Review of the book:
Introduction to Abstract Algebra

by Jonathan D. H. Smith
Iowa State University, Ames, Iowa, USA
ISBN: 978-1-4200-6371-4

Frédéric A. B. Edoukou
Nanyang Technological University, Singapore
SPMS, Division of Mathematical Sciences
SPMS-04-01, 21 Nanyang Link, Singapore 637371
E. mail: abfedoukou@ntu.edu.sg

October 11, 2010

1 What the book is about

The book of Jonathan D. H. Smith, "Introduction to Abstract Algebra" is a careful treatment of the principal topics of Abstract Algebra in 327 pages. It contains 11 chapters (318 pages) and an index of terms (9 pages). There is no bibliography. Taking a different approach from several books, it helps the reader to have a solid introduction to abstract algebra and establishes the link between it and the cryptographic world in many "Study projects". The first chapters, Chapter 1 (Numbers), Chapter 2 (Functions) and Chapter 3 (Equivalence) are an introduction to the arithmetical proprieties of the integers, functions, composite functions, relations on arbitrary sets which will be used to formalize abstract and sophisticated algebraic structures, Groups and Monoids (Chapter 4), Rings (Chapter 6), Fields (Chapter 7) and properties, Homomorphisms (Chapter 5) and Factorization (Chapter 8). In the final chapters the author present more advanced topics such as Modules (Chapter 9), Groups actions (Chapter 10) and Quasigroups (Chapter 11). The following will summarize the content of each chapter.

Chapter 1: Numbers, This chapter starts with the introduction of the order relation. It has been proved that $(\mathbb{R}, \leq)$ and $(\mathbb{N}, |)$ are ordering sets. Based on the Well-Ordering Principle, the author shows the principle of induction, the division algorithm and the first part of the Fundamental Theorem of Arithmetic (Existence of factorizations). The second part of the Fundamental Theorem of Arithmetic (Uniqueness of factorizations) and some arithmetical properties on the greatest common divisors, the least common multiple are established. The Euclidean algorithm is presented in a new version using matrix equations.

Chapter 2: Functions, Here first of all, the author recalls the notion of functions, and some classical functions. By the help of semigroups of functions he introduces the monoid of functions. There is a study of the injectivity and surjectivity of a function via retraction and section. He also shows how domain and codomain are integral parts in the specification of a function. The isomorphisms (bijections) which combine both injection and surjection are introduced. This chapter ends on the groups of permutations defined as a monoid of bijective functions. An interesting application to this last notion into the cryptographical world is given in the "Study Project" 3 and 4, where the reader should find the inverse of the "keyboard permutation" or a permutation to decode a text.

Chapter 3: Equivalence, This chapter starts with the definition of the kernel relation of a function, whose properties (reflexivity, symmetry and transitivity) are formalized in the important notion of equivalence relations. Equivalence relations are used to introduce rational numbers and modular arithmetic. They also lead to the First Isomorphism Theorem which states that every function can be written as a composition of an injection, an isomorphism and a surjection. It has also been proved that irrational numbers exist and in the "Study Projects" 2, good rational approximations for some irrational numbers can be found by continued fractions.

Chapter 4: Groups and monoids, In this chapter, the key properties of semigroups of functions, monoids of functions and groups of permutations are used to formalize central concepts of semigroups, monoids and groups. The direct product construction is a method used to obtain new semigroups, monoids and groups from the given ones. A group is constructed from the set of units of a monoid. Subsemigroups, submonoids and subgroups are new semigroups, monoids and groups producing inside semigroups, monoids and groups. The subgroup test as well as the characterization of subgroups of the integers via the Well-Ordering Principle are given. Cosets of semigroups and related properties are introduced to prove Lagrange's Theorem useful for limiting the possible subgroups of a given finite group. Finally it has been proved that the body of the multiplication table of a finite group is a Latin square.

Chapter 5: Homomorphisms, In this chapter the author introduces the homomorphisms of semigroups, functions which preserve the algebraic structure and characterizes them by their corresponding graphs. For semigroup, monoid and group homomorphisms, the image carries the corresponding algebraic structure. Normal subgroups are presented via the equivalence class of the kernel relation of the identity of the domain of group homomorphism. The quotient group of a group by normal subgroups are introduced. The First Isomorphism Theorem is revised for groups and leads to the classical Chinese Remainder Theorem. Finally Cayley's Theorem which shows isomorphism between abstract group and group of permutations is established. Applications of these notions to information theory are given by the two first "Study projects": error-correcting codes and Hamming codes.

