is $Stabilizer_G(x) = G_x = \{g \in G | g(x) = x\}$.

Theorem: If *G* is a *group* that acts on a set *X*, and if $x \in X$, then the *stabilizer of x by G* is a *subgroup* of *G*.

Proof: To verify that $Stabilizer_G(x) = G_x$ is a *subgroup* of *G*, we need to show that for every $g \in Stabilizer_G(x) = G_x$ we have that $g^{-1} \in Stabilizer_G(x) = G_x$, and that for every $g_1, g_2 \in Stabilizer_G(x) = G_x$, we have that $g_1 \circ g_2 \in Stabilizer_G(x) = G_x$.

Thus, suppose $g \in Stabilizer_G(x) = G_x$. Then $x = e(x) = (g^{-1} \circ g)(x) = g^{-1}(g(x)) = g^{-1}(x)$. Hence, $g^{-1} \in Stabilizer_G(x) = G_x$.

Now suppose $g_1, g_2 \in Stabilizer_G(x) = G_x$. Then $(g_1 \circ g_2)(x) = g_1(g_2(x)) = g_1(x) = x$. Consequently, $g_1 \circ g_2 \in Stabilizer_G(x) = G_x$.

Therefore, it now follows that $Stabilizer_G(x) = G_x$ is a subgroup of *G*.

□

Theorem: If *G* is a *finite group* that acts on a set *X*, and if $x \in X$, then the number of elements in the *orbit of x* is $\left|Orbit_G(x)\right| = \left[G : G_x\right] = \frac{|G|}{|G_x|} = \frac{|G|}{\left|Stabilizer_G(x)\right|}$.

Proof: Since $Stabilizer_G(x) = G_x$ is a *subgroup* of *G*, we can consider the *left cosets* of G_x in *G*. In particular, notice that if $g_1, g_2 \in Stabilizer_G(x) = G_x$, then $g_1(x) = x = g_2(x)$. Now consider a *left coset* hG_x and suppose $h_1, h_2 \in hG_x$. Then $h_1 = hg_1$ & $h_2 = hg_2$ for some $g_1, g_2 \in G_x \Rightarrow h = h_1 g_1^{-1} \Rightarrow h_2 = hg_2 = (h_1 g_1^{-1}) g_2 = h_1 (g_1^{-1} g_2) = h_1 g$ where $g = g_1^{-1} g_2 \in G_x$. Hence, $h_2(x) = (h_1 g)(x) = (h_1 \circ g)(x) = h_1(g(x)) = h_1(x)$. Thus, all elements in the same *left coset* of G_x yield the same value when applied to *x*.

Furthermore, if aG_x and bG_x are two different *left cosets* of G_x, then $a(x) \neq b(x)$ since, otherwise, if it were true that $a(x) = y = b(x)$, then $(a^{-1}b)(x) = (a^{-1} \circ b)(x) = a^{-1}(b(x)) = a^{-1}(y) = x \Rightarrow a^{-1}b = g$ for some $g \in G_x \Rightarrow ag = a(a^{-1}b)$ $= (aa^{-1})b = e \cdot b = b \Rightarrow$ *a* and *b* belong to the same *left coset* of G_x. But this contradicts our assumption that $aG_x \neq bG_x$.

From the above it follows that we can find all the elements in the *orbit of x* by simply picking an arbitrary function from each *left coset* of G_x and applying it to *x*. In particular, the number of elements in the *orbit of x* is the same as the number of *left cosets* of G_x in *G*. Therefore, by *Lagrange's Theorem*, $\left|Orbit_G(x)\right| = \left[G : G_x\right] = \frac{|G|}{|G_x|} = \frac{|G|}{\left|Stabilizer_G(x)\right|}$.

$\square$

Corollary: We can also rewrite $\left|Orbit_G(x)\right| = \frac{|G|}{|G_x|} = \frac{|G|}{\left|Stabilizer_G(x)\right|}$ as $|G_x| = \left|Stabilizer_G(x)\right| = \frac{|G|}{\left|Orbit_G(x)\right|}$.

Definition: Let *G* be a *group* that acts upon a set *X*, and let $x \in X$. Then the *fixer of g in X* is $Fixer_X(g) = \{x \in X \mid g(x) = x\}$.

Theorem: Let *G* be a *group* that acts on a set *X* and let $A = \{(g,x) \mid g(x) = x \text{ where } g \in G \text{ and } x \in X\}$. Then the number of elements in *A*, denoted by $|A|$, is $|A| = \sum_{x \in X} \left|Stabilizer_G(x)\right| = \sum_{x \in X} |G_x| = \sum_{g \in G} \left|Fixer_X(g)\right|$.

Proof: The statement is obvious once you realize that $\sum_{x \in X} \left|Stabilizer_G(x)\right|$ and $\sum_{g \in G} \left|Fixer_X(g)\right|$ are just counting the same thing in two different ways. In $\sum_{x \in X} \left|Stabilizer_G(x)\right|$, we're fixing an $x \in X$ and then counting up all the functions $g \in G$ such that $g(x) = x$. And then we go on to the next $x \in X$. On the other hand, in $\sum_{g \in G} \left|Fixer_X(g)\right|$ we fix $g \in G$ and then count up the number of elements $x \in X$ such that $g(x) = x$. And then we move on to another $g \in G$.

As an example, suppose $X = \{1,2,3\}$, $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$, (as defined at the beginning of this chapter), and $A = \{(g_1,1),(g_1,2),(g_1,3),(g_4,1),(g_5,2),(g_6,3)\}$. Then $|A| = 6$, and we can count this total in either of the two ways below.

x	|Stabilizer(x)|
1	2
2	2
3	2
	Sum=6

g	|Fixer(g)|
g1	3
g2	0
g3	0
g4	1
g5	1
g6	1
	Sum=6

In other words, 1 is stabilized by g_1 & g_4, 2 is stabilized by g_1 & g_5, and 3 is stabilized by g_1 & g_6. On the other hand, g_1 fixes 1, 2, & 3, g_2 and g_3 fix no elements in *X*, g_4 fixes 1, g_5 fixes 2, and g_6 fixes 3. Either way, the final sum is the same. Thus, $|A| = \sum_{x \in X} |Stabilizer_G(x)| = \sum_{x \in X} |G_x| = \sum_{g \in G} |Fixer_X(g)|$.

□

Burnside's Counting Theorem: If *G* is a *finite group* that acts on a set *X*, then the number of *orbits* created by *G* acting on *X* is $\frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{x \in X} |Stabilizer_G(x)| = \frac{1}{|G|} \sum_{g \in G} |Fixer_X(g)|$.

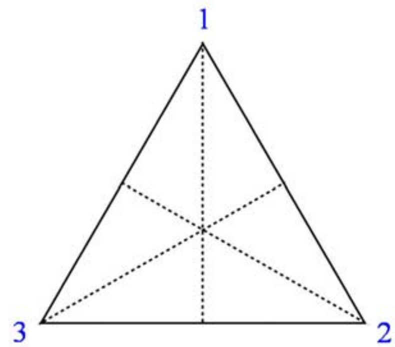
Proof: At this point, we have pretty much developed all the pieces of the puzzle, and we just need to put them together. Recall that our corollary above says that $|G_x| = |Stabilizer_G(x)| = \frac{|G|}{|Orbit_G(x)|}$.. Hence,

$\frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|Orbit_G(x)|} = \frac{|G|}{|G|} \sum_{x \in X} \frac{1}{|Orbit_G(x)|} = \sum_{x \in X} \frac{1}{|Orbit_G(x)|}$. Now what is this last expression going to add up to? Well, suppose, for example, that one particular *orbit by a group G* contains just three points – a, b, and c. In this case, $Orbit_G(a) = Orbit_G(b) = Orbit_G(c)$, and $|Orbit_G(a)| = |Orbit_G(b)| = |Orbit_G(c)| = 3$.

Consequently, $\frac{1}{|Orbit_G(a)|} + \frac{1}{|Orbit_G(b)|} + \frac{1}{|Orbit_G(c)|} = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$. Similarly, if an *orbit* produced by a *group G* consisted of four elements, d, e, f, and g, then we would have $\frac{1}{|Orbit_G(d)|}+\frac{1}{|Orbit_G(e)|}+\frac{1}{|Orbit_G(f)|}+\frac{1}{|Orbit_G(g)|}=\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=1$. Thus, if we arrange the sum $\sum_{x\in X}\frac{1}{|Orbit_G(x)|}$ in such a way that we add up all the terms corresponding to the elements of one *orbit* before going on to the next *orbit*, then the sum simply becomes $1+1+\ldots+1$ where the term "1" occurs as many times as there are distinct *orbits* in *X* produced by the action of the *group G*. In other words, $\frac{1}{|G|}\sum_{x\in X}|G_x|=\frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|Orbit_G(x)|}=\frac{|G|}{|G|}\sum_{x\in X}\frac{1}{|Orbit_G(x)|}=\sum_{x\in X}\frac{1}{|Orbit_G(x)|}$ is equal to the total number of *orbits* produced on *X* by *G*. And since one of our theorems above demonstrated that $\sum_{x\in X}|Stabilizer_G(x)|=\sum_{x\in X}|G_x|=\sum_{g\in G}|Fixer_G(g)|$, we can also write this result as $\frac{1}{|G|}\sum_{x\in X}|Stabilizer_G(x)|=\frac{1}{|G|}\sum_{g\in G}|Fixer_X(g)|$ is equal to the number of *orbits* on *X* produced by *G*.

□

Example 1: Let's apply this theorem to the example at the top of this chapter where *G* is the *group* of six permutations we can make of the elements of $X=\{1,2,3\}$.



$g_1 =$ the identity $= e = (\ )$
$g_2 = (1,2,3)$
$g_3 = (1,3,2)$
$g_4 = (2,3)$
$g_5 = (1,3)$
$g_6 = (1,2)$

On the one hand, it should be clear that there is only one *orbit* consisting of $\{1,2,3\}$. This is true because we can change each of these elements into any of the others just by repeated applications of a clockwise rotation of our triangle.

x	**|Stabilizer(x)|**
1	2
2	2
3	2
	Sum=6

g	**|Fixer(g)|**
g1	3
g2	0
g3	0
g4	1
g5	1
g6	1
	Sum=6

Additionally, by counting up for each $x \in X$ the number of elements in $Stabilizer(x)$, and by counting up for each $g \in G$ the number of elements in $Fixer(g)$, we obtain the same result from *Burnside's Counting Theorem*,

$$\frac{1}{|G|}\sum_{x\in X}|Stabilizer_G(x)| = \frac{1}{|G|}\sum_{g\in G}|Fixer_X(g)| = \frac{1}{6}\cdot 6 = 1$$

<u>Example 2:</u> Let $X = \{1,2,3,4\}$ and let $G = \{(\ ),(1,2),(3,4),(1,2)(3,4)\}$, $|G| = 4$. This group is called the *Klein 4*-group, and it is analogous to the states that can result when you have two lamps, one to your left and one to your right. You can leave both lamps off (the *identity*), or you can turn on the lamp on your left, or you can turn on the lamp on your right, or you can turn on both lamps. Each transposition

in our group *G*, $(1,2)$ and $(3,4)$, is analogous to flipping a switch on a lamp, thus turning the lamp on or off.

Now as for the number of orbits that *X* will have under the action of *G*, it should be clear that there are two. We can change 1 to 2 and we can change 3 to 4 and that's it. Hence, we might write $Orbit1=\{1,2\}$ and $Orbit2=\{3,4\}$. And if we count the orbits using *Burnside's Counting Theorem*, then once again we get the same result.

x	|Stabilizer(x)|
1	2
2	2
3	2
4	2
	Sum=8

g	|Fixer(g)|
( )	4
(1,2)	2
(3,4)	2
(1,2)(3,4)	0
	Sum=8

Hence, $\frac{1}{|G|}\sum_{x\in X}|Stabilizer_G(x)|=\frac{1}{4}\cdot 8=2$ and $\frac{1}{|G|}\sum_{g\in G}|Fixer_X(g)|=\frac{1}{4}\cdot 8=2$.

<u>Example 3:</u> Let $X=\{1,2,3\}$ and let $G=\{(\ ),(1,2,3),(1,3,2)\}$, $|G|=3$. Again, since the permutations in *G* can change 1 into 2 and 1 into 3, there should be only one *orbit*, $Orbit1=\{1,2,3\}$. We can confirm this using *Burnside's Counting Theorem*.

x	|Stabilizer(x)|
1	1
2	1
3	1
	Sum=3

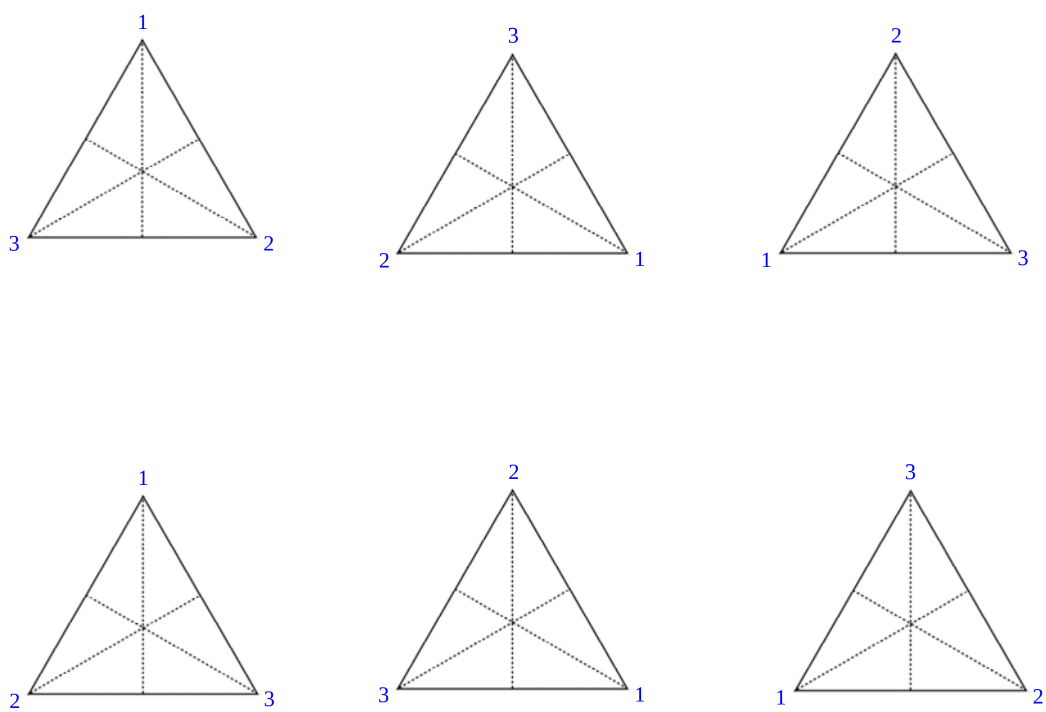
g	|Fixer(g)|
( )	3
(1,2,3)	0
(1,3,2)	0
	Sum=3

Thus, the number of orbits is $\frac{1}{|G|}\sum_{x\in X}|Stabilizer_G(x)|=\frac{1}{|G|}\sum_{g\in G}|Fixer_X(g)|=\frac{1}{3}\cdot 3=1$.

