A CHILD'S GARDEN OF GROUPS

Proving Theorems!

(Part 9)

by

Doc Benton

CONTENTS (PART 9)

INTRODUCTION (PART 9)

In Part 9 of this *group theory* saga we finally encounter theorem proving. This, of course, is where most college level courses on *group theory* and *abstract algebra* begin, but we have found so much other stuff to discuss that proving theorems in our work comes at the very end. Also, in this part, we restrict ourselves to theorems that have proofs that are generally very short and easy to comprehend. Nonetheless, we begin with an introductory chapter on *symbolic logic* and what expressions like *"If A, then B,"* and *"A if and only if B"* actually mean. Additionally, we sometimes color-code parts of our proofs in order to make them easier to follow. Furthermore, in this part and in Part 10 which will look at more advanced proofs and theorems, we often are more verbose than most mathematicians might be, and we do this in order to make our explanations as clear as possible. Enjoy!

SYMBOLIC LOGIC

This lesson is an introduction to symbolic logic and what we actually mean in mathematics by statements such as "*a* implies *b*" and "*a* if and only if *b*." Below are some common symbols that are used in logic followed by the corresponding math symbols that I will use instead.

LOGIC	**MATH**
~ or $\neg$	not
$\vee$	or
$\wedge$	and
$a \rightarrow b$	$a \Rightarrow b$
$a \leftrightarrow b$	$a \Leftrightarrow b$

The statement "$a \Rightarrow b$" can be read as *"a implies b"* or *"if a then b"* or *"a is a sufficient condition for b"* or *"b is a necessary condition for a."*

The statement "$a \Leftrightarrow b$" can be read or written as *"a iff b"* or *"a if and only if b"* or *"a implies b and b implies a"* or *"a is a necessary and sufficient condition for b."*

Using the logical connectives above, we can rewrite "$a \Rightarrow b$" as "$\text{not } (a \text{ \& not-}b)$." Similarly, since "$a \Leftrightarrow b$" means "$a \Rightarrow b$ & $b \Rightarrow a$," we can rewrite "$a \Leftrightarrow b$" as "$[\text{not } (a \text{ \& not-}b)]$ & $[\text{not } (b \text{ \& not-}a)]$."

In mathematics, for a compound statement *"A & B"* to be true, both of the statements *A* and *B* must be true. On the other hand, for the compound statement *"A or B"* to be true, only one of the statements must be true. You can construct some simple examples to convince yourself that this is the correct way to proceed. Also, in mathematics, unless stated otherwise, we always use an *inclusive or*. That means that for *“A or B”* to be true, we either have *A* true or *B* true or both *A* and *B* true. In an *exclusive or*, either *A* or *B* can be true, but not both at the same time.

To determine the truth possibilities for a statement or a combination of statements, we often set up what we call a *truth table.* For example, below is a *truth table* for a statement in the form *Not-A*. We begin by noting that *A* can be a statement that is either *true* or *false*, and then we will always assume that the opposite of *true* is *false,* and the opposite of *false* is *true*. This assumption is known as the *Law of the Excluded Middle*. In other words, we’ll assume that there is nothing in between *true* and *false* that could happen. This is what is generally assumed when doing mathematics, but to be honest, this is not always the case. For example, consider the following statement: *This statement is false*. Notice that if our statement is *true*, then it follows that it is *false*, and if it is *false*, then it follows that it is *true*. This type of statement is an example of a paradox that is neither *true* nor *false*. However, we generally take it for granted when doing mathematics that we are not dealing with paradoxes, and given that, here is the *truth table* for *Not-A*, where the final truth values are presented in the yellow column.

Not	**A**
F	T
T	F

From this *truth table*, we see that if *A* is *true*, then *Not-A* is *false,* and if *A* is *false*, then *Not-A* is *true*. Simple!

Now let's look at a *truth table* for a compound statement of the form *A & B*. Notice that since both *A* and *B* can be either *true* or *false* statements, there are four separate combinations of *true* and *false* that we can come up with.

A	**&**	**B**
T	**T**	T
T	**F**	F
F	**F**	T
F	**F**	F

Notice, also, that this time that our compound statement is *true* only when both *A* and *B* are *true*.

In our next example, we'll examine the possible truth values of a compound statement of the form *A or B*.

A	**or**	**B**
T	**T**	T
T	**T**	F
F	**T**	T
F	**F**	F

This time, for the compound statement to be *true*, only one of the statements, *A* or *B*, need be true, and that the compound statement is *false* only when both *A* and *B* are *false.*

When we have an assertion in a mathematical proof such as *A implies B or* $A \Rightarrow B$ or *if A, then B*, then what we are trying to say is that if *A* is *true*, then *B* has to be *true* as well. In the language of symbolic logic, we consider all of the formulations in the previous sentence to be equivalent to the statement *Not-(A & Not-B)*. In other words, it's not the case that *A* can be *true* and *B* not be *true*. Below is our *truth table* for such a statement.

Not	**[A**	**&**	**(Not**	**B)]**
T	T	F	F	T
F	T	T	T	F
T	F	F	F	T
T	F	F	T	F

There are a couple of things to notice here. First, a *true* statement cannot imply a *false* statement. Thus, the ultimate *truth* value of a compound statement such as, *"If I am an old mathematician, then the moon is made of green cheese,"* is *false*. In this example, the first statement is *true*, but the second statement is *false*, and thus, the *truth* value of the whole implication is *false*. But on the other hand, a *false* statement can always imply anything. For instance, if I say, *"If the moon is made of green cheese, then I am Superman,"* then that compound statement is considered true. In other words, you can't argue logically that the assertion *A implies B* is *false* simply because the first statement in our assertion isn't *true* to begin with. In symbolic logic, a *false statement* can imply anything, and the proof of this is in the *truth table* where we clearly see that if our first statement is *false*, then the implication is *true* regardless of whether the second statement is *true* or *false*.

When doing proofs in mathematics, the other type of compound statement you are likely to encounter is something of the form *A if and only if B* or $A \Leftrightarrow B$. This is basically a shortened form for *A implies B* and *B implies A*. In other words, the *implication* goes in both directions! And then we can break this done further into the complex statement,

Not-[A & Not-B] & Not-[B & Not-A]

Our *truth table* for this is as follows:

{ Not	**[A**	**&**	**(Not**	**B)] }**	**&**	**{ Not**	**[B**	**&**	**(Not**	**A)] }**
F	T	F	F	T	**F**	F	T	F	F	T
F	T	T	T	F	**F**	T	F	T	F	T
T	F	F	F	T	**F**	F	T	T	T	F
T	F	F	T	F	**T**	T	F	F	T	F

From this *truth table* we see that the statement $A \Leftrightarrow B$ or *A if and only if B* is *true* only when both statements *A* and *B* are *true*.

When we are doing proofs in mathematics that involve *implications*, we generally use argument forms that look like one of the following. The first form is called *modus ponens* and the second form is called *modus tolens*.

Modus Ponens

a. *If A, then B*
b. *A*
c. Therefore, *B*

Modus Tolens

a. *If A, then B*
b. *Not-B*

c. Therefore, *Not-A*

This second form, *modus tolens*, is related to what in mathematics is known as *proof by contradiction*. In this method of proof, you assume *A* is *true* and you want to prove that *B* is *true*. However, instead of arguing directly from *A* to *B*, you essentially say, *"Suppose B isn't true,"* and then you show that this implies that *A* isn't *true*, thus arriving at a contradiction of your initial hypothesis and leaving the conclusion $A \Rightarrow B$ as your only way out of the contradiction.

And now you're ready to see some basic proofs in *group theory*! Enjoy them and study them well so that you can make these techniques your own!

THEOREM 1

THE UNIQUENESS OF THE IDENTITY

Theorem 1: A *group G* has a unique *identity element*. In other words, it has only one element *e* with the property that for every $a \in G$, $e \cdot a = a = a \cdot e$.

.

Proof: Suppose that e_1 and e_2 are both *identity elements* in *G*. Then since e_1 is an *identity element*, it follows that $e_1 \cdot e_2 = e_1 \cdot (e_2) = e_2$. On the other hand, since e_2 is an *identity element*, we also have that $e_1 \cdot e_2 = (e_1) \cdot e_2 = e_1$. Therefore, $e_1 = e_1 \cdot e_2 = e_2$, and the *identity element* in a *group* is unique.

□

THEOREM 2

LEFT CANCELLATION

<u>Theorem 2:</u> Let *G* be a *group*, and let $a,b,c \in G$. If $ab = ac$, then $b = c$.

