SUSHANT UNIVERSITY ORGANIZED INTERNATIONAL CONFERENCE ON
"ADVANCES IN MULTIDISCIPLINARY RESEARCH AND INNVOATION" ICAMRI-2023
ON 28-29TH OCTOBER 2023
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

A Study of Implication of Abstract Algebra and Its Logic

1Aarti Goel* 2 Dr. Manjeet Singh Jakhar
1 Scholar, Department of Mathematics, NIILM University, Kaithal, India.
2 Associate Professor, Department of Mathematics, NIILM University, Kaithal, India.

ABSTRACT

The difficulties students experience in drawing conclusions from logical implications and factual verification are explored here. Insights from auditing the fields of education and psychology into student reasoning with logical implications and empirical data suggest that a lack of familiarity with counterexamples may be a major contributor. The purpose of this study was to examine the role of argument and counterexample preparation in improving students' logical thinking and several aspects of numerical demonstration, including Evidence Development, Evidence Validation, and Proof Method Awareness. In particular, the study hypothesized that fair planning, by placing an emphasis on counterexamples, was superior to the other two approaches, which placed a greater emphasis on rule violations and reality tables, for improving students' reasoning by logical ramifications as effectively as numerical explanation.

KEYWORDS: Abstract Algebra, Logic, students experience, logical implications, logical ramifications, numerical explanation.

INTRODUCTION

Our emphasis shifts from a polynomial's roots (Galois's original difficulty) in network-coding applications to its factor ring itself, which is the center of our attention in abstract algebraic applications. Finding the roots of an irreducible polynomial necessitates first creating a field extension. Since a polynomial does not have to be irreducible to create an ideal, it also does not have to be irreducible to form a ring of factors. The notion that the concept of "ideal" might be used in a recursive manner is another way to tie the work in [10] into this issue. A factor ring may be constructed by "splitting" a ring GF(2)[x] by an ideal, such as [(x n 1)]. Factor rings may include ideas as well. We'll be focusing mostly on the latter ideas. This study of cyclic codes uses the factor ring and one of its ideals to help us better understand the vector space F n.

Every time a cyclic shift is made to any of its codewords, a new codeword is created. The n-tuple that results from shifting each element to the right (or left) and then re-wrapping the last element back to the beginning of the list is known as a cyclic shift. In the case of cyclic codes, the coefficients of the polynomials associated with each codeword may be used as the coordinates of the code vector:

The coding polynomial is C(x) F[x]. There is no field in which the set of k code polynomials for a code C is included, since the factor ring GF(2)[x]/[(x n 1)] is factorizable. Moreover, we may derive that every finite field has a set of elements equal to an integer power of the prime number, but the opposite is not true: every set of elements equal to an integer power of the prime number is not always a field. It is not a field since not all of its elements have the same inverse (because the GCD of each element and (x n 1) is not always 1), hence it is not GF (2) [[[(x n 1)]]. The factor ring is a one-dimensional object from this vantage point. It's also possible to think of the identical item in terms of a "vector field" of dimension (F n) and length (D n). The name "field" alludes to the fact that the ground field 0, 1 is truly a field from this second perspective. Notice that in this factor ring, operations between its members are done using (x n 1) as the modulus. To create the ring, rather than an irreducible polynomial of the same number of degrees, the factor ring must be constructed using (x n 1), rather than an irreducible polynomial of the same degree. Next, we'll see why this is important.

The multiplication modulo (x n 1) of the relevant code polynomial by x k is like the cyclic shift of a codeword by GF (2)[x]/ [(x n 1)]. Even if this fact is uninteresting, we should keep in mind

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

that every given polynomial may be thought of as the linear combination of shifts that, according to the definition, generates an identical c(x). Adding two vectors to one other generates another vector in the same plane, even if this plane is submerged in a 3-D space. This is because C is a subspace of F n (or a subring of factor ring). Therefore, the code C passes the ideal test and is a GF(2)[x]/ [(x n 1)] ideal. In this case, error correction is feasible since the Hamming distance between the codewords is larger than 0.

