A Brief History of Ring Theory

by Kristen Pollock
Abstract Algebra II, Math 442
Loyola College, Spring 2005
1. Introduction

In order to fully define and examine an abstract ring, this essay will follow a procedure that is unlike a typical algebra textbook. That is, rather than initially offering just definitions, relevant examples will first be supplied so that the origins of a ring and its components can be better understood. Of course, this is the path that history has taken so what better way to proceed?

First, it is important to understand that the abstract ring concept emerged from not one, but two theories: commutative ring theory and noncommutative ring theory. These two theories originated in different problems, were developed by different people and flourished in different directions. Still, these theories have much in common and together form the foundation of today's ring theory. Specifically, modern commutative ring theory has its roots in problems of algebraic number theory and algebraic geometry. On the other hand, noncommutative ring theory originated from an attempt to expand the complex numbers to a variety of hypercomplex number systems.

2. Noncommutative Rings

We will begin with noncommutative ring theory and its main originating example: the quaternions. According to Israel Kleiner’s article “The Genesis of the Abstract Ring Concept,” [2], these numbers, created by Hamilton in 1843, are of the form \(a + bi + cj + dk\) \((a, b, c, d \in \mathbb{R})\) where addition is through its components and multiplication is subject to the relations \(i^2 = j^2 = k^2 = ijk = -1\). Thus, each number \(i, j, \text{and } k\) acts like the complex number \(\sqrt{-1}\) and the whole collection is an extension of \(\mathbb{C}\). In particular these numbers satisfy the usual algebraic properties such as being distributive and associative. Today, this kind of system is called a skew field or a division algebra. Hamilton’s original goal was to define an algebra of three-dimensional vectors in which multiplication would represent the composition of rotations. This would have extended a property of the complex numbers where multiplication by \(i\) is equivalent to rotating the complex plane by 90°. However, this turned out to be impossible, so he moved on to quadruples of reals and created ‘the algebra of quaternions.’ Although the ‘pure’ quaternions did end up yielding the necessary components for three-space rotations, it took many other mathematicians several years to come around to Hamilton’s point of view. Eventually, these quaternions sparked the exploration of different number systems which would extend both the real and complex numbers. Further examples of hypercomplex number systems are octonions, exterior algebras, group algebras, matrices, and biquaternions.

The movement towards defining more number systems spanned the forty years following Hamilton’s discover of quaternions in 1843. These extended number systems form what are called semi-simple algebras. In 1890, Cartan, Frobenius, and Molien proved that any “finite-dimensional semi-simple algebra over the real or complex numbers is a finite unique direct sum of simple algebras. These, in turn, are isomorphic to matrix algebras with entities in division algebras” [2]. Representing Quaternions as matrices allows for Quaternion addition and multiplication to correspond to matrix addition and multiplication. Here is a representation of the Quaternion \(a + bi + cj + dk\) as a 4 \times 4 matrix over \(\mathbb{R}\) where the conjugate of the
A Brief History of Ring Theory

Kristen Pollock

quaternion corresponds to the transpose of the matrix:

\[
\begin{bmatrix}
a & -b & d & -c \\
b & a & -c & -d \\
-d & c & a & -b \\
c & d & b & a \\
\end{bmatrix}
\]

The Cartan-Frobenius-Molien theorem includes the Quaternions, and essentially describes all possible similar extensions. For example, if we have a 12 dimensional semi-simple algebra \(A\) over the real numbers, it must be a product of matrix algebras: \(\mathbb{M}_{n_1}(\mathbb{R}) \times \mathbb{M}_{n_2}(\mathbb{R}) \times \ldots\) where \(\dim \mathbb{M}_{n_1}(\mathbb{R}) = n_1 \times n_1 = n_1^2\). Thus we must have \(n_1^2 + n_2^2 + \cdots = 12\). It can be seen then that \(n_1 = n_2 = n_3 = 2\) and so \(A = \mathbb{M}_2(\mathbb{R}) \times \mathbb{M}_2(\mathbb{R}) \times \mathbb{M}_2(\mathbb{R})\). (Note: keep \(\mathbb{M}_n(\mathbb{R})\) in mind as one of the examples that will be incorporated later in our definition of rings). Furthermore, Wedderburn, in 1907, generalized this result and extended it to algebras over arbitrary fields. His theorem forms the basis of all modern ring-theoretic structure theorems.

3. Commutative Rings

3.1. Algebraic Number Theory. This brings us now to commutative ring theory and its many components, of which we will first consider algebraic number theory. More specifically, algebraic number theory arose from three central number-theoretic problems: reciprocity laws, binary quadratic forms, and Fermat’s Last Theorem. The following examples will further explain and illustrate the similarities and differences between these problems and serve as concrete, significant examples in commutative ring theory.