<u>Proof:</u> Let *G* be a *group* with $a,b,c \in G$, and suppose that $ab = ac$. Then $a^{-1}(ab) = a^{-1}(ac)$. But by the *associative property*, this means that $(a^{-1}a)b = (a^{-1}a)c$ which implies that $eb = ec$ which implies that $b = c$. Therefore, if $ab = ac$, then $b = c$.

$\square$

THEOREM 3

RIGHT CANCELLATION

<u>Theorem 3:</u> Let *G* be a ***group***, and let $a,b,c \in G$. If $ba = ca$, then $b = c$.

<u>Proof:</u> Let *G* be a *group* with $a,b,c \in G$, and suppose that $ba = ca$. Then $(ba)a^{-1} = (ca)a^{-1}$. But by the *associative property*, this means that $b(aa^{-1}) = c(aa^{-1})$ which implies that $be = ce$ which implies that $b = c$. Therefore, if $ba = ca$, then $b = c$.

□

THEOREM 4

THE UNIQUENESS OF INVERSES

Theorem 4: Let *G* be a *group*, and let $a \in G$. Then *a* has a unique *inverse*, denoted by a^{-1}.

Proof: Let *G* be a *group*, and let $a \in G$. Now suppose that $b, c \in G$ such that both *b* and *c* are *inverses* of *a*. Then $ab = e$, the *identity*, and $ac = e$. Hence, $ab = ac$. But by our *Left Cancellation Theorem* (Theorem 2), this implies that $b = c$. Therefore, in a *group* an element *a* has only one, unique *inverse*, denoted by a^{-1}.

□

THEOREM 5

THE INVERSE OF THE INVERSE

Theorem 5: Let *G* be a *group*, and let $a \in G$. Then $a = (a^{-1})^{-1}$.

Proof: Let *G* be a *group*, and let $a, a^{-1} \in G$. Then $aa^{-1} = e$, the *identity*. But on the other hand, $(a^{-1})^{-1}(a^{-1}) = e$. Hence, by the *Right Cancellation Theorem* (Theorem 3), it follows that $a = (a^{-1})^{-1}$.

□

THEOREM 6

THE INVERSE OF *ab*

Theorem 6: Let *G* be a *group*, and let $a,b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: Let *G* be a *group*, and let $a,b \in G$. Then $(ab)^{-1}(ab) = e$, the *identity*. But on the other hand, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$. Hence, $(ab)^{-1}(ab) = (b^{-1}a^{-1})(ab)$, and by the *Left Cancellation Theorem* (Theorem 2), it follows that $(ab)^{-1} = b^{-1}a^{-1}$.

□

THEOREM 7

A CONDITION FOR BEING AN ABELIAN GROUP

Theorem 7: Let *G* be a *group*. If $x^2 = e$ for every $x \in G$, then *G* is *abelian*.

Proof: Let *G* be a *group*, let $a, b \in G$, and suppose that for every $x \in G$, $x^2 = e$. Then, in particular, $(ab)^2 = (ab)(ab) = e$, the identity. Hence, $ab = (ab)^{-1} = b^{-1}a^{-1}$. But since we also have that $a^2 = aa = e$ and $b^2 = bb = e$, it follows that $a = a^{-1}$ and $b = b^{-1}$. Therefore, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ and *G* is *abelian*.

□

THEOREM 8

A PROOF ABOUT THE IDENTITY

Theorem 8: Let *G* be a *group* and let $a, b \in G$. If $ab = e$, then $ba = e$.

Proof: If $ab = e$, then $b = a^{-1}$, and it now immediately follows that $ba = a^{-1}a = e$.

$\square$

THEOREM 9

SUBGROUP OF A GROUP

Theorem 9: Let *G* be a *group* and let *H* be a subset of *G*. If for every $a \in H$ we have that $a^{-1} \in H$ and if for every $a, b \in H$ we have that $ab \in H$, then *H* is a *subgroup* of *G*.

Proof: Let *G* be a *group* and let *H* be a subset of *G*, and assume that for every $a \in H$ we have that $a^{-1} \in H$ and for every $a, b \in H$ we have that $ab \in H$. To show that *H* is a *subgroup* of *G*, we need to show four things – *closure* under the *group* multiplication, the *associative law*, the *existence of an identity*, and the *existence of inverses*. We are assuming in our hypothesis that the *closure* and *inverse properties* are satisfied, and we get the *associative property* for free since it holds for all elements in the *group G*. Thus, we just need to establish the *existence of an identity element*. But this is easy because if $a \in H$, then $a^{-1} \in H$, and since we are assuming *closure* under multiplication in *H*, we have that $aa^{-1} = e \in H$. Therefore, *H* is a *subgroup* of *G*.

□

THEOREM 10

SUBGROUP OF A FINITE GROUP

Theorem 10: Let *G* be a *finite group* and let *H* be a subset of *G*. If for every $a, b \in H$ we have that $ab \in H$, then *H* is a *subgroup* of *G*.

Proof: Let *G* be a *finite group* and let *H* be a subset of *G*, and assume that for every $a, b \in H$ we have that $ab \in H$. Now let $a \in H$. Then our *closure property* tells us that all powers of *a* must also belong to *H*. But since *G* is a *finite group*, eventually one of our powers of *a* will have to be equal to the *identity*. More specifically, if the order of *G* is *n*, $|G| = n$, then because *G* has only a finite number of elements, at least one of the powers in the list $a, a^2, a^3, \ldots, a^n$ must be the *identity*. In particular, if $a^m = e$, then we can rewrite this as $a^{m-1} \cdot a$, and it now follows that $a^{m-1} = a^{-1} \in H$. Thus, it follows from the *closure property* that not only is $e \in H$, but $a^{-1} \in H$ as well, and, therefore, *H* is a *subgroup* of *G*.

□

THEOREM 11

INTERSECTION OF COSETS

Theorem 11: If *H* is a *subgroup* of a *finite group G*, then any two *right* (*left*) *cosets* either coincide or have an empty intersection.

Proof: We will prove the theorem just for *right cosets* since the argument for *left cosets* is the same. Thus, let *H* is a *subgroup* of a *finite group G* and suppose that $a, b \in G$ and that *Ha* and *Hb* are *right cosets*. Recall that if *H* has *m* elements, $e = h_1, h_2, h_3, \ldots, h_m$,then the members of *Ha* are $a, h_2a, h_3a, \ldots, h_ma$ and the members of *Hb* are $b, h_2b, h_3b, \ldots, h_mb$. Also, if $Ha \cap Hb = \varnothing$, then we're done. Thus assume that the intersection is non-empty. Then that means there exist $h_ja \in Ha$ and $h_kb \in Hb$ such that $h_ja = h_kb$. But this also means that $a = h_j^{-1}h_kb$ and $b = h_k^{-1}h_ja$. Hence, every element in *Hb* can be written as a product of an element in *H* with *a*, and every element in *Ha* can be written as a product of an element in *H* with *b*. From this it follows that every element in *Hb* is also an element in *Ha*, and every element in *Ha* is also an element in *Hb*. And from this it follows that *Hb* is a *subset* of *Ha* and *Ha* is a *subset* of *Hb*, $Ha \subseteq Hb$ and $Hb \subseteq Ha$. Thus, $Ha = Hb$, and, in general, for any two *right cosets Ha* and *Hb*, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$.

□

NOTE: This proof can be extended to include *infinite groups*, but we don't want to get into the complexities of infinite sets at this point.

THEOREM 12

SIZE OF COSETS

Theorem 12: If *H* is a *subgroup* of a *finite group G*, then any two *right* (*left*) *cosets* have the same number of elements.

Proof: We will prove the theorem just for *right cosets* since the argument for *left cosets* is the same. Thus, let *H* be a *subgroup* of a *finite group G* and suppose that $a \in G$ and that *H* and *Ha* are distinct *right cosets*. Recall that if *H* has *m* elements, $e = h_1, h_2, h_3, \ldots, h_m$,then the members of *Ha* are $a, h_2 a, h_3 a, \ldots, h_m a$. It now follows from the *right cancellation law* that these are *m* distinct elements in *Ha* since otherwise, for example, if we had $h_2 a = h_3 a$, then this would incorrectly imply that $h_2 = h_3$. And since *a* was chosen to be any arbitrary element that is not in *H*, this argument shows that all *right cosets* of *H* in *G* will have the same number of elements as the *subgroup H*. Therefore, any two *right cosets* of *H* in *G* have the same number of elements.

□

NOTE: This proof can be extended to include *infinite groups*, but we don't want to get into the complexities of infinite sets at this point.

