INTRODUCTORY GROUP THEORY AND FERMAT'S LITTLE THEOREM

JENNY MOMKUS

Abstract. In this paper, we will prove a theorem from elementary number theory called Fermat's Little Theorem. The theorem was first proposed by Fermat in 1640, but a proof was not officially published until 1736. Fermat's Little Theorem is useful in the study of the integers and their properties, which is an area of mathematics known as number theory. There are several different types of proofs to Fermat's Little Theorem, but group theory provides a very elegant one. Group theory involves the study of algebraic structures known as groups and it is a central part of abstract algebra. Group theory has applications in many fields of mathematics and we will first go through some basics of group theory so we have the tools necessary for the proof of Fermat's Little Theorem.

Contents

1. Basic Definitions 1
2. Cosets 2
3. Lagrange's Theorem 4
4. Subgroups of the Integers 4
5. Bezout's Lemma 4
6. Fermat's Little Theorem 5
7. Acknowledgements 7

1. Basic Definitions

Definition 1.1. A group is a set G with a binary operation $* : G \times G \to G$ such that:

(1) G is closed under the binary operation $*$, which means for all $a, b \in G$,

$$a * b \in G.$$

(2) The operation $*$ is associative, so for all $a, b, c \in G$,

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

(3) There exists an identity e contained in G such that

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

(4) There are inverses for all elements in G, thus for all $a \in G$, there exists $a^{-1} \in G$ such that

$$a * a^{-1} = e.$$

Date: DEADLINE AUGUST 26, 2011.

Definition 1.2. A group is called an abelian group if it also satisfies commutativity in addition to the axioms above.

(5) The operation $*$ is commutative, meaning for all $a, b \in G$,

$$a * b = b * a.$$

An example of an abelian group is the integers with the operation of addition, $(\mathbb{Z}, +)$. We generally use multiplicative notation when talking about general groups and additive notation when talking about abelian groups. In this paper, we will assume all groups are abelian, so we will use $+$ as the binary operation.

Definition 1.3. A subgroup H is a nonempty subset of a group G which is a group under the restricted operation. We denote a subgroup by $H \leq G$.

Proposition 1.4. *Let G be a group. A nonempty subset $H \subseteq G$ is a subgroup if and only if for all $a, b \in H$, $a - b \in H$.*

Proof. Let $a \in H$. If $a - b \in H$ for all $a, b \in H$, then

$$a - a = 0 \in H$$

thus satisfying axiom (3) of the criteria for a group. Observe that

$$0 - a = -a \in H$$

hence axiom (4) is satisfied. For $a, b \in H$ we have

$$a - (-b) = a + b \in H$$

which demonstrates that axiom (1) also holds. Note that H inherits associativity from G.

Therefore, by showing that $a - b \in H$ for all $a, b \in H$, we verify that $H \leq G$. □

An example of a subgroup of $(\mathbb{Z}, +)$ is the even numbers, $2\mathbb{Z}$. In fact, all sets of the form $n\mathbb{Z}$ are subgroups. We will show later that these are the only possible subgroups of $(\mathbb{Z}, +)$.

2. Cosets

Given a group G and a subgroup $H \leq G$, we define an equivalence relation $\sim_H$ on G by $g \sim_H g'$ if $g - g' \in H$.

Definition 2.1. The cosets of H in G are given by

$$g + H = \{f \in G \mid g \sim_H f\}$$

Proposition 2.2. *An equivalent definition for the coset is*

$$g + H = \{f \in G \mid f = g + h, h \in H\}$$

.

Proof. If we take the first definition, we know that $g - f \in H$ from the definition of the equivalence relation. This implies that the inverse $f - g \in H$ as well. Hence, there exists an $h \in H$ such that $f - g = h$, which means $f = g + h$ and as a result $f \in g + H$. □

Definition 2.3. The order of an element g, denoted $ord(g)$, in a group G is the smallest positive integer n such that $g + g + ... + g$ added n times is equal to 0 (that is, $n \cdot g = 0$) if such an n exists. Otherwise, if there is no such n then we say the order of g is infinite.

Definition 2.4. The order of a group or subgroup, denoted $|G|$, is the number of elements contained in it (its cardinality).

