A Short Introduction to Groups and Rings

Joshua W. Mercer

April 7, 2001

Abstract

The purpose of this paper is to prove three theorems, Euler's, Fermat's, and Wilson's, by using introductory concepts in groups and rings.

1 Introduction

This paper is intended to introduce the first step towards familiarity when using groups and rings. It will give first some basic definitions and then some properties of these. The goal of the paper is to prove Euler's theorem, Fermat's theorem (also known as Fermat's Little Theorem), and Wilson's theorem.

However, the main tool in accomplishing this is using the result of Lagrange's theorem.

2 Groups

Definition 1. *A nonempty set A with binary operation $\cdot$ is a group (denoted by $A\{\cdot\}$)* $\Leftrightarrow$

i.) $\forall a, b \in A, a \cdot b \in A$

ii.) $\forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot d)$

iii.) $\forall a \in A, \exists \ell : a \cdot \ell = \ell \cdot a = a$

iv.) $\forall a \in A, \exists a^{-1} : a \cdot a^{-1} = \ell$

Now, it is important at this point to make a clarification on the binary operation. While we denote it by $\{\cdot\}$, this does not necessarily imply that the operation is multiplication. You could just as easily replace this $\cdot$ with $+, \triangle$, or even put in a dodecahedron or a pink and purple polka-dotted elephant. In other words, we can say nothing apriori about this binary operation. As long as this operation satisfies the above requirements, then the set will be a group. Furthermore, these arbitrary operations may have other properties, and so we can define the operations we choose to use. This being said, throughout the rest of this paper $\cdot$ will denote multiplication and $+$ will denote addition since the focus shall be restrained to integers. Just keep in mind that these things might just as well be a battery re-charger or a sad song.

Notice also how the definition of the group does not include commutivity. So for some arbitrary operation, we do not necessarily get $a \triangle b = b \triangle a$. Groups that do satisfy this are given a special definition.

Definition 2. *A group $A\{\cdot\}$ will be called a commutative group or abelian group $\Leftrightarrow a \cdot b = b \cdot a \ \forall a, b \in A$.*

It is very important to remember that when proving properties for groups in general, one not assume commutivity. Since, however, we will deal only with abelian groups in this paper, we will not need to be concerned about this.

Now we should spend a little time on a few properties of groups.

Proposition 1. *The identity element ℓ of a group $A\{\cdot\} : a \cdot \ell = a$ is unique.*

Proof. Suppose not. Then $a \cdot \ell_1 = a$ and $a \cdot \ell_2 = a \Rightarrow a \cdot \ell_1 = a \cdot \ell_2 \Rightarrow \ell_1 = \ell_2$ Therefore ℓ is unique, and shall hitherto be denoted by the symbol 1. □

Proposition 2. *Let $A\{\cdot\}$ be a group. Each element a's inverse a^{-1} is unique.*

Proof. Suppose not. Then $a \cdot a_1^{-1} = 1$ and $a \cdot a_2^{-1} = 1 \Rightarrow a \cdot a_1^{-1} = a \cdot a_2^{-1} \Rightarrow a_1^{-1} = a_2^{-1}$ Therefore, each element's inverse is unique. □

The next property holds for all groups, but will be proven only for abelian groups here. Otherwise the proof following would differ slightly.

Proposition 3. *Let $A\{\cdot\}$ be an abelian group. Then, $(a^{-1})^{-1} = a \ \forall a \in A$.*

Proof. Since each element has a unique inverse, let $b = a^{-1} \Rightarrow b^{-1} = (a^{-1})^{-1}$, but $b \cdot b^{-1} = 1 \Rightarrow a^{-1} \cdot (a^{-1})^{-1} = 1$ and since each element has a unique inverse and we know $a^{-1} \cdot a = 1$, then $(a^{-1})^{-1} = a$. □

Definition 3. *If a group A has finitely many elements, say n, then we say it is a finite group of order n, denoted by $o(A) = n$ Otherwise, it has infinitely many elements and we say it an infinite group.*

We will further denote $a^m = a \cdot a \cdot a \cdot ... \cdot a$ (m times) and trivially following will be that $a^m \cdot a^k = a^{m+k}$. This should provide us with the basics to move on towards our goal.

The next interesting area of groups that we will deal with are subgroups.

Definition 4. *A group $B\{\cdot\}$ is a subgroup of $A\{\cdot\}$ if $B \subset A$ is nonempty and they have the same binary operation that satisfies the condition for the definition of a group.*

¿From this definition, it is clear that every group will be a subgroup of itself. Also, the set of the identity element, in our case $\{1\}$, will be a subgroup of *every* group.

The next thing we must define will be called cosets.

