Group Theory in Number Theory

Mingshen Wang

School of Mathematics, Northwest University, Xi'an, Shaanxi, 710127, China

2019114051@stumail.nwu.edu.cn

Abstract. The theory of groups exists in many fields of mathematics and has made a great impact on many fields of mathematics. In this article, this paper first introduces the history of group theory and elementary number theory, and then lists the definitions of group, ring, field and the most basic prime and integer and divisor in number theory that need to be used in this article. Then from the definitions, step by step, Euler's theorem, Bézout's lemma, Wilson's theorem and Fermat's Little theorem in elementary number theory are proved by means of definitions of group theory, cyclic groups, and even polynomials over domains. Finally, some concluding remarks are made. Many number theory theorems can be proved directly by the method of group theory without the action of tricks in number theory. Number theory is the thinking of certain special groups (e.g., $(Z,+),(Z,\times)$), so the methods of group theory work well inside number theory.

Keywords. Group theory, Number theory, Ring theory.

1. Introduction

Number theory was introduced before algebra, but the groups and semigroups (e.g. $(Z,+),(Z,\times)$) in algebra are the basis of number theory. In the 18th century, the French mathematician Lagrange used the concept of substitution groups in his paper to deal with many equations of order 3 and 4 [1]. Van also refined this theory and gave some insights of his own [2]. Many developments in permutation groups was further made by Augustin-Louis Cauchy and Camille Jordan [3-4], who defined the concept of isomorphism, although only in the permutation groups. Moreover, it was the man who made the term "group" widely available. Galois first proposed the definition of a cluster, making much work [5]. Gauss published a book-Disquisitiones Arithmeticae [6], in which he proved that some number theory results apply the theory of some finite Abelian groups. Many years have passed since then, until today. This is the combination of group theory and elementary number theory. Elementary number theory has many theorems whose proofs do not depend on group theory but using a more systematic language like group theory can also add a new flavour to the proofs of number theory.

In this paper, section 2 is devoted to give some definition of group theory and number theory. The theorems and their proof will be presented in section 3. The conclusion belonging to this paper is going to be shown in section 4.

2. Definition

Next we will give some definition of group theory and number theory.

2.1. Definition in group theory [7]

Definition 2.1.1. A semigroup is a double (S, p) where S denotes a non-empty set, and p denotes an associative binary composition belonging to M.

Definition 2.1.2. A triple $(\mathrm{S}, \mathrm{p}, 1)$ is denoted by a monoid in which (S, p) is the semigroup, and $\exists 1 \in \mathrm{M}$ such that $\mathrm{p}(1, \mathrm{x}) = \mathrm{x} = \mathrm{p}(\mathrm{x}, 1)$ for all $\mathrm{x} \in \mathrm{M}$.

Definition 2.1.3. In a monoid M, if $\mathrm{u} \in \mathrm{M}$ is said to be invertible if $\exists \mathrm{v} \in \mathrm{M}$ satisfies $\mathrm{uv} = 1 = \mathrm{vu}$.

Definition 2.1.4. If all elements in a manoid are invertible, it is called a group.

Definition 2.1.5. If $\mathrm{O} \subset \mathrm{G}$ for a group $(\mathrm{G}, \mathrm{p}, 1)$, and $(\mathrm{O}, \mathrm{p}, 1)$ is also a group, then we name H is a subgroup of G.

Definition 2.1.6. For a subgroup O of a group G, $\mathrm{x} \in \mathrm{G}$, we name $\mathrm{Ox} = \{\mathrm{ox} | \mathrm{o} \in \mathrm{O}\}$ is the right coset of x related to O. We name $\mathrm{xO} = \{\mathrm{xo} | \mathrm{o} \in \mathrm{O}\}$ is the left coset of x related to O.

Definition 2.1.7. For a subgroup H of G. If $\mathrm{G} = \mathrm{Hx}_1 \cup \mathrm{Hx}_2 \cup \mathrm{Hx}_3 \cup \cdots \cup \mathrm{Hx}_\mathrm{r}$, where we have displayed the distinct cosets, and $\mathrm{Hx}_\mathrm{i} \cup \mathrm{Hx}_\mathrm{j} = \emptyset$ if $\mathrm{i} \neq \mathrm{j}$, then we donate r=[G:H] called the index belonging to H in G.