(i) First, we begin with the famous Bachet equation, \(x^2 + k = y^3\). Let us consider the case for \(k = 2\). The issue here has two parts: finding some solutions and showing that these are all of the solutions. Thus, the equation \(x^2 + 2 = y^3\) can be solved over \(\mathbb{Z}\) yielding \(x = \pm 5\) and \(y = 3\) as solutions. To find all solutions, one would have to factor \(x^2 + 2\) so that \((x + 2i)(x - 2i) = y^3\). Now our equation is in the domain \(D = \{a + b\sqrt{2i} \mid a, b \in \mathbb{Z}\}\). It can be shown that \(D\) is a UFD (unique factorization domain) and that \(x + \sqrt{2i}\) and \(x - \sqrt{2i}\) are relatively prime in \(D\). Since their product is a cube – namely, \(y^3\) – each factor must be a cube in \(D\). Specifically, \(x + \sqrt{2i} = (a + b\sqrt{2i})^3\) where \(a, b\) are in \(\mathbb{Z}\). Cubing and then solving for the coefficients will give \(x = \pm 5\) and \(y = 3\) as the only solutions of the Bachet equation for \(k = 2\). This process could not have been completed without the use of complex integers.

(ii) Next, in reference to the reciprocity laws, Gauss introduced the domain \(G = \{a + bi \mid a, b \in \mathbb{Z}\}\) in order to state the biquadratic reciprocity law. Specifically, to determine which integers are sums of two squares, a concrete way of thinking about it is to factor the right side of \(n = x^2 + y^2\). This would yield \(n = (x+yi)(x-yi)\) which is in the domain \(G\) of Gaussian integers and so we have again a factoring problem. The crucial case of solving \(n = (x+yi)(x-yi)\) is when \(n\) is a prime integer. This means that the main question is which primes in \(\mathbb{Z}\) stay prime considered as elements of \(G\). This is easily stated (but takes some time to prove) an odd prime \(p\) stays odd in \(G\) if and only if \(p = 3 \mod 4\). Proving this, and applying it to the original problem, shows how the arithmetic of \(G\) plays a critical role. Thus, we have taken a problem using arithmetic of natural numbers and extended it to a problem involving arithmetic in the ring \(G\) of Gaussian integers. This problem is
only one instance of the problem of representing integers by binary quadratic forms $ax^2 + bxy + cy^2$ ($a, b, c \in \mathbb{Z}$). The typical approach is to factor $ax^2 + bxy + cy^2$ and consider the resulting equation in a domain of complex integers.

(iii) Finally, we look at Fermat’s Last Theorem which states that $x^n + y^n = z^n$ has no nontrivial integer solutions for $n > 2$. Let us consider the case for $n = 3$ and factor the left side as follows: $(x + y)(x + yw)(x + yw^2) = z^3$ where $w = e^{2\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. We now have an equation that is in the domain $D_3 = \{a + bw \mid a, b \in \mathbb{Z}\}$.

One can show that no solutions exist in this domain without unique factorization, whence $x^3 + y^3 = z^3$ has no solutions over the integers. After many calculations, one can see that doing arithmetic in $D_3$ is easier and more relevant than in $\mathbb{Z}$ and thus, sheds light on an original problem.

All of the previous examples proved to be too difficult to be computed without expanding their domains. Here, additive problems in $\mathbb{Z}$ were solved by translating them into multiplication problems using the domains $D_3$, $G$, and $D$. This all can be made possible using unique factorization in the domain under consideration. Now, $D_3$, $G$, and $D$ are UFD’s but the domains arising from the respective general problems (FLT, binary quadratic forms, and the Bachet equation) are not. For example, factoring the left side of the Bachet equation for $k = 5$ with the domain $\{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ is not a UFD. The problem then became having to restore unique factorization in such domains. This issue was largely faced by Kummer for ideal numbers, Dedekind for ideals, and by Kronecker for divisors.

Dedekind’s solution for establishing unique factorization in more domains took some time, but the results were astounding. After defining the concepts of an ideal and a prime ideal as well as the notion of the domain of integers of an algebraic number field, Dedekind was able to formulate his main theorem. Namely, he concluded that every nonzero ideal in the domain of integers of an algebraic number field is a unique product of prime ideals. This result replaces the idea of unique factorization of elements with the unique factorization of ideals. The reason to do this is that unique factorization often fails for elements but succeeds for ideals.