Chapter 6: Rings, In this chapter, the author studies the structure of nonunital and unital rings from a commutative group and gives several examples. The distributivity laws which are supposed to be satisfied in the ring structure generate many identities. The concept of subrings is defined and a test is given to recognize them. Thus, the ring of Gaussian integers is constructed as subring of the ring of complex numbers. The characteristic of a ring is defined via the order of its prime subring. The homomorphisms of rings are approached and some examples such as inclusion of subrings, projections, insertions have been studied. Further examination of the relationship between nonunital and unital rings shows that every nonunital ring embeds into a unital ring. Ideals are presented via the absorption property of the kernel group of a homomorphism of ring. Ideals in the ring of integers and their relationship with the divisibility relation are explained. Quotient rings of rings by ideals and the factorization of ring homomorphisms under a strengthened version of the First Isomorphism Theorem are studied. Finally the ring of polynomials in one indeterminate is introduced. Applications of these notions to information theory are given by the second "Study projects": check digits.

Chapter 7: Fields, In this chapter, the author defines integral domains (ID), zero divisor of a ring, establishes the connection between them and enumerates several examples. Some inequalities for the degrees of the sum and the product of two polynomials over a ring are given. It has been proved that when the ring is an (ID) the last inequality becomes an equality. A field is defined here as an (ID) in which the nonzero elements form a group. Thus, every finite (ID) is a field and several examples of fields are constructed. The structure of principal ideal domain (PID) of the ring of polynomials over a field, the representation of the elements of its quotient by an ideal, the relation between the number of roots of a polynomial and its degree are investigated via the division algorithm for polynomials over a field. The irreducibility of polynomials is studied, and irreducible polynomials are used to construct new fields. The Lagrange interpolation is discussed as an application of fields to the specification of functions. Finally the construction of the fields of fractions of an (ID) is done.

Chapter 8: Factorization, In this chapter, the author introduces the concepts of being irreducible and being prime elements in an (ID) as well as the relationship between them (prime implies irreducible) via the factorization. Noetherian domains are defined as rings satisfying the ascending chain condition (ACC). The author proves the factorization into irreducible factors in Noetherian domains, (PID) implies (ACC) and subsequently the factorization in (PID). The idea of unique factorization domains (UFD) is formalized from the Fundamental Theorem of Arithmetic. Thus it has been proved that an (ID) in which every nonzero and nonunit element admits a factorization in a product of irreducible elements is a (UFD) if and only if irreducible implies prime. One result states that every (PID) is a (UFD). The ring of polynomials over a field is studied as a (UFD), in which the Kronecker's Theorem shows that each nonconstant polynomial has a root in some extension field. The multiplicity of this root is analyzed by the help of formal derivative. Kronecker's Theorem leads to the splitting and the splitting fields of a nonconstant polynomial. The uniqueness of these splitting fields is proved to within isomorphim. This chapter ends on the theory of finite fields where it is proved that the group of nonzero elements is cyclic, the order of a finite field is a power of a prime number p (the characteristic of the field) and inversely for each power $q = p^n$ of a prime number p there is a unique field of order q (called the Galois field $GF(q)$) within isomorphism. It has been proved that the only possible orders of subfields of $GF(q)$ are the powers p^r for r a divisor of n.

Chapter 9: Modules, This chapter begins with the study of the endomorphisms of an arbitrary abelian group (A, +, 0). First of all, End A, the set of all endomorphisms of the abelian group A carries a group structure. End A carries also a unital ring structure (End A, +, $\circ$) in which the multiplicative group structure is given by the functional composition. Secondly, analogous Cayley's Theorem for rings is given. It states that there is always an injective unital ring homomorphism from unital rings R to the endomorphism ring End (R, +, 0) of the additive group (R, +, 0) of R. If there is a unital ring homomorphism σ from unital ring R to the endomorphism ring End A of the group A, then the abelian group A is defined as a R-module (A, +, σ). Several examples of modules and a new characterization of modules leading to the standard (well known) definition of modules are given. Submodules, intersections of submodules and submodules generated by a subset are studied via R-linear combination. The notions of finitely generated modules, R-homomorphism, R-isomorphism, direct sums of R-modules and internal direct sums of submodules are explained. For abelian groups, direct sums and direct products are the same. Results characterizing modules that are isomorphic to direct sums and those that are internal direct sums of a family of their submodules are proved. Free modules, their structure as well as their universality property are studied. The computation of the endomorphism ring of a finite cyclic group of order n is done by the help of the universality property of the abelian group $\mathbb{Z}/n\mathbb{Z}$. The theory of vector spaces is treated as a particular case of modules over a field. Finally it has been proved that a finitely generated, nontrivial abelian group is isomorphic to the direct sums of nontrivial cyclic groups which are quotients of $\mathbb{Z}$ by proper ideals in a finite ascending chain.