Definition 2.1.8. If a group can be written by $\mathrm{C} =< \mathrm{a} >= \{\mathrm{a}^\mathrm{m} | \mathrm{m} \in \mathrm{Z}\}$, then we say C is a cyclic group, and we call that a is the generator of group C.

Definition 2.1.9. If every two elements $\mathrm{a}, \mathrm{b} \in \mathrm{G}$ in a group G adapt $\mathrm{ab} = \mathrm{ba}$, then G is a abelian group.

Definition 2.1.10. We say the order of an element c in group G, $\mathrm{ord}(\mathrm{x})$, that is the least positive integers i which makes $\mathrm{c}^\mathrm{i} = 1$. And the order of a group is how many elements are in this group.

Definition 2.1.11. A ring is a triple $(\mathrm{R}, +, \cdot)$ where R is a a non-vacuous set, and the binary compositions $+, \cdot$ and particular elements $0,1$ in it satisfying

$(R, +, 0)$ must be an abelian group.

$(R, \cdot, 1)$ must be a monoid.

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma 、 (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha \text{ hold for all } \alpha, \beta, \gamma \in R.$$

Definition 2.1.12. For a ring $(\mathrm{R}, +, \cdot)$, it is a field if $(\mathrm{R} \backslash \{0\}, \cdot, 1)$ has the nature of a abelian group.

2.2. Definition in number theory [8]

In this chapter, a, b, c, d, n denote integers.

Definition 2.2.1. We say d divides n and we write $\mathrm{d} | \mathrm{n}$ whenever $\mathrm{n} = \mathrm{cd}$ for some c. The d is also called a divisor of n. Besides, d is some factor of n. If d does not divide n we put down $\mathrm{d} \nmid \mathrm{n}$.

Definition 2.2.2. A prime number is describing that a number greater than 1 and the positive divisors of it just have 1 and itself. If a integer is not prime, then it is called composite.

Definition 2.2.3. The greatest common divisor of two or more integers($\neq 0$), is the biggest positive integer which divides each of the integers. We can write it as (a, b) for two integers a and b.

Definition 2.2.4. We say two integers a and b are coprime if $(a, b) = 1$.

3. Theorem and Proof

Theorem 3.1. (Lagrange's theorem). If G have a subgroup H, then $|G| = [G: H] \cdot |H|$.

Proof. Any two cosets Hx and Hy have a bijective map $(x^{-1}y)_R: z \to z(x^{-1}y)$ because for any $h \in H$ there exists $hx(x^{-1}y) = hy$ and it inverse $(y^{-1}x)_R: z \to z(y^{-1}x)$, so cardinality of every coset is equal. And $H1 = H$ is one of the cosets relatives to H. So the $|G| = [G: H] \cdot |H|$.

Theorem 3.2. Assume $\mathbf{C}$ is the cyclic group, $\mathbf{H}$ is certain subgroup belonging to $\mathbf{C}$, then we have that $\mathbf{H}$ must be a cyclic group.

Proof. If $\mathbf{C}$ is a cyclic group, then $\mathbf{C} =< \mathbf{a} >$. Then every element $\mathbf{g} \in \mathbf{C}$ can be put down as a form $\mathbf{g} = \mathbf{a}^{\mathbf{k}}, \mathbf{k} \in \mathbf{Z}$.

If $\mathbf{H}$ is a subgroup of $\mathbf{C}$, and $\mathbf{H}$ can be written by $\mathbf{H} = \{\mathbf{a}^{\mathbf{k}_1}, \mathbf{a}^{\mathbf{k}_2}, \mathbf{a}^{\mathbf{k}_3}, \cdots\}$.