Notice, too, that if we label the vertices of an equilateral triangle with the number 1, 2, and 3, then we can interpret the permutations in *G* as corresponding to clockwise rotations of $0°$, $120°$, and $240°$, respectively.

<u>Example 4:</u> Let *X* equal the set of all distinct arrangements of the numbers 1, 2, and 3 on the vertices of an equilateral triangle, and let $G = \{(\ ), (1,2,3), (1,3,2)\}$, $|G| = 3$.

Notice that the permutations in our *group G* can once again be thought of as clockwise rotations of our triangle through angles that are multiples of $120°$, but our set *X* is different from what it was in the previous example. In particular, *X* is comprised of the following six arrangements:



Using *Burnside's Counting Theorem*, we discover that there are two *orbits*.

x	|Stabilizer(x)|
1	1
2	1
3	1
4	1
5	1
6	1
	Sum=6

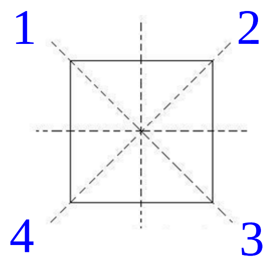
g	|Fixer(g)|
( )	6
(1,2,3)	0
(1,3,2)	0
	Sum=6

The number of *orbits* is $\frac{1}{|G|}\sum_{x\in X}|Stabilizer_G(x)| = \frac{1}{|G|}\sum_{g\in G}|Fixer_X(g)| = \frac{1}{3}\cdot 6 = 2$.

Notice that $Orbit1$ could be the configurations of the triangles in the first row above, and $Orbit2$ corresponds to the configurations in the second row above.

<u>Example 5:</u> Suppose you have four colors, red, green, blue, and yellow, and you paint each edge of a square a different color, and <u>let *X* be the set of all possible color configurations</u>. For example, on such configuration cold be top=red, bottom=blue, left=green, and right=yellow, and another possible configuration would be top=green, bottom=red, left=blue, and right=green. In all, the number of possible configurations is $4! = 4\cdot 3\cdot 2\cdot 1 = 24$. This is because we have four choices for the top color, then three left for the bottom color, two choices for the left side color, and then only one choice left for the right side color.

For our group, we will use D_4, the symmetries of a square. In other words, we can rotate our square clockwise through angles that are multiples of $90°$, or we can flip our square about any of four axes of symmetry.



The number of elements in this *group* is eight, $|D_4| = 8$, and if we label the vertices of our square 1, 2, 3, and 4, then we can represent D_4 as the following set of permutations, $D_4 = \{(\ ), (1,2,3,4), (1,4,3,2), (2,4), (1,3), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

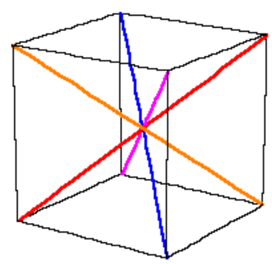
If two color configurations are in the same orbit, then we can change one into the other through some sequence of rotations and flips. Thus, the number of truly distinct color configurations possible is equal to the number of *orbits* in *X* created by D_4. Fortunately, this is easy to count. All we need to realize is that the *identity* keeps all 24 color configurations fixed while every other rotation or flip keeps none of the <u>color configurations fixed</u> (even though some vertices may remain fixed).

g	**|Fixer(g)|**
( )	24
(1,2,3,4)	0
(1,4,3,2)	0
(2,4)	0
(1,3)	0
(1,2)(3,4)	0
(1,3)(2,4)	0
(1,4)(2,3)	0
	Sum=24

Hence, the number of *orbits* is $\frac{1}{|D_4|}\sum_{x \in X} |Stabilizer_{D_4}(x)| = \frac{1}{|D_4|}\sum_{g \in D_4} |Fixer_X(g)| = \frac{1}{8} \cdot 24 = 3$.

<u>Example 6:</u> We'll now give a quick answer to the problem we posed at the beginning of this chapter where we can paint the six faces of a cube with six colors such that each color is used only once. This allows for $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ ways to paint the cube. However, we also allow rotations that are multiples of $90°$ in any of six directions, and this will make some of our coloring schemes equivalent to others. In particular, two color schemes will be

equivalent if the are in the same *orbit* created by our *rotation group G*, and so the number of distinct color schemes will be the same as the number of *orbits* that *G* creates when it acts on our colored cube. Using the same logic as before, we can say that <u>the *identity* of our *group* fixes all 720 coloring schemes, but every other element in *G* changes one color scheme into another</u>. Thus, the total number of coloring schemes fixed by *G* is 720. Now, however, we need to know how many elements there are in *G*, but that's not hard to count if we realize that our cube has four diagonal lines going through the center, and our rotations can create any possible permutation of these four diagonal lines.



Alternatively, think of taking a Rubik's cube and trying to count the different ways you can rotate it so that in the end everything is still oriented with respect to top, bottom, front, back, left, and right. In this case, you could say that we have 6 choices for the color on top, 4 choices for the color in front, and then everything else is determined by that. Hence, we can count the number of elements in *G* either as $|G| = 6 \cdot 4 = 24$ or $|G| = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, and from this it follows that the number of *orbits* created by *G* for the coloring schemes for our cube is $\frac{1}{|G|}\sum_{x \in X}|Stabilizer_G(x)| = \frac{1}{|G|}\sum_{g \in G}|Fixer_X(g)| = \frac{1}{24} \cdot 720 = 30$. In other words, there are 30 ways to color the faces of our cube that are distinct from one another when we allow for rotations of the cube.

MATHEMATICAL INDUCTION

Mathematical induction is a standard proof technique for showing that some proposition *P* about natural numbers holds true for all $n \in \mathbb{N}$ where, as a reminder, $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$. The basic idea is that you prove your proposition is true for some starting point such as $n = 1$, and then you prove that if it is true for some arbitrary natural number *n*, then it's true for *n*+1. If you prove both of these things, then you've established that your proposition is true for $n = 1$, and if it's true for $n = 1$, then it's true for $n = 2$, and if it's true for $n = 2$, then it's true for $n = 3$, and so on and so on.

<u>Mathematical Induction:</u> If *P* is a proposition about natural numbers $n \in \mathbb{N}$, then *P* is true for all $n \in \mathbb{N}$ if,

1. *P* is true for $n = 1$, and
2. *P* true for $n \in \mathbb{N} \Rightarrow$ *P* is true for $n + 1 \in \mathbb{N}$.

There are several variations we can do of this basic principle. For example, if we begin by showing that *P* is true for $n = 0$, then we could possibly prove that *P* is true for all whole numbers $W = \{0, 1, 2, 3, 4, \ldots\}$. Similarly, if we started our argument by showing that *P* is true for $n = 10$, then a successful induction argument could show that *P* is true for all natural numbers greater than or equal to 10. Another variant form of mathematical induction is shown below.

<u>The Second Principle of Mathematical Induction:</u> If *P* is a proposition about natural numbers $n \in \mathbb{N}$, then *P* is true for all $n \in \mathbb{N}$ if,

1. *P* is true for $n = 1$, and
2. *P* true for all natural numbers less than $n \in \mathbb{N} \Rightarrow$ *P* is true for $n \in \mathbb{N}$.

We'll now give a few examples of proofs that use mathematical induction.

<u>Prove:</u> $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

<u>Proof:</u> Let $n=1$. Then $\frac{1(1+1)}{2} = \frac{2}{2} = 1 = \sum_{k=1}^{1} k$. Hence, the statement is true for $n=1$. Assume now that the statement is true for some natural number *n*, and consider if it is true for $n+1$. Clearly,

$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)\left[(n+1)+1\right]}{2}.$$

Hence, if the formula is true for *n*, then it is also true for $n+1$. Therefore, by mathematical induction, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all natural numbers *n*.

□

<u>Prove:</u> $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{N}$

<u>Proof:</u> Let $n=1$. Then $\frac{1(1+1)(2+1)}{6} = \frac{6}{6} = 1 = \sum_{k=1}^{1} k^2$. Hence, the statement is true for $n=1$. Assume now that the statement is true for some natural number *n*, and consider if it is true for $n+1$. Clearly,

$$\sum_{k=1}^{n+1} k^2 = \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} = \frac{(n+1)\left[n(2n+1) + 6(n+1)\right]}{6}$$

$$= \frac{(n+1)\left[2n^2 + 7n + 6\right]}{6} = \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)\left[(n+1)+1\right]\left[2(n+1)+1\right]}{6}.$$

Hence, if the formula is true for *n*, then it is also true for $n+1$. Therefore, by mathematical induction, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ for all natural numbers *n*. □

As a final exercise, see if you can find the flaw in the following inductive argument that all horses are the same color.

By way of induction, suppose that you have a set containing $n=1$ *horses. Then clearly all the horses in that set are the same color. Now assume that it is true that in any set of n horses, all the horses have the same color (our induction hypothesis). At this point we want to argue that it is also true that any set of* $n+1$*horses will also all be the same color. Thus, suppose we are given a set containing* $n+1$ *horses. If we remove one horse, then by our inductive hypothesis the remaining n horses will all be the same color. Now return the horse we originally removed and remove a different horse. Then once again our inductive hypothesis states that the resulting set of n horses all have the same color. From this it follows that the two horses we successively removed have the same color, and therefore, all of the horses in our set of* $n+1$ *horses have the same color. It now follows by mathematical induction that for any set of n horses,* $n \in \mathbb{N}$, *all the horses have the same color.*

Solution: In the reading of the above argument, one often imagines a case where we might have, for example, 10 horses. We remove one horse, and then our induction hypothesis says that the remaining 9 horses are all the same color. We then replace our first horse, remove another horse, and again our induction hypothesis says that the remaining 9 horses are all the same color. And then finally, we conclude that because of the overlap of the two situations that all 10 horses are the same color. It is, indeed, clear that the induction argument works for the case of $n=10$. However, where the argument breaks down is for $n=2$. When we have 2 horses, then we can remove either one, but the resulting singleton sets this time have no intersection or overlap, and thus, we can't conclude that the two horses have to be of the same color. This is the one break in the chain of the induction argument that at first glance would appear to prove the assertion true for all natural numbers *n*.

CONJUGAL MATH

We've already introduced the definition of the *conjugate* of *x* by *a* as being the product $x^a = a^{-1}xa$. However, many *group theorists* prefer to define the conjugate slightly differently as $x^a = axa^{-1}$, and so below we'll switch to that definition so that you can be more familiar with it. Remember, though, that in the long run, it really doesn't make any difference which definition you use because if $a \in G$, then $a^{-1} \in G$ also, and both *conjugates*, axa^{-1} and $a^{-1}xa$, will reside in *G*. Additionally, another change in notation we will make is that we will use the symbol "$\sim$" instead of "$\equiv$" to denote an *equivalence relation*. Again, both symbols have been used for this purpose, and it's good to be familiar with several different notations for a particular concept. For the same reason, we will also work with *left cosets* this time instead of *right cosets*. And with that said, let's explore *conjugates* in greater depth!

Centers, Centralizers, Conjugacy Classes, and the *Class Equation*

The main goal in this section is to develop the *Class Equation* which is a useful tool for proving some of the theorems in subsequent sections. Of course, along the way we'll see a lot of other cool definitions and theorems, too. Also, in this chapter we'll use capital letters as labels for the theorems just to make life easier for when we inevitably have to refer back to a previous proof.

Definition: Let *G* be a *group* and let $x, a \in G$. Then the *conjugate of x by a* is axa^{-1}.

In Part 2 we introduced the idea of an *equivalence relation* which generalizes the notion of equality. In particular, for a condition to be an *equivalence relation*, it must be *reflexive, symmetric,* and *transitive* just like equality is. And now we'll prove that if we divide a *group* into subsets of elements that are *conjugate* to one another, that results in an *equivalence relation* among the elements of a *group G*.

<u>Theorem A:</u> Let *G* be a *group*. Then *conjugacy of elements* in *G* is an *equivalence relation*.

<u>Proof:</u> Let $x \sim y$ mean that *x* is *conjugate* to *y*. In other words, $x \sim y$ implies that there exists $a \in G$ such that $axa^{-1} = y$. Then to show that *conjugacy of elements* in *G* is an *equivalence relation* we have to show that it is *reflexive*, *symmetric*, and *transitive*.

1. (*reflexive*): Let $x \in G$ and let *e* be the *identity element* in *G*. Then the *conjugate* of *x* by *e* is $exe^{-1} = exe = xe = x$. Therefore, $x \sim x$, and $\sim$ is reflexive.

2. (*symmetric*): Let $x, y \in G$ such that *x* is *conjugate* to *y*. Then there exists $a \in G$ such that $axa^{-1} = y$. Hence, the *conjugate* of *y* by a^{-1} is $a^{-1}ya = a^{-1}(axa^{-1})a = (a^{-1}a)x(a^{-1}a) = exe = x$. Therefore, if $x \sim y$, then $y \sim x$ and, thus, $\sim$ is *symmetric*.