THEOREM 13

LAGRANGE'S THEOREM – PART 1

Notation: The number of elements in a *group* (or set) *G*, also called the *order of G*, is denoted by $|G|$.

Theorem 13: If *H* is a *subgroup* of a *finite group G*, then the *order of H* is a divisor of the *order of G*.

Proof: Suppose that *H* is a *subgroup* of a *finite group G*, and suppose that $|G| = n$ and $|H| = m$. If $H = G$, then clearly $m = n$ and, thus, *m* divides *n*. Hence, suppose that $H \neq G$. Then there exists $a \in G$ such that $a \notin H$, and by previous proof (Theorems 11 & 12), $|H| = |Ha|$ and $H \cap Ha = \varnothing$. Continuing in this manner, if $H \cup Ha \neq G$, then there exists $b \in G$ such that $b \notin H$ and $|H| = |Ha| = |Hb|$ and no two of these *right cosets* have any elements in common. If now $H \cup Ha \cup Hb \neq G$, then we can continue once again in this manner, but since *G* is a *finite group*, we will eventually arrive at a set of *right cosets* whose union is *G*. Furthermore, since these *cosets* all contain *m* elements and since no two *cosets* have any elements in common, then if we have exactly *k* such *right cosets* whose union is *G* then the number of elements in *G* is equal to the number of elements in *H* times the number of distinct *right cosets* of *H* in *G*. In other words, $n = mk$ and, therefore, $m = |H|$ is a divisor of $n = mk = |G|$.

□

THEOREM 14

LAGRANGE'S THEOREM – PART 2

Definition: If *H* is a *subgroup* of a *finite group G*, then the number of *right* (*left*) *cosets* of *H* in *G* is called the *index of H* in *G* and is denoted by $[G:H]$.

Theorem 14: If *H* is a *subgroup* of a *finite group G*, then the number of *right* (*left*) *cosets of H* in *G*, denoted by $[G:H]$, is equal to $\frac{|G|}{|H|}$.

Proof: By previous proof (Theorem 13), if $|G| = n$ and $|H| = m$, then $n = mk$ where *k* is the number of distinct *right* (*left*) *cosets* of *H* in *G*. Therefore,

$$[G:H] = k = \frac{mk}{m} = \frac{n}{m} = \frac{|G|}{|H|}.$$

□

THEOREM 15

SUSBET PRODUCT

Definition: If *H* is a *subgroup* or subset of a *group G*, then *HH* is the set of all products h_1h_2 such that $h_1, h_2 \in H$.

Theorem 15: If *H* is a *subgroup* of a *finite group G*, then $HH = H$.

Proof: On the one hand, if $h_1, h_2 \in H$, then we not only have $h_1h_2 \in HH$, but also $h_1h_2 \in H$ since *H* is *closed* under multiplication. Hence, *HH* is a subset of *H,* $HH \subseteq H$*.* But on the other hand, if $h \in H$, then $h = eh \in HH$ and, thus, *H* is a subset of *HH,* $H \subseteq HH$. Therefore, if $HH \subseteq H$ and $H \subseteq HH$, then it follows that $HH = H$.

□

THEOREM 16

COSETS AND EQUIVALENCE RELATIONS

Definition: If *X* is a *non-empty set*, then a *relation* between elements in *X*, denoted by $\equiv$, is called an *equivalence relation* if and only if the following conditions are met:

1. For every $a \in X$, $a \equiv a$ (*reflexive*),
2. For every $a,b \in X$, if $a \equiv b$, then $b \equiv a$ (*symmetric*), and
3. For every $a,b,c \in X$, if $a \equiv b$ and $b \equiv c$, then $a \equiv c$ (*transitive*).

Theorem 16: If *H* is a *subgroup* of a *group G*, then the *right* (*left*) *cosets* of *H* in *G* define an *equivalence relation*.

Proof: The easy way to prove this is to simply note that from previous proofs (theorems 11 & 13) that the intersection of any two distinct *right* (*left*) *cosets* is the *null set* and the union of all the *right* (*left*) *cosets* gives us back all of *G*. Hence, the *cosets* form a partition of *G* into *disjoint sets* whose union is *G*, and, therefore, *coset* membership defines an *equivalence relation*. More specifically, previous proofs have shown that any two *right* (*left*) *cosets* either have an empty intersection or they are equal to one another, and thus, it follows that (1) $Ha = Ha$, (2) if $Ha = Hb$, then $Hb = Ha$, and (3) if $Ha = Hb$ and $Hb = Hc$, then $Ha = Hc$. Hence, the *right* (*left*) *cosets* define an equivalence relation.

□

THEOREM 17

WHEN MULTIPLICATION IS WELL-DEFINED

By *well-defined multiplication* we mean that if we define multiplication of *cosets* by $Ha \cdot Hb = Hab$, then we'll get the same result even if we do this multiplication using different representatives, besides *a* and *b*, from our two *cosets*. We'll prove that this is what happens when *H* is a *normal subgroup* of *G*.

Theorem 17: If *H* is a *normal subgroup* of *G* and $Ha_1 = Ha_2$ and $Hb_1 = Hb_2$, then $Ha_1b_1 = Ha_2b_2$.

Proof: Suppose that *H* is a *normal subgroup* of *G*. Then for every $a \in G$, we have that $Ha = aH$. That means that for every product ha where $h \in H$, there exists $h_1 \in H$ such that $ah_1 = ha$. Now suppose that $Ha_1 = Ha_2$. Then $a_1, a_2 \in Ha_1 = Ha_2$, and, hence, there exists $h_2 \in H$ such that $a_1 = h_2a_2$. In a similar manner, if $b_1, b_2 \in Hb_1 = Hb_2$, then there exists $h_3 \in H$ such that $b_1 = h_3b_2$. Putting this all together, we can now conclude that $Ha_1b_1 = H(h_2a_2)(h_3b_2) = Hh_2(a_2h_3)b_2 = Hh_2(h_4a_2)b_2 = Hh_2h_4(a_2b_2) = Ha_2b_2$. What this means is that when *H* is a *normal subgroup*, we can define multiplication of *cosets* in a way that is independent of which representative we pick of that *coset*. And this is what we mean when we say that the multiplication is *well-defined*.

□

THEOREM 18

WHEN MULTIPLICATION IS NOT WELL-DEFINED

<u>Theorem 18:</u> If *H* is a *subgroup* that is not a *normal subgroup* of *G* and $Ha_1 = Ha_2$ and $Hb_1 = Hb_2$, then Ha_1b_1 is not necessarily equal to Ha_2b_2.

<u>Proof:</u> If *H* is a *subgroup* of *G*, but *H* is not *normal* in *G*, then there exists at least one $a_1 \in G$ such that $Ha_1 \neq a_1H$. In particular, that means that there are no $h_3, h_4 \in H$ such that $a_1h_4 = h_3a_1$. Now suppose that $Ha_1 = Ha_2$ and $Hb_1 = Hb_2$, and assume that $Ha_1b_1 = Ha_2b_2$. Then there exists $h_1, h_2 \in H$ such that $a_2 = h_1a_1$ and $b_2 = h_2b_1$. Hence, $Ha_1b_1 = Ha_2b_2 = H(h_1a_1)(h_2b_1) = (Hh_1)a_1h_2b_1 = Ha_1h_2b_1$. But this implies that there exists $h_3 \in H$ such that $a_1b_1 = h_3a_1h_2b_1$ which implies that $a_1 = h_3a_1h_2$. Now let $h_4 = h_2^{-1} \in H$. Then $a_1 = h_3a_1h_2 \Rightarrow a_1h_2^{-1} = h_3a_1 \Rightarrow a_1h_4 = h_3a_1$. But this contradicts our initial assumption about a_1. Therefore, if *H* is a *subgroup* that is not a *normal subgroup* of *G* and $Ha_1 = Ha_2$ and $Hb_1 = Hb_2$, then Ha_1b_1 is not necessarily equal to Ha_2b_2 and, thus, our multiplication of *cosets* is not *well-defined*.

□

THEOREM 19

QUOTIENT OR FACTOR GROUPS

Theorem 19: If *N* is a *normal subgroup* of a *group G,* then $G/N = \{Na \mid a \in G\}$ is a *group* where the multiplication of *right* (*left*) *cosets* is defined in terms of the multiplication of elements in *G*. In other words, by $Na \cdot Nb = N(ab)$.