Let $\mathbf{k}_\mathbf{j} = \mathbf{min}\{\mathbf{k}_\mathbf{i} | \mathbf{k}_\mathbf{i} > \mathbf{0}\}$. $< \mathbf{a}^{\mathbf{k}_\mathbf{j}} >= \left\{\mathbf{a}^{\mathbf{m}\mathbf{k}_\mathbf{j}} \middle| \mathbf{m} \in \mathbf{Z}\right\} \in \mathbf{H}$ because $\mathbf{H}$ is a group. If $\mathbf{b} \in \mathbf{H} \backslash < \mathbf{a}^{\mathbf{k}_\mathbf{j}}$, then because $\mathbf{b} \in \mathbf{C}$, b can be written as $\mathbf{b} = \mathbf{a}^{\mathbf{t}}$. Because every element has its inverse. If $\mathbf{t} \leq \mathbf{0}$, then we can choose $\mathbf{c} = \mathbf{a}^{-\mathbf{t}}$. Assume that $\mathbf{t} > \mathbf{0}$. Because $\mathbf{b} \notin < \mathbf{a}^{\mathbf{k}_\mathbf{j}} >$ so $\mathbf{k}_\mathbf{j} \nmid \mathbf{t}$. So we can find $\mathbf{m} \in \mathbf{Z}$ such that $\mathbf{t} - \mathbf{m}\mathbf{k}_\mathbf{j} = \mathbf{r}, \mathbf{0} < \mathbf{r} < \mathbf{k}_\mathbf{j}$. And because $\mathbf{H}$ is a group, so $\mathbf{b} \cdot (\mathbf{a}^{\mathbf{k}_\mathbf{j}})^{-\mathbf{m}} = \mathbf{a}^{\mathbf{r}} \in \mathbf{H}$ and $\mathbf{r} < \mathbf{k}_\mathbf{j}$ which are introduced contradictions. So $\mathbf{H} =< \mathbf{a}^{\mathbf{k}_\mathbf{j}} >$.

Theorem 3.3. (Bézout's Lemma). If $\mathbf{a}, \mathbf{b}$ are integers and $(\mathbf{a}, \mathbf{b}) = \mathbf{d}$, then there exist integers $\mathbf{x}, \mathbf{y}$, where $\mathbf{ax} + \mathbf{by} = \mathbf{d}$.

Proof. Z is a cyclic group. Then $\mathbf{H} = \{\boldsymbol{\mu}\mathbf{a} + \boldsymbol{\tau}\mathbf{b} | \boldsymbol{\mu}, \boldsymbol{\tau} \in \mathbf{Z}\}$ is a subgroup of Z because $(\boldsymbol{\mu}_1\mathbf{a} + \boldsymbol{\tau}_1\mathbf{b}) + (\boldsymbol{\mu}_2\mathbf{a} + \boldsymbol{\tau}_2\mathbf{b}) = (\boldsymbol{\mu}_1 + \boldsymbol{\mu}_2)\mathbf{a} + (\boldsymbol{\tau}_1 + \boldsymbol{\tau}_2)\mathbf{b}$ and $(\boldsymbol{\mu}\mathbf{a} + \boldsymbol{\tau}\mathbf{b}) + ((-\boldsymbol{\mu})\mathbf{a} + (-\boldsymbol{\tau})\mathbf{b}) = \mathbf{0}$. So H is also a cyclic group because of Theorem 2. So there must have a generator $\mathbf{H} =< \mathbf{g} >$ which $\mathbf{g} = \mathbf{ax} + \mathbf{by}$ and when $\boldsymbol{\mu} = \mathbf{0}, \boldsymbol{\tau} = \mathbf{1}$ or $\boldsymbol{\mu} = \mathbf{1}, \boldsymbol{\tau} = \mathbf{0}$, $\mathbf{a}, \mathbf{b} \in \mathbf{H}$, so $\mathbf{g} | (\mathbf{a}, \mathbf{b})$. And because $\mathbf{g} = \mathbf{ax} + \mathbf{by}$, so $\mathbf{d} | \mathbf{g}$. So $\mathbf{d} = \mathbf{g}$.

We can easily proof if **there exits d which is bigger than 0 and d $\in$ Z** such that **ax plusing by equals to d** which $|\mathbf{a}, \mathbf{b}$, such that $\mathbf{d} = (\mathbf{a}, \mathbf{b})$. If $\mathbf{d} \neq (\mathbf{a}, \mathbf{b})$, and $(\mathbf{a}, \mathbf{b}) | \mathbf{a}$, $(\mathbf{a}, \mathbf{b}) | \mathbf{b}$, so $(\mathbf{a}, \mathbf{b}) | \mathbf{d}$. Because d is a positive integer, so $\mathbf{d} > (\mathbf{a}, \mathbf{b})$. This makes contradictions of $(\mathbf{a}, \mathbf{b})$ is the greatest divisor.