To put it simply, the GF(2)[x] polynomial ring is a Primary Ideal Domain, meaning each of its ideals is principal. We're dealing with (x n - 1) in this scenario. The GF(2)[x]/ [(x n 1)] factor ring is neither a field nor a PID. Every one of its values, on the other hand, is of paramount importance ([12], 245). There is just one polynomial g(x) that generates our code C, and it is called the generator polynomial. The generator polynomial is the monic polynomial with the lowest degree (for a certain code) that belongs to C and may be used to produce every element of C by multiplying it by elements of GF(2)[x] modulo (x n 1). Every ideal of GF(2)[x]/ [(x n 1)] has a single such polynomial, and each such instance divides (x n1) ([13], 32). As a result, finding all the irreducible components of (x n1) is required to produce all possible cyclic codes for each given value of n. If g(x) has all the divisors of (x n > 1), it is feasible to generate polynomials with all these components. For example, if g(x) is chosen to have degree n > k, a linear code is generated, and the generator matrix may be constructed from the simple assertion m[g(x)] g(x) = c[g(x)]. In addition, a polynomial h(x) exists such that g(x)h(x) = (x n 1), resulting in the check matrix.

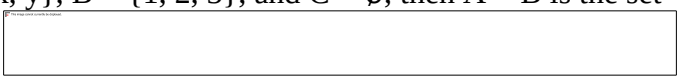
The length and width of cyclic codes can easily be altered during the creation process. To make matters even more complicated, c(x) codewords aren't always evenly spaced across F n, which implies that determining the smallest distance between any two codewords is impossible, particularly as n grows. At the beginning of the cycle of BCH codes, a new constraint is introduced that allows the minimum distance d to be specified. There's a risk of confusion here since, as we've just shown, the vector field of F n has the same cardinality as the field of 2n GF(2n), and we've just spent substantial work proving that it is a ring, not a field. Cardinality alone does not guarantee isomorphism. When multiplying components modulo distinct ideals, it becomes clear that this vector field of remainders cannot be viewed independent of the ideal that formed it as a factor ring.

Cartesian Products and Mappings

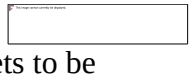
Given sets A and B, we can define a new set A × B, called the Cartesian product of A and B, as a set of ordered pairs. That is,

$$A \times B = \{(a, b): a \in A \text{ and } b \in B\}.$$

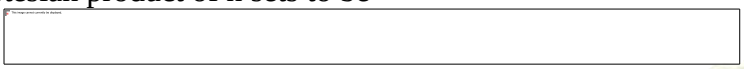
Example 3 If A = {x, y}, B = {1, 2, 3}, and C = ∅, then A × B is the set



And



We define the Cartesian product of n sets to be



If A = A1 = A2 = · · · = an, we often write a for A × · · · × A (where A would be written n times). For example, the set R 3 consists of all of 3-tuples of real numbers.

Relations are subsets of A B. This is the specific sort of relation in which for every element an in A, there is an element b in B that is unique to that element; another way of putting this is that for every element in A, the mapping (or function) (a, b) f assigns to it. In most cases, we use the notation f: A f B. F(a) = b is used instead of (a, b) – A–B, or (a, a) = (a, b): A–B In mathematics, the set A is known as the f-domain.

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

The range or image of f is referred to as A function's input values and output values may be conceptualized as a domain and range, respectively.