3. (*transitive*): Suppose $x \sim y$ and $y \sim z$ for some $x, y, z \in G$. Then there exists $a, b \in G$ such that $axa^{-1} = y$ and $byb^{-1} = z$. Hence, $z = byb^{-1} == b(axa^{-1})b^{-1} = (ba)x(a^{-1}b^{-1}) = (ba)x(ba)^{-1}$ which implies that $x \sim z$ and, thus, $\sim$ is *transitive*.

Therefore, it now follows that *conjugacy of elements* is an *equivalence relation* on *G*.

□

A consequence of *conjugacy* defining an *equivalence relation* on *G* is that *G* can be partitioned into a collection of disjoint subsets whose union is *G*, and the elements in each subset will be *conjugate* to one another. Furthermore, the number of elements in *G* will be equal to the sum of the number of elements in each individual *conjugacy class*. Also, notice that the different *conjugacy classes* need not be the same size. For example, the *conjugacy class* of the *identity* is just the *identity* since for each $a \in G$ we always have that $aea^{-1} = aa^{-1} = e$. However, it is reasonable to expect that other *conjugacy classes* will exist that consist of more than one element, and the following theorem shows that this will always be the case if *G* is *nonabelian*.

Theorem B: *G* is *abelian* if and only if every *conjugacy class* in *G* contains just one element.

Proof: Suppose *G* is *ableian* and let $x, a \in G$. Then $axa^{-1} = aa^{-1}x = ex = x$. Thus, the *conjugacy class* of *x* contains just one element. Now suppose that $x, y \in G$ and that the *conjugacy class* of *x* contains just one element. Then we know this element must be *x* since $exe^{-1} = x$. Hence, it follows that the *conjugate* of *x* by any $y \in G$ also equals *x*. But

$yxy^{-1} = x \Rightarrow (yxy^{-1})y = xy \Rightarrow yx(y^{-1}y) = xy \Rightarrow yxe = xy \Rightarrow yx = xy$. Therefore, *G* is *ableian*.

□

Corollary B: The above theorem is logically equivalent to saying that *G* is *nonabelian* if and only if there exists a *conjugacy class* in *G* that contains more than just one element.

Previously in Part 2 we defined the *center* of a *group* as the set of all elements in the *group* that *commute* with every other element. We'll now introduce the notion of a *centralizer* of a single element, and you'll see that its definition is similar to that of the *center* of a *group*. Also, the *centralizer* is going to be central (pun intended!) to our development of the *Class Equation*.

Definition: Let $a \in G$, a group. Then the ***centralizer of a in G***, denoted by $C_G(a)$, is the set of all elements in *G* that *commute* with *a*. Notice that $C_G(a)$ is never empty since $e, a \in C_G(a)$.

Our next step is to establish that the *centralizer* of an element *a* is always a *subgroup* of our *group G*.

Theorem C: $C_G(a)$ is a *subgroup* of *G*.

Proof: To show that $C_G(a)$ is a subgroup of *G*, we need to show that for every $x \in C_G(a)$ that $x^{-1} \in C_G(a)$, and we need to show that for every $x, y \in C_G(a)$ that $xy \in C_G(a)$.

We'll first establish the existence of *inverses*. Thus, suppose $x \in C_G(a)$. Then $xa = ax \Rightarrow a = x^{-1}ax \Rightarrow ax^{-1} = x^{-1}ax \cdot x^{-1} = x^{-1}a \cdot e = x^{-1}a \Rightarrow x^{-1} \in C_G(a)$.

Now we'll show *closure* under multiplication. Thus, suppose $x, y \in C_G(a)$. Then $xy(a) = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$. Thus, $xy \in C_G(a)$, and, therefore, $C_G(a)$ is a *subgroup* of *G*.

□

And now we'll show that if $C_G(a)$ is the *centralizer* of *a* in a group *G*, then elements from the same *left coset* of $C_G(a)$ in *G* will always produce the same *conjugate* of *a* in *G*. And a consequence of this will be that the number of distinct *conjugates* of *a* in *G* will be equal to the number of *left cosets* of $C_G(a)$ in *G*.

Theorem D: If $C_G(a)$ is the *centralizer* of *a* in a group *G*, then $xax^{-1} = yay^{-1}$ for $x, y \in G$ if and only if *x* and *y* belong to the same *left coset* of $C_G(a)$ in *G*.

Proof: Suppose *x* and *y* belong to the same *left coset* of $C_G(a)$ in *G*. Then $x = yh$ for some $h \in C_G(a)$. Recall, also, that since $h \in C_G(a)$, then, by definition, *h commutes* with *a*. Hence,

$xax^{-1} = (yh)a(yh)^{-1} = y(ha)(h^{-1}y^{-1}) = ya(hh^{-1})y^{-1} = yaey^{-1} = yay^{-1}$.

Now suppose that $xax^{-1} = yay^{-1}$. Then

$xax^{-1} = yay^{-1} \Rightarrow (y^{-1}x)ax^{-1} = ay^{-1} \Rightarrow (y^{-1}x)a = a(y^{-1}x) \Rightarrow y^{-1}x \in C_G(a)$ which means that there exists $h \in C_G(a)$ such that $y^{-1}x = h$. Hence, $yh = y(y^{-1}x) = (yy^{-1})x = ex = x$, $h \in C_G(a)$, which implies that *x* and *y* belong to the same *left coset* of $C_G(a)$ in *G*.

□

Corollary D: If $C_G(a)$ is the *centralizer* of *a* in a *finite group G*, then the number of distinct *conjugates* of *a* in *G* is the same as the number of *left cosets* of $C_G(a)$ in *G*, and by *Lagrange's Theorem*, this number is $[G : C_G(a)] = \frac{|G|}{|C_G(a)|}$.

Recall that we noted previously that the number of elements in *G*, $|G|$, is equal to the sum of the number of elements in each distinct *conjugacy class* of *G*. Also, from our corollary above it follows that the number of elements in a *conjugacy class* containing a particular $a \in G$ is $[G : C_G(a)] = \frac{|G|}{|C_G(a)|}$, and from this it follows that $|G| = \sum_a \frac{|G|}{|C_G(a)|}$ where for each distinct *conjugacy class*, $a \in G$ represents a single representative from that class. In other words, begin by picking $a \in G$. Then its *conjugacy class* is the set of all elements that $a \in G$ is *conjugate* to, and the number of elements in this *conjugacy class* to is equal to $\frac{|G|}{|C_G(a)|}$. If there now exists $b \in G$ such that a is not *conjugate* to b, then we can add on to this the number of elements that are *conjugate* to b. In other words, form the sum $\frac{|G|}{|C_G(a)|}+\frac{|G|}{|C_G(b)|}$. And now we can continue in this manner until we have accounted for each element in *G*, and when we arrive at that point, then we will have that the number of elements in *G* is equal to the sum of the number of elements in each *conjugacy class* in *G*. That is, $|G|=\frac{|G|}{|C_G(a)|}+\frac{|G|}{|C_G(b)|}+\ldots+\frac{|G|}{|C_G(m)|}=\sum_a \frac{|G|}{|C_G(a)|}$ where for each distinct *conjugacy class*, $a \in G$ represents a single representative from that class.

We previously defined the *center* of a *group* back in Part 2, but we'll repeat that definition before continuing.

<u>Definition:</u> The <u>*center*</u> of a *group G*, denoted by $Z(G)$, is the set of all elements in *G* that *commute* with every other element in *G*.

Since each element in $Z(G)$, the *center* of *G*, creates a *conjugacy class* with only one element (itself) in it, we can rewrite the above equation $|G|=\sum_a \frac{|G|}{|C_G(a)|}$ as follows, and this is what is usually known as the <u>*Class Equation*:</u>

<u>The Class Equation:</u> The *order* of a *group G* is $|G|=|Z(G)|+\sum_a \frac{|G|}{|C_G(a)|}$ where $a \in G \text{ such that } a \notin Z(G)$ and in our summation only a single $a \in G$ is chosen from each distinct *conjugacy class* that contains more than one element.

<u>*Conjugate Subgroups*, *Inner Automorhisms*, and Another Way to Sometimes Express *a Group* as a *Permutation Group*</u>

And now, for future reference we are just going to restate without proof Theorem 22 from Part 9 and then we will move deeper into the consequences of *conjugates*.

Theorem 22 (Part 9): Let *G* be a *group*, *H* a *subgroup* of *G*, and let $a \in G$. Then aHa^{-1} is a *subgroup* of *G* where $aHa^{-1} = \left\{aha^{-1} \mid h \in H\right\}$.

From Theorem 22 (Part 9) we know that the *conjugate* of a *subgroup* is another *subgroup*. We'll now show that the *relation* of two *subgroups* being *conjugate* to one another is an *equivalence relation*.

Theorem E: Let *G* be a *group*, let H_1 and H_2 be *subgroups* of *G*, and define a *relation* $\sim$ by $H_1 \sim H_2$ if and only if there exists $a \in G$ such that $H_2 = aH_1a^{-1}$. Then $\sim$ is an *equivalence relation*.

Proof: As usual, we need to show that $\sim$ is *reflexive*, *symmetric*, and *transitive*.

1. (*reflexive*): If *H* is a *subgroup* of *G*, then since $H = eHe = eHe^{-1}$, $H \sim H$ and, hence, $\sim$ is *reflexive*.

2. (*symmetric*): If H_1 and H_2 are *subgroups* of *G* with $H_1 \sim H_2$, then there exists $a \in G$ such that $H_2 = aH_1a^{-1}$. Consequently, it follows that $H_1 = a^{-1}H_2a$ and $H_2 \sim H_1$. Thus, $\sim$ is *symmetric*.

3. (*transitive*): Suppose $H_1, H_2, \text{ and } H_3$ are *subgroups* of *G* with $H_1 \sim H_2$ and $H_2 \sim H_3$. Then there exist $a, b \in G$ such that $aH_1a^{-1} = H_2$ and $bH_2b^{-1} = H_3$. Hence, $H_3 = bH_2b^{-1} = b(aH_1a^{-1})b^{-1} = (ba)H_1(a^{-1}b^{-1}) = (ba)H_1(ba)^{-1}$ implies that $H_1 \sim H_3$. Therefore, $\sim$ is *transitive*, and, hence, $\sim$ is an *equivalence relation*.

□

In our chapter, *A Third Application*, from Part 10 we proved that if *G* is a *group*, $g \in G$, and $f_g : G \to G$ is defined by $f_g(a) = g^{-1}ag$ for every $a \in G$, then f_g is an *automorphism*, an *isomorphism* from *G* onto *G*. In particular, we call such an *isomorphism* an *inner automoprhism*. A consequence of this and the above Theorem 22 is the following result.

Theorem F: If *G* is a *finite group*, H_1 and H_2 are *subgroups* of *G*, and $a \in G$ such that $aH_1a^{-1} = H_2$, then $|H_1| = |H_2|$.

Proof: In order to show that $|H_1| = |H_2|$, it suffices to show that $f_a : H_1 \to H_2$ defined by $f_a(x) = axa^{-1}$ is a *bijection* (*one-to-one* and *onto*). But we already know this from the theorem that we proved in the chapter titled *A Third Application*. This theorem tells us that $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is an *isomorphism.* Hence, if we simply restrict the domain of f_a to any *subset* of *G* and then look at the image of that *subset* under f_a, then the result will also be a *bijection*. Therefore, $f_a : H_1 \to H_2$ is a *bijection*, and it follows that $|H_1| = |H_2|$.

□

Now we are going to look at a theorem which gives us a condition under which a *finite group G* will be *isomorphic* to a *group* of permutations of the sort gxg^{-1} where $x, g \in G$.

Theorem G: If *G* is a *finite group* such that $Z(G) = e$, then *G* is *isomorphic* to a *permutation group* that may be obtained by *conjugation* by elements of *G*. In particular, each $g \in G$ is associated with a permutation of elements in *G* by applying gxg^{-1} to every $x \in G$.

Proof: Let *G* be a *finite group* such that $Z(G)=e$, and let $g\in G$. Then *conjugation* by *g* produces a permutation of the elements of *G*. We know this because it follows from our *cancellation laws* that if $x,y\in G$, then $gxg^{-1}=gyg^{-1}$ if and only if $x=y$. Thus, if the elements of *G* are labeled $x_1,x_2,x_3,\ldots,x_n$, then $gx_1g^{-1},gx_2g^{-1},gx_3g^{-1},\ldots,gx_ng^{-1}$ produces a permutation of this list.

Now let *A* be the *group* generated by all permutation of the sort described above, and define $T:G\to A$ by setting $T(g)$ equal to the permutation of elements of *G* created by mapping *x* to gxg^{-1} for all $x\in G$. We'll now show that *T* is an *isomorphism.* Thus, let $g_1,g_2\in G$ and let's examine the effect that $T(g_1\cdot g_2)$ and $T(g_1)\cdot T(g_2)$ have on an arbitrary $x\in G$. First, note that $\left[T(g_1\cdot g_2)\right](x)=(g_1g_2)x(g_1g_2)^{-1}=(g_1g_2)x(g_2{}^{-1}g_1{}^{-1})$. Second, note that since we multiply permutations by following one by another, we can think of $T(g_1)\cdot T(g_2)$ essentially as a composition of functions. In other words, to evaluate $\left[T(g_1)\cdot T(g_2)\right](x)$ for $x\in G$, we first *conjugate* *x* by g_2 and then we follow that result with *conjugation* by g_1. [Note, too, that we are now applying our permutations in order from right to left instead of left to right in order to make the direction correspond to our function notation.] Thus, $\left[T(g_1)\cdot T(g_2)\right](x)=\left[T(g_1)\right](g_2xg_2{}^{-1})=g_1(g_2xg_2{}^{-1})g_1{}^{-1}=(g_1g_2)x(g_2{}^{-1}g_1{}^{-1})$ $=(g_1g_2)x(g_1g_2)^{-1}=\left[T(g_1\cdot g_2)\right](x)$. Therefore, $T:G\to A$ is a *homomorphism*.

