Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 53 (1998)

Artikel: From Numbers to Rings: The Early History of Ring Theory
Autor: Kleiner, Israel
DOI: https://doi.org/10.5169/seals-3627

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 13.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Elem. Math. 53 (1998) 18 – 35
0013-6018/98/010018-18 $1.50+0.20/0

© Birkhäuser Verlag, Basel, 1998

Elemente der Mathematik

From Numbers to Rings: The Early History of Ring Theory*

Israel Kleiner

Israel Kleiner is professor at York University in Toronto. He received his PhD in ring theory from McGill University. His current research interests are the history of mathematics, mathematics education, and their interface. He was for many years co-ordinator of an in-service Master's Programme for teachers of mathematics. Recently he served as vice president of the Canadian Society for the History and Philosophy of Mathematics, and is currently on the advisory board of the International Study Group for the Relations between the History and Pedagogy of Mathematics.

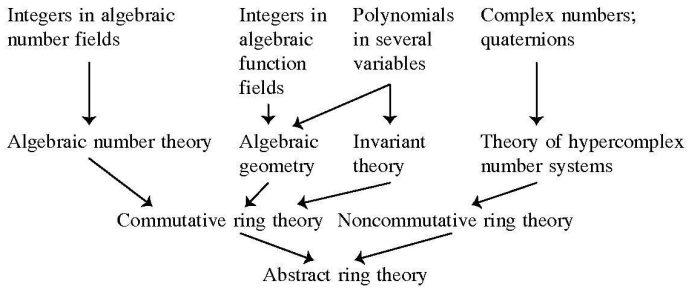
Rings fall into two broad categories: commutative and noncommutative. The abstract theories of these two categories came from distinct sources and developed in different directions. Commutative ring theory originated in algebraic number theory, algebraic geometry, and invariant theory. Central to the development of these subjects were the rings of integers in algebraic number fields and algebraic function fields, and the rings of polynomials in two or more variables. Noncommutative ring theory began with attempts

Wie Gruppen und Körper spielen Ringe in fast allen Gebieten der Mathematik eine grundlegende Rolle. Heutzutage ist diese Feststellung offensichtlich, aber historisch hