**International Journal of Theoretical and Applied Mathematics**
2019; 5(4): 57-62
http://www.sciencepublishinggroup.com/j/ijtam
doi: 10.11648/j.ijtam.20190504.11
ISSN: 2575-5072 (Print); ISSN: 2575-5080 (Online)

# Using Divisor Function and Euler Product Function in Abstract Algebra Concepts

**K. Subbanna[1, *], S. Venkatarami Reddy[1], S. Gouse Mohiddin[2], R. Bhuvana Vijaya[3]**

[1]Department of Mathematics, Besant Theosophical College, Madanapalle Andhra Pradesh, India

[2]Department of Mathematics, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India

[3]Department of Mathematics, Jntua College of Engineering Anantapur, Anantapuramu, Andhra Pradesh, India

**Email address:**
subbu07mtech@gmail.com (K. Subbanna), drsubbanna19@gmail.com (K. Subbanna)

[*]Corresponding author

**To cite this article:**
K. Subbanna, S. Venkatarami Reddy, S. Gouse Mohiddin, R. Bhuvana Vijaya. Using Divisor Function and Euler Product Function in Abstract Algebra Concepts. *International Journal of Theoretical and Applied Mathematics.* Vol. 5, No. 4, 2019, pp. 57-62.
doi: 10.11648/j.ijtam.20190504.11

**Received**: August 10, 2019; **Accepted**: September 19, 2019; **Published**: October 9, 2019

**Abstract:** Algebraic number theory is a branch of number theory that uses the techniques of abstract algebra to study the integers, rational numbers, and their generalizations. Number-theoretic questions are expressed in terms of properties of algebraic objects such as algebraic number fields and their rings of integers, finite fields, and function fields. These properties, such as whether a ring admits unique factorization, the behavior of ideals, and the Galois groups of fields, can resolve questions of primary importance in number theory. In this paper for the most part centered around number theory ideas which are utilized in different themes like group theory and ring theory, these speculations are extremely unique ideas to comprehend among this we might want to express our perspectives as far as number hypothesis/theory ideas, such as, to calculate some subgroups of a cyclic group, number of ideals, principal ideals of a ring and number of generators of a cyclic group as far as both regular procedure and number speculation/hypothesis thoughts.

**Keywords:** Divisors Function, Euler's Phi-function, Field, Number Theory, Abstract Algebra

## 1. Introduction

The theory of numbers is an area of mathematics which deals with the properties of whole and rational numbers. Analytic number theory is one of its branches, which involves study of arithmetical functions, their properties and the interrelationships that exist among these functions. In this paper I will introduce some of the three very important examples of arithmetical functions, as well as a concept of the possible operations we can use with them. There are four propositions which are mentioned in this paper and I have used the definitions of these arithmetical functions and some Lemmas which reflect their properties, in order to prove them.

Algebraic number theory is a branch of number theory that uses the techniques of abstract algebra to study the integers, rational numbers, and their generalizations. Number-theoretic questions are expressed in terms of properties of algebraic objects such as algebraic number fields and their rings of integers, finite fields, and function fields. These properties, such as whether a ring admits unique factorization, the behavior of ideals, and the Galois groups of fields, can resolve questions of primary importance in number theory, like the existence of solutions to Diophantine equations.

List of Symbols:

$\sum$ : Summation

$\prod$ : Product

$\tau(n)$ : Number of divisors function

$\phi(n)$ : Euler's phi-function

## 2. Number of Subgroups of a Cyclic Group

Definition. Let $G$ be an abelian group, and let $H$ be a

non-empty subset of *G* such that

$a+b\in H$ for all $a,b\in H$ and $-a\in H$ for all $a\in H$

Then *H* is called a subgroup of *G*.

In words: *H* is a subgroup of *G* if it is closed under the group operation and taking inverses.

Multiplicative notation: if the abelian group *G* in the above definition is written using multiplicative notation, then *H* is a subgroup if $ab\in H$ and $a^{-1}\in H$ for all $a,b\in H$.

Definition:

A group G is called cyclic if there exists an element g in G such that G = <g> = {$g^n$ | n is an integer}. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains g is G itself suffices to show that G is cyclic.