Theorem 3.4 (Euler's theorem). if there are two coprime integers n and a, and $\varphi(n)$ is Euler's totient function, $\varphi(n)$ donates the number of elements which coprime to n in $\{0,1, \cdots, n - 1\}$, then we can discover $a^{\varphi(n)} \equiv 1(\text{mod } n)$.

Proof. We first prove that elements which coprime to n in $\{0,1, \cdots, n - 1\}$ are a group H with common multiplication (mod n), which is called reduced residues system.

If $b, c \in H$, then we have $k_1b + k_2n = 1$, $k_3c + k_4n = 1$. Then $(k_1b + k_2n)(k_3c + k_4n) = k_1k_3bc + (k_1k_4b + k_2k_3c + k_2k_4)n = 1$. So $(bc, n) = 1$ and $bc \in H$. $(1, n) = 1$ give that $1 \in H$.

We should prove if X is a reduced residues system of n and b is coprime to n, then bX is also a reduced residues system modulo n.

We know that for $x \in X$, $(x, n) = 1$, so $(bx, n) = 1$. And for any $x_1, x_2 \in X$, if $bx_1 \equiv bx_2(\text{mod } n)$, we know $k_1b + k_2n = 1$ and $k_1bx_1 + k_2nx_1 \equiv (k_1b + k_2n)x_1 \equiv (k_1b + k_2n)x_2 \equiv k_1bx_2 + k_2nx_2(\text{mod } n)$. We have $x_1 \equiv x_2(\text{mod } n)$. So elements in bX is also $\varphi(n)$. This also is a reduced residues system.

So there exists an element c, such that $bc \equiv 1(\text{mod } n)$ because $1 \in bX$. A reduced residues system of n with common multiplication (mod n) is a group.

Because $(a, n) = 1$, So $a \in H$ and $< a >$ is a subgroup of H. Because of Theorem 1, $a^{\varphi(n)} \equiv a^{|H|} \equiv a^{k|<a>|} \equiv 1^k \equiv 1(\text{mod } n)$.

Theorem 3.5 (Fermat's little theorem). Assume p is a prime number and p is not a divisor of an integer a, then the $p-1$ power of a is equal to 1 in the sense of module p.
Proof. Because $p \nmid a$ and p is a prime, so $(p,a)=1$. Because all number is coprime to a prime, so $\varphi(n)=p-1$.

Theorem 3.6 (Wilson's theorem). p is a prime is a sufficient necessary condition for $(p-1)! = -1(\mathrm{mod}\ p)$.

Proof. First, because of the process in Theorem 3.4, we know $(Z/Zp\backslash\{0\},\cdot)$ is a abelian group. (Because every positive integer under p is coprime to p.) So we know $(Z/Zp,+,\cdot)$ is a field. Because it is a field, so every product by some elements $\neq 0$ cannot be 0. So if the equation $x^n = 1, x \in Z/Zp$ has more than n solves $\gamma_1, \gamma_2, \gamma_3 \cdots \gamma_{n+1} \cdots$

We have $(\gamma_{n+1}-\gamma_1)(\gamma_{n+1}-\gamma_2)\cdots(\gamma_{n+1}-\gamma_n)=0$ but every product by some elements $\neq 0$ cannot be 0. So every $x^n = 1, x \in Z/Zp$ should have $\leq n$.

Because it is a finite field. So we could find an element g in $(Z/Zp\backslash\{0\},\cdot)$ which has the biggest order. If $\mathrm{ord}(g) = p$. Because of Theorem 3.1, $q|p-1$. If $(Z/Zp\backslash\{0\},\cdot)$ is not a cyclic group, $q < p-1$.

Now we want to prove that in finite abelian group G, if the biggest order of elements in G equals to m, then $\forall g \in G, \mathrm{ord}(g)|m$.

If $\exists g \in G$, but $\mathrm{ord}(g) \nmid m$, then $\exists p$ such that (assume the biggest order element is x) $\mathrm{ord}(g) = p^a m, \mathrm{ord}(x) = p^b n\ \big((p,m)=(p,n)=1\big), a > b$.