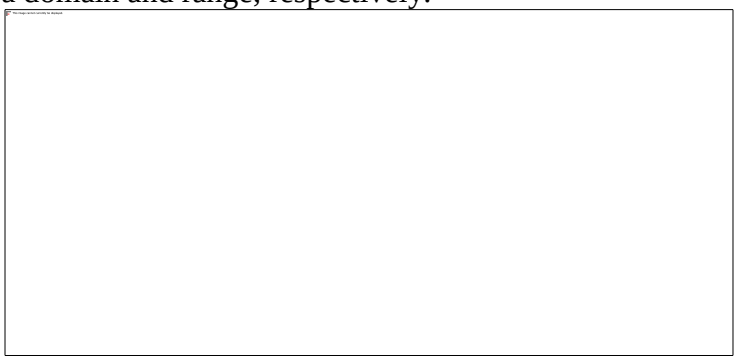


Figure 1 Mappings

Example 1 Suppose A and B are 1, 2, 3 and a, b, c respectively. Relationships f and g between A and B are shown in Figure 1. In f, the relationship between A and B may be described as a mapping, but the relationship between A and B can't be described as a mapping since g (1) = a and b.

It is typically feasible to make a list of what the function performs to each individual element in the domain given a function f: A B. There are certain functions, however, that do not lend themselves well to this kind of description. Functions that take real numbers and transform them into their cubes, such as the function f: R = R, are mapped to their cubes by writing f: R = R.

Let's have a look at the f: Q Z connection provided by f(p/q) = p. 1/2 is equal to 2/4, but what about f (1/2)? Because it lacks definition, this relationship cannot be a mapping. If each element in the domain is assigned to a distinct element in the range, then the relation is well-defined.

Maps that are onto or subjective if the image of the map is the same as the image of the map itself, i.e., f (A) = B, are known as onto maps. F is onto when there is an A for each B in which the f (a) Equals the f(b) of the other. A map might be injective or one-to-one. A1 6= a2 implies that f(a1) 6= f. (a2). One-to-one functions are defined as f (a1) = f(a2) = a1. Injective refers to a map that is both one-to-one and onto.

Example 2 Let f(n) = n/1 be the definition of f: Z Q. Then f is one-to-one but not onto. If you want to know how to calculate the difference between Q and Z, you may use the formula g(q/q) = p. Although g is a one-to-one function, it is not onto.

It is possible to create a third function from a set of two existing functions by reusing one of those functions' regions as the domain for the third function. There are two mappings that may be used to express this. Define a new map, the composition of f and g from A to C, by (g ◦ f) (x) = g (f(x)).

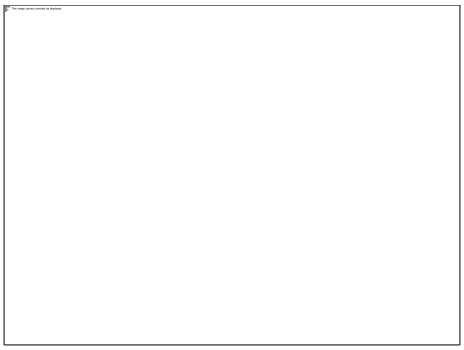


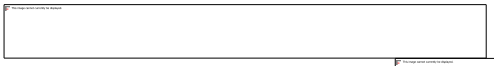
Figure 2 Composition of maps

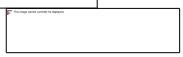
Example 3 If you'd want to see how this works, you may look at the diagram in Figure 2. (a). Figure 1.2 shows how these functions, g f: A C, come together (b).

Example 4 Let

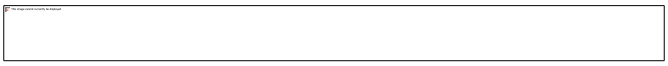
Then,

And

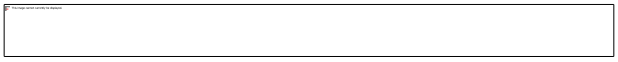


In general, order makes a difference; that is, in most cases 

Example 5 Sometimes it is the case that  and 
Then,

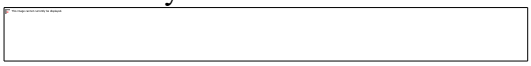


And



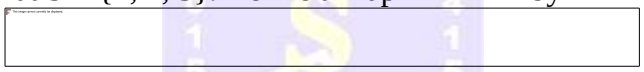
Example 6 Given a 2 × 2 matrix

We can define a map TA: R 2 → R 2 by

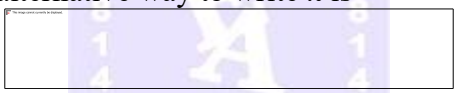


For (x, y) in R 2 This is matrix multiplication; that is,

Maps from R n to R m given by matrices are called linear maps or linear transformations.
Example 7 Suppose that S = {1, 2, 3}. Define a map π: S → S by