Proof: In a previous proof (Theorem 17) we showed that this multiplication is *well-defined*. That means that we get the same result regardless of which element from a *coset* is used to represent it. Having noted that, it's obvious that the *closure property* holds. In other words, if $a,b \in G$, then the product of the two *right cosets* Na and Nb is again a *right coset* that is obtained by multiplying together the representatives from these two given *right cosets*, $Na \cdot Nb = N(ab)$. Furthermore, we get the *associative property* for free, because multiplication in *G* is *associative*. Hence, $N(ab)c = Na(bc)$. Additionally, the *identity element* in G/N is $N = Ne$. Furthermore, for any *right* coset Na, its *inverse* is Na^{-1} since $Na \cdot Na^{-1} = N(aa^{-1}) = Ne = N$. Therefore, G/N with the multiplication inherited from *G* is a *group*. This *group* is called a *quotient* or *factor group*.

□

THEOREM 20

THE CENTER IS NORMAL

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

Theorem 20: The *center* of a *group G* is a *normal subgroup* of *G*.

Proof: We'll begin by showing that $Z(G)$ is at least a *subgroup* of *G*. Thus, first note that the *center* of a *group* always exists since the *identity element* always belongs to the *center* (since it *commutes* with every other element in *G*). Second, we'll show that the *center* is a *subgroup* by showing that it is *closed* under multiplication and every that element in the *center* has an inverse in the *center*. Thus, let $a,b \in Z(G)$ and let $c \in G$. Then $(ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab)$. Hence, since *ab commutes* with an arbitrary element of *G*, *ab* is in the *center* of *G*, and, thus, $Z(G)$ is closed under multiplication. Now let $a \in Z(G)$ and let $c \in G$. Then $ac = ca \Rightarrow (ac)a^{-1} = (ca)a^{-1} \Rightarrow aca^{-1} = c(aa^{-1}) = c \Rightarrow aca^{-1} = c \Rightarrow a^{-1}(aca^{-1}) = a^{-1}c$ $\Rightarrow (a^{-1}a)ca^{-1} = a^{-1}c \Rightarrow eca^{-1} = a^{-1}c \Rightarrow ca^{-1} = a^{-1}c.$ Therefore, if *a commutes* with *c*, then a^{-1} *commutes* with *c*, and, thus, $a^{-1} \in Z(G)$ and $Z(G)$ is a *subgroup* of *G.*

To show that $Z(G)$ is a *normal subgroup*, let $a \in Z(G)$ and let $c \in G$. Then it suffices to show that $c^{-1}ac \in Z(G)$. But this is easy since, *a commutes* with every element in *G*. In other words, $c^{-1}ac = (c^{-1}a)c = (ac^{-1})c = a(c^{-1}c) = ae = a \in Z(G)$. Therefore, the *center* of a *group G* is a *normal subgroup* of *G*.

□

THEOREM 21

THE COMMUTATOR SUBGROUP IS NORMAL

Definition: The *commutator* or *derived subgroup* of a *group G*, denoted by G', is the set of all finite products of *commutators* in *G* where a *commutator* is a product of either the form $a^{-1}b^{-1}ab$ or $aba^{-1}b^{-1}$ or $bab^{-1}a^{-1}$ or $b^{-1}a^{-1}ba$ for $a,b \in G$.

Theorem 21: The *commutator* (or *derived*) subgroup of a *group G* is *normal* in *G*.

Proof: First of all, by definition the set of all finite products of *commutators* is *closed* under multiplication. Also, if $a^{-1}b^{-1}ab$ is a *commutator* in *G*, then its inverse, $(a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}(b^{-1})^{-1}(a^{-1})^{-1} = b^{-1}a^{-1}ba$ is also a *commutator* in *G*. From this it follows that any finite product of *commutators* will have an *inverse* that belongs to the set of all finite products of *commutators* in *G*. For example, if $a^{-1}b^{-1}ab \cdot c^{-1}d^{-1}cd$ is a product of *commutators* in *G*, then its inverse, $d^{-1}c^{-1}dc \cdot b^{-1}a^{-1}ba$, also belongs to *G*. Hence, the set of all finite products of *commutators* in *G* is a *subgroup* of *G*. To show that the *commutator subgroup* is a *normal subgroup* of *G*, let $a \in G'$ and let $b \in G$. It now suffices to show that $b^{-1}ab \in G'$. To do this, note that $(b^{-1}ab)a^{-1} = b^{-1}aba^{-1} = b^{-1}(a^{-1})^{-1}ba^{-1}$ is a *commutator* of *b* and a^{-1}, and, hence, it is equal to some element *c* in G'. But if $(b^{-1}ab)a^{-1} = b^{-1}aba^{-1} = c \in G'$, then $b^{-1}ab = ca$. However, since $a,c \in G'$, that means that $b^{-1}ab = ca \in G'$, and that means that the *commutator* subgroup of a *group G* is *normal* in *G*.

□

THEOREM 22

THE CONJUGATE OF A SUBGROUP

Definition: If *H* is a *subgroup* of a *group* *G* and $a \in H$, then aHa^{-1} and $a^{-1}Ha$ are *conjugates* of *H* in *G*.

Theorem 22: If *H* is a *subgroup* of a *group* *G* and $a \in G$, then $a^{-1}Ha$ (and aHa^{-1}) is a *subgroup* of *G*.

Proof: Let *G* be a *group* and let *H* be a *subgroup*, and let $a \in G$. To show that $a^{-1}Ha$ is a *subgroup* of *G*, we need to show that $a^{-1}Ha$ *is closed* under multiplication and that every element in $a^{-1}Ha$ has an *inverse*. Thus, let $x, y \in H$. Then $a^{-1}xa, a^{-1}ya \in a^{-1}Ha$. Also, since $xy \in H$, we have that $a^{-1}(xy)a \in a^{-1}Ha$. Now suppose we pick two arbitrary elements of $a^{-1}Ha$. Then we can write them as $a^{-1}xa$ and $a^{-1}ya$ since every element in $a^{-1}Ha$ is the conjugate of some element in *H*. But now we have that $a^{-1}xa \cdot a^{-1}ya = a^{-1}x \cdot e \cdot ya = a^{-1}(xy)a \in a^{-1}Ha$, and, hence, $a^{-1}Ha$ is *closed* under multiplication. Furthermore, if $a^{-1}xa \in a^{-1}Ha$, then $x^{-1} \in H$ implies that $a^{-1}x^{-1}a \in a^{-1}Ha$, too, and since $a^{-1}xa \cdot a^{-1}x^{-1}a = a^{-1}x \cdot e \cdot x^{-1}a = a^{-1}(xx^{-1})a = a^{-1} \cdot e \cdot a = a^{-1}a = e$, it follows that every element in $a^{-1}Ha$ has an inverse that belongs to $a^{-1}Ha$. Therefore, $a^{-1}Ha$ is a *subgroup* of *G*.

□

THEOREM 23

THE SUBGROUP GENERATED BY CONJUGATE SUBGROUPS

Definition: If *H* is a *subgroup* of a *group G* and $a \in H$, then aHa^{-1} and $a^{-1}Ha$ are *conjugates* of *H* in *G*.

Theorem 23: If *H* is a *subgroup* of a *group G*, then the *subgroup N* generated by elements of *H* and elements of its *conjugates* is *normal* in *G*.

Proof: Let *G* be a *group* and let *H* be a *subgroup*. If *H* is *normal* (*self-conjugate*) in *G*, then set *N* equal to *H* and we are done. On the other hand, if *G* contains several *subgroups* that are *conjugate* to *H*, then let *N* be the *subgroup* generated by taking all finite products of elements of *H* with the elements in the corresponding *conjugates* of *H*. Now let *abc* represent a typical product of such elements from either *H* or its *conjugates* and let $g \in G$, and let's consider the product $g^{-1}(abc)g$. Clearly, we could also write this as

$g^{-1}(abc)g = g^{-1}(aebec)g = g^{-1}a(gg^{-1})b(gg^{-1})cg) = (g^{-1}ag)(g^{-1}bg)(g^{-1}cg)$. From this last form we see that $g^{-1}(abc)g$ will be equal to a product of conjugates of *a, b,* and *c*, and these *conjugates* will be elements of either *H* or one of the *conjugates* of *H*. Thus, $g^{-1}(abc)g$ belongs to the *subgroup N* generated by elements of *H* and its *conjugates*. Therefore, *N* is a *normal subgroup* of *G*.

□

THEOREM 24

GROUPS WITH AN EVEN NUMBER OF ELEMENTS

Theorem 24: If a f*inite group G* has an even number of elements, then at least one *non-identity element* is its own *inverse*.