Example1:

If G is a cyclic group of order 12 then the number of subgroups of G.

Solution:

Here the number is 12 is finite and small number so to find out subgroup of these are very small task because the number of divisors of 12 are 1, 2, 3, 4, 6, and 12 so number of subgroups is 6.

*If the number is large then* to find out the number of subgroups is very difficult and time consuming process so to reduce this difficulty by using the following number theory concepts.

Definition: (Prime and Composite). An integer n > 1 is prime if it the only positive divisors of n are 1 and n. We call n composite if n is not prime.

The number 1 is neither prime nor composite.

The first few primes of N are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79.. ……. and

The first few composites are

4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34.. ……

Definition: (Divisor function)

The divisor function $\sigma_k(n)$ for n an integer is defined as the sum of the $k^{th}$ powers of the (positive integer) divisors of n,

$$\sigma_k(n)=\sum_{d/n} d^k$$

It is implemented in the Wolfram Language as Divisor Sigma [*k*, *n*].

The notations d (n) (Hardy and Wright 1979, p. 239), v (n) (Ore 1988, p. 86), and $\tau(n)$ (Burton 1989, p. 128) are sometimes used for $\sigma_0(n)$, which gives the *number* of divisors of n. Rather surprisingly, the number of factors of the polynomial $a^n-b^n$ are also given by d (n). The values of $\sigma_0(n)$ can be found as the inverse Möbius transform of 1, 1, 1,….. (Sloane and Plouffe 1995, p. 22). Heath-Brown (1984) proved that $\sigma_0(n)=\sigma_0(n+1)$ infinitely often. The numbers having the incrementally largest number of divisors are called highly composite numbers. The function $\sigma_0(n)$ satisfies the identities

$$\sigma_0(p^a)=a+1$$

$$\sigma_0(p^{a1}p^{a2}....)=(a_1+1)(a_2+1)....$$

Where the $p_i$ are distinct primes and $p^{a1}p^{a2}....$ is the prime factorization of a number n.

The divisor function $\sigma_0(n)$ is odd iff n is a square number.

The function $\sigma_1(n)$ that gives the *sum* of the divisors of n is commonly written without the subscript, i.e., $\sigma(n)$.

As an illustrative example of computing $\sigma_k(n)$, consider the number 140, which has divisors $d_i=1,$ 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, and 140, for a total of N=12 divisors in all. Therefore,

$$\sigma_0(140)=N=12$$

$$\sigma_1(140)=\sum_{i=1}^{N} d_i=336$$

$$\sigma_2(140)=\sum_{i=1}^{N} d_i^2=27300$$

$$\sigma_2(140)=\sum_{i=1}^{N} d_i^3=3164112$$

The divisor function can also be generalized to Gaussian integers. The definition requires some care since in principle, there is ambiguity as to which of the four associates is chosen for each divisor. Spira (1961) defines the sum of divisors of a complex number Z by factoring Z into a product of powers of distinct Gaussian primes,

Theorem 1: (fundamental theorem of arithmetic)

Every integer n ≥ 2 has a factorization as a

Product of prime powers:

$$n=p_1^{e_1}p_2^{e_2}p_2^{e_2}.....p_k^{e_k}$$

Where the $p_i$ are distinct primes and the $e_i$ are positive integers. Furthermore, the factorization is unique up to rearrangement of factors.

To find the number of divisors of any positive integer first to express different types of prime product in a unique way

i.e., $n=p_1^{e_1}p_2^{e_2}p_2^{e_2}.....p_k^{e_k}$

Number of divisors of n is denoted by the symbol $\tau(n)$

$$\tau(n)=(1+e_1).(1+e_2).....(1+e_k)$$

∴ Number of subgroups of a cyclic group is of order n is $\tau(n)$

Example 2:

If G is a cyclic group of order 2512 then the no. of subgroups.

Here to find the number of divisors of 2512 manually is difficult but it can be reduced as product of primes is the easy way

So, 2512 = 2×1256

=22×628

=2×2×2×314

=2×2×2×2×157

$=2^4\times157^1$

here 157 is prime number

$\therefore$ $2512 = 2^4\times157^1$

$\therefore$ Number of subgroups of a cyclic group is of order 2512 is $\tau(n) = (4+1).(1+1) = 5.2 = 10$.