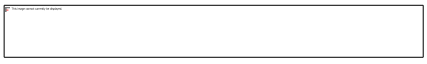
This is an injective map. An alternative way to write π is



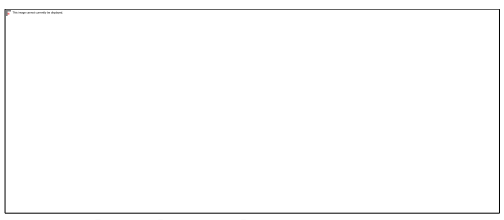
For any set S, a one-to-one and onto mapping π: S → S is called a permutation of S.
Theorem 1 Let f: A → B, g: B → C, and h: C → D. Then

1. There are two ways to combine mappings: (hg)f = (h + g) f.
2. The mapping g f is one-to-one if f and g are both one-to-ones.
3. Assuming that both of the following conditions are met.
4. 4. Assuming that the two variables f and g are both injective, then g f.

Proof (1) and (2) will be shown by us (3). There is no need to complete the second section of the assignment. Part (4) immediately follows Parts (2) and (3).
(1) We must show that

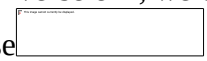


For a ∈ A we have



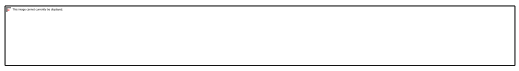
If f and g are both onto functions, then this is the case. We must prove that a A exists such that (g – f)(a) = g(f(a) = c. However, because g is onto, there is a b ∈ B such that g(b) = c. Similarly, f(a) = b is true for a A. Accordingly,

We shall use idS or id to represent the identity mapping from S to itself if S is any set. Create an id(s) = s map for every s > S and use it to define this map. To put it another way, the reverse function of a function is just "undoing" the function; in other words, the mapping of B to A and A to B is known as an inverse mapping of the mapping of B to A and A to B. If a map has an inverse, it is referred to be invertible. For the inverse of f, we often use the notation f 1.

Example 8 The function  has inverse  by Example 8.

Example 9 F(x) = e^x; F(x) = ln X, are the natural logarithm and the exponential functions, respectively, when the domains are well chosen. Notice that.

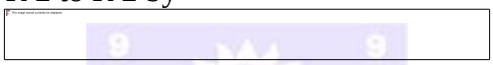
And



Whenever composition makes sense

Example 10 Suppose that,

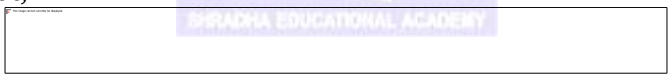
Then A defines a map from R 2 to R 2 by



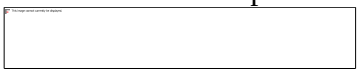
By simply inverting the matrix A, we can obtain the inverse map of TA,  in this example,

Hence, the inverse map is given by,

It is easy to check that,

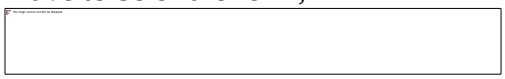


Not every map has an inverse. If we consider the map

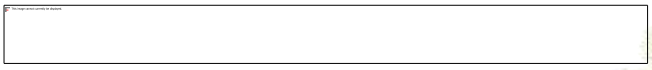


Given by the matrix,

Then an inverse map would have to be of the form,

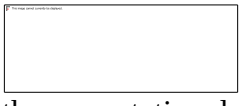


And

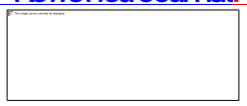


For all x and y clearly, this is impossible because y might not be 0.