To show that *T* is an *isomorhphism* we will show first that $Ker(T)=e$. Thus, suppose that $x\in G$ is an arbitrary element of *G* and $g\in Ker(T)$. Then $\left[T(g)\right](x)=gxg^{-1}=x$ since *g* must be mapped onto the *identity permutation* in *A*. But this implies that $gx=xg$ and, hence, $g\in Z(G)$, the *center* of *G*. However, since part of our hypothesis is that $Z(G)=e$, it follows that $T:G\to A$ is *one-to-one*. Furthermore, $T:G\to A$ is also *onto* since *T* is a *homomorphism* and *A* is generated by elements of the form $T(g)$. Consequently, $T:G\to A$ is an *isomorphism* and, therefore, *G* is *isomorphic* to a *group* of permutations of the elements of *G*.

□

The Final Goal: Showing that if a *Group* has a Prime p that Divides the *Order* of a *Finite Group G*, the *G* has a *Subgroup* of *Order p*

We're now going to go down a path that will ultimately show us that if a prime *p* divides the order of a *finite group*, then our *group* has a *subgroup* of order *p*. Enjoy the ride!

Theorem H: If $|G| = p^n$, *p* a prime, then $|Z(G)| > 1$.

Proof: Let $z = |Z(G)|$. Then $z \geq 1$ since $e \in Z(G)$. Also, if $Z(G) \neq G$, then there exists $b \in G$ such that $b \notin Z(G)$. Furthermore, the *centralizer* of *b* in *G*, $C_G(b)$, is a proper *subgroup* of *G* since, otherwise, if we had $C_G(b) = G$, then everything in *G* would *commute* with *b*, and *b* would be an element of $Z(G)$. Thus, it also follows that $|C_G(b)| < |G|$, and by *Lagrange's Theorem*, $|C_G(b)|$ divides $|G|$. Since $|G| = p^n$, it now follows that $|C_G(b)| = p^m$ where $1 \leq m < n$. In particular, we'll denote the power *m* that corresponds to the order of $C_G(b)$ by m_b. The rest now follows easily from the *Class Equation*. By this equation, $|G| = p^n = |Z(G)| + \sum_b \frac{|G|}{|C_G(b)|}$ where $b \notin Z(G)$ and we choose only one *b* from each of the remaining *conjugacy classes*. The *Class Equation* can clearly be rewritten as $|G| - \sum_b \frac{|G|}{|C_G(b)|} = |Z(G)|$ which now implies that $p^n - \sum_b \frac{p^n}{p^{m_b}} = |Z(G)|$. Also, since for each term in our summation, $m_b < n$, it follows that *p* can be factored out of each term on the left-hand side of the equation to give us $p\left[p^{n-1}-\sum_{b}\frac{p^{n-1}}{p^{m_b}}\right]=|Z(G)|$. Since *p* divides the left-hand side of this equation, it must also divide the right-hand side, and, thus, $|Z(G)|>1$. In particular, $|Z(G)|$ is at least *p*.

□

<u>Corollary:</u> If $|G|=p^n$, *p* a prime, then $|Z(G)|=p^k$ where $1\le k\le n$.

<u>Theorem I:</u> If *G* is a *group* such that $|G|=p^2$ where *p* is a prime, then *G* is *abelian*.

<u>Proof:</u> By our previous theorem, it follows that $|Z(G)|>1$. Hence, by *Lagrange's Theorem*, either $|Z(G)|=p$ or $|Z(G)|=p^2$. If $|Z(G)|=p^2$, then $Z(G)=G$ which implies that *G* is *abelian* and we are done. Thus, suppose $|Z(G)|=p$. Then $Z(G)$ is *cyclic*, and, thus, $Z(G)=\langle a\rangle$ for some $a\in Z(G)$ with $a\ne e$. Now consider $x\in G$ such that $x\notin Z(G)$. Then clearly $Z(G)\subseteq C_G(x)$, the set of all elements of *G* that *commute* with *x*. However, since $x\in C_G(x)$ and $x\notin Z(G)$, it follows that $|Z(G)|<|C_G(x)|$. But his means that $|C_G(x)|=p^2$, and, hence, $C_G(x)=G$. And this now implies that everything in *G commutes* with *x*, and, thus, $x\in Z(G)$. However, this contradicts our assumption that there exists an $x\in G$ such that $x\notin Z(G)$. Thus, that assumption is wrong (since it led to a contradiction), and $Z(G)=G$ which implies that *G* is *abelian*.

□

<u>Definition:</u> Suppose *m* and *n* are *natural numbers* such that their only common divisor is 1. Then we say that *m* and *n* are <u>*relatively prime*</u>.

Theorem J: Suppose *G* is *abelian* and $|G| = p^n m$ where *p* is prime and *p* & *m* are *relatively prime*. Then *G* has a *subgroup* of order *p*.

Proof: Let $x \in G$.

(Case 1) If the order of the *cyclic subgroup* generated by *x* is p, then we're done.

(Case 2) If the order of the *cyclic subgroup* generated by *x* is p^k with $2 \le k \le n$, (i.e. $|\langle x \rangle| = p^k$), then $x^{\frac{p^k}{p}} = x^{p^{k-1}}$ generates a *subgroup* of this *cyclic group* generated by *x* such that this *subgroup* has order *p*, $\left(\left| \left\langle x^{p^{k-1}} \right\rangle \right| = p \right)$, where $(x^{p^{k-1}})^p = x^{p^{k-1} \cdot p} = x^{p^k} = e$, and we are done.

(Case 3) If $|\langle x \rangle| = p^k q$ where $q > 1$ and $1 \le k \le n$, *q* divides *m*, and *p* & *q* are *relatively prime*, then $x^{\frac{p^k q}{p}} = x^{p^{k-1} q}$ generates a *subgroup* of $\langle x \rangle$ of order *p* since $(x^{p^{k-1} q})^p = x^{p^{k-1} q \cdot p} = x^{p^k q} = e$, and again, we are done.

(Case 4) Suppose that for every non-trivial element x_i of *G* we have that $|\langle x \rangle| = q_i$ where, regardless of the value of *i*, $q_i > 1$, q_i divides *m*, and *p* & q_i are relatively prime. Thus, let $x_1 \in G$ such that $|\langle x_1 \rangle| = q_1$. Also, let $N_1 = \langle x_1 \rangle$. Then N_1 is a *normal subgroup* of *G* since *G* is *abelian*, and $|G / N_1| = |G| / |N_1| = p^n \cdot \frac{m}{q_1}$. Now let $x_2 \in G$ where $|\langle x_2 \rangle| = q_2$, q_2 divides *m*, and *p* & q_2 are *relatively prime*. Also, let $N_2 = \langle x_2 \rangle$. Then by our *second isomorphism theorem*, $\frac{N_2}{N_2 \cap N_1} \cong \frac{N_2 N_1}{N_1}$. Now let $r_2 = \frac{q_2}{|N_2 \cap N_1|} = \frac{|N_2|}{|N_2 \cap N_1|} = \left| \frac{N_2}{N_2 \cap N_1} \right| = \left| \frac{N_2 N_1}{N_1} \right| = \frac{|N_2 N_1|}{|N_1|} = \frac{|N_2 N_1|}{q_1}$. This string of equalities tells us two things. First, since $r_2 = \dfrac{q_2}{|N_2 \cap N_1|}$, r_2 divides q_2, and thus, r_2 and *p* are *relatively prime*. Additionally, $r_2 q_1 = |N_2 N_1|$ (just multiply both sides of the equation above by q_1) and hence, $r_2 q_1$ also divides $|G|$, and $r_2 q_1$ and *p* are relatively prime. Consequently, $r_2 q_1$ divides *m*, and $\left|\dfrac{G}{N_2 N_1}\right| = \dfrac{|G|}{|N_2 N_1|} = \dfrac{p^n m}{r_2 q_1} = p^n \cdot \dfrac{m}{r_2 q_1}$. Now let $N_3 = \langle x_3 \rangle$ where $|N_3| = |\langle x_3 \rangle| = q_3$, q_3 divides *m*, and *p* & q_3 are *relatively prime*. Then $\dfrac{N_3}{N_3 \cap N_2 N_1} \cong \dfrac{N_3 N_2 N_1}{N_2 N_1}$. Additionally, let

$$s_3 = \frac{q_3}{|N_3 \cap N_2 N_1|} = \frac{|N_3|}{|N_3 \cap N_2 N_1|} = \left|\frac{N_3}{N_3 \cap N_2 N_1}\right| = \left|\frac{N_3 N_2 N_1}{N_2 N_1}\right| = \frac{|N_3 N_2 N_1|}{|N_2 N_1|} = \frac{|N_3 N_2 N_1|}{r_2 q_1}.$$

Then s_3 divides q_3 which means that *p* and s_3 are *relatively prime*. Furthermore, $s_3 r_2 q_1 = |N_3 N_2 N_1|$ tells us that $s_3 r_2 q_1$ divides $|G| = p^n m$, but since *p* is *relatively prime* to the product $s_3 r_2 q_1$, it follows that $s_3 r_2 q_1$ divides *m*. Hence, $\left|\dfrac{G}{N_3 N_2 N_1}\right| = \dfrac{|G|}{|N_3 N_2 N_1|} = \dfrac{p^n m}{s_3 r_2 q_1} = p^n \cdot \dfrac{m}{s_3 r_2 q_1}$. Now, on the one hand, we can continue this process of taking the elements x_i, letting $N_i = \langle x_i \rangle$ where $z_i = |\langle x_i \rangle| = |N_i|$, and forming *quotient groups* $\dfrac{G}{N_1 N_2 N_3 \ldots N_i}$ and showing that their order is $p^n \cdot \dfrac{m}{q_1 r_2 s_3 \ldots z_i}$ where $q_1 r_2 s_3 \ldots z_i$ divides *m* and is *relatively prime* to *p*. However, if we keep picking elements x_i in this manner, then we eventually we will get to the point where we have factored everything out and are left with only the trivial group of order 1. But on the other hand, our process also yields a *quotient group* of order $p^n \cdot \dfrac{m}{q_1 r_2 s_3 \ldots z_k} \geq p^n > 1$ at each step along the way. And this is a contradiction. We can't factor out everything and still be left with a *quotient group* whose size is bigger than 1. Thus, there must exist a non-trivial element *x* of *G* such that the *order* of $|\langle x \rangle|$ is either p^k or $p^k q$ for $1 \leq k \leq n$, and we have shown above how each of these cases allows us to find an element of *order p*. □

Corollary J: If *G* is *abelian* and $|G| = p^n$ where *p* is a prime, then *G* has a *subgroup* of order *p*.

Theorem K: If *G* is a *group* such that $|G| = p^n$ where *p* is a prime, then *G* contains a *normal subgroup* of order p^{n-1}.

Proof: We prove this theorem by applying *mathematical induction* to the power *n*. Thus, suppose $|G| = p^1 = p$. Then $p^{1-1} = p^0 = 1$, and $\{e\}$ is a *normal subgroup* of order 1.

Now suppose that our theorem is true for all *k* such that $1 \le k < n$, and we'll prove that our theorem is also true for $k = n$. Hence, suppose that $|G| = p^n$. Then by Theorem H, $|Z(G)| > 1$ and so there exists $a \in Z(G)$ such that $a \ne e$. Furthermore, since $|G| = p^n$, it follows that $|\langle a \rangle| = p^m$ for some *m* such that $1 \le m \le n$. Hence, consider $a^{\frac{p^m}{p}}$. Clearly, $(a^{\frac{p^m}{p}})^p = a^{p^m} = e \Rightarrow \left|\left\langle a^{\frac{p^m}{p}} \right\rangle\right| = p$, and $\left\langle a^{\frac{p^m}{p}} \right\rangle = \left\langle a^{p^{m-1}} \right\rangle$ is a *normal subgroup* of *G* since $a \in Z(G)$. Let $b = a^{\frac{p^m}{p}} = a^{p^{m-1}}$, let $H = \langle b \rangle = \left\langle a^{\frac{p^m}{p}} \right\rangle = \left\langle a^{p^{m-1}} \right\rangle \lhd G$, and consider G/H where $|G/H| = |G|/|H| = \dfrac{p^n}{p} = p^{n-1}$. By our induction hypothesis, G/H has a *normal subgroup* of the form N/H of order $p^{(n-1)-1} = p^{n-2}$ and $H \subseteq N \subseteq G$. However, by our *Correspondence Theorem* this means that $N \lhd G$ and $p^{n-2} = |N/H| = |N|/|H| = \dfrac{|N|}{p}$. Thus, $|N| = p^{n-2}p = p^{n-1}$, and the theorem is proved by *mathematical induction*.

□

<u>Cauchy's Theorem:</u> If *G* is a *finite group* and *p* is a prime such that *p* divides $n = |G|$, then *G* has *cyclic subgroup* of order *p*.

<u>Proof:</u> We'll let *p* be a prime, and we'll proceed by *induction* on *n*, the order of the group. In this case, the smallest possible value for $|G|$ such that *p* divides $|G|$ is *p* itself. But in this case, every nontrivial element of *G* generates a *cyclic subgroup* of order *p*. Thus, let's assume that $|G| = n > p$, where *p* divides *n*, and by way of *induction* we'll also assume that if *G* has a *subgroup H* of any order $m < n$ such that *p* divides *m*, then *G* has a *cyclic subgroup* of order *p*. We'll now extend this result to the case $m = n$.

If *G* is *abelian*, then the result has already been established by Theorem J and Corollary J. Thus, assume that *G* is not *abelian* and let $x \in G$ such that $x \notin Z(G)$, the *center* of *G*. Note that if there were no elements in *G* that did not belong to the *center*, then *G* would be *abelian*. Also, let $C_G(x)$ be the *centralizer of x*, the set of all elements of *G* that *commute* with *x*. Then $|C_G(x)| < |G|$ since, otherwise, we would have $C_G(x) = G$ which would mean that every element in *G* would *commute* with *x*, and, hence, *x* would belong to $Z(G)$. Thus, $|C_G(x)| < |G|$, and if *p* divides $|C_G(x)|$, then our induction hypothesis tells us that $C_G(x)$ has a *cyclic subgroup* of order *p*, and we're done. Thus, assume that *p* doesn't divide $|C_G(x)|$.

If *p* divides $|G|$ but *p* does not divide $|C_G(x)|$, then clearly *p* must divide $\dfrac{|G|}{|C_G(x)|}$.