***Table 1.*** *Number of Subgroups of Some groups.*

| S. No | Order of Group | Prime factorization | No. of subrings |
|---|---|---|---|
| 1 | 100000000 | 2×2×2×2×2×2×2×2 x 5×5×5×5×5×5×5×5 | 81 |
| 2 | 123456789 | 127×9721 | 4 |
| 3 | 987654321 | 2×2×2 x 37×333667 | 16 |
| 4 | 432198765 | 29 x 149 | 4 |
| 5 | 765432198 | 2×3×3×13×1847 | 24 |
| 6 | 2029 | 2029 | 2 |

Note:

If n is composite number then no. of subgroups are $\tau(n)$

If n is Prime number then the no of subgroups are 2 only.

No. of proper subgroups of order n is $\tau(n)$ -2

No. of improper subgroups are 2 only

## 3. Number of Ideals and Principal Ideals of a Ring R

Definition: A non-empty subset S of a ring (R, +, *) is called an ideal of R if

(S,+) is an abelian group of (R,+)

for all $s \in S$ then rs & $sr \in S$

Definition: An ideal of a ring R is said to be a principal ideal it is generated by single element of R

i.e., if $a \in R$ then a set generated by "a" or <a> is a principal ideal of r

$< a > = \{ax / \forall x \in R\} \subseteq R$

Fact: Number of different ideals and principal ideals for the ring $(Z_n, +, \bullet)$ is $\tau(n)$

Example 3: Number of different ideals and principal ideals of the ring $(Z_{2019}, +, \bullet)$

n = 2019

= 3×673 here 673 is a prime number

$\therefore$ Number of different ideals and principal ideals are (1+1).(1+1) = 2.2 = 4.

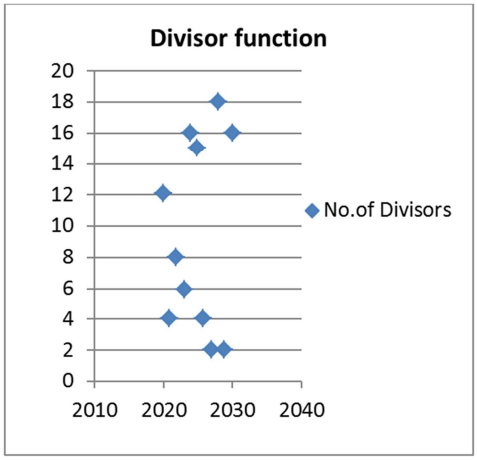


***Figure 1.*** *Divisor Function.*

***Table 2.*** *Number of Ideals and Principal ideals of a Ring.*

| S. No | Ring | Prime factorization | No. of ideals and principal ideals |
|---|---|---|---|
| 1 | $(Z_{2020}, +, \bullet)$ | 2×2×5×101 | 12 |
| 2 | $(Z_{2021}, +, \bullet)$ | 43×47 | 4 |
| 3 | $(Z_{2022}, +, \bullet)$ | 2×3×337 | 8 |
| 4 | $(Z_{2023}, +, \bullet)$ | 7×17×17 | 6 |
| 5 | $(Z_{2024}, +, \bullet)$ | 2×2×2×11×23 | 16 |
| 6 | $(Z_{2025}, +, \bullet)$ | 3×3×3×3×5×5 | 15 |
| 7 | $(Z_{2026}, +, \bullet)$ | 2×1013 | 4 |
| 8 | $(Z_{2027}, +, \bullet)$ | 2027 | 2 |
| 9 | $(Z_{2028}, +, \bullet)$ | 2×2×3×13×13 | 18 |
| 10 | $(Z_{2029}, +, \bullet)$ | 2029 | 2 |

Graphical Representation of Euler totient function use of between 2020-2030.

# 4. Number Generators of a Cyclic Group

Proposition: Let G be a cyclic group of order n, then G has $\phi(n)$ generators.

Theorem: (A product formula for $\phi(n)$)

Statement: for $n \geq 1$ we have $\phi(n) = n \prod_{p/n} (1-\frac{1}{p})$.