Example 11 Given the permutation,



On S = {1, 2, 3}, it is easy to see that the permutation defined by



Is the inverse of π. In fact, any injective mapping possesses an inverse, as we will see in the next theorem.

A LOGICAL APPROACH TO ABSTRACT ALGEBRA

For the sake of mathematical logic, this article will look at some of our most recent work in constructive algebra. Constructive algebra may benefit from basic logical considerations, as we show here.

The logical difficulty of abstract algebraic statements and proofs is examined. The geometric and first-order properties of equations will be critical. In general, the two concepts cannot be compared. If a proposition can be proven in a first-order fashion and is expressed in first-order logic, we say that it possesses a basic "analytical" quality. In the same way, if a geometric assertion is true, it has a simple tree-like constructive proof.

As a starting point, we'll look at two simple instances of algebraic logic: the first is an implication between educational assertions, and the second is a geometric and first-order example. We next show a more complex case, which was a mathematical hypothesis and where a first-order formulation is not evident. We can take it a step farther and come up with a logical conclusion. To find a proof, we had to know in advance that we had to use only simple algebraic operations. We next demonstrate based on a specific example courtesy of Kronecker that we may get nontrivial polynomial algorithms in this manner. This is one of the work's central themes: eliminating Noetherian assumptions to prove basic first-order truths. We provide a tangible understanding of the concept of minimum prime ideals in certain difficult cases.

1. Logical complexity

Commutative ring theory is a first-order theory that may be instructional as well as theoretical. In addition to the three symbols for the functions +, and, we also require two constants 0, 1, and the axioms are

$$x + (-x) = 0,\ x + (y + z) = (x + y) + z,\ x + y = y + x,\ x + 0 = x$$

$$X1 = x,\ xy = yx,\ x\,(yz) = (xy)\,z,\ x(y + z) = xy + xz$$

Commutative abstract algebra topics and theorems may be expressed in this language. A globally quantified first-order formula may describe the concept of an integral ring, which is not pedagogical.

$$xy = 0 \rightarrow (x = 0 \vee y = 0)$$

When a theorem can be expressed in a first-order method, it has a proof in first-order logic, according to the first-order logic completeness theorem. Using Birkhoff's completeness theorem, we may even say that there is a purely educational proof if it is further expressed equationally. The program of Hilbert may be viewed in this way, as we will see later.

The inclusion of abstract ideas means that even the simplest theorems in books like Atiyah-Macdonald or Matsumura cannot be stated in a first-order manner. Such fanciful concepts are a waste of time.

(1) First-order subsets of arbitrary ideals, which are specified as subsets and hence not represented in a first-order method,

(2) Secondly, prime, or maximal ideals, whose existence is often dependent on Zorn's lemma,

(3) There are three Noetherian theories.

The non-affectivity of these ideas varies. A broader inductive definition of being Noetherian may be given, although this leaves out the concept of first-order logic. To make matters worse, Zorn's lemma is often used to justify the existence of prime ideals.

The fact that "being nilpotent" implies an infinite number of disjunctions means that it cannot be represented in a first-order manner.

For constructive algebra, G. Wraith lays out the importance of the idea of geometric formula. There are two types of atoms in a positive formula: atoms that are equal and atoms that are equal and atoms that are equal to each other. An exception to this is the false formula of an empty disjunction, and the true formula of an empty conjunction. Aside from that, we provide for infinite disjunction indexed over natural numbers as well as existential quantification1. It is possible to derive geometric formulas by combining two positive formulas. A formula that is both geometric and first-order is a formula that is coherent. There are two special cases to this rule: any positive formula and its negation (the inverse of the positive formula). Horn formula is a specific instance of coherent formula, and it is an implication C = A, in which C is a combination of atomic formulas and A is an atomic formula. This is an example of a Horn formula. The concept of atomic systems is closely related to horn theories [26]. There are several examples of Horn theories, such as educational theories. The phrase "a ring is a field" is an effective approach to convey the idea that,

$$\forall x.\ x = 0 \vee \exists y.\ xy = 1$$

In contrast, the following formula is not geometric, although being classically comparable.