Definition 5. *Let $B\{\cdot\}$ be a subset of $A\{\cdot\}$. Then if $a \in A$, then $aB = \{a \cdot b \mid b \in B\}$ is called a left coset of B in A determined by a.*

Now, there is analogously such a thing as a right coset, but in this is equivalent to a left coset of the same term when considered for an abelian group.

It is appropriate at this point to use some examples using the set that we will be working in to prove our three theorems.

First, we will show that the set $\mathbb{Z}$ is a group. This is clear as $+$ respects the properties of the binary operation for groups; that is, closure, associativity, an identity element, and an inverse for each element. Furthermore, this group respects commutivity, and hence, is abelian.

In order to proceed further now, we must deal with congruences.

3 Congruences

Definition 6. *Let $B\{\cdot\}$ be a subgroup of $A\{\cdot\}$ and $a, b \in A$. Then $a = b(modB)$, or, a is congruent to b modulo B if $b^{-1} \cdot a \in B$.*

Let us give an example of this. Let $a, b \in \mathbb{Z}$. a is congruent to b modulo m $\Leftrightarrow m \mid (a - b)$. This derives from the fact that we can express both a and b as $a = k_1 m + r$ and $b = k_2 m + r$ and so $(b - a) = m(k_1 - k_2)$. This is the same as saying that $\exists z \in \mathbb{Z} : b = zm + a$ and so they are congruent.

Actually, from this we can make a stronger statement. This statement of congruence is actually a relation of equivalence. For what we are saying is that the remainder of a and the remainder of b are equivalent when divided by m. This allows some interesting consequences. To show this, let us first define equivalence classes.

Theorem 1. *Let $B\{\cdot\}$ be a subgroup of $A\{\cdot\}$. $\forall a, b \in A$,let $[a]$ be called the equivalence class of a of the relation $a \equiv b(modB)$. In other words, $[a] \equiv \{y \in A \mid y = a(modB)\}$. Then, $[a] = aB$, that is, the equivalence class is exactly the coset aB.*

Proof. $[a] = \{y \in A \mid y = a(modB)\} \Rightarrow$
$[a] = \{y \in A \mid y \cdot a^{-1} = d \text{ for some } d \in B)\} \Rightarrow$
$[a] = \{y \in A \mid y = d \cdot a(modB)\} \Rightarrow$
$[a] = aB$ □

Proposition 4. *Every coset B of A has the same number of elements, or the same order.*

Proof. Let $a \in A, b \in B$. aB is a coset of A in B, and so is bB. However, $bB = B$. Also, by definition of a group $ab \in A$ hence abB is also a coset. But $abB = aB$ and $\therefore$ all cosets have the same number of elements. □

Lemma 1. *Two different cosets are disjoint, or have intersection of $\emptyset$.*

Proof. Take $xB, yB : xB \cap yb \neq \emptyset$. Then $\exists b_1, b_2 \in B : xb_1 = yb_2 \Rightarrow y^{-1}x = b_2 b_1^{-1} \in B$. Then if $xb \in xB, xb = yy^{-1}xh \in yB$ since $y^{-1}xb \in B$. But this b is for any b and so the cosets must be the same. □

Now we are ready to state and prove Lagrange's theorem.

Theorem 2 (Lagrange). *The order of a subgroup of a finite group divides the order of the group.*

Proof. Let B be a subgroup of A. Let $o(B) = m$ and let $o(A) = n$. Let $c_1B, c_2B, c_3B, ..., c_kB$ be the k different cosets. If they were disjoint, $m \mid n$ as $\cup_{n=1}^{k} c_nB = A$ since $\cap_{n=1}^{k} c_nB = \emptyset$ and each coset has m elements (i.e. $mk = n$).

Suppose not. Then $m \nmid n \Rightarrow \cap_{n=1}^{k} c_nB \neq \emptyset \Rightarrow \exists c_i \neq c_j : c_iB \cap c_jB \neq \emptyset$. A contradiction by the previous lemma. □

With Lagrange's theorem in hand, it will be nearly trivial to proceed. Before, however, we proceed to prove Euler's theorem, we need to define rings and a few of their properties.