Now consider the *Class Equation* $|G| = |Z(G)| + \sum_x \dfrac{|G|}{|C_G(x)|}$ where $x \notin Z(G)$ and we pick just one *x* from each *conjugacy class* that doesn't contain elements of the *center*, $Z(G)$. If we rewrite this equation as $|G| - \sum_x \dfrac{|G|}{|C_G(x)|} = |Z(G)|$, then *p* divides the left-hand side of this equation, and so it must divide $|Z(G)|$ as well. But since

$Z(G)$ is *abelian*, Theorem J and Corollary J guarantee that $Z(G)$ has a *cyclic subgroup* of order *p*, and this *subgroup* is a *subgroup* of *G* as well. Therefore, *G* has a *cyclic subgroup* of order *p*, and the theorem is proved by *mathematical induction*.

□

Corollary: If *G* is a *finite group* such that $|G| = p^n$, then $Z(G)$ contains an element that is not the *identity*.

Proof: Using the *Class Equation* again, we have $|G| = |Z(G)| + \sum_x \frac{|G|}{|C_G(x)|}$ where $x \notin Z(G)$ and we pick just one *x* from each *conjugacy class* that doesn't contain elements of the *center*, $Z(G)$. Thus, as in our theorem above, $|C_G(x)| < |G|$ and since every *subgroup* of *G* has order a power of *p*, it follows that $\frac{|G|}{|C_G(x)|}$ is divisible by *p*. Hence, *p* divides the left-hand side of the equation $|G| - \sum_x \frac{|G|}{|C_G(x)|} = |Z(G)|$, and, thus, it also divides the right-hand side. Therefore, $|Z(G)| > 1$, and $Z(G)$ contains an element that is not the *identity*.

□

THE SYLOW THEOREMS

Remember: Here are a few definitions and other facts you might want to recall.

Definitions: Let *X* be a set and let *G* be a *group*.

$$Fixer_X(g) = X_g = \{x \in X \mid g(x) = x \text{ for } g \in G\}$$

$$Stabilizer_G(x) = G_x = \{g \in G \mid g(x) = x \text{ for } x \in X\}$$

$$Orbit_G(x) = \{y \in X \mid g(x) = y \text{ for some } g \in G \text{ and } x, y \in X\}$$

Definition: To the above we will add the following definition of the *center of X under G* (the *center* when *G* acts on a set *X)* as $Center_G(X) = Z_G(X) = \{x \in X \mid g(x) = x \text{ for all } g \in G\}$. Notice that we define things this way because if *G* is acting on *G* by *conjugation*, then we get back the usual definition for the *center* of *G*. In other words, if $Center_G(G) = Z_G(G) = \{x \in G \mid g(x) = gxg^{-1} = x \text{ for all } g \in G\}$, then $x \in G$ is in this *center* if and only if $gxg^{-1} = x \Leftrightarrow gx = xg \text{ for all } g \in G$.

Fact: Recall that if *G* is a *finite group* that acts on a set *X*, and if $x \in X$, then the number of elements in the *orbit of x* is $|Orbit_G(x)| = [G : G_x] = \frac{|G|}{|G_x|} = \frac{|G|}{|Stabilizer_G(x)|}$. From this we derived *Burnside's Counting Theorem*, that the number of *orbits* created by *G* acting on *X* is $\frac{1}{|G|}\sum_{x \in X}|G_x| = \frac{1}{|G|}\sum_{x \in X}|Stabilizer_G(x)| = \frac{1}{|G|}\sum_{g \in G}|Fixer_X(g)|$, (see the chapter *Orbits, Stabilizers, Fixers, and Burnside's Counting Theorem* in Part 10). Also, recall the *Class Equation* (see *Conjugal Math* in Part 10),

$\left|G\right| = \left|Z(G)\right| + \sum_{x \notin Z(G)} \frac{\left|G\right|}{\left|C_G(x)\right|}$ where in our summation only a single value *x* is chosen from each distinct *conjugacy class* that contains more than one element. The *Class Equation* simply says that the number of elements in *G* is just the sum of the number of elements in each *orbit* where an *orbit* is produced by letting elements of *G* act upon *G* itself by means of *conjugation*. What might now start to become obvious to you is that the traditional *Class Equation* is just a special case of a *group G* acting on a set *X* where in this case $X = G$ and the permutations are created by the operation of *conjugation*. We can replace this special case, however, by the following more general formula where we state that the number of elements in the set *X* is the sum of the number of elements in each *orbit* produced by permutations in *G*, or in other words, $\left|X\right| = \left|Z_G(X)\right| + \sum_{x \notin Z_G(X)} \frac{\left|G\right|}{\left|G_x\right|}$. And now we'll prove a useful theorem about *groups* of order p^n.

<u>Theorem I:</u> Let *G* be a *group* such that $\left|G\right| = p^n$ and let *X* be a set that *G* acts on. Then $\left|X\right| - \left|Z_G(X)\right|$ is divisible by *p*.

<u>Proof:</u> Since $Stabilizer_G(x) = G_x = \{g \in G \mid g(x) = x \text{ for } x \in X\}$ is a *subgroup* of *G*, $\left|G_x\right|$ divides $\left|G\right|$, and since $\left|G\right| = p^n$, it follows that $\left|G_x\right| = p^k$ where $0 \le k \le n$. Now we will use our generalized *Class Equation*, $\left|X\right| = \left|Z_G(X)\right| + \sum_{x \notin Z_G(X)} \frac{\left|G\right|}{\left|G_x\right|}$ where in our summation only a single value *x* is chosen from each distinct *conjugacy class* that contains more than one element. In this case, we can conclude that $G_x \neq G$ since if it were, then we would have $x \in Z_G(X)$. Thus, we also now have that $\left|G_x\right| < \left|G\right|$, and, hence, $\frac{\left|G\right|}{\left|G_x\right|} = p^m$ where $0 < m < n$. Therefore, *p* divides $\sum_x \frac{\left|G\right|}{\left|G_x\right|} = \left|X\right| - \left|Z_G(X)\right|$, and we're done.

□

In Part 9 we defined what the *centralizer* of an element is, and now we'll define a slightly more general concept known as the *normalizer*.

Definition: If *H* is a *subgroup* of a *group G*, then the set of all $x \in G$ such that $xHx^{-1} = H$ is called the ***normalizer of H in G*** and is denoted by $N_G(H)$.

Our first task will be to prove that the *normalizer* of a *subgroup H* is also a *subgroup* of our *group G*.

Theorem II: If *H* is a *subgroup* of a *group* G*, then the normalizer of H in G* in *G* is a *subgroup* of *G*.

Proof: To show that $N_G(H)$ is a *subgroup* of *G*, we need to establish both *closure* and *existence of inverses*. Thus, suppose $x, y \in N_G(H)$. Then $(xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$. Therefore, $xy \in N_G(H)$

Now suppose $x \in N_G(H)$ and consider $x^{-1}Hx$. Clearly, $x^{-1}Hx = x^{-1}(H)x = x^{-1}(xHx^{-1})x = (x^{-1}x)H(x^{-1}x) = eHe = H$. Hence, $x^{-1} \in N_G(H)$, and therefore, *H* is a *subgroup* of *G*.

□

Next, we'll prove a few more preliminary results that will help us to complete the proofs of the *Sylow Theorems*.

Theorem III: If *H* is a *p-subgroup* of a *finite group G* for some prime *p*, then $\frac{|G|}{|H|} - \frac{|N_G(H)|}{|H|}$ is divisible by *p*.

<u>Proof:</u> Let *X* be the set of *left cosets* of *H* in *G*, and let *H* act on *X* by letting $h(xH) = (hx)H$ where $x \in G$ and $h \in H$. Then $Z_H(X) \subseteq X$ is the set of *left cosets* of *H* in *G* such that $h(xH) = xH$ for all $h \in H$. Given such a *left coset* we have that $h(xH) = xH \Leftrightarrow hxH = xH \Leftrightarrow x^{-1}hxH = H \Leftrightarrow x^{-1}hx \in H$ for all $h \in H$, and this in turn means that $x \in N_G(H)$, the *normalizer* of *H* in *G*. In other words, $x \in N_G(H)$ if and only if $x^{-1}hx \in H$ when $h \in H$ if and only if $x^{-1}hxH = H$ if and only if $hxH = xH$ if and only if $h(xH) = xH$ for all $h \in H$ if and only if $xH \in Z_H(X)$. Additionally, the number of such distinct *left cosets* involving elements of $N_G(H)$ is $\left|\frac{N_G(H)}{H}\right| = \frac{|N_G(H)|}{|H|} = |Z_H(X)|$.

Also, since *H* is a *p-group*, $|H| = p^n$ for some $n \in \mathbb{N}$. Furthermore, our previous theorem tells us that *p* divides $|X| - |Z_H(X)|$. But in this case $|X| = \text{ the number of left-cosets of } H \text{ in } G = \frac{|G|}{|H|}$ and $|Z_H(X)| = \frac{|N_G(H)|}{|H|}$. Therefore, *p* divides $\frac{|G|}{|H|} - \frac{|N_G(H)|}{|H|}$.

□

<u>Corollary III:</u> If $|G| = p^n m$ where $n \geq 1$ and *p* is a prime that does not divide *m*, and if *H* is a *subgroup* of *G* such that $|H| = p^i$ for $1 \leq i < n$, then $N_G(H) \neq H$ and *p* divides $|N_G(H)/H|$.

<u>Proof:</u> By our theorem, *p* divides $\frac{|G|}{|H|} - \frac{|N_G(H)|}{|H|}$. However, since $|G| = p^n m$ and $|H| = p^i$ for $1 \leq i < n$, it immediately follows that *p* divides $\frac{|G|}{|H|} = p^{n-i}m$. Hence, *p*

must also divide $\frac{|N_G(H)|}{|H|}$. However, this also means that $\frac{|N_G(H)|}{|H|} \neq 1$, and therefore, $N_G(H) \neq H$. □

<u>The First Sylow Theorem:</u> Let *G* be a *finite group* and let $|G| = p^n m$ where $n \geq 1$ and *p* is a prime that does not divide *m*. Then:

1. *G* contains a *subgroup* of order *p* for each *I* such that $1 \leq i \leq n$.

2. Every *subgroup H* of *G* of order p^i is a *normal subgroup* of a *subgroup* of order p^{i+1} for $1 \leq i < n$.

<u>Proof:</u> (1) We will proceed by *induction* on the power of *p*. First, by *Cauchy's Theorem*, we know that a *subgroup* of order *p* exists. Now suppose that for all *i* such that $1 \leq i < n$ that it is true that there exists a *subgroup* of *G* of order p^i. in particular, let *H* be a *subgroup* such that $|H| = p^i$. Now consider $N_G(H)$, the *normalizer* of *H* in *G*. By definition, $H \triangleleft N_G(H)$. Also, by the corollary to Theorem III above, $N_G(H) \neq H$ and *p* divides $|N_G(H)/H|$. Hence, since $|N_G(H)/H|$ is divisible by *p*, it follows from *Cauchy's Theorem* that $N_G(H)/H$ has a *subgroup* K/H of order *p* where $K = \{x \in N_G(h) \mid xH \in K/H\}$ and *K* is a *subgroup* of $N_G(H)$. Hence, *K* is also a *subgroup* of *G*. Furthermore, since $p = |K/H| = \frac{|K|}{|H|} = \frac{|K|}{p^i}$, it now follows that $|K| = p^{i+1}$, and our *induction* argument is complete.

(2) For the second part of this theorem, note that $H \triangleleft N_G(H)$, $H \leq K$, and $K \leq N_G(H)$. Since every element of *K* is also an element of $N_G(H)$, it follows that if $k \in K$, then $kHk^{-1} = H$. Hence, $H \triangleleft K$, and since $|H| = p^i$ and $|K| = p^{i+1}$, we're done. □

We defined a *Sylow subgroup* previously in Part 2, but we'll repeat it again for reference.

Definition: If *G* is a *finite group* and $|G| = p^n m$ where $n \geq 1$ and *p* is a prime that does not divide *m*, then any subgroup of *G* of order p^n is called a *Sylow p-subgroup*.

The Second Sylow Theorem: If P_1 and P_2 are distinct *Sylow p-subgroups* of a *finite group G*, then P_1 and P_2 are *conjugate*.

Proof: Let $X =$ the set of *left cosets* of P_1 in *G* and let P_2 act on *X* as follows: If $xP_1 \in X$ and $y \in P_2$, then $y(xP_1) = (yx)P_1$. Also, let $Z_{P_2}(X) = \{xP_1 \in X \mid \text{ for every } y \in P_2,\ y(xP_1) = (yx)P_1 = xP_1\}$. Then by Theorem I, $|X| - |Z_{P_2}(X)|$ is divisible by *p*. Also, since $|X| = \frac{|G|}{|P_1|}$ is not divisible by *p* (since P_1 is a *Sylow p-subgroup*), it follows that $|Z_{P_2}(X)| \neq 0$. Hence, $yxP_1 = xP_1 \text{ for all } y \in P_2 \Leftrightarrow x^{-1}yxP_1 = P_1 \Leftrightarrow x^{-1}yx \in P_1 \Leftrightarrow x^{-1}P_2 x \leq P_1$. However, since $|P_1| = |P_2|$, we can conclude that $x^{-1}P_2 x = P_1$, and P_1 and P_2 are *conjugate*.

□

The Third Sylow Theorem: If *G* is a *finite group* and a prime *p* divides *G*, then the number of *Sylow p-subgroups* minus one is also divisible by *p*. Additionally, the number of *Sylow p-subgroups* is also a divisor of $|G|$.

Proof: Let *P* be a *Sylow p-subgroup* and let *X* be the set of all *Sylow p-subgroups* in *G*, and let *P* act on *X* by *conjugation*. Then by previous proof, $|X| - |Z_P(X)|$ is divisible by *p*. If $T \in Z_P(X)$, then $xTx^{-1} = T$ for all $x \in P$. Hence, $P \leq N_G(T)$. Also, $T \leq N_G(T)$. Furthermore, since *P* and *T* are both *Sylow p-*

subgroups of *G*, they are also *Sylow p-subgroups* of $N_G(T)$, and since *T* and *P* are *conjugate* with $T \lhd N_G(T)$, it follows that $T = P$. Thus, $Z_P(X) = \{T\} = \{P\}$, and $|Z_P(X)| = 1$. Hence, *p* divides $|X| - |Z_P(X)| = |X| - 1$.