$$\forall x.\ (\neg x = 0) \rightarrow \exists y.\ xy = 1$$

Nilpotence is not first-order, but it may be represented as a positive formula: An is nilpotent only when and only when n > N. To the contrary, the following Horn formula may describe "to be reduced," which is to have just 0 as a powerless element.

$$\forall x.\ x2 = 0 \rightarrow x = 0$$

The concept of a flat module M over a ring R is another common example of a geometrically stated concept. If P Q = 0, we can find an RQ and a MQ such that QQY = X and P Q = 0 for any RQ or MQ with the same row vector coefficients in R and M respectively. This assertion implies an endless disjunction over natural numbers since we don't specify the magnitude of Q. A flat module is thus not a first-order concept, but rather a geometry-based one.

Barr's theorem emphasizes the significance of geometric formula, as did G. Wraith.

KRONECKER'S THEOREM

These findings, which are given in first-order logic and are a priori far removed from real calculations, may be utilized to get specific computations on polynomials, as we demonstrate in this section. Kronecker theorem: abstract version of Serre's theorem is easier to understand than Serre's theorem since it does not need complex calculations. Kronecker's method may be derived from an abstract proof in this scenario. We begin by proving the abstract version.

Theorem 1. Kdim R n and n+2 elements such as g0, g1, .., gn+1 allow us to identify n + 1 elements such as f0, F1,.., fn that provide the same radical ideal as g0, g1,.., g_n as well.

To put it another way, certain powers of fj and gi are equal to zero when modified by g1, g2...., g_{n+2}. An inductive proof of this theorem is provided in geometric logic. Let's use n = 2 to make things easier. For any x1, x2, and x3 R, there exists p1, p2, and k1 to R and N to N such that k1 to R and N to R.

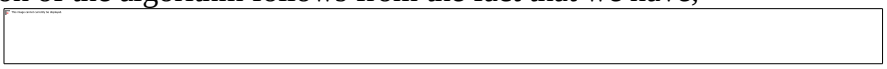
Theorem 2 Given such an algorithm that creates such an algebraic identity having as input x1, x2, x3 R, we may propose another method that produces f0... and f2 as functions of [g0

Given the procedure corresponding to Kdim R2, this approach is much simpler and more transparent, and hence corresponds to the proof in If we know how to solve the following equations, then we know how to solve the following equations, one for each of the following numbers: g1: G2: G3: p1: P2: K1:

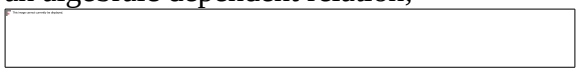
And we can then take,

Where,

The correction of the algorithm follows from the fact that we have,



We show in [6] that Kdim Q[X1..., Xn] n directly. If we choose three items in Q[X1-X2], they are algebraically dependent if we take three elements in Q[X1-X2] (See [28 14].) It is always possible to express such an algebraic dependent relation,



P1, P2, and P3 are equal to Q [X1, X2]. Consequently, we get a solution of Kdim Q [X1, X2] 2. In general, sophisticated calculations are required since this technique relates to finding an algebraic dependent relationship.

After that, we can combine the two techniques to arrive at a nontrivial algorithm for polynomials that yields f0, f1, f2 given g0, g1, g2, and g3, such that g0, g1, g2, and g3 and f0, f1, f2 yield the same radical ideal. According to Kronecker's theorem, the following result has a convincing proof.