Proof: for n=1 the product is empty since there are no primes which divide 1

In this case it is understood that the product is to be assigned the value 1

$\therefore \phi(1) = 1$.

Suppose that $n > 1$ and let $p_1, p_2, p_3, \ldots\ldots\ldots p_r$ be distinct prime divisors of n. Now the product can be taken as

$$\prod_{p/n}(1-\frac{1}{p}) = \prod_{i=1}^{r}(1-\frac{1}{p_i}),\ \prod_{p/n}(1-\frac{1}{p}) = (1-\frac{1}{p_1})(1-\frac{1}{p_2}).....(1-\frac{1}{p_r})$$
$$\prod_{p/n}(1-\frac{1}{p}) = 1-\Sigma\frac{1}{p_i}+\Sigma\frac{1}{p_i p_j}-\Sigma\frac{1}{p_i p_j p_k}+.....+\Sigma\frac{1}{p_i p_j p_k \ldots p_r} \quad (1)$$

On the right hand side, in a term such as $\Sigma\frac{1}{p_i p_j p_k}$ it is understood that we consider all possible products $p_i p_j p_k$ of distinct prime factors of n taken three at a time. Also each term on the right hand side of equation (1) is of the form $\pm\frac{1}{d}$ where d is a divisor of n which is either 1 or a product of distinct primes. The numerator $\pm 1$ is exactly $\mu(d)$.

Since $\mu(d) = 0$ if d is divisible by the square of any $p_i$, the sum in equation (1) is exactly the same as $\sum_{d/n}\frac{\mu(d)}{d}$.

$\therefore$ Equation (1) can be written as

$$\prod_{p/n}(1-\frac{1}{p}) = \sum_{d/n}\frac{\mu(d)}{d}$$

now multiplying the above relation with n on both sides, we get

$$n\prod_{p/n}(1-\frac{1}{p}) = n\sum_{d/n}\frac{\mu(d)}{d}, n\prod_{p/n}(1-\frac{1}{p}) = n\sum_{d/n}\mu(d)\frac{n}{d}$$

But we know that

$$\phi(n) = \sum_{d/n}\mu(d).\frac{n}{d}$$

$$\phi(n) = n\prod_{p/n}(1-\frac{1}{P})$$

$$\therefore \phi(n) = n\prod_{p/n}(1-\frac{1}{P})$$

Complete the proof.

Example 4: If G is a cyclic group of order 2512 then the numbers of generators of G are

2512 = 2×2×2×2×157

$$\phi(2512) = 2512(1-\frac{1}{2})(1-\frac{1}{157}) = 2512(\frac{1}{2})(\frac{156}{157})$$
$$= 1256(\frac{156}{157})$$
$$= 8X156$$
$$= 1248$$

Number of generators of cyclic group of order 2512 is 1248.

***Table 3.*** *No of generators of a cyclic group between 1 to 143.*

| **Φ (*n*) for 1 ≤ *n* ≤ 143** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **+** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| 0 | N/A | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 |
| 12 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 | 12 | 10 | 22 |
| 24 | 8 | 20 | 12 | 18 | 12 | 28 | 8 | 30 | 16 | 20 | 16 | 24 |
| 36 | 12 | 36 | 18 | 24 | 16 | 40 | 12 | 42 | 20 | 24 | 22 | 46 |
| 48 | 16 | 42 | 20 | 32 | 24 | 52 | 18 | 40 | 24 | 36 | 28 | 58 |
| 60 | 16 | 60 | 30 | 36 | 32 | 48 | 20 | 66 | 32 | 44 | 24 | 70 |
| 72 | 24 | 72 | 36 | 40 | 36 | 60 | 24 | 78 | 32 | 54 | 40 | 82 |
| 84 | 24 | 64 | 42 | 56 | 40 | 88 | 24 | 72 | 44 | 60 | 46 | 72 |
| 96 | 32 | 96 | 42 | 60 | 40 | 100 | 32 | 102 | 48 | 48 | 52 | 106 |
| 108 | 36 | 108 | 40 | 72 | 48 | 112 | 36 | 88 | 56 | 72 | 58 | 96 |
| 120 | 32 | 110 | 60 | 80 | 60 | 100 | 36 | 126 | 64 | 84 | 48 | 130 |
| 132 | 40 | 108 | 66 | 72 | 64 | 136 | 44 | 138 | 48 | 92 | 70 | 120 |

Graphical Representation of $\varphi$ (*n*) for 1 ≤ *n* ≤ 143.