Now let *G* act on *X* by *conjugation*. Then since all the *Sylow p-subgroups* are *conjugate*, *G* produces only one orbit on *X*. Thus, if $P \in X$, then $|X| = |\text{orbit of } P| = \frac{|G|}{|G_P|} = \frac{|G|}{|Stabilizer_G(P)|}$. Since we can rewrite this as $|Stabilizer_G(P)| = \frac{|G|}{|X|}$, it follows that the number of *Sylow p-subgroups* is a divisor of $|G|$.

□

<u>Corollary 3a:</u> If *G* is a *finite group* such that $|G| = p^n m$ where *p* is a prime that does not divide *m,* then the number of *Sylow p-subgroups* is a divisor of *m*.

<u>Proof:</u> Let *k* be the number of *Sylow p-subgroups*. Then *k* divides $|G| = p^n m$. Additionally, *p* divides $k-1$. If $k = p^i q$ for $1 \le i \le n$ and *q* a divisor of *m*, then we have a problem since *p* does not evenly divide $p^i q - 1$. Therefore, $k = q$ where *q* is a divisor of *m*.

□

<u>Corollary 3b:</u> If *G* is a *finite group* such that $|G| = p^n m$ where *p* is a prime that does not divide *m* and if *P* is a *Sylow p-subgroup,* then the number of *Sylow p-subgroups* is equal to $[G : N_G(P)] = \frac{|G|}{|N_G(P)|}$.

<u>Proof:</u> Let's consider the *left cosets* of $N_G(P)$ in *G*. If $x \in N_G(P)$, then $xPx^{-1} = P$. Furthermore, if $y \cdot N_G(P) = z \cdot N_G(P)$, then $z^{-1}y \cdot N_G(P) = N_G(P)$. But this means that

$z^{-1}y \in N_G(P)$ and, hence, $(z^{-1}y)P(z^{-1}y)^{-1} = P \Leftrightarrow (z^{-1}y)P(y^{-1}z) = P \Leftrightarrow yPy^{-1} = zPz^{-1}$. In other words, two elements belong to the same *left coset* of $N_G(P)$ if and only if they generate the same *conjugate subgroup* of *P*. Thus, the number of *conjugate subgroups* of *P* is equal to the number of *left cosets* of $N_G(P)$ in *G*, and this, in turn, is equal to $[G : N_G(P)] = \dfrac{|G|}{|N_G(P)|}$.

□

<u>Corollary 3c:</u> If *G* is a *finite abelian group* and $|G| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ for primes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, then $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$ where each $S_{p_i^{n_i}}$ is a *Sylow* p_i-subgroup.

<u>Proof:</u> We know that each $S_{p_i^{n_i}}$ is *normal* in *G*, that $\left|S_{p_i^{n_i}}\right| = p_i^{n_i}$, that $S_{p_i^{n_i}} \cap S_{p_j^{n_j}} = e$ when $i \neq j$, and that $\left|S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}\right| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$. Therefore, it must follow that $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$.

□

THE FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

Theorem: Let *G* be an *abelian group* such that $|G| = p^n$ for some prime *p*. Then $G = A \oplus Q$ where *A* is a *cyclic subgroup* of *G* that is of maximal order.

Proof: Let *G* be an *abelian group* such that $|G| = p^n$ for some prime *p*. We will proceed by *induction* on *n*. Thus, if $n = 1$, then $|G| = p$, *G* is *cyclic*, we can let $A = \langle a \rangle$ for any $a \in G$, $G = A$, and we are done. Hence, suppose that $n \neq 1$ and assume the *induction hypothesis* that the theorem is true for any $m < n$. If there exists $a \in G$ such that $A = \langle a \rangle = G$, then, again, we are done. Thus, suppose *G* is not *cyclic* and that $a \in G$ such that $A = \langle a \rangle = p^m$ where p^m is the largest order of any *cyclic subgroup* of *G*. Suppose also that there exists $b \in G - A$ such that $B = \langle b \rangle$, $|B| = |\langle b \rangle| = p^r$ where $p^r \leq p^m$, and $A \cap B = e$. Now consider G/B. We have that $|G/B| = \dfrac{|G|}{|B|} = \dfrac{p^n}{p^r} = p^{n-r} \neq 1$. Hence, our *induction hypothesis* applies and since $A \cap B = \langle a \rangle \cap \langle b \rangle = e$, it follows that for $aB \in G/B$, $|\langle aB \rangle| = |\langle a \rangle| = |A| = p^m$. Thus, using our *induction hypothesis*, $G/B = \langle aB \rangle \oplus Q/B$ for some *subgroup Q* of *G* such that $B \leq Q \leq G$. We now ask the question is $A \cap Q = e$? If not, then there exists $a^i \in A \cap Q$ such that $a^i \neq e$ and $a^i \notin B$. Hence, $a^i B \in \langle aB \rangle \cap Q/B$ and $a^i B \neq B$. But this contradicts our *induction hypothesis* that $G/B = \langle aB \rangle \oplus Q/B$ since by definition of a *direct sum* we must have $\langle aB \rangle \cap Q/B = B$, the *identity* in G/B. Consequently, it must be true that $A \cap Q = e$. Furthermore, since $G/B = \langle aB \rangle \oplus Q/B$, it follows that $G = AQ$, and since $A \cap Q = e$, we now have that $G = A \oplus Q$. Notice also that if $|B| = |\langle b \rangle| = p^r$, then $\left|\left\langle b^{p^{r-1}} \right\rangle\right| = p$ and $A \cap B = \langle a \rangle \cap \left\langle b^{p^{r-1}} \right\rangle = e$. In other words, if *G* has a *subgroup* of order p^r whose intersection with *A* is *e*, then *G* has a *subgroup* of order p whose intersection with *A* is *e*.

Now suppose that there exists $b \in G - A$, $A = \langle a \rangle$, such that $\langle a \rangle \cap \langle b \rangle \neq e$ and $|\langle b \rangle| = p^r \leq p^m = |\langle a \rangle|$. In this case, just as we assumed that p^m is the maximum order for any *cyclic subgroup* of *G*, we may assume that p^r is the minimum order for any *cyclic subgroup* of *G* that meets the conditions above. In particular, if we consider b^p, then $|\langle b^p \rangle| = p^{r-1} < p^r = |\langle b \rangle|$ implies that $b^p \notin G - A$, and, hence, $b^p \in A$. Thus, there exists a positive integer *i* such that $b^p = a^i$. Our claim now is that *p* divides *i*, and we'll prove this claim using proof by contradiction. Thus, assume that *p* does not divide *i*. Then it is also true that p^m does not divide $\frac{ip^m}{p} = ip^{m-1}$.

Hence, $\frac{ip^m}{p} = ip^{m-1}$ is not a multiple of p^m, and therefore, $a^{\frac{ip^m}{p}} = a^{ip^{m-1}} \neq e$. But on the other hand, $a^{ip^{m-1}} = (a^i)^{p^{m-1}} = (b^p)^{p^{m-1}} = (b^p)^{p^m/p} = b^{p^m} = (b^{p^r})^{p^m/p^r} = (e)^{p^m/p^r} = e$, and this is a contradiction. Therefore, *p* divides *i,* and so we can write $i = jp$ for some positive integer *j*. Now let $y = a^{-j}b$. If *y* were an element of *A*, then $a^j y = b$ is also an element of *A* contradicting our assumption that $b \notin A$. Thus, $y \notin A$. Furthermore, $y^p = (a^{-j}b)^p = a^{-jp}b^p = a^{-i}a^i = e$. But now since we have found an element $y \notin A$ such that $y^p = e$ for *p* a prime, it follows also that $\langle a \rangle \cap \langle y \rangle = e$ and we can now repeat our earlier arguments to conclude that there exists a *subgroup Q* such that $G = A \oplus Q$.

□

<u>Corollary:</u> Since when *G* is an *abelian group* such that $|G| = p^n$ for some prime *p*, we can write $G = A \oplus Q$ where *A* is a *cyclic subgroup* of *G* that is of maximal order,

it follows that we can do the same with *Q* and then continue until we have *G* written as a *direct sum* of cyclic *p-groups*.

□

<u>The Fundamental Theorem of Finite Abelian Groups:</u> If *G* is a *finite abelian group* such that $|G| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ for primes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, then we can write *G* as a *direct sum* of cyclic *p-groups* using each prime p_i that divides the order of *G*.

<u>Proof:</u> Our last corollary to the *Sylow theorems* showed that we can write *G* as a *direct sum* of its *Sylow p-subgroups*, $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$. Also, our theorem and corollary above show that each *Sylow p-subgroup* can be written as a *direct sum* of *cyclic p-groups*. Thus, combining these results, we can also write *G* as a *direct sum* of *cyclic p-groups* using each prime p_i that divides the order of *G*.

□

HOW TO USE GAP (PART 10)

As usual we will begin as usual by repeating all the GAP commands with learned up to this point so that you don't have to reference earlier parts of this work, and then at the end we'll introduce in red a few new GAP commands.

1. *How can I redisplay the previous command in order to edit it?*

   Press down on the control key and then also press p. In other words, "Ctrl p".

2. *If the program gets in a loop and shows you the prompt "brk>" instead of "gap>", how can I exit the loop?*

   Press down on the control key and then also press d. In other words, "Ctrl d".

3. *How can I exit the program?*

   Either click on the "close" box for the window, or type "quit;" and press "Enter."

4. *How do I find the inverse of a permutation?*

```
gap> a:=(1,2,3,4);
(1,2,3,4)
gap> a^-1;
```

```
(1,4,3,2)
```

5. *How can I multiply permutations and raise permutations to powers?*

```
gap> (1,2)*(1,2,3);
(1,3)

gap> (1,2,3)^2;
(1,3,2)

gap> (1,2,3)^-1;
(1,3,2)

gap> (1,2,3)^-2;
(1,2,3)

gap> a:=(1,2,3);
(1,2,3)

gap> b:=(1,2);
(1,2)

gap> a*b;
(2,3)

gap> a^2;
(1,3,2)

gap> a^-2;
(1,2,3)
```

```
gap> a^3;
()
gap> a^-3;
()

gap> (a*b)^2;
()

gap> (a*b)^3;
(2,3)
```

6. *How can I create a group from permutations, find the size of the group, and find the elements in the group?*

```
gap> a:=(1,2);
(1,2)

gap> b:=(1,2,3);
(1,2,3)

gap> g1:=Group(a,b);
Group([ (1,2), (1,2,3) ])

gap> Size(g1);
6

gap> Elements(g1);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> g2:=Group([(1,2),(1,2,3)]);
```

Group([(1,2), (1,2,3)])

gap> g3:=Group((1,2),(2,3,4));
Group([(1,2), (2,3,4)])

7. *How can I create a cyclic group of order 3?*

gap> a:=(1,2,3);
(1,2,3)

gap> g1:=Group(a);
Group([(1,2,3)])

gap> Size(g1);
3

gap> Elements(g1);
[(), (1,2,3), (1,3,2)]

gap> g2:=Group((1,2,3));
Group([(1,2,3)])

```
gap> g3:=CyclicGroup(IsPermGroup,3);
Group([ (1,2,3) ])
```

8. *How can I create a multiplication table for the cyclic group of order 3 that I just created?*

```
gap> ShowMultiplicationTable(g1);

*       | ()      (1,2,3)  (1,3,2)
--------+---------------------------------
()      | ()      (1,2,3)  (1,3,2)
(1,2,3) | (1,2,3) (1,3,2)  ()
(1,3,2) | (1,3,2) ()       1,2,3)
```

9. *How do I determine if a group is abelian?*

```
gap> g1:=Group((1,2,3));
Group([ (1,2,3) ])
gap> IsAbelian(g1);
true

gap> g2:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])
gap> IsAbelian(g2);
false
```

10. *What do I type in order to get help for a command like "Elements?"*

```
gap> ?Elements
```

11. *How do I find all subgroups of a group?*

```
gap> a:=(1,2,3);
(1,2,3)
gap> b:=(2,3);
(2,3)
gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])
gap> Size(g);
6
gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=AllSubgroups(g);
```

```
[ Group(()), Group([ (2,3) ]), Group([ (1,2) ]), Group([ (1,3) ]),
Group([ (1,2,3) ]), Group([ (1,2,3), (2,3) ]) ]

gap> List(h,i->Elements(i));
[ [ () ], [ (), (2,3) ], [ (), (1,2) ], [ (), (1,3) ], [ (), (1,2,3),
(1,3,2) ], [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ] ]

gap> Elements(h[1]);
[ () ]

gap> Elements(h[2]);
[ (), (2,3) ]

gap> Elements(h[3]);
[ (), (1,2) ]

gap> Elements(h[4]);
[ (), (1,3) ]


gap> Elements(h[5]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(h[6]);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
```

12. *How do I find the subgroup generated by particular permutations?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=Subgroup(g,[(1,2)]);
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]
```

13. *How do I determine if a subgroup is normal?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> h1:=Group((1,2));
Group([ (1,2) ])
gap> IsNormal(g,h1);

gap> h2:=Group((1,2,3));
Group([ (1,2,3) ])

gap> IsNormal(g,h2);
true
```

14. *How do I find all normal subgroups of a group?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> n:=NormalSubgroups(g);
[ Group([ (1,2), (1,2,3) ]), Group([ (1,3,2) ]), Group(()) ]

gap> Elements(n[1]);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> Elements(n[2]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(n[3]);
[ () ]
```

15. *How do I determine if a group is simple?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> IsSimple(g);
false


gap> h:=Group((1,2));
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]

gap> IsSimple(h);
true
```