Theorem 3 G1, G2, G3, G4, G5, G6, and G7 are given polynomials with rational coefficients, and let m be bigger than the sum of all the polynomials. Make the following n + 1 polynomials in the same set of determinates that have the condition that some power of gi for each I = 1, 2, ..., m is zero mod the first two of these polynomials, f1 and f2, respectively, and fn+1 has the same property as the first two of these polynomials, f1 and f2.

An algebraic variety in C n is the intersection of n + 1 hyper surfaces, according to this geometric interpretation.

CONCLUSION

Strategic use of the counterexample method has a profound impact on students' capacity for deductive reasoning. Students' usage of logical inductions was streamlined thanks to enhancements made possible by The Planning Reason in their digital evidence. The ability of pupils to recognize scientific instances and to determine and employ scientific representations was previously thought to be a limiting factor in their performance with digital evidence. Students' ability to make a connection between their own logical thought and the quantitative aspect of productive scientific information is a result of their own digital knowledge acquired via earlier study. To conclude the logical introduction of the Enlightenment, a study of the causes of the movement's development and an improvement in students' logical grasp of their own recommendations are both viable analytical options. It is possible that the association between pupils who are ready for rational thinking and those who are not may highlight the need for more careful preparation and training on the part of teachers in the main classroom. When carrying out the investigations to fortify conceptual capability, it is important to keep the aforesaid caveats in mind.

REFERENCES

[1] Burris, Stanley N.; Sankappanavar, H. P. (2010), A Course in Universal Algebra

[2] Byrnes J. P., Takahira S. (1993). Explaining gender differences on SAT-math items. Dev. Psychol. 29 805–810 10.1037/0012-1649.29.5.805

[3] Carraher D. W., Schlieamann A. D., Brizuela B. M., Earnest D. (2006). Arithmetic and algebra in early mathematics education, J. Res. Math. Educ. 37 87–115

[4] Charles C Pinter (2015) A Book of Abstract Algebra Second Edition ISBN 978-0-486-47417-5

[5] Chazan D., Yerushalmy M. (2003). "On appreciating the cognitive complexity of school algebra: Research on algebra learning and directions of curricular change," in A Research Companion to Principles and Standards for School Mathematics, eds

Kilpatrick J., Martin W. G., Schifter D. (Reston, VA: NCTM) 123–135

[6] Cohors-Fresenborg E., Kramer S., Pundsack F., Sjuts J., Sommer N. (2010). The role of metacognitive monitoring in explaining differences in mathematics achievement. ZDM 42 231–244 10.1007/s11858-010-0237-x

[7] Collins, A. The changing infrastructure of education research. In Issues in Education Research; Lagemann, E., Shulman, L., Eds.; Jossey-Bass: San Francisco, CA, USA, 1999; pp. 289–298

[8] Collins, A. Towards a design science of education. In New Directions in Educational Technology; Scanlon, E., O'Shea, T., Eds.; Springer: Berlin, Germany, 1992; pp. 15–22

[9] Collins, A.; Joseph, D.; Bielaczyc, K. Design research: Theoretical and methodological issues. J. Learn. Sci. 2004, 13, 15–42

[10] Conceicao, S.; Sherry, L.; Gibson, D. Using developmental research to design, develop and evaluate an urban education portal. J. Int. Learn. Res. 2004, 15, 271–286.

[11] Copeland, W. D.; Doyle, W. Laboratory skill training and student teacher classroom performance. J. Exp. Educ. 1973, 42, 16–21

[12] David Ross. Aristotle. Barnes and Noble, 5th revised edition, 1964.

[13] David S. Dummit , Abstract Algebra , 3rd Edition ISBN -13:978-0471433347.

[14] Davis, E.A.; Palincsar, A.S.; Smith, P.; Arias, A. K. S. Educative Curriculum Materials: Uptake, Impact, and Implications for Research and Design. Educ. Res. 2017, 46, 293–304

[15] Scriven, M. The Logic of Evaluation, 1st ed.; Edgepress: Iverness, CA, USA, 1980.