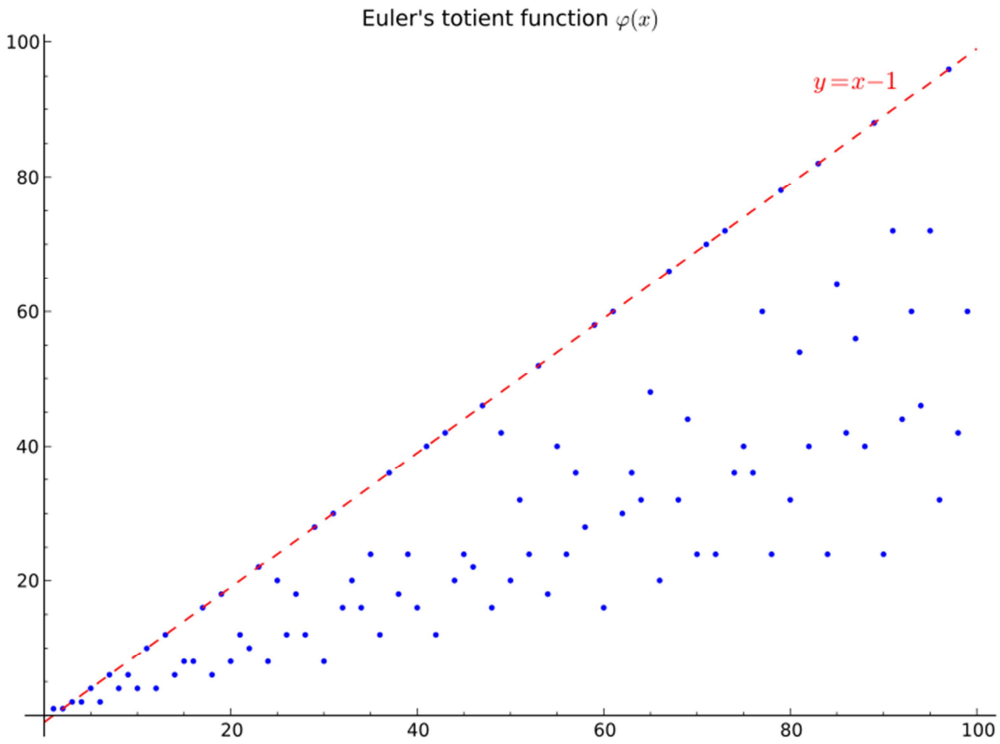


***Figure 2.*** *Euler's totient function.*

*Properties of Euler's Totient Function:*

1. For a prime number p, $\phi(p)$ is p-1. For example $\phi(5)$ is 4, $\phi(7)$ is 6 and $\phi(13)$ is 12. This is obvious; gcd of all numbers from 1 to p-1 will be 1 because p is a prime.
2. For two numbers a and b, if gcd (a, b) is 1, then ϕ (ab) = ϕ (a) * ϕ (b). For example ϕ (5) is 4 and ϕ (6) is 2, so ϕ (30) must be 8 as 5 and 6 are relatively prime.
3. For any two prime numbers p and q, ϕ (pq) = (p-1)*(q-1). This property is used in RSA algorithm.
4. If p is a prime number, then ϕ ($p^k$) = $p^k - p^{k-1}$. This can be proved using Euler's product formula.
5. Sum of values of totient functions of all divisors of n is equal to n. $\sum_{d/n} \phi(d) = n$
6. The most famous and important feature is expressed in Euler's theorem
   The theorem states that if n and a are coprime (or relatively prime) positive integers, then $a^{\phi(n)} = 1 \pmod n$
7. Number of generators of a finite cyclic group under modulo n addition is ϕ (n).