Proof: We will illustrate the argument by assuming we have a *group* of order 8. If we remove the *identity element*, then that leaves 7 *non-identity elements*. Now let's consider the consequences of each of the remaining elements having an *inverse* that is different from itself. If this were the case, then we would need an even number of elements since every *non-identity element* would be paired with a different element that is also its *inverse*. However, since in actuality we have 7 *non-identity elements* left in the *group*, it follows that at least one of the elements is its own *inverse*. And now you can, hopefully, see that this same argument can be applied to any *finite group* with an even number of elements.

□

THEOREM 25

COMMUTATORS IN NORMAL SUBGROUPS

Theorem 25: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G*, and let $m \in M$ and $n \in N$. Then the *commutator* of *m* by *n*, $m^{-1}n^{-1}mn$, is an element of $M \cap N$.

Proof: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G*, and let $m \in M$ and $n \in N$, and consider the *commutator* $m^{-1}n^{-1}mn$. Since *N* is a *normal subgroup* of *G*, it follows that $m^{-1}n^{-1}m \in N$ and, hence, $(m^{-1}n^{-1}m)n = m^{-1}n^{-1}mn \in N$. But on the other hand, since *M* is a *normal subgroup* of *G*, it also follows that $n^{-1}mn \in M$ and, hence, $m^{-1}(n^{-1}mn) = m^{-1}n^{-1}mn \in M$. Therefore, $m^{-1}n^{-1}mn \in M \cap N$.

□

THEOREM 26

COMMUTATIVITY IN NORMAL SUBGROUPS

Theorem 26: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $M \cap N = e$ (the *identity*), and let $m \in M$ and $n \in N$. Then *m* and *n commute* with one another, or in other words, $mn = nm$.

Proof: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $M \cap N = e$ (the identity), and let $m \in M$ and $n \in N$. Then by our previous proof (Theorem 25), the *commutator* $m^{-1}n^{-1}mn$ is in the intersection of *M* and *N*, But this means that $m^{-1}n^{-1}mn = M \cap N = e$. However,

$$m^{-1}n^{-1}mn = e \Rightarrow m \cdot m^{-1}n^{-1}mn = m \cdot e \Rightarrow n^{-1}mn = m \Rightarrow n \cdot n^{-1}mn = n \cdot m \Rightarrow mn = nm .$$

Therefore, *m* and *n commute* with one another.

□

THEOREM 27

PRODUCT OF NORMAL SUBGROUPS

Theorem 27: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $MN = G$ and $M \cap N = e$ (the *identity*). Then if $m_1, m_2 \in M$ and $n_1, n_2 \in N$ such that $m_1 n_1 = m_2 n_2$, it follows that $m_1 = m_2$ and $n_1 = n_2$. In other words, each element in *G* can be represented in a unique way as a product of an element in *M* with an element in *N*.

Proof: Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $MN = G$ and $M \cap N = e$ (the *identity*), and suppose that $m_1, m_2 \in M$ and $n_1, n_2 \in N$ with $m_1 n_1 = m_2 n_2$. Then

$$\begin{aligned} & m_1 n_1 = m_2 n_2 \Rightarrow m_2^{-1} \cdot m_1 n_1 = m_2^{-1} \cdot m_2 n_2 \Rightarrow m_2^{-1} m_1 n_1 = n_2 \\ & \Rightarrow m_2^{-1} m_1 n_1 \cdot n_1^{-1} = n_2 \cdot n_1^{-1} \Rightarrow m_2^{-1} m_1 = n_2 n_1^{-1} \end{aligned}.$$

But $m_2^{-1} m_1 \in M$ and $n_2 n_1^{-1} \in N$. Hence, if $m_2^{-1} m_1 = n_2 n_1^{-1}$, then $m_2^{-1} m_1, n_2 n_1^{-1} \in M \cap N$. However, since $M \cap N = e$, it follows that $m_2^{-1} m_1 = e$ and $n_2 n_1^{-1} = e$. From this it follows that $m_1 = m_2$ and $n_2 = n_1$. Therefore, each element in *G* can be represented in a unique way as a product of an element in *M* with an element in *N*.

□

THEOREM 28

ISOMORPHISM TO DIRECT PRODUCT

Theorem 28: If *M* and *N* are *normal subgroups* of *G* such that $M \cap N = e$ and $G = MN$, then *G* is *isomorphic* to the *direct product* of *M* and *N*, $G \cong M \times N$.

Proof: Recall that when we say that two *groups* are *isomorphic*, that means that the *groups* are essentially the same except for the labeling of the elements. More specifically, that means that there is a *one-to-one correspondence* between elements of the two groups such that multiplication in one group corresponds to multiplication in the other. To show that such an *isomorphism* exists in this case, we'll first recall some consequences of the last two theorems (Theorem 26 & Theorem 27) we proved. Namely, that, given that *M* and *N* are *normal subgroups* of *G* such that $M \cap N = e$ $M \cap N = e$ and $G = MN$, we are able to write each element of *G* in a unique way as a product of an element of *M* and an element of *N*, and that the elements of *M* and *N* *commute* with one another.

Now, a *one-to-one correspondence* means that each element in *G* will be paired with exactly one element in $M \times N$ and vice-versa, and we will establish our correspondence as follows. If $g \in G$, then *g* can be written in a unique way as $g = mn$ for some $m \in M$ and $n \in N$. We'll now let $g = mn$ correspond to (m,n) in the direct product $M \times N$. It should now be fairly obvious that every element of $M \times N$ corresponds to exactly one element of $G = MN$, and every element of $G = MN$ corresponds to exactly one element of $M \times N$. In other words, we have established a *one-to-one correspondence* between elements in the two *groups*.

To show that multiplication in one *group* corresponds to multiplication in the other, let's suppose that $g_1 = m_1 n_1$ and $g_2 = m_2 n_2$ where $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then since elements in *M* and *N* *commute* with one another,

$g_1 g_2 = (m_1 n_1)(m_2 n_2) = (m_1 m_2) \cdot (n_1 n_2)$. But this last product corresponds to the ordered pair $(m_1 m_2, n_1 n_2)$ in $M \times N$. Furthermore, the ordered pair $(m_1 m_2, n_1 n_2) = (m_1, n_1) \cdot (m_2, n_2)$. In other words, $g_1 = m_1 n_1$ corresponds to (m_1, n_1), $g_2 = m_2 n_2$ corresponds to (m_2, n_2), and the product $g_1 g_2$ corresponds to $(m_1, n_1) \cdot (m_2, n_2)$. Therefore, since we have a *one-to-one correspondence* between the *groups* such that multiplication in one *group* corresponds to multiplication in the other, the two *groups* are *isomorphic*, $G \cong M \times N$.

□

THEOREM 29

CORRESPONDENCE OF SUBGROUPS

Theorem 29: 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.

Proof: Let *H* be a *subgroup* of *G*, let *N* be a *normal subgroup* of *G*, and consider the *right* (*left*) *cosets* in G/N that correspond to elements of *H*. By previous proof (Theorem 17), we know that when *N* is a *normal subgroup* of *G* that multiplication in G/N defined by $Na \cdot Nb = N(ab)$ is *well-defined*, and recall that that means that it doesn't matter which elements of the *cosets* we use when performing the multiplication. Thus, to show that the *cosets* corresponding to elements in *H* form a *subgroup*, all we need to do is demonstrate *closure* under multiplication and the existence of *inverses*. But that is easy to do. For example, if $h_1, h_2 \in H$, then $Nh_1 \cdot Nh_2 = N(h_1h_2)$ is also a *right coset* involving an element of *H* since $h_1h_2 \in H$. Similarly, if $h, h^{-1} \in H$, then $Hh \cdot Hh^{-1} = H(hh^{-1}) = He = H$ implies that $Hh^{-1} = (Hh)^{-1}$. Hence, *inverses* also exist in this collection of *cosets*, and so the *cosets* in G/N that correspond to elements of *H* form a *subgroup* of G/N.

□

THEOREM 30

CORRESPONDENCE OF NORMAL SUBGROUPS

Theorem 30: If *H* is a *normal 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 *normal subgroup* of G/N.