16. *How do I find the right cosets of a subset H of G?*

```
gap> g:=Group([(1,2,3),(1,2)]);
Group([ (1,2,3), (1,2) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=Subgroup(g,[(1,2)]);
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]

gap> c:=RightCosets(g,h);
```

```
[ RightCoset(Group( [ (1,2) ] ),()), RightCoset(Group( [ (1,2) ] ),(1,3,2)),
RightCoset(Group( [ (1,2) ] ),(1,2,3)) ]

gap> List(c,i->Elements(i));
[ [ (), (1,2) ], [ (2,3), (1,3,2) ], [ (1,2,3), (1,3) ] ]

gap> Elements(c[1]);
[ (), (1,2) ]

gap> Elements(c[2]);
[ (2,3), (1,3,2) ]

gap> Elements(c[3]);
[ (1,2,3), (1,3) ]
```

17. *How can I create a a quotient (factor) group?*

```
gap> g:=Group([(1,2,3),(1,2)]);
Group([ (1,2,3), (1,2) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> n:=Group((1,2,3));
Group([ (1,2,3) ])

gap> Elements(n);
[ (), (1,2,3), (1,3,2) ]

gap> IsNormal(g,n);
true

gap> c:=RightCosets(g,n);
[ RightCoset(Group([ (1,2,3) ]),()), RightCoset(Group([ (1,2,3) ]),(2,3)) ]

gap> Elements(c[1]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(c[2]);
[ (2,3), (1,2), (1,3) ]

gap> f:=FactorGroup(g,n);
Group([ f1 ])

gap> Elements(f);
[ <identity> of ..., f1 ]

gap> ShowMultiplicationTable(f);
*                  | <identity> of ... f1
-------------------+-----------------------------------
<identity> of ...  | <identity> of ... f1
f1                 | f1                <identity> of ...
```

18. *How do I create a dihedral group with 2n elements for an n-sided regular polygon?*

```
gap> d4:=DihedralGroup(IsPermGroup,8);
Group([ (1,2,3,4), (2,4) ])

gap> Elements(d4);
[ (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) ]
```

19. *How can I express the elements of a dihedral group as rotations and flips rather than as permutations?*

```
gap> d3:=DihedralGroup(6);
<pc group of size 6 with 2 generators>

gap> Elements(d3);
[ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2 ]

gap> ShowMultiplicationTable(d3);
*                 | <identity> of ... f1                f2                f1*f2             f2^2              f1*f2^2
------------------+-----------------------------------------------------------------------------------------------------------\
---------
<identity> of ... | <identity> of ... f1                f2                f1*f2             f2^2              f1*f2^2
f1                | f1                <identity> of ... f1*f2             f2                f1*f2^2           f2^2
f2                | f2                f1*f2^2           f2^2              f1                <identity> of ... f1*f2
f1*f2             | f1*f2             f2^2              f1*f2^2           <identity> of ... f1                f2
f2^2              | f2^2              f1*f2             <identity> of ... f1*f2^2           f2                f1
f1*f2^2           | f1*f2^2           f2                f1                f2^2              f1*f2
<identity> of ...
```

20. *How do I create a symmetric group of degree n with n! elements?*

```
gap> s4:=SymmetricGroup(4);
Sym( [ 1 .. 4 ] )

gap> Elements(s4);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3),
(1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2),
  (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3),
(1,4), (1,4,2,3), (1,4)(2,3) ]
```

21. *How do I create a direct product of two or more groups?*

```
gap> g1:=Group((1,2,3));
Group([ (1,2,3) ])

gap> g2:=Group((4,5));
Group([ (4,5) ])

gap> dp:=DirectProduct(g1,g2);
Group([ (1,2,3), (4,5) ])

gap> Size(dp);
6
```

```
gap> Elements(dp);
[ (), (4,5), (1,2,3), (1,2,3)(4,5), (1,3,2), (1,3,2)(4,5) ]

gap> ShowMultiplicationTable(dp);
*             | ()            (4,5)         (1,2,3)       (1,2,3)(4,5) (1,3,2)
(1,3,2)(4,5)
-------------+---------------------------------------------------------------------
---
()            | ()            (4,5)         (1,2,3)       (1,2,3)(4,5) (1,3,2)
(1,3,2)(4,5)
(4,5)         | (4,5)         ()            (1,2,3)(4,5) (1,2,3)       (1,3,2)(4,5) (1,3,2)
(1,2,3)       | (1,2,3)       (1,2,3)(4,5) (1,3,2)       (1,3,2)(4,5) ()            (4,5)
(1,2,3)(4,5) | (1,2,3)(4,5) (1,2,3)       (1,3,2)(4,5) (1,3,2)       (4,5)         ()
(1,3,2)       | (1,3,2)       (1,3,2)(4,5) ()            (4,5)         (1,2,3)
(1,2,3)(4,5)
(1,3,2)(4,5) | (1,3,2)(4,5) (1,3,2)       (4,5)         ()            (1,2,3)(4,5) (1,2,3)
```

22. *How do I find the conjugate of a permutation in the form* $a^b = b^{-1}ab$ *?*

```
gap> a:=(1,2,3,4,5);
(1,2,3,4,5)

gap> b:=(2,4,5);
(2,4,5)

gap> a^b;
(1,4,3,5,2)

gap> b^-1*a*b;
(1,4,3,5,2)
```

23. *How do I divide up a group into classes of elements that are conjugate to one another? (Note that "conjugacy" is an equivalence relation on our group G. That means that G can be separated into nonintersecting subsets that contain only elements that are conjugate to one another.)*

```
gap> d3:=DihedralGroup(IsPermGroup,6);
Group([ (1,2,3), (2,3) ])


gap> Size(d3);
6


gap> Elements(d3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]


gap> cc:=ConjugacyClasses(d3);
[ ()^G, (2,3)^G, (1,2,3)^G ]
```

```
gap> Elements(cc[1]);
[ () ]

gap> Elements(cc[2]);
[ (2,3), (1,2), (1,3) ]

gap> Elements(cc[3]);
[ (1,2,3), (1,3,2) ]
```

24. *How do I find all conjugates of a subgroup H of a group G?*

```
gap> d3:=DihedralGroup(IsPermGroup,6);
Group([ (1,2,3), (2,3) ])

gap> Elements(d3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=Group((1,2));
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]

gap> cs:=ConjugateSubgroups(d3,h);
[ Group([ (1,2) ]), Group([ (1,3) ]), Group([ (2,3) ]) ]

gap> Elements(cs[1]);
[ (), (1,2) ]

gap> Elements(cs[2]);
[ (), (1,3) ]

gap> Elements(cs[3]);
[ (), (2,3) ]
```

25. *How do I input a 3x3 matrix in GAP and display in its usual rectangular format?*

```
gap> x:=[[1,2,3],[4,5,6],[7,8,9]];
[ [ 1, 2, 3 ], [ 4, 5, 6 ], [ 7, 8, 9 ] ]

gap> PrintArray(x);
[ [  1,  2,  3 ],
  [  4,  5,  6 ],
  [  7,  8,  9 ] ]
```

26. *How do I do arithmetic with matrices?*

```
gap> x:=[[1,2],[3,4]];
[ [ 1, 2 ], [ 3, 4 ] ]

gap> y:=[[5,6],[7,8]];
[ [ 5, 6 ], [ 7, 8 ] ]

gap> PrintArray(x+y);
[ [   6,   8 ],
  [  10,  12 ] ]

gap> PrintArray(x-y);
[ [  -4,  -4 ],
  [  -4,  -4 ] ]

gap> PrintArray(x*y);
[ [  19,  22 ],
  [  43,  50 ] ]
```

27. *How do I multiply a matrix by a number (scalar)?*

```
gap> x:=[[1,2],[3,4]];
[ [ 1, 2 ], [ 3, 4 ] ]

gap> PrintArray(x);
[ [  1,  2 ],
  [  3,  4 ] ]

gap> PrintArray(2*x);
[ [  2,  4 ],
  [  6,  8 ] ]

gap> PrintArray(x/2);
[ [  1/2,    1 ],
  [  3/2,    2 ] ]
```

28. *How do I find the inverse of a matrix?*

```
gap> x:=[[1,2],[3,4]];
[ [ 1, 2 ], [ 3, 4 ] ]

gap> PrintArray(x);
[ [  1,  2 ],
  [  3,  4 ] ]

gap> xinverse:=x^-1;
[ [ -2, 1 ], [ 3/2, -1/2 ] ]

gap> PrintArray(xinverse);
[ [    -2,     1 ],
  [   3/2,  -1/2 ] ]

gap> xinverse:=1/x;
[ [ -2, 1 ], [ 3/2, -1/2 ] ]

gap> PrintArray(xinverse);
[ [    -2,     1 ],
  [   3/2,  -1/2 ] ]

gap> PrintArray(x*xinverse);
[ [  1,  0 ],
  [  0,  1 ] ]
```

29. *How do I find the transpose of a matrix?*

```
gap> x:=[[1,2],[3,4]];
[ [ 1, 2 ], [ 3, 4 ] ]

gap> PrintArray(x);
[ [  1,  2 ],
  [  3,  4 ] ]

gap> xtranspose:=TransposedMat(x);
[ [ 1, 3 ], [ 2, 4 ] ]

gap> PrintArray(xtranspose);
[ [  1,  3 ],
  [  2,  4 ] ]
```

30. *How do I find the determinant of a matrix?*

```
gap> x:=[[1,2],[3,4]];
[ [ 1, 2 ], [ 3, 4 ] ]

gap> PrintArray(x);
[ [  1,  2 ],
  [  3,  4 ] ]

gap> DeterminantMat(x);
-2
```

31. *How do I input the generators for the Rubik's cube group into GAP?*

In *Windows*, use *Notepad* to type the following file, and save it to your *C*-drive.

```
r:=(25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24);
l:=(9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35);
u:=(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19);
d:=(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40);
f:=(17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11);
b:=(33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27);
```

Now enter the following commands.

```
gap> Read("C:/rubik.txt");
gap>

gap> rubik:=Group(r,l,u,d,f,b);
<permutation group with 6 generators>
```

32. *How do I find the center of the Rubik's cube group?*

```
gap> c:=Center(rubik);
Group([ (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,4
5)(39,47) ])

gap> Size(c);
2
gap> Elements(c);
[ (),
(2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,45)(39,47
) ]
```

33. *How do I find the orbits that the Rubik's cube group creates on the set* $\{1, 2, 3, \ldots, 48\}$ *?*

```
gap> Orbit(rubik,1);
[ 1, 17, 3, 14, 41, 9, 19, 38, 8, 22, 48, 40, 43, 11, 33, 46, 24, 6, 30, 27, 16,
35, 25, 32 ]
```

```
gap> Orbit(rubik,2);
[ 2, 5, 13, 18, 36, 37, 42, 39, 34, 12, 10, 31, 15, 7, 4, 26, 20, 45, 21, 44,
47, 28, 29, 23 ]
```

```
gap> o:=Orbits(rubik);
[ [ 1, 17, 3, 14, 41, 9, 19, 38, 8, 22, 48, 40, 43, 11, 33, 46, 24, 6, 30, 27,
16, 35, 25, 32 ],
[ 2, 5, 12, 36, 7, 10, 47, 45, 34, 4, 28, 13, 44, 29, 21, 26, 37, 20, 42, 15,
31, 23, 18, 39 ] ]
```

```
gap> Size(o);
2
```

```
gap> Elements(o);
[ [ 1, 17, 3, 14, 41, 9, 19, 38, 8, 22, 48, 40, 43, 11, 33, 46, 24, 6, 30, 27,
16, 35, 25, 32 ],
[ 2, 5, 12, 36, 7, 10, 47, 45, 34, 4, 28, 13, 44, 29, 21, 26, 37, 20, 42, 15,
31, 23, 18, 39 ] ]
```

34. *How do I find the derived or commutator subgroup of the Rubik's cube group?*

```
gap> d:=DerivedSubgroup(rubik);
<permutation group with 5 generators>
```

```
gap> Size(d);
21626001637244928000
```

35. *How do I find the quotient or factor group corresponding to the commutator subgroup?*

```
gap> q:=CommutatorFactorGroup(rubik);
Group([ f1 ])
```

```
gap> Size(q);
2
```

```
gap> Elements(q);
[ <identity> of ..., f1 ]
```

```
gap> ShowMultiplicationTable(q);
*                  | <identity> of ... f1
-------------------+-----------------------------------
<identity> of ... | <identity> of ... f1
f1                 | f1                <identity> of ...
```

36. *How do I work with functions in GAP?*

```
gap> f:=x->x^2;
function( x ) ... end

gap> g:=x->x+2;
function( x ) ... end

gap> f(3);
9

gap> g(3);
5

gap> f(g(3));
25

gap> g(f(3));
11
```