To understand the main theorem a little better, we will look at the defining characteristics in Dedekind’s work. First, it is important to understand that all of the elements of an algebraic number field $\mathbb{Q}(\alpha)$ are an extension of the domain of integers whose elements are the roots of monic linear polynomials with integer coefficients. He showed that these elements ‘behave’ like integers in that they are closed under addition, subtraction, and multiplication. For example, Dedekind defined the integers of $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ as $\left\{\frac{a + b\sqrt{5}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod{2}\right\}$ rather than $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. This is because the integers of the form $a + b\sqrt{5}$ do not form a UFD. Additionally, he called a set of algebraic integers that is closed under addition, subtraction, and multiplication of $\mathbb{Q}(\alpha)$ orders, which today we would call subrings. This was the essentially the first clear definition of a commutative ring in a concrete setting (that is, the domain $R$ of integers of $\mathbb{Q}(\alpha)$ is the largest order).

Secondly, to comprehend Dedekind’s theory, one must also see his concept of an ideal as a derivative from Kummer’s ideal numbers. Dedekind wanted to characterize the ideal numbers within the domain of $D_p$ of cyclotomic integers. So, for each $\sigma$ he considered the set of cyclotomic integers divisible by $\sigma$. Again, the subsets of $D_p$ are closed when added, subtracted, and multiplied by elements of $D_p$. It was these subsets of $D_p$ that Dedekind called ideals, which motivated the introduction of ideals in arbitrary domains of algebraic integers. Dedekind took his definition
of an ideal one step further and said an ideal \( P \) of \( R \) is prime if its only divisors are \( R \) and \( P \). Here, \( R \) is the “unit” of \( P \) because when multiplying by \( R \), the ideal is left unchanged. Finally, having defined the notion of the domain of integers of an algebraic number field, an ideal, and thus a prime ideal, Dedekind was able to prove his theorem that every nonzero ideal in the ring of integers of an algebraic number field is a unique product of prime ideals.

In the end, although Dedekind’s extensive work on this subject originated from number-theoretic problems, the importance of his results spanned far beyond these specific circumstances. Edwards said that despite being largely based upon theories of Kummer and his ideal number, “Dedekind’s legacy... consisted not only of important theorems, examples, and concepts, but of a whole style of mathematics that has been an inspiration to each succeeding generation” [3, p. 10].

3.2. Algebraic Geometry. To continue the search for the roots of ring theory, we now turn to algebraic geometry: the second source for modern commutative ring theory. “Algebraic geometry is the study of algebraic curves and their generalizations to \( n \) dimensions, algebraic varieties” [2]. Further, we define an algebraic curve as the set of roots of an algebraic function, \( y = f(x) \), that is implicitly defined by the polynomial equation \( P(x, y) = 0 \). Standard basic examples include the geometry of parabolas, both \( x = y^2 \) and \( y = x^2 \), as well as hyperbolas \( xy = 1 \), and circles \( x^2 + y^2 = 1 \), all of which can be rewritten in the form \( P(x, y) = 0 \). To continue with algebraic curves, we rely heavily on the work of Riemann from the 1850s, where algebraic functions \( f(w, z) = 0 \) of a complex variable and their integrals are the focus.

Dedekind and Weber provided a major basis for this theory of algebraic functions that Reimann had originally worked analytically on. They were able to concretely establish a strong analogy between algebraic number fields and algebraic function fields. This brought forth the connection between algebraic number theory and algebraic geometry. Numbers were replaced by ideals in Dedekind’s arithmetic, so lines, curves, and points were then replaced by ideals in algebraic geometry.

