History topic: The development of Ring Theory

Article by: J J O'Connor and E F Robertson

September 2004

MacTutor History of Mathematics

[http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html]

Any book on Abstract Algebra will contain the definition of a ring. It will define a ring to be a set with two operations, called addition and multiplication, satisfying a collection of axioms. These axioms require addition to satisfy the axioms for an abelian group while multiplication is associative and the two operations are connected by the distributive laws. A ring is therefore a setting for generalising integer arithmetic. Familiar examples of rings such as the real numbers, the complex numbers, the rational numbers, the integers, the even integers, 2 cross 2 real matrices, the integers modulo m for a fixed integer m, will almost certainly be given in the Abstract Algebra book as will many beautiful theorems on rings but what will be missing are the reasons systems satisfying these particular axioms have been singled out for such intensive study. What motivated this abstract definition of a ring?

In this article we shall be concerned with the development of the theory of commutative rings (that is rings in which multiplication is commutative) and the theory of non-commutative rings up to the 1940's. These two theories were studied quite independently of each other until about 1930 and as

traces of the commutative theory appear first it is with this theory that we begin.

Our comment above that study of a ring provided a generalisation of integer arithmetic is the clue to the early development of commutative ring theory. For example Legendre and Gauss investigated integer congruences in 1801. However, the motivation for generalising arithmetic came mostly from attempts-to prove Fermat's Last Theorem. This theorem, proved as recently as 1995, states:

The equation x^n+ y^n= z^n has no solution for positive integers x, y, z when n > 2.

This statement, thought to have been made in the late 1630's, was found in the marginal notes that Fermat had made in Bachet's translation of Diophantus's Arithmetica.

Attempts to prove this result led to proofs in the following special cases:

- n = 4 Fermat about 1640
- n = 3 Euler 1753
- n = 5 Legendre and Dirichlet 1825
- n = 14 Dirichlet 1832
- n = 7 Lamé 1839

Euler's work on the case n = 3 involved extending ordinary integer arithmetic to apply to the ring of numbers of the form a + b√-3 where a, b are integers. However, Euler failed to grasp the difficulties of working in this ring and made certain assertions which, although true, would be hard to justify.

In 1847 Lamé announced that he had a solution of Fermat's Last Theorem and sketched out a proof. Liouville suggested that the proof depended on a

unique decomposition into primes which was unlikely to be true. However, Cauchy supported Lamé. The argument which followed indicates the totally different atmosphere surrounding mathematical research of this period from that which we know today. Perhaps we could illustrate the point causing this argument. Complex numbers of the form a + b√-3, where a, b are integers, form a ring. A prime number in this ring is defined in an analogous way to a prime integer, namely a number whose only divisors of the form a + b√-3 other than itself are those numbers with multiplicative inverses. In this ring 4 can be written as a product of prime numbers in two different ways

4 = 2 * 2 and 4 = (1 + √-3) * (1 -√-3).

Gauss had proved around 1801 that numbers of the form a + b√-1, where a, b are integers, could be written uniquely as a product of prime numbers of the form a + b√-1 in an analogous manner to the unique decomposition of an integer as a product of prime integers. In fact, numbers of the form a + b +c2 where a, b, c are integers and is a complex cube root of 1, also have unique factorisation, and this can be used to prove the n = 3 case of Fermat's last Theorem.

The argument following Lamé's announcement was settled by Kummer who pointed out that he had published an example in 1844 to show that the uniqueness of such decompositions failed and in 1846 he had restored the uniqueness by introducing "ideal complex numbers". He then saw the relevance of his theory to Fermat's Last Theorem. The popular story that Kummer invented "ideal complex numbers" in an attempt to correct an error in this proof of Fermat's Last Theorem is almost certainly false; see Edwards [1]. In 1847, just after Lamé's announcement, Kummer used his "ideal complex numbers" to prove Fermat's Last Theorem for all n < 100 except n = 37, 59, 67 and 74.

Up to this point we are still firmly within the realms of number theory but the genius of Dedekind pinpointed the important properties of the "ideal complex numbers". Dedekind defined an "ideal", characterising it by its now familiar properties: namely that of being a subring whose elements, on being multiplied by any ring element, remain in the subring. Ring theory in its own right was born together with an early hint of the axiomatic method which was to dominate algebra in the 20thCentury. Dedekind also introduced the word "module" (early spelling: "modul") in 1871 although its initial definition was considerably more restricted than the present definition, being first introduced as a subgroup of the additive group of a ring; the term is now used for a "vector space with coefficients from a ring".

Prime numbers were generalised to prime ideals by Dedekind in 1871. A prime ideal is an ideal which contains the product of two elements only if it contains one of the two elements. For example all integers divisible by a fixed prime p form a prime ideal of the ring of integers. This trend towards looking at ideals rather than elements marks an important stage in the development of the theory.