Proof: In our previous theorem (Theorem 29) we demonstrated that the *right* (*left*) *cosets* corresponding to elements of *H* form a *subgroup* of G/N, and so all that is left is to demonstrate that this will be a *normal subgroup* of G/N if *H* is a *normal subgroup* of a *group G*. Thus, note that since *H* is *normal* in *G*, if $g \in G$ and $h \in H$, then $g^{-1}hg \in H$. Recall also from the proof of Theorem 29 that $(Ng)^{-1} = Ng^{-1}$. Consequently, if follows that $(Ng)^{-1} \cdot Nh \cdot Ng = Ng^{-1} \cdot Nh \cdot Ng = N(g^{-1}hg)$ where, again, $g^{-1}hg \in H$. Therefore, the *cosets* in G/N corresponding to elements of *H* form a *normal subgroup* of G/N.

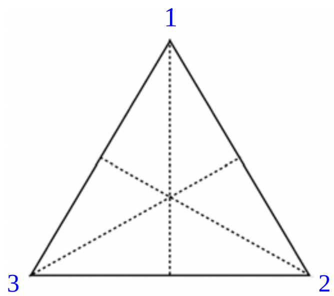
□

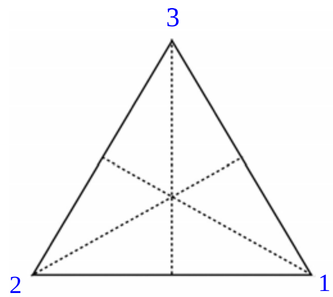
THEOREM 31

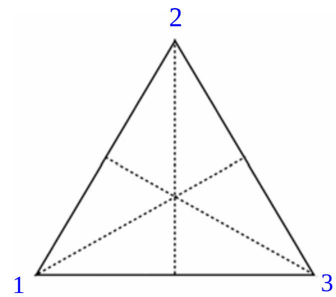
CAYLEY'S THEOREM

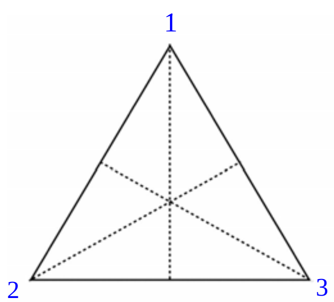
Theorem 31: Every *finite group G* is *isomorphic* to a *group* of permutations acting on a set of objects.

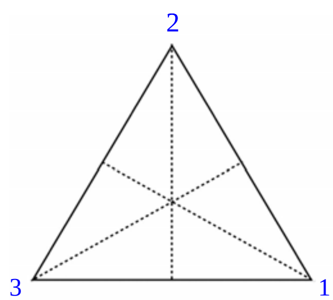
Proof: Instead of a more formal argument, we'll simply take a typical *finite group* and show how to find a *permutation group* that is *isomorphic* to it. In particular, let's look at D_3, the *group* of symmetries of an equilateral triangle.

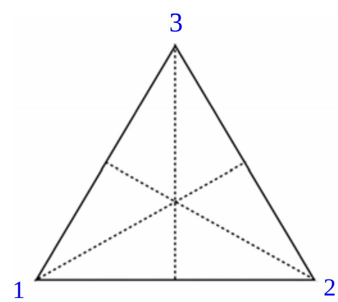












This *group* is generated by rotations about the center and flips about various axes of symmetry. Also, below is a multiplication table for D_3 expressed in terms of the possible permutations of the vertices of the equilateral triangle.

	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$

If we use letters to represent the various rotations and flips, then we can rewrite our multiplication table as follows.

$$\begin{aligned}
e &= (1)(2)(3) \\
R &= (1\ 2\ 3) \\
R^2 &= (1\ 3\ 2) \\
F &= (2\ 3) \\
FR &= (1\ 2) \\
FR^2 &= (1\ 3)
\end{aligned}$$

	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

When we look at this table, we notice that each row is a permutation of the elements in the very first row. However, this does not mean that we are going to say that *R*, for instance, is given by the following permutation:

$$R = \begin{pmatrix} e & R & R^2 & F & FR & FR^2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ R & R^2 & e & FR^2 & F & FR \end{pmatrix} = (e, R, R^2)(F, FR^2, FR)$$

No, instead we have to be a little more sophisticated so that things will work out properly with regard to multiplication. In particular, remember that we want to think of our initial elements as occupying positions. Thus, in our very top row, *e* is in the first position, *R* is in the second position, R^2 is in the third position, *F* is in the fourth position, *FR* is in the fifth position, and FR^2 is in the sixth position.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

We can now set up our permutations correctly. In the maneuver *R,* the first element, *e*, moves from position one to position three which corresponds to R^2 in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

Similarly, the element in the third position of the top row, R^2, moves to the second position which corresponds to *R* in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

And the element in the second position of the top row, *R*, moves to the first position which corresponds to *e* in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

In other words, so far, we have the permutation (e, R^2, R). Continuing, we see that the element originally in the fourth position of the top row, *F*, moves to the fifth position which corresponds to *FR* in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

The element originally in the fifth position of the top row, FR, moves to the sixth position which corresponds to FR^2 in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

And the element in the sixth position in the top row, FR^2, moves to the fourth position which corresponds to *F* in the top row.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}
	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

Thus, the complete permutation associated with *R* is $R \leftrightarrow (e, R^2, R)(F, FR, FR^2)$. Similarly, the permutation associated *F,* when we construct it by thinking of the positions that our original top row elements get moved to, is $F \leftrightarrow (e, F)(R, FR)(R^2, FR^2)$. Now from our multiplication table we can see that $R \cdot F = FR^2$, and this latter element corresponds to the permutation $RF = FR^2 \leftrightarrow (e, FR^2)(R, F)(R^2, FR)$. And finally, if we manually multiply our permutations, then we get that the permutation corresponding to *R* times the permutation corresponding to *F* gives us the permutation corresponding to $R \cdot F = FR^2$.

$$RF \leftrightarrow (e, R^2, R)(F, FR, FR^2)(e, F)(R, FR)(R^2, FR^2) = (e, FR^2)(R, F)(R^2, FR) \leftrightarrow FR^2 .$$

So what does this show us? Well, we've demonstrated how to convert each element in our *group* to a permutation that acts upon the elements of the *group*, and we've shown that a product such as $R \cdot F = FR^2$ gives us the same result when we express our *group* elements as permutations,

$$RF \leftrightarrow (e, R^2, R)(F, FR, FR^2)(e, F)(R, FR)(R^2, FR^2) = (e, FR^2)(R, F)(R^2, FR) \leftrightarrow FR^2 .$$

Therefore, this example suggests that every *finite group G* is indeed *isomorphic* to a *group* of permutations that acts upon the set *G* of *group* elements themselves. □

THEOREM 32

AN IMPORTANT BIJECTION

Theorem 32: Let *G* be a *group*, let $g \in G$, and define a function $T_g : G \to G$ by $T_g(x) = gxg^{-1}$. Then $T_g : G \to G$ is a *one-to-one* and *onto function*, or in other words, a *bijection*.

Proof: Let $T_g : G \to G$ be defined by $T_g(x) = gxg^{-1}$ for $x \in G$. To show that T_g is *one-to-one*, we just need to demonstrate that if $T_g(x) = T_g(y)$, then $x = y$. However, this follows immediately from our right and left cancellation laws in a *group*. That is,

$$T_g(x) = T_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow g^{-1}(gxg^{-1})g = g^{-1}(gyg^{-1})g \Rightarrow exe = eye \Rightarrow x = y .$$

Thus, T_g is *one-to-one*.

To show that T_g is *onto*, that means that if $b \in G$, then there exists $x \in G$ such that $T_g(x) = b$. But it is easy to find such an *x*. Just let $x = g^{-1}bg \in G$. Then $T_g(x) = T_g(g^{-1}bg) = g(g^{-1}bg)g^{-1} = ebe = b$, and T_g is onto. Therefore, since $T_g : G \to G$ defined by $T_g(x) = gxg^{-1}$ for $x \in G$ is both *one-to-one* and *onto*, it follows that $T_g : G \to G$ is a *bijection*.

□

SUMMARY (PART 9)

As we indicated at the beginning, this part has been an introduction to theorem proving which is the primary activity of a research mathematician. Thus, it's important to study the proofs that have been presented in this part and to learn to replicate them. This will help enable to eventually create more complex proofs of your own for theorems that are more complicated than the ones given here. Excelsior!

Practice (Part 9)

Prove each theorem below. For the most part, they are either theorems already presented in this section or theorems where we proved the veracity in one case, such as for *right cosets*, and we now ask you to provide a proof in another case, such as for *left cosets*. A few of the theorems below, however, may be a little more original. See first if you can construct a proof on your own, but if need be, simply copy or modify one of the proofs given in this part. If you pay attention to what you are doing, then even copying will help train you in the right direction.