We now consider polynomial rings and their ideals as another major component of algebraic geometry. It was Lasker and Macauley who ventured into this domain and identified the correspondence between varieties (the set of points in \( \mathbb{R}^n \) or \( \mathbb{C}^n \) satisfying a system of polynomial equations over an algebraically closed field \( K \)) and their largest defining ideals. Here, prime ideals correspond to irreducible varieties. In order to more clearly understand algebraic varieties, Lasker and Macauley closely studied ideals in polynomial rings. So, a curve, or variety, in \( \mathbb{R}^2 \) could be given by a parabola and a circle that’s tangent to that parabola. These are defined by \( y = x^2 \) and \( x^2 + (y - 1)^2 = 1 \). So, the variety equals the union of these two curves. The corresponding ideal equals the set of all polynomials in \( \mathbb{R}[x, y] \) (two variables) which equal zero on all points of the variety. For example, this polynomial \( x^4 + x^2y^2 - 3x^2y - y^3 + 2y^2 \) vanishes on all points. Specifically, if you plug in \((0, 0)\), or \((1, 1)\) (from the parabola), or \((2, 4)\) (from the parabola) or \((0, -2)\) (from the circle) or \((-1, -1)\) (from the circle) the result is always zero. So, the ideal associated with this variety equals all the polynomials that are zero for all points on the variety. Now, that ideal can be written as a product of two ideals by \( P_1 \) and \( P_2 \) which are prime ideals. What are \( P_1 \) and \( P_2 \)? They are the ideals generated by \( x^2 - y \) and \( x^2 + (y - 1)^2 - 1 \). Similarly, points and lines in \( \mathbb{R}^2 \) can be defined by their ideals (the ideal for the point \((a, b)\) is generated by the polynomials \( P_1 = x - a \) and \( P_2 = y - b \)).
Thus, all of geometry can be translated into facts about different kinds of ideals. Lasker’s major result was the “primary decomposition” of ideals where every ideal in a polynomial ring $F[x_1, \ldots, x_n]$ is a finite intersection of primary ideals. Viewing this result in light of algebraic geometry yields the conclusion that every variety is a finite union of irreducible varieties. Additionally, Macauley implied that every variety can be expressed uniquely as a union of irreducible varieties proving the uniqueness of the primary decomposition. The importance of this conclusion lies within the methods chosen by both Lasker and Macauley; determining when a curve is algebraically irreducible is much easier than doing so geometrically. Thus, today, we are grateful for their contributions to the study of algebraic geometry.

4. Ring Axioms

After closely reviewing both commutative and noncommutative ring theory, we can now begin to form a true definition of abstract rings. We begin with Fraenkel’s definition from his 1914 paper, “On zero divisors and the decomposition of rings.” Here he defines a ring as a system with two abstract operations, addition and multiplication satisfying the following five conditions:

1. The associative law for addition.
2. The associative law for multiplication.
3. The commutative law for multiplication.
4. The distributive law for multiplication over addition.
5. For any $a$ and $b$ in $R$, there exist unique elements $x$ and $y$ satisfying the equation $a + x = b$ and $y + a = b$.

Fraenkel’s main contribution was that rings now began to be studied as independent, abstract objects, not just as rings of polynomials, as rings of algebraic integers, or as rings of hypercomplex numbers. It was Masazo Sono who provides us with the current definition of a commutative ring in 1917 by extending Fraenkel’s axioms to include commutativity under multiplication as well as addition. In total, we have:

1. If $a, b \in R$, then $a + b \in R$.
2. If $a, b \in R$, then $a + b = b + a$ (commutative law).
3. If $a, b \in R$, then $(a + b) + c = a + (b + c)$ (associative law).
4. There exists $z \in R$ such that $z + b = b$ for every $b \in R$.
5. Corresponding to every $a \in R$, there exists in $R$ another $x$ such that $a + x = z$, where $z$ is the element referred to in 4.
6. If $a, b \in R$, then $a \cdot b \in R$.
7. If $a, b \in R$, then $a \cdot b = b \cdot a$ (commutative law).
8. If $a, b, c \in R$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associative law).
9. If $a, b, c \in R$, then $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributive law).

[1]. In addition to Sono’s very modern definition, he also proceeded to add some extremely important and vital theorems on rings. For example, one of his main contributions to ring theory is his characterization of simple rings $R$ as havings no ideals other than $R$ and $\{0\}$.

Still, the mathematician who “best advanced the abstract point of view in ring theory” was Emmy Noether [1]. Noether was able to extend and abstract the decomposition theories of polynomial rings as well as the rings of integers of algebraic number fields and algebraic function fields. This allowed her to abstract commutative rings with the ascending chain condition, we now call noetherian rings. More
specifically, Noether proved that Lasker and Macauley’s results on primary decomposition in polynomial rings holds true for any abstract ring with the ascending chain condition. She also introduced what are now called *dedekind domains* by defining abstract commutative rings where every nonzero ideal is a unique product of prime ideals. Kaplansky was quoted saying, “...it is surely not much of an exaggeration to call her the mother of modern algebra” [1]. It was Noether who first proved unique factorization theorems for rings assuming only general algebraic properties about their ideals. It is because of her that modern algebra textbooks prove general factorization theorems about principal ideal domains, or Euclidean domains. She proved the isomorphism theorems about quotient rings, gave axioms for this approach, etc. Despite this drive towards abstraction however, Noether was always interested in applying the results to real things like numbers and physical theories.

Although Frankel was the one who gave the first abstract definition of a ring, it was Sono, Noether, and a few others who established the abstract ring concept in algebra by identifying the major theorems beneath it. With the help of these brilliant mathematicians, ring theory began to take form as one of the great theories of abstract algebra, right along side the established theories of groups and fields.

References