In 1882 an important paper by Dedekind and Weber accomplished two things; it related geometric ideas with rings of polynomials and extended the use of modules. It is important to realise that at this stage rings of polynomials and rings of numbers were being studied, but it was to be another 40 years before an axiomatic theory of commutative rings was to be developed bringing these theories together.

Although the concept of a ring is due to Dedekind, one of the first words used was an "order" or "order-modul". This term, invented by Kronecker, is still used today in algebraic number theory. Dedekind did introduce the term "field" (Körper) for a commutative ring in which every non-zero element has

a multiplicative inverse but the word "number ring" (Zahlring) or "ring" is due to Hilbert. Hilbert, motivated by studying invariant theory, studied ideals in polynomial rings proving his famous "Basis Theorem" in 1893. Special cases of this theorem had been studied by Gordan from 1868 and on seeing Hilbert's proof Gordan is said to have exclaimed "This is not mathematics, it's theology".

The decomposition of an integer into the product of powers of primes has an analogue in rings where prime integers are replaced by prime ideals but, rather surprisingly, powers of prime integers are not replaced by powers of prime ideals but rather by "primary ideals". Primary ideals were introduced in 1905 by Lasker in the context of polynomial rings. (Lasker was World Chess Champion from 1894 to 1921.) Lasker proved the existence of a decomposition of an ideal into primary ideals but the uniqueness properties of the decomposition were not proved until 1915 by Macaulay.

I D Macdonald notes in his article [2] that algebra texts such as that of Weber [4] in 1895 contained axioms for groups similar to many present-day texts. However, axioms for rings are not given by Weber and the axiomatic treatment of commutative rings was not developed until the 1920's in the work of Emmy Noether and Krull. Emmy Noether, one of the world's greatest women mathematicians, was a student of Gordan's. In about 1921 she made the important step, which we commented on earlier, of bringing the two theories of rings of polynomials and rings of numbers under a single theory of abstract commutative rings. Discrimination made it difficult for her to publish her work and it was not until Van der Waerden's important work on Modern Algebra [3] was published in 1930 that Noether's results become widely known.

In contrast to commutative ring theory, which as we have seen grew from number theory, non-commutative ring theory developed from an idea which, at the time of its discovery, was heralded as a great advance in applied mathematics. Hamilton attempted to generalise the complex numbers as a two dimensional algebra over the reals to a three dimensional algebra. Hamilton, who introduced the idea of a vector space, felt that this three dimensional analogue of the complex numbers would revolutionise applied mathematics but he struggled unsuccessfully with the idea for many years. In 1843 inspiration struck Hamilton - the generalisation was not to three dimensions but to four dimensions and the commutative property of multiplication no longer held. The quaternion algebra, as Hamilton called this four dimensional algebra, was widely used in applied mathematics (where it was later replaced by the vector product) and it launched non-commutative ring theory.

Matrices with their laws of addition and multiplication were introduced by Cayley in 1850 while, in 1870, Pierce noted that the now familiar ring axioms held for square matrices - another early example of the axiomatic approach to rings. The greatest early contributor to the theory of non-commutative rings was the Scottish mathematician Wedderburn. In 1905 he proved that every finite division ring (a ring in which every non-zero element has a multiplicative inverse) is commutative and so is a field. In 1908 Wedderburn had the important idea of splitting the study of a ring into two parts, one part he called the radical, the part which was left being called semi-simple. He used matrix rings to classify the semi-simple part. The importance of this work can be seen from the fact that the next 56 years were spent generalising it. We should point out that Wedderburn did not prove his results for rings but rather for hypercomplex systems - a term no longer in use which meant a finite dimensional algebra over a field.

The Wedderburn theory was extended to non-commutative rings satisfying both ascending and descending finiteness conditions (called chain conditions) by Artin in 1927. It was not until 1939 that Hopkins showed that only the descending chain condition was necessary.

Around the 1930's the theories of commutative and non-commutative rings came together and the ideas of one began to influence the other. For example, chain conditions in both commutative and non-commutative rings are investigated at much the same time. Modules, originally introduced for commutative rings, were studied for general rings. Some ideas, however, were slow to filter from one theory to the other, for example, prime ideals for non-commutative rings were not studied until 1949 by McCoy.

In the 1940's attempts were made to prove results of the Wedderburn-Artin type for rings without chain conditions. The breakthrough here was made in 1945 by Jacobson who was a student of Wedderburn's using ideas of Perlis in 1942. It is interesting to note that this fundamental work by Jacobson hinges on the idea of the "Jacobson radical" of a ring which is an analogue of a group theory idea due to Frattini as early as 1885.