<u>Theorem:</u> A group *G* has a unique *identity element*. In other words, it has only one element *e* with the property that for every $a \in G$, $e \cdot a = a = a \cdot e$.

<u>Theorem:</u> Let *G* be a *group*, and let $a \in G$. Then *a* has a unique inverse, denoted by a^{-1}.

<u>Theorem:</u> Let *G* be a group and let $a, b \in G$. If $ab = e$, then $ba = e$.

<u>Theorem:</u> Let *G* be a group and let $a, b \in G$. If $ab = e$, then $b^{-1}a^{-1} = e$ and then $a^{-1}b^{-1} = e$.

<u>Theorem :</u> Let *G* be a *group* and let *H* be a subset of *G*. If for every $a \in H$ we have that $a^{-1} \in H$ and if for every $a, b \in H$ we have that $ab \in H$, then *H* is a *subgroup* of *G*.

<u>Theorem:</u> If *H* is a *subgroup* of a *finite group G*, then any two *left cosets* either coincide or have an empty intersection.

Theorem: If H is a *subgroup* of a *finite group G*, then any two *left cosets* have the same number of elements.

Theorem: If H is a *subgroup* of a *finite group G*, then the *order of H* is a divisor of the *order of G*.

Theorem: If H is a *subgroup* of a *group G*, then the *right* (*left*) *cosets* of H in G define an *equivalence relation*.

Theorem: The *center* of a *group G* is a *normal subgroup* of G.

Theorem: If H is a *subgroup* of a *group G* and $a \in G$, then aHa^{-1} is a *subgroup* of G.

Theorem: Let G be a *group*, let M and N be *normal subgroups* of G such that $M \cap N = e$ (the *identity*), and let $m \in M$ and $n \in N$. Then m and n *commute* with one another, or in other words, $mn = nm$.

PRACTICE (PART 9) - ANSWERS

Theorem: A group *G* has a unique *identity element*. In other words, it has only one element *e* with the property that for every $a \in G$, $e \cdot a = a = a \cdot e$.

Proof: Suppose that e_1 and e_2 are both *identity elements* in *G*. Then since e_1 is an *identity element*, $e_1 \cdot (e_2) = e_2$. On the other hand, since e_2 is an *identity element*, $(e_1) \cdot e_2 = e_1$. Therefore, $e_1 = e_1 \cdot e_2 = e_2$, and the *identity element* in a group is unique.

□

Theorem: Let *G* be a *group*, and let $a \in G$. Then *a* has a unique inverse, denoted by a^{-1}.

Proof: Let *G* be a *group*, and let $a \in G$. Now suppose that $b, c \in G$ such that both *b* and *c* are inverses of *a*. Then $ab = e$, the *identity*, and $ac = e$. Hence, $ab = ac$. But by our Left Cancellation Theorem, this implies that $b = c$. Therefore, in a *group* an element *a* has only one, unique inverse, denoted by a^{-1}.

$\square$

Theorem: Let G be a group and let $a, b \in G$. If $ab = e$, then $ba = e$.

Proof: If $ab = e$, then $b = a^{-1}$, and it now immediately follows that $ba = a^{-1}a = e$.

$\square$

Theorem: Let *G* be a *group* and let $a, b \in G$. If $ab = e$, then $b^{-1}a^{-1} = e$ and then $a^{-1}b^{-1} = e$.

Proof: If $ab = e$, then $(ab)^{-1} = e^{-1} = e$. But $(ab)^{-1} = b^{-1}a^{-1}$, and hence, $b^{-1}a^{-1} = e$, and that proves the first part of this theorem. To prove the second part, we just invoke the previous theorem to conclude that if $b^{-1}a^{-1} = e$, then $a^{-1}b^{-1} = e$.

□

Theorem : Let *G* be a *group* and let *H* be a subset of *G*. If for every $a \in H$ we have that $a^{-1} \in H$ and if for every $a, b \in H$ we have that $ab \in H$, then *H* is a *subgroup* of *G*.

Proof: Let *G* be a *group* and let *H* be a subset of *G*, and assume that for every $a \in H$ we have that $a^{-1} \in H$ and for every $a, b \in H$ we have that $ab \in H$. To show that *H* is a *subgroup* of *G*, we need to show four things – *closure* under the group multiplication, the *associative law*, the *existence of an identity*, and the *existence of inverses*. We are assuming in our hypothesis that the *closure* and *inverse properties* are satisfied, and we get the *associative property* for free since it holds for all elements in the group *G*. Thus, we just need to establish the *existence of an identity element*. But this is easy because if $a \in H$, then $a^{-1} \in H$, and since we are assuming *closure* under multiplication in *H*, we have that $aa^{-1} = e \in H$. Therefore, *H* is a *subgroup* of *G*.

□

Theorem: If *H* is a *subgroup* of a *finite group G*, then any two *left cosets* either coincide or have an empty intersection.

Proof: Let *H* is a *subgroup* of a *finite group G* and suppose that $a, b \in G$ and that *aH* and *bH* are *left cosets*. Recall that if *H* has *m* elements, $e = h_1, h_2, h_3, \ldots, h_m$,then the members of *aH* are $a, ah_2, ah_3, \ldots, ah_m$ and the members of *Hb* are $b, bh_2, bh_3, \ldots, bh_m$. If $aH \cap bH = \varnothing$, then we're done. Thus assume that the intersection is non-empty. Then that means there exist $ah_j \in aH$ and $bh_k \in bH$ such that $ah_j = bh_k$. But this means that $a = bh_k h_j^{-1}$ and $b = ah_j h_k^{-1}$. Hence, every element in *bH* can be written as a product of *a* with an element in *H* , and every element in *aH* can be written as a product of *b* with an element in *H*. From this it follows that every element in *bH* is also an element in *aH*, and every element in *aH* is also an element in *bH*. Thus, $aH = bH$, and, in general, for any two *left cosets aH* and *bH*, either $aH \cap bH = \varnothing$ or $aH = bH$.

□

Theorem: If *H* is a *subgroup* of a *finite group G*, then any two *left cosets* have the same number of elements.

Proof: Let *H* be a *subgroup* of a *finite group G* and suppose that $a \in G$ and that *H* and *aH* are distinct *left cosets*. Recall that if *H* has *m* elements, $e = h_1, h_2, h_3, \ldots, h_m$,then the members of *aH* are $a, ah_2, ah_3, \ldots, ah_m$. It now follows from the *left cancellation law* that these are *m* distinct elements in *aH* since otherwise if, for example, we had $ah_2 = ah_3$, then this would incorrectly imply that $h_2 = h_3$. And since *a* was chosen to be any arbitrary element that is not in *H*, this argument shows that all *left cosets* of *H* in *G* will have the same number of elements as the *subgroup H*. Therefore, any two *left cosets* of *H* in *G* have the same number of elements.

□

Theorem: If *H* is a *subgroup* of a *finite group G*, then the *order of H* is a divisor of the *order of G*.

Proof: Suppose that *H* is a *subgroup* of a *finite group G*, and suppose that $|G| = n$ and $|H| = m$. If $H = G$, then clearly $m = n$ and, thus, *m* divides *n*. Hence, suppose that $H \neq G$. Then there exists $a \in G$ such that $a \notin H$, and by previous proof, $|H| = |Ha|$ and $H \cap Ha = \varnothing$. Continuing in this manner, if $H \cup Ha \neq G$, then there exists $b \in G$ such that $b \notin H$ and $|H| = |Ha| = |Hb|$ and no two of these *right cosets* have any elements in common. If now $H \cup Ha \cup Hb \neq G$, then we can continue once again in this manner, but since *G* is a *finite group*, we will eventually arrive at a set of *right cosets* whose union is *G*. Furthermore, since these *cosets* all contain *m* elements and since no two *cosets* have any elements in common, then if we have exactly *k* such right cosets whose union is *G* then the number of elements in *G* is equal to the number of elements in *H* times the number of distinct *right cosets* of *H* in *G*. In other words, $n = mk$ and, therefore, $m = |H|$ is a divisor of $n = mk = |G|$.

□

Theorem: If *H* is a *subgroup* of a *group G*, then the *right* (*left*) *cosets* of *H* in *G* define an *equivalence relation*.

Proof: The easy way to prove this is to simply note that from previous proofs that the intersection of any two distinct *right* (*left*) *cosets* is the null set and the union of all the *right* (*left*) *cosets* gives us back all of *G*. Hence, the *cosets* form a partition of *G* into disjoint sets whose union is *G*, and, therefore, *coset* membership defines an *equivalence relation*. More specifically, previous proofs have shown that any two *right* (*left*) *cosets* either have an empty intersection or they are equal to one another, and thus, it follows that (1) $Ha = Ha$, (2) if $Ha = Hb$, then $Hb = Ha$, and (3) if $Ha = Hb$ and $Hb = Hc$, then $Ha = Hc$. Hence, the *right* (*left*) *cosets* define an equivalence relation.