Proposition 2.5. *Fix a subgroup $H \leq G$. Then H itself is a coset and all the cosets of H are the same size, so it follows that $|H| = |g + H|$ for every $g \in G$.*

Proof. Let $g \in G$. Let us define a function $\phi_g : H \to g + H$ by

$$\phi_g(h) = g + h.$$

We will show that this map is bijective, and therefore each set has the same number of elements.

Given some $f \in g + H$, we know by the definition of the coset that there exists some h such that $f = g + h = \phi_g(h)$. Hence, if $f \in g + H$ then there exists some $h \in H$ such that $\phi_g(h) = f$ and the function ϕ_g is surjective.

Now let us take $h_1, h_2 \in H$. If $\phi_g(h_1) = \phi_g(h_2)$ then $g + h_1 = g + h_2$ and when we add $-g$ to both sides we get $h_1 = h_2$. As a result, the function is also injective. Since the defined function is both surjective and injective, it must be bijective and $|H|=|g + H|$ for every $g \in G$.

Furthermore, since G is a group, it must contain the identity 0, therefore H itself must be a coset because we can have $0 + H = H$. □

Definition 2.6. Fix a subgroup $H \leq G$. It is especially important to be sure that G is an abelian group. We define the quotient group G/H to be $\{g + H | g \in G\}$. The binary operation is addition of the cosets. Addition is defined by

$$(g_1 + H) + (g_2 + H) = g_1 + g_2 + H$$

Proposition 2.7. *This addition of the cosets is well defined.*

Proof. Let $g_1 + H = g_1' + H$ and $g_2 + H = g_2' + H$. It follows that $g_1' \in g_1 + H$ and $g_2' \in g_2 + H$. This implies that there exists $h_1, h_2 \in H$ such that $g_1' = g_1 + h_1$ and $g_2' = g_2 + h_2$. Thus, we have that two elements lie in the same coset if and only if their difference lies in H. We need to show that if $g_1 - g_1', g_2 - g_2' \in H$ then $(g_1 + g_2) - (g_1' + g_2') \in H$. Note that since the groups are commutative, $(g_1+g_2)-(g_1'-g_2') = (g_1-g_1')+(g_2-g_2')$. We already have that both $g_1-g_1', g_2-g_2' \in H$, so their sum must lie in H by the definition of a subgroup. □

Proposition 2.8. *The set of all cosets of H in G form a partition of G.*

Proof. In order for the cosets to form a partition of G, they must satisfy two conditions:

(1)Let us take the union of all cosets. We need to show that the union of all cosets is equal to G. If $g \in G$, then $g \in g + H$, so every g is in some coset and $G = \cup_i g_i + H$.

(2) If we take some $g_1, g_2 \in G$, then we need to show that either $g_1 + H = g_2 + H$ or $g_1 + H \cap g_2 + H = \emptyset$ (in other words, the cosets of H are disjoint). Let us assume that two cosets are not disjoint, so $g_1 + H \cap g_2 + H \neq \emptyset$. Since the intersection is nonempty, there must exist some $f \in G$ such that $f \in g_1 + H$ and $f \in g_2 + H$. By the definition of the cosets, we also know that there exists some $h_1, h_2 \in H$ such that $g_1 + h_1 = f = g_2 + h_2$.

Thus, for all $h \in H$, $g_1 + h = g_2 + (h_2 - h_1 + h)$. Since $h_2 - h_1 + h \in H$, we have that $g_1 + h \in g_2 + H$ and $g_1 + H \subseteq g_2 + H$. We can repeat this same procedure to show that $g_2 + H \subseteq g_1 + H$. Therefore, $g_1 + H = g_2 + H$ and the set of all cosets in H of G form a partition of G. □

Now that we have defined cosets and demonstrated some of their properties, we can go on to one of the most important theorems involved with groups.

3. Lagrange's Theorem

Lagrange's theorem is essential to understanding groups and many other mathematical concepts. Lagrange's theorem connects finite group theory to arithmetic, so it is very useful in connecting group theory and number theory. It involves the relationship between groups and subgroups.