37. *If a group G acts on a set X, how do I find the stabilizer subgroup for a point in X?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> b:=(2,3);
(2,3)

gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])

gap> s:=Stabilizer(g,1);
Group([ (2,3) ])

gap> Size(s);
2

gap> Elements(s);
[ (), (2,3) ]
```

SUMMARY (PART 10)

In part 10 we've covered quite a lot! And yet there are many more topics in group theory that I've have paid little or no attention to. The bottom line is that there is always much, much more to learn, and it is likely that no book will ever exhaust what is known or what can be known. I have simply focused on those things I like best and those things that I consider most important. And if you've made it this far, then you are, indeed, exceptional. The rest of the journey is now up to you. However, for now you want to be familiar with the following topics that we discussed in Part 10.

- Homomorphisms
- Isomorphisms
- Kernel of a homomorphism
- The natural homomorphism
- The correspondence theorem
- The 1st isomorphism theorem
- The 2nd isomorphism theorem
- The 3rd isomorphism theorem
- Quotient groups
- Orbits
- Stabilizers
- Fixers
- Burnside's Counting Theorem
- Mathematical induction
- Conjugacy classes
- The Class Equation
- The 1st Sylow theorem
- The 2nd Sylow theorem
- The 3rd Sylow theorem
- The Fundamental Theorem of Finite Abelian Groups

PRACTICE (PART 10)

1. Construct proofs for each of the three *isomorphism* theorems.

   <u>The First Isomorphism Theorem:</u> Let $f: A \to B$ be a *homomorphism* from a *group A onto* a *group B*, and let $N = Ker(f)$. Then $A/Ker(f) = A/N \cong B$.

   <u>The Second Isomorphism Theorem:</u> If *H* and *N* are *subgroups* of a *group G* with *N normal* in *G*, then $H/H \cap N \cong HN/N$.

   <u>The Third Isomorphism Theorem:</u> Let *G* be a *group*, let *N* and *H* be *normal subgroups* of *G*, and suppose that $N \subseteq H \subseteq G$. Then H/N is a *normal subgroup* of G/N, and $(G/N)/(H/N) \cong G/H$.

2. If S_5 acts on the set $X = \{1, 2, 3, 4, 5\}$, find the size and elements of the *stabilizer subgroup* $Stabilizer_{S_5}(2)$.

3. Suppose you have a pentagonal bracelet with 5 differently colored, equally spaced beads, and suppose that you either rotate the bracelet clockwise through multiples of $72°$, or you can flip the bracelet about any of 5 axes of symmetry. .Then the *dihedral group* D_5 acts upon the beads of this regular pentagon that may be labeled by $X = \{1, 2, 3, 4, 5\}$. Use *Burnside's Counting Theorem* to find the number of orbits in *X* under the action by D_5.

4. Use the *Fundamental Theorem of Abelian Groups* to find all *abelian groups* of order 16.

5. You have done exceptionally well to make it to this point. Now relax!

PRACTICE (PART 10) - ANSWWERS

1. Construct proofs for each of the three *isomorphism* theorems.

<u>The First Isomorphism Theorem:</u> Let $f: A \to B$ be a *homomorphism* from a *group A onto* a *group B*, and let $N = Ker(f)$. Then $A/Ker(f) = A/N \cong B$.

<u>Proof:</u> Recall that $\pi: A \to A/N$ defined by $\pi(a) = Na$ is called the *natural homomorphism*. Now define a function *i* from A/N to *B* by $i(Na) = f(a)$. What we want to do now is to verify that *i* is an *isomorphism* from A/N to *B*. First, we will show that this function is *onto*. Thus, if $b \in B$, then there exists $a \in A$ such that $f(a) = b$ since *f* is *onto*. Hence, $i(\pi(a)) = i(Na) = f(a) = b$ shows that *i* is also *onto*.

To show that *i* is *one-to-one*, let $Nx, Ny \in A/N$ such that $Nx \neq Ny$. Then, in particular, Nx and Ny have no elements in common because if they did, then we would have $n_1 x = n_2 y \Rightarrow x = n_1^{-1} n_2 y \Rightarrow x \in Ny \Rightarrow Nx = Ny$. Furthermore, $f(x) \neq f(y)$ because if $f(x) = f(y)$, then $e = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ implies that $xy^{-1} \in N = Ker(f)$ which implies that $xy^{-1} = n \in N \Rightarrow x = ny \Rightarrow Nx = Ny$. But his contradicts our assumption that $Nx \neq Ny$, and, hence, $Nx \neq Ny \Rightarrow f(x) \neq f(y)$, and so $i: A/N \to B$ is *onto-to-one*.

Before we show that $i: A/N \to B$ is a *homomorphism*, notice that it doesn't matter what representative we use from a coset such as *Na*. In other words, since $N = Ker(f)$, if $a, b \in Na$, then $a = nb$ and $f(a) = f(nb) = f(n)f(b) = e \cdot f(b) = f(b)$. Hence, it is also true that $i(a) = i(b)$. Now let $Nx, Ny \in A/N$. Then $i(NxNy) = i(Nxy) = f(xy) = f(x)f(y) = i(Nx)i(Ny)$. Therefore, $i: A/N \to B$ is an *isomorphism*, and $A/Ker(f) = A/N \cong B$.

□

The Second Isomorphism Theorem: If *H* and *N* are *subgroups* of a *group G* with *N normal* in *G*, then $H/H \cap N \cong HN/N$.

Proof: Recall that earlier we proved that if *H* is a *subgroup* of *G*, then there will exist a corresponding *subgroup* of G/N that is obtained by looking at the *cosets* *Nh* where $h \in H$. This theorem, the *Second Isomorphism Theorem*, sharpens and clarifies the result. To prove it, though, we first need to show that $H \cap N$ is a *normal subgroup* of *H* and that *HN* is a *subgroup* of *G* that contains *N*. So let's begin!

To show that $H \cap N$ is a *normal subgroup* of *H*, we first need to show that it is at least a *subgroup* by verifying properties of *closure* and existence of *inverses*. Thus, let $n_1, n_2 \in H \cap N$. Since $n_1, n_2 \in H$, a *subgroup* of *G*, it follows that $n_1 n_2 \in H$. But by the same token, $n_1, n_2 \in N$ implies that $n_1 n_2 \in N$. Hence, $n_1 n_2 \in H \cap N$, and *closure* is satisfied.

Now suppose that $n \in H \cap N$. Then an *inverse* to *n* exists in both *H* and in *N*. In other words, $n^{-1} \in H$ and $n^{-1} \in N$ implies that $n^{-1} \in H \cap N$. Thus, existence of *inverses* is satisfied, and $H \cap N$ is a *subgroup* of *H*.

To show that $H \cap N$ is a *normal subgroup* of *H*, let $h \in H$ and let $n \in H \cap N$. Then $h^{-1}nh \in H$ since all three elements belong to *H*. But on the other hand, $h^{-1}nh \in N$ since *N* is a *normal subgroup* of *G*. Hence, $h^{-1}nh \in H \cap N$, and so $H \cap N$ is a *normal subgroup* of *H*.

Now let's show that *HN* is a *subgroup* of *G*. Thus, to show *closure*, let $h_1 n_1, h_2 n_2 \in HN$, and consider the product $h_1 n_1 h_2 n_2$. Since *N* is a *normal subgroup* of *G*, every *left coset* of *N* is equal to the corresponding *right coset*, and that means that $h_2 N = Nh_2 = Nn_1 h_2$. Hence, there exists $n_3 \in N$ such that $n_1 h_2 = h_2 n_3$. Thus, $h_1 n_1 h_2 n_2 = h_1 h_2 n_3 n_2 \in HN$, and *closure* is satisfied. To show the existence of *inverses* in *HN*, let $hn \in HN$. Then it's *inverse* is $n^{-1}h^{-1}$. However, again since *N* is *normal* in *G*, there exists $n_4 \in N$ such that $n^{-1}h^{-1} = h^{-1}n_4 \in HN$. Therefore, *inverses* exist in *HN*, and *HN* is a subgroup of *G*. Furthermore, $N \subseteq HN$ since every element of *N* can be written as $e \cdot n$ where $e \in H$ and $n \in N$.

And finally, we need to state and prove our *isomorphism* from $H/H \cap N$ to HN/N. In this case, define $f : H/H \cap N \to HN/N$ by $f[(H \cap N)h] = Nh$. To show that *f* is a *homomorphism*, observe that $f[(H \cap N)h_1] \cdot f[(H \cap N)h_2] = Nh_1 \cdot Nh_2 = N(h_1h_2) = f[(H \cap N)h_1h_2]$ Notice, too, that elements in $H/H \cap N$ look like $\{H \cap N, (H \cap N)h_1, (H \cap N)h_2, (H \cap N)h_3, \ldots\}$ where $h_1, h_2, h_3, \ldots \notin H \cap N$, and the corresponding elements in HN/N look like $\{N, Nh_1, Nh_2, Nh_3, \ldots\}$. From this it should be clear that $Ker(f) = H \cap N$ because if $h \notin H \cap N$, then it gets mapped to $Nh \neq N$, the *identity* in HN/N. Thus, from previous proof on *homomorphisms* and *one-to-one functions*, it follows that *f* is *one-to-one*. And finally, to show that *f* is *onto*, suppose that $Nhn \in HN/N$. Then since *N* is a *normal subgroup*, we can rewrite *hn* as n_1h for some $n_1 \in N$. Hence, $Nhn = Nn_1h = Nh = f[(H \cap N)h]$, and therefore, *f* is *onto* and $H/H \cap N \cong HN/N$.

□

The Third Isomorphism Theorem: Let *G* be a *group*, let *N* and *H* be *normal subgroups* of *G*, and suppose that $N \subseteq H \subseteq G$. Then H/N is a *normal subgroup* of G/N, and $(G/N)/(H/N) \cong G/H$.

Proof: It follows immediately from the *Correspondence Theorem* that H/N is a *normal* subgroup of G/N. Now let $i : G \to G/N$ be the *natural homomorphism*, and let $j : G/N \to (G/N)/(H/N)$ be another *natural homomorphism*. Then $j \circ i$ is a *homomorphism* from *G onto* $(G/N)/(H/N)$.

$$G \xrightarrow{i} G/N \xrightarrow{j} (G/N)/(H/N)$$

Hence, our *First Isomorphism Theorem* tells us that $(G/N)/(H/N)$ is *isomorphic* to $G/Ker(j \circ i)$. Thus, we just need to figure out what is contained in $Ker(j \circ i)$. Thus, let $h \in H \subseteq G$. Then $Nh \in H/N \subseteq G/N$ tells us that $h \in Ker(j \circ i)$. On the other hand, if $g \in G$, but $g \notin H$, then $Ng \notin H/N$, and, thus, $g \notin Ker(j \circ i)$. Therefore, $Ker(j \circ i) = H$, and by the *First Isomorphism Theorem*, G/H is *isomorphic* to $(G/N)/(H/N)$.

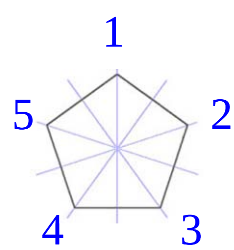
$\square$

2. If S_5 acts on the set $X = \{1,2,3,4,5\}$, find the size and elements of the *stabilizer subgroup* $Stabilizer_{S_5}(2)$.

```
gap> s5:=SymmetricGroup(5);
Sym( [ 1 .. 5 ] )

gap> h:=Stabilizer(s5,2);
Sym( [ 1, 3, 4, 5 ] )

gap> Size(h);
24

gap> Elements(h);
[ (), (4,5), (3,4), (3,4,5), (3,5,4), (3,5), (1,3), (1,3)(4,5), (1,3,4),
(1,3,4,5), (1,3,5,4), (1,3,5), (1,4,3),
  (1,4,5,3), (1,4), (1,4,5), (1,4)(3,5), (1,4,3,5), (1,5,4,3), (1,5,3), (1,5,4),
(1,5), (1,5,3,4), (1,5)(3,4) ]
```

3. Suppose you have a pentagonal bracelet with 5 differently colored, equally spaced beads, and suppose that you either rotate the bracelet clockwise through multiples of $72°$, or you can flip the bracelet about any of 5 axes of symmetry. .Then the *dihedral group* D_5 acts upon the beads of this regular pentagon that may be labeled by $X = \{1,2,3,4,5\}$. Use *Burnside's Counting Theorem* to find the number of orbits in *X* under the action by D_5.

Suppose you have a pentagonal bracelet with 5 differently colored, equally spaced beads, and suppose that you either rotate the bracelet clockwise through multiples of $72°$, or you can flip the bracelet about any of 5 axes of symmetry. Then our set *X* will consist of $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$ color configurations, and our group is D_5, the group of symmetries of a regular pentagon with $|D_5| = 10$. Again, if we label the vertices 1, 2, 3, 4, and 5, then we can describe D_5 in terms of the following permutations, $D_5 = \left\{ \begin{matrix} (\ ),(1,2,3,4,5),(1,3,5,2,4),(1,4,2,5,3),(1,5,4,3,2), \\ (2,5)(3,4),(1,2)(3,5),(1,3)(4,5),(1,4)(2,3),(1,5)(2,4) \end{matrix} \right\}$.

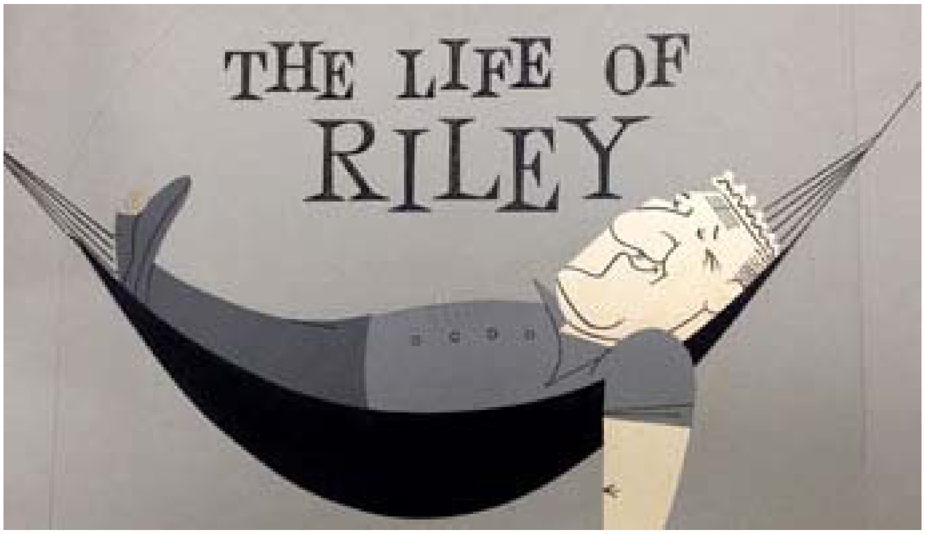


Now, as before, the *identity* fixes all $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$ color configurations, and the remaining elements of D_5 fix none of the configurations. Hence, the number of *orbits* in *X* under D_5 is $\frac{1}{|D_5|}\sum_{x\in X}\left|Stabilizer_{D_5}(x)\right| = \frac{1}{|D_5|}\sum_{g\in D_5}\left|Fixer_X(g)\right| = \frac{1}{10}\cdot 120 = 12$. In other words, there are 12 distinct ways to color the beads with different colors when we allow for the symmetries of the pentagon.

4. Use the *Fundamental Theorem of Abelian Groups* to find all *abelian groups* of order 16.

C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2 \times C_2$, $C_2 \times C_2 \times C_2 \times C_2$

5. You have done exceptionally well to make it to this point. Now relax!



THE GROUP THEORY IS STRONG IN YOU!