So $\mathrm{ord}\left(x^{p^b}\right) = n, \mathrm{ord}(g^s) = p^a$, then $\mathrm{ord}\left(g^s x^{p^b}\right) = p^a n > p^b n = m$ which makes contradiction. So order of any elements must divide q. So $x^q = 1$ have $p-1$ solves. But $p-1 > q$, which makes contradiction. So $(Z/Zp\backslash\{0\},\cdot)$ must be a cyclic group. If its generator is a. And it has odd number of elements. Because $\prod_{g\in(Z/Zp\backslash\{0\},\cdot)} g = a^{\frac{p-1}{2}}$ and every element has it inverse s, but $a^{\frac{p-1}{2}}$ is the only 2 order element because p-1 is even, p is odd.

Because of Theorem 3.4, we know $\varphi(p) = p-1$. So we can see that $a^{\varphi(p)} \equiv 1(\mathrm{mod}\ p)$ and then we can see that $a^{p-1} \equiv 1(\mathrm{mod}\ p)$ and we can see $a^{\frac{p-1}{2}} \equiv \pm 1(\mathrm{mod}\ p)$. At this point, there are only two scenarios to consider, so we discuss them in separate cases. If $a^{\frac{p-1}{2}} = 1, a^{\frac{p-1}{2}+1} = a$ which make contradiction because every element in <a> must be different. So $a^{\frac{p-1}{2}} = -1$, $\prod_{g\in(Z/Zp\backslash\{0\},\cdot)} g = -1$. So we proof $(p-1)! = -1(\mathrm{mod}\ p)$.

4. Conclusion

This paper uses the ideas of group theory to prove the problems of number theory, although they are all elementary number theory problems. Few people go back to elementary number theory after studying group theory, because for non-numerical math students, elementary number theory is just a key to group theory. But when they look back, and the ideas of group theory are applied to prove the theorems of elementary number theory, it is rare to find that the theorems of elementary number theory, which require so much skill to prove. After all, elementary number theory is nearly inseparable from difficult constructions and flashy tricks [9], but group theory seems very simple but useful. During the proof, the author spent a lot of time thinking about avoiding group theory proofs that use the basic theory of number theory, because if the proof of group theory uses the theory of number theory again, it would essentially be a circular argument, which is very unnecessary and needing to be avoid. This allows many of the theorems of number theory in this paper to be supported almost entirely by the system of group theory. Many theorems of number theory are proved in group theory without many complex definitions, and in fact many of them can be proved in three sentences. But if one does not learn group theory well, one may not quite understand them. This paper assumes that the reader does not understand group theory and number theory at all, and proves these theorems in an initial way, so that they can be easily read and understood. Although the study of algebraic number theory is very deep [10], the study and learning of elementary number theory is very often divorced from the language of algebra. As algebra becomes more and more an important part of modern mathematics, elementary number theory will also have more of an algebraic flavor. Number theory and algebra will progress together to the next level.

References

[1] Lagrange J L 1770 Reflexions sur la resolution algebrique des equations, Nouveaux Memoires de l'Acade. Royale des sciences et belles-letteres, avec l'histire pour la meme annee, vol.1, pp. 134-215.
[2] Sturm P C 2009 Mémoire sur la résolution des équations numériques. In Collected Works of Charles François Sturm. Birkhäuser Basel.
[3] Belhoste B 2012 Augustin-Louis Cauchy: A Biography. Springer Science & Business Media.
[4] Jordan C 1882 Mémoire sur le nombre des valeurs des fonctions. Ecole polytechnique.
[5] Galois É Neumann P M 2011 The mathematical writings of Évariste Galois. European mathematical society.
[6] Gauss C F 2014 Disquisitiones arithmeticae. Mathematical perspectives: essays on Mathematics and its historical development. Academic Press, New York
[7] Apostol T M 1998 Introduction to analytic number theory. Springer Science & Business Media. New York.
[8] Jacobson N 2012 Basic algebra I. Courier Corporation.
[9] Rosen K H 2005 Elementary number theory and its applications. Pearson, Addison Wesley.
[10] Weil A 2013 Basic number theory. Springer Science & Business Media. New York