4 Rings

Definition 7. *A ring is a set $R\{+, \cdot\}$ equipped with two binary operations (for our purposes addition and multiplication) such that R is an abelian group under addition with 0 being the additive identity, and associative and distributive laws for multiplication hold $\forall a, b \in R$.*

In otherwords, the set R must respect the following:

i.) $\forall a, b \in R, a + b \in R$

ii.) $\forall a, b, c \in R, (a + b) + c = a + (b + d)$

iii.) $\forall a \in R, \exists 0 : a + 0 = 0 + a = a$

iv.) $\forall a \in R, \exists - a : a + (-a) = 0$

v.) $\forall a, b \in R, a + b = b + a$

vi.) $\forall a, b, c \in R, (ab)c = a(bc)$

vii.) $\forall a, c, b\ a(b + c) = ab + ab$

Definition 8. *An integral domain is a ring D which satisfies the following:*

i.) $\forall a, b \in D,\ ab = ba$

ii.) $\forall a \in D,\ \exists 1 \in D : a1 = 1a = a$

iii.) $\forall a, b \in D ab = 0 \Leftrightarrow a = 0 \vee b = 0$

Definition 9. *A field is a ring $F : F\backslash\{0\}$ is an abelian group under multiplication and every non-zero element has an inverse.*

Remark 1. *Every field is an integral domain as it satisfies the necessary conditions.*

We can give some concrete examples of these new things. Basically, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are all integral domains. However, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are also fields, but $\mathbb{Z}$ is not.

Definition 10. *A set of invertible elements is given by $R^x = \{a \in R : \exists b \in R : ab = 1\}$*

Proposition 5. *A set of invertible elements is a group.*

Proof. Let $R^x = \{a \in R : \exists b \in Rab = 1\}$. If $ab = 1$ then $a = b^{-1}$ satisfying i.) and iv.) from Definition 1. Furthermore, $ab \cdot 1 = 1 = 1 \cdot ba$ satisfying the remaining two conditions. □

To reach our goal, which is but a step away, we should use the ring $\frac{\mathbb{Z}}{m\mathbb{Z}}$ where $m \in \mathbb{Z}$, that is, the ring of integers modulo m, to form the group of invertible elements given by $(\frac{\mathbb{Z}}{m\mathbb{Z}})^x = \{[a] : (a, m) = 1\}$. This is the group of elements from the ring of integers modulo m that are coprime to m.

In fact, this group of invertible elements is Euler's ϕ-function.

Definition 11. *The number of elements in a reduced set of modulo m is given by Euler's ϕ-function, denoted by $\phi(m) =\mid (\frac{\mathbb{Z}}{m\mathbb{Z}})^x \mid$.*

Now it is time to state and prove our final three theorems.

5 The Three Theorems

Theorem 3 (Euler's). $(a, m) = 1 \Rightarrow a^{\phi(m)} = 1 \ (mod\ m)$.

Proof. By Lagrange's theorem, we know that if $a \in A$ then $a^{|A|} = 1$. So there is nothing to prove. We know $a \in \frac{\mathbb{Z}}{m\mathbb{Z}})^x \therefore a^{\phi(m)} = a^{|(\frac{\mathbb{Z}}{m\mathbb{Z}})^x|} = 1$ □

Corollary 1 (Fermat's Theorem). *If p is prime and $p \nmid a$ then $a^{p-1} = 1(modp)$.*

Proof. All there is to show is that $\phi(p) = p-1$. But this is trivial because every number between p and 1 are coprime with the exception of p, hence $\phi(p) = p-1$. $\therefore a^{\phi(p)} = a^{p-1} = 1$. □

Theorem 4 (Wilson). *Let p be prime. Then $(p-1)! \equiv 1(modp)$.*

Proof. Let us consider the field $\frac{\mathbb{Z}}{p\mathbb{Z}}$. $(p-1)! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)$. In this field, $(p-1) = -1$ for we are dealing with equivalence classes. Notice further that within all $2 \cdot 3 \cdot ... \cdot (p-2)$ every number can be realized as a pair of which when multiplied become 1. $\therefore (p-1)! = 1 \cdot 2 \cdot .... \cdot (p-1) = 1 \cdot (p-1) = (p-1) = -1$ $(mod\ p)$. □

It should be noted that Wilson's theorem will not hold if p is not prime. However, it can indeed be reformulated to work for composite numbers with the exception of 4.

Proposition 6. *If $n > 4$ and n composite, then $(n-1)! = 0(mod\ n)$.*

Proof. Let $n = ab : a \neq b \neq 1$. Then $(n-1)!$ contains both a and b. Assume $a < b$. Then $(n-1)! = 1 \cdot 2 \cdot ... \cdot a... \cdot b... \cdot (n-1) = C \cdot a \cdot b = C \cdot n = 0(mod\ n)$. □

6 Acknowledgements

References

[1] Max D. Larsen: Introduction to Modern Algebraic Concepts. Addison-Wesley Pucblishing Co. 1969.

[2] Andrew O. Lindstrum, Jr.: Abstract Algebra. Holden-Day, Inc. 1967.

[3] Alexander Bogomolny: www.cut-the-knot.com