Chapter 10: Groups Actions, This chapter starts with the definition of the action λ of a group G on a set X, denoted by (X, G, λ), which is in fact a generalization of Cayley's Theorem. Several actions of a group such as the regular action, the conjugation, and a new characterization for a group action are studied. The stabilizer G_x and the orbit $\lambda_G(x)$ of an element x of X are defined. It has been proved that stabilizers are subgroups of G and orbits of a general group action (X, G, λ) are the classes of an equivalence relation. The action is said to be transitive if there is just one orbit. Transitive actions are studied via homogeneous spaces (the set of left cosets of a subgroup H of G). For an element x of X and an element g of G, x is said to be a fixed point of g under λ if $\lambda_g(x) = x$. The theory of fixed points is largely studied and includes Burnside's Lemma which relates the total number of orbits in a group action (X, G, λ), to the number of points that are fixed by each element of G. When the homomorphism λ is injective, (X, G, λ) is said to be faithful. Several actions regarding to the faithfulness are studied. Thus, for every faithful action (X, G, λ), the group G is isomorphic to a group of permutations of the set X. The First Isomorphism Theorem for groups shows that every action (X, G, λ) induces a faithful action $(X, \overline{G}, \overline{\lambda})$ where $\overline{G}$ is the quotient group $G/\ker(\lambda)$ and $\ker(\lambda)$ is the intersection of the stabilizers G_x of the elements x of X. The inner automorphisms of the group G used to introduce conjugacy and core of subgroups, plays an important role in the study of the stabilizers. This chapter ends on the applications of groups actions to alternating groups and to Sylow Theorems.

Chapter 11: Quasigroups, This chapter studies quasigroups which are sets $(Q, \star)$ that are closed under a multiplication $\star$ for which if the equation $x \star y = z$ holds for elements x, y, z of Q, then the knowledge of any two of x, y, z specifies the third uniquely. Several examples of quasigroups as well as a characterization of finite quasigroup by the structure of Latin square of the body of their multiplication table are studied. The left and right divisions in a quasigroup are defined with their properties, providing new quasigroup multiplications. The opposite multiplication is also another way to obtain new quasigroups by reversing given quasigroup multiplications. Subquasigroups, subquasigroup test, quasigroup homomorphism, quasigroup isomorphism and product of quasigroups are studied. The quasigroup homomorphism respect division. The important concepts of quasigroup homotopy and isotopy are introduced. Isotopy forms an equivalence relation on any set of quasigroups. Principal isotopies are particular isotopies and to within isomorphism, every isotopy is principal, and two quasigroups $(Q, \star)$ and $(Q, .)$ share a Latin square $L(Q)$ built on Q (finite, nonempty set) as the common body of their multiplication tables if and only if they are related by a principal isotopy. Quasigroups with an identity element are called loops. Finally it has been proved that Latin squares built from Q (finite, nonempty set) are the body of the multiplication table of loops, and a loop isotopic to a group is isomorphic to that group; thus two isotopic groups are isomorphic.

2 What the book is like (style)

This is a very interesting book by its style. In fact as we know, most of the books in mathematics pretending to give a basis to students in abstract algebra begin by a small chapter or some notions in logic where they try to lay the foundations of mathematics: the universal quantifiers, the existential quantifiers, and several symbols. In this book the author try to avoid this way of writing. Thus we could not see in the whole book the symbols of inclusion of sets, belong of an element, etc...

When the author refers to an example, theorem, lemma, etc... outside its chapter he puts also the exact page where we can find it. All the chapter of the book have the same structure. The author develops the concepts which should be known deeply in each chapter by giving several examples, pictures and figures to make the ideas concrete.