□

Theorem: The *center* of a *group G* is a *normal subgroup* of *G*.

Proof: We'll begin by showing that $Z(G)$ is at least a *subgroup* of *G*. Thus, first note that the *center* of a *group* always exists since the *identity element* always belongs to the *center* (since it *commutes* with every other element in *G*). Second, we'll show that the *center* is a *subgroup* by showing that it is *closed* under multiplication and every that element in the *center* has an inverse in the *center*. Thus, let $a,b \in Z(G)$ and let $c \in G$. Then $(ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab)$. Hence, since *ab commutes* with an arbitrary element of *G*, *ab* is in the *center* of *G*, and, thus, $Z(G)$ is closed under multiplication. Now let $a \in Z(G)$ and let $c \in G$.

Then $$\begin{aligned} &ac = ca \Rightarrow (ac)a^{-1} = (ca)a^{-1} \Rightarrow aca^{-1} = c(aa^{-1}) \Rightarrow aca^{-1} = c \Rightarrow a^{-1}(aca^{-1}) = a^{-1}c \\ &\Rightarrow (a^{-1}a)ca^{-1} = a^{-1}c \Rightarrow eca^{-1} = a^{-1}c \Rightarrow ca^{-1} = a^{-1}c. \end{aligned}$$

Therefore, if *a commutes* with *c*, then a^{-1} *commutes* with *c*, and, thus, $a^{-1} \in Z(G)$ and $Z(G)$ is a *subgroup* of *G.*

To show that $Z(G)$ is a *normal subgroup*, let $a \in Z(G)$ and let $c \in G$. Then it suffices to show that $c^{-1}ac \in Z(G)$. But this is easy since, *a commutes* with every element in *G*. In other words, $c^{-1}ac = (c^{-1}a)c = (ac^{-1})c = a(c^{-1}c) = ae = a \in Z(G)$. Therefore, the *center* of a *group G* is a *normal subgroup* of *G*.

□

Theorem: If *H* is a *subgroup* of a *group G* and $a \in G$, then aHa^{-1} is a *subgroup* of *G*.

Proof: Let *G* be a *group* and let *H* be a *subgroup*, and let $a \in G$. To show that aHa^{-1} is a *subgroup* of *G*, we need to show that aHa^{-1} *is closed* under multiplication and that every element in aHa^{-1} has an *inverse*. Thus, let $x, y \in H$. Then $axa^{-1}, aya^{-1} \in aHa^{-1}$. Also, since $xy \in H$, we have that $a(xy)a^{-1} \in aHa^{-1}$. Now suppose we pick two arbitrary elements of aHa^{-1}. Then we can write them as axa^{-1} and aya^{-1} since every element in aHa^{-1} is the conjugate of some element in *H*. But now we have that $axa^{-1} \cdot aya^{-1} = ax \cdot e \cdot ya^{-1} = a(xy)a^{-1} \in aHa^{-1}$, and, hence, aHa^{-1} is *closed* under multiplication. Furthermore, if $axa^{-1} \in aHa^{-1}$, then $ax^{-1}a^{-1} \in aHa^{-1}$, too, and since $axa^{-1} \cdot ax^{-1}a^{-1} = ax \cdot e \cdot x^{-1}a^{-1} = a(xx^{-1})a^{-1} = a \cdot e \cdot a^{-1} = aa^{-1} = e$, it follows that every element in aHa^{-1} has an inverse that belongs to aHa^{-1}. Therefore, aHa^{-1} is a *subgroup* of *G*.

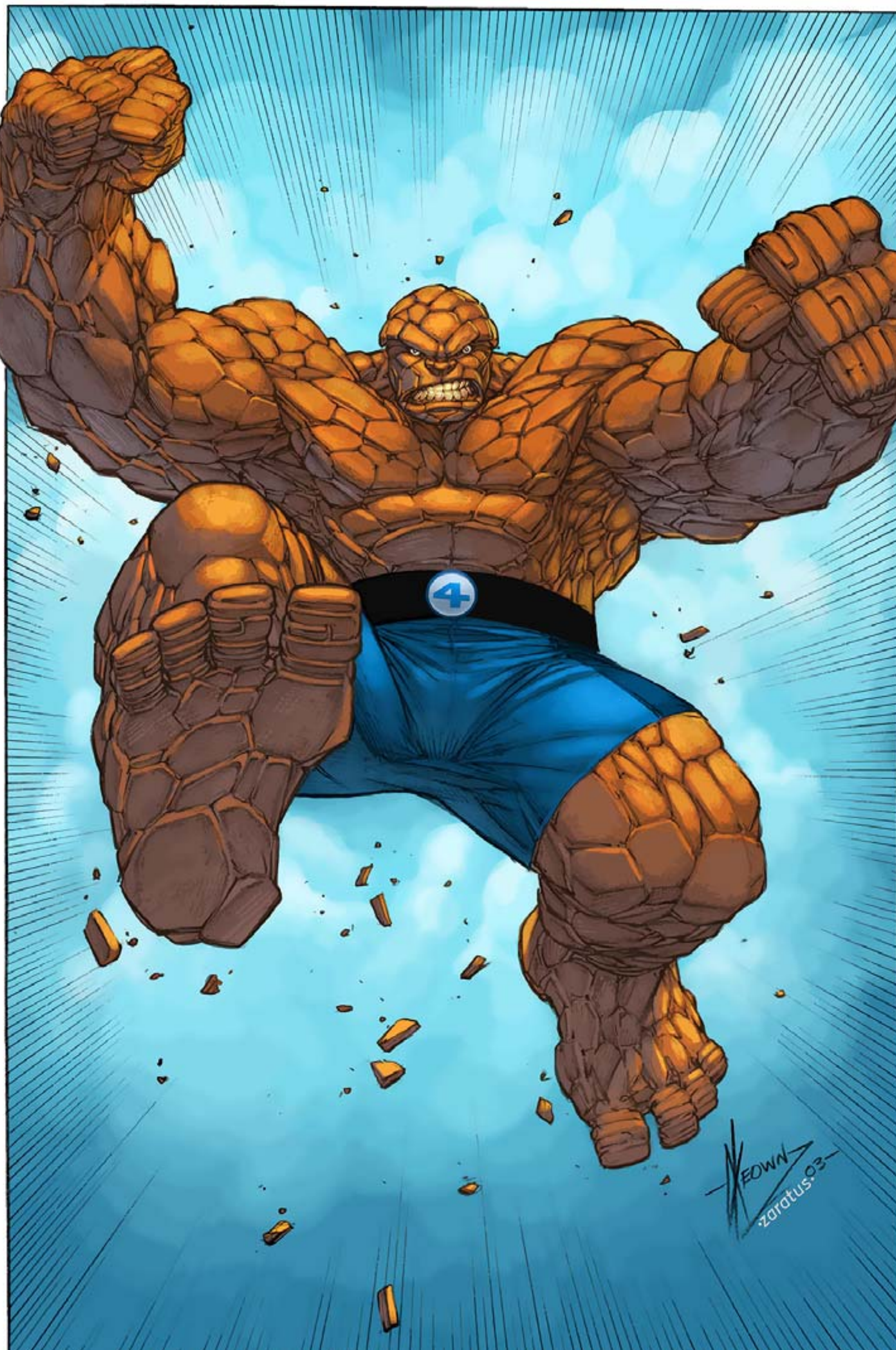
□

<u>Theorem:</u> Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $M \bigcap N = e$ (the *identity*), and let $m \in M$ and $n \in N$. Then *m* and *n commute* with one another, or in other words, $mn = nm$.

<u>Proof:</u> Let *G* be a *group*, let *M* and *N* be *normal subgroups* of *G* such that $M \bigcap N = e$ (the identity), and let $m \in M$ and $n \in N$. Then by our previous proof, the *commutator* $m^{-1}n^{-1}mn$ is in the intersection of *M* and *N*, But this means that $m^{-1}n^{-1}mn = M \bigcap N = e$. However, $m^{-1}n^{-1}mn = e \Rightarrow n^{-1}mn = m \Rightarrow mn = nm$. Therefore, *m* and *n commute* with one another.

□

IT'S GROUP THEORY TIME!



IT'S GROUP THEORY TIME!