*Algebraic Significance*

a) Number of subgroups of the cyclic group: For any natural number n, $\sigma_0(n)$? equals the number of subgroups of the cyclic group of order n, under the action of the automorphism group.

b) Number of automorphism classes of elements in the cyclic group: For any natural number n, $\sigma_0(n)$? equals the number of equivalence classes of elements in the cyclic group of order n, under the action of the automorphism group. In fact, two elements are in the same automorphism class if and only if they generate the same subgroup. The sizes of these equivalence classes are ϕ (d) for the divisors d of n, and this is a combinatorial proof of the fact that $\sum_{d/n} \phi(d) = n$.

c) Number of associate classes of elements in the ring of integers modulo n: For any natural number n, $\sigma_0(n)$? equals the number of equivalence classes of elements in the ring of integers modulo n, under the relation of being associate elements. In fact, the equivalence classes of associate elements are precisely the same as the equivalence classes under the action of auto morphisms of the additive group of the ring. Thus, their sizes are ϕ (d), for the divisors d of n.

d) Number of irreducible factors of the polynomial $x^n - 1$ over Q: This polynomial is a product of irreducible factors called cyclotomic polynomials for the divisors d of n, where $\phi_d$ has as its roots the primitive $d^{th}$ roots of unity. The degree of $\phi_d$ is ϕ (d).

## 5. Conclusions

In number theory, the divisor function is a function that is a sum over the divisor function. It every now and again happens in the investigation of the asymptotic behavior of the Riemann zeta function. The different investigations of the behavior of the divisor function are sometimes called divisor problems.

Euler's totient function is a multiplicative function, meaning that if two numbers m and n are relatively prime, then

$$\Phi (mn) = \varphi (m) \varphi (n)$$

This function gives the order of the multiplicative group of

integers modulo n (the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$). It additionally assumes a key job in the meaning of the RSA encryption framework.

## Acknowledgements

I would like to express my very great appreciation to our Post graduate students for his valuable and constructive suggestions during the planning and development of this work. I would also like to thank our staff members, Head and Principal of the Besant Theosophical College.

Finally, I wish to thank my parents for their support and encouragement throughout my study.

## References

[1] W. W. Adams and L. J. Goldstein, Introduction to Number Theory, Prentice-Hall, Englewood Cliffs, New Jersey, 1g76.

[2] G. E. Andrews, Number Theory, w. B. Saunders, Philadelphia, lg7l.

[3] T. A. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[4] R' G. Archibald, an Introduction to the Theory of Numbers, Merrill, Columbus, Ohio, 1970.

[5] N. S. Gopalakrishnan, University algebra, Second edition, New Age International (P) limited, publishers.

[6] Kratzel E., Lattice points, Kluwer Academic Publishers, 1988.

[7] Petermann Y.-F. S. and Wu Jie, on the sum of the exponential divisors of an integer, Acta Math. Hungar., 77 (1997), 159-175.

[8] Pillai S. S., On an arithmetic function, Journ. Annamalai Univ., 2 (1933), 243-248.

[9] Subbarao M. V., on some arithmetical convolutions, the theory of arithmetical functions, Lecture Notes in Mathematics 251, Springer Verlag, 1972, 247-271.

[10] Toth L., On certain arithmetical functions involving exponential divisors, Annales Univ. Sci. Budapest. Sect. Comp., 24 (2004), 285-294.

[11] Toth L., on certain arithmetical functions involving exponential divisors Annales Univ. Sci. Budapest. Sect. Comp., 27 (2007), 155-166.

[12] D. S. Dummit and R. M. Foote, Abstract algebra, third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[13] C. F. Gauss, Untersuchungen ¨Uber Hohere Arithmetik, second edition, reprinted, Chelsea publishing company, New York 1981.

[14] K. Ireland and M. Rosen, A classical introduction to modern number theory, second edition, Springer-Verlag, GTM Vol 84 (second edition) 1990.

[15] T. W. Judson, Abstract Algebra: Theory and Applications, PWS-Kent, Boston, 1994.

[16] Daniel Marcus, Number Fields.

[17] Serge Lang, Algebraic Number Fields.

[18] Pierre Samuel, Algebraic Theory of Numbers.

[19] Gerald Janusz, Algebraic Number Fields.