At the end of each chapter there is a large number of exercises of varying difficulty. There are also the "Study Projects" which are some particular exercises generally much longer and deeper, an extension and advanced topics related to what has been expound in the chapter. There are also chapter notes pointing out variations in the notations and approach used in this book to other authors. The author gives also a short description of all mathematicians whose theories are involved in each chapter.

3 Would you recommend this book

This is an attractive book which could be read by everybody because the author supposes not so much knowledge from the reader and gives all the necessary information to continue the reading from a chapter to the next. The approach used by the author to introduce Modules (Chapter 9) and Group Actions (Chapter 10) is new and innovative. The book is well written even if there are sometimes some misprints (which can be corrected by the reader).

We think that the author misses to lay an emphasis on the polynomials rings in $\mathbb{R}[X]$ and $\mathbb{C}[X]$, the elementary symmetric functions of the roots of a polynomial in Chapter 8, Section 8.4. By the way, the introduction of derivative of polynomial in $K[X]$ should have helped the author to present Taylor formulas and Euler formulas but this is not done. The author studies briefly the field of fractions of $K[X]$ (the fields of rational functions) in Example 7.47 p.177.

The ring of integers $\mathbb{Z}$, the ring of Gaussian integers $\mathbb{Z}[i]$ and the ring of polynomial $K[X]$ over a field K have been studied by the author. The introduction of the absolute value function (Chapter 2, Section 2.1, p.25), the composite function of conjugate function and the squaring function (Chapter 2. Section 2.2, p.27), the degree (Chapter 7, Section 7.2, pp.160-161), the Euclidean division (Chapter 1, Section 1.4, pp.6-7, Chapter 7, Section 7.4, pp.164-165) should have helped the author to define Euclidean Domains (ED) and to show that $\mathbb{Z}$, $\mathbb{Z}[i]$ and $K[X]$ are (ED). Subsequently the result which states that (ED) implies (PID) is one thing we expect to have here in this book.

The author establishes a connection between the important concept of (PID) studied in (Chapter 7, Section 7.5, pp.167-169) with several results in Chapter 8 (Factorization); this is great. We also expect an extension of this connection with Chapter 9. But nothing is said about modules over (PID). We think that the study of the structure of finitely generated abelian groups (Chapter 8, Section 9.8, pp. 240- 242) is an opportunity to establish this connection. Thus, instead of what has been studied by the author, we expect he would study the structure of a finite generated R-module over a (PID) R. Since abelian groups are seen as $\mathbb{Z}$- modules (Example 9.18, p.221), and $\mathbb{Z}$ is a (PID) (Example 7.26, p.167), then Theorem 9.56 p. 240 becomes a consequence of the general result on the structure of a finite generated R-module over a (PID) R.

In Chapter 10 (Section 10.4, pp.263-264), Burnside's Lemma is discussed. We think that as expressed in [2, p.488] this was an accident of history that this result has been affected to William Burnside. In fact it was a result of Georg Frobenuis in 1887 which will become well known when it appeared in the book of William Burnside, Theory of groups of finite order, second edition, Cambridge, 1911. So the author should try to re-establish the truth or to say something like this in Chapter 10, (Section 10.4).

Finally we believe that the readers, students and even experienced researchers may benefit strongly from this book. Moreover we have the pleasure to announce that the author of this book, Jonathan D. H. Smith has put a lot of effort to correct all the 447 exercises (even if there are several misprints). This is again a testimony of the great work he has done. The book of solutions is: Solutions Manual for Introduction to Abstract Algebra, ISBN: 978-1-4200-9478-7, Chapman & Hall/CRC.

As no biographical sketches are given, we suggest the below books to the reader.

4 References

[1] J. Calais, Eléments de théorie des groupes, 3^e édition, PUF 1998.

[2] J. A. Gallian, Contemporary abstract algebra, Seventh Edition, International Edition.

[3] S. Lang, Algebra, (Revised Third Version), GTM 211, Springer-Verlag.

[4] M. Queysanne, Algèbre M. P. et Spéciales AA', Armand Colin Paris. 1964.

[5] J. Querré, Cours d'Algèbre, Maîtrise de Mathématiques, Masson 1976.

[6] J. D. H. Smith, Solutions manual for introduction to abstract Algebra, Chapman & Hall/CRC 2009.

[7] S. Touré, Algèbre, Premier Cycle MP1, EDICEF 1991.

The reviewer is a Research Fellow at Nanyang Technological University in Singapore