Theorem 3.1. *(Lagrange) For any finite group G, the order of every subgroup H of G divides the order of G.*

Proof. Let G be a group and H some subgroup with $g + H$ representing a coset of H in G. We know from Proposition 2.8 that the cosets $g + H$ partition G and each coset must have the same order as H. Let n be the number of cosets of H in G, and q be the order of H. Since G is the disjoint union of its cosets and each coset has q elements, there are qn elements in G, so q divides the order of G. □

4. Subgroups of the Integers

Since we are studying the integers and the group $(\mathbb{Z}, +)$, it is important to understand the subgroups of $(\mathbb{Z}, +)$

Proposition 4.1. *A subset of $(\mathbb{Z}, +)$ is a subgroup if and only if the subset is of the form $n\mathbb{Z}$ for some positive integer n.*

Proof. Take a subset $H \subseteq \mathbb{Z}$ that is of the form $n\mathbb{Z}$. We will show that this is a subgroup of $(\mathbb{Z}, +)$. Let $a, b \in H$. From Proposition 1.3, we can show that H is a subgroup if $a - b \in n\mathbb{Z}$.. Since $a, b \in n\mathbb{Z}$, they can also be written as $a = n \cdot a'$ and $b = n \cdot b'$ with $a', b' \in \mathbb{Z}$. Therefore, $a - b = n \cdot a' - n \cdot b' = n \cdot (a' - b') \in n\mathbb{Z}$. Hence, all subsets of the form $n\mathbb{Z}$ are subgroups of the group $(\mathbb{Z}, +)$.

Now take a subgroup $H \leq (\mathbb{Z}, +)$. We need to show that $H = n\mathbb{Z}$. If $H = \{0\}$ then we have that $H = 0\mathbb{Z}$. Otherwise, we will take only the positive elements of H that are contained in $\mathbb{N}$. Let $H_+ = \{h \in H \mid h > 0\}$. Observe that H_+ is nonempty because H is nonempty and contains nonzero elements. Since $\mathbb{N}$ is well ordered, this means that there exists a unique least element that is contained in H_+. Let n be the least element in H_+.

Note that $H \leq (\mathbb{Z}, +)$, so it follows that H is closed under addition, hence

$$\{nx | x \in \mathbb{Z}\} \subseteq H.$$

Therefore, $n\mathbb{Z} \leq H$. Now we need to show that $H \leq n\mathbb{Z}$.

Suppose there exists a $g \in H$ such that $g \notin n\mathbb{Z}$. By the division algorithm, there exists $nq + r = g$ such that $0 < r < n$. Since H is a subgroup and $g, nq \in H$, then $g - nq = r \in H$.

This is a contradiction because $0 < r < n$ and we already assumed that n is the least element in H_+. Therefore, $H \leq n\mathbb{Z}$ and it follows that $H = n\mathbb{Z}$, which concludes the proof. □

We can now use the information we have about subgroups of $(\mathbb{Z}, +)$ to help us prove Bezout's Lemma.

5. Bezout's Lemma

Bezout's Lemma is an important concept needed for the proof of Fermat's Little Theorem and involves both number theory and group theory.

Lemma 5.1. *(Bezout) Let a, b be integers such that at least one is nonzero. Then there exist two integers x and y such that $gcd(a, b) = ax + by$.*

Proof. Let the set of linear combinations of integers a and b be called L. It must be a subset of the group $(\mathbb{Z}, +)$. We will show that L is also a subgroup of $(\mathbb{Z}, +)$.

Let $x, y, w, z \in \mathbb{Z}$. Let us take two elements $(xa + yb), (wa + zb) \in L$.

$$\begin{aligned}\text{Observe that } (xa + yb) - (wa + zb) &= xa - wa + yb - zb \\ &= (x - w)a + (y - z)b).\end{aligned}$$

We already know that $(\mathbb{Z}, +)$ is group, hence, for all $x, y, w, z \in \mathbb{Z}$, we have $(x - w), (y - z) \in \mathbb{Z}$. Therefore, $(x - w)a + (y - z)b \in L$, so by Proposition 1.3, L is a subgroup of $(\mathbb{Z}, +)$.

Since L is a subgroup of $(\mathbb{Z}, +)$, we know from Conjecture 4.1 that L must be of the form $n\mathbb{Z}$, in other words, for all $x, y \in \mathbb{Z}$

$$xa + yb \in n\mathbb{Z}.$$

Hence, $n \in L$ and there exists $z \in \mathbb{Z}$ such that $xa+yb = nz$. Since this must hold for all $x, y \in \mathbb{Z}$, we can let $x = 0$ and $y = 1$ to show that there exists $z_1 \in \mathbb{Z}$ such that $0 \cdot a+1 \cdot b = b = nz_1$ and it follows that $n \mid b$. We can repeat the same procedure with $x = 1$ and $y = 0$ to show that there exists z_2 such that $1 \cdot a + 0 \cdot b = a = nz_2$ which means $n \mid a$. Now that $n \mid a$ and $n \mid b$, we know that

$$n \mid gcd(a, b).$$

By the definition of greatest common divisor, $gcd(a, b)$ divides both a and b. Since $n \in L$, it can be written as an integer combination of a and b, thus $gcd(a, b)$ must divide n. It follows that $n = gcd(a, b)$. □

6. Fermat's Little Theorem

Now that we have proven Lagrange's Theorem and Bezout's Lemma, we have the tools necessary to prove Fermat's Little Theorem using group theory.

Theorem 6.1. *(Fermat) Given an integer a and prime number p, the number $a^p - a$ is divisible by p, that is,*

$$a^p \equiv a \mod p.$$

Proof. Take the set $G = \{\mathbb{Z}/p\mathbb{Z}\} - \{0\} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$. Let us take this set modulo p over the binary operation of multiplication. We will show that G is a group. We define multiplication such that

$$(a \mod p) \cdot (b \mod p) \equiv ab \mod p.$$

Observe that both associativity and commutativity are inherited from $\mathbb{Z}$. We can check to see if G is closed by verifying that the product of any elements in G are not equivalent to $0 \mod p$ (meaning that no divisors of p are in G). We know that p is prime, hence its only divisors are 1 and p itself. Therefore, there is no way that the product of any two elements to be equal to $0 \mod p$.

We can use Bezout's Lemma to show that the elements of G are in fact invertible. If we take $g \in G$ and the prime number p, they must be relatively prime since at least one of the numbers is prime. This implies that $gcd(g, p) = 1$. By Bezout's Lemma there exists integers x, y such that

$$gx + py = gcd(g, p) = 1$$

When we put this in terms of modular arithmetic,

$$gx \equiv 1 \mod p.$$

As a result, x must be an inverse g and the set G satisfies axiom (4) of a group. Thus, G satisfies all the conditions that make it a group. Observe that $|G| = p - 1$.

Let $a \in G$, and let $k = ord(a)$. We can generate a subgroup $H \leq G$ from the integer a such that $H = \{a, a^2, a^3, \ldots, a^k\}$. It follows from the definition of the order of an element that

$$a^k \equiv 1 \mod p$$

so H contains the identity. Let $n, m \in \mathbb{N}$ such that $n, m \leq k$. We find the inverse of an element a^n is contained in H because

$$a^n \cdot a^{k-n} = a^k \equiv 1 \mod p.$$

Note that $a^{k-n} \in H$ because $n \leq k$. The product of two elements $a^n, a^m \in H$ is given by

$$a^n \cdot a^m = a^{n+m}$$

and we know that $a^{n+m} \in H$ because even if $n + m > k$, there exists $u, r \in \mathbb{N}$ such that $r < k$ and $n + m = uk + r$. Thus,

$$\begin{aligned} a^{n+m} &= a^{uk+r} \\ &= a^{uk} \cdot a^r \\ &= (a^k)^u \cdot a^r \\ &\equiv 1^u \cdot a^r \mod p \\ &\equiv a^r \mod p. \end{aligned}$$

Therefore, H satisfies all the requirements that make H a subgroup of G. Notice that $|H| = k$.

By Lagrange's Theorem, we know that $|H|$ divides $|G|$, so it follows that k divides $(p - 1)$. In other words, there exists $n \in \mathbb{Z}$ such that

$$p - 1 = k \cdot n.$$

Now we can look at a^{p-1} in terms of k.

$$\begin{aligned} a^{p-1} &= a^{kn} \\ &= (a^k)^n \\ &\equiv 1^n \mod p \\ &\equiv 1 \mod p \end{aligned}$$

And we have $a^{p-1} \equiv 1 \mod p$. When we multiply each side by a, we get

$$a^p \equiv a \mod p$$

which concludes the proof. □

7. Acknowledgements

I would like to thank my undergraduate mentor Paige North for teaching me about group theory and for helping with the production of this paper. I would also like to thank Daniel Schaeppi for all his help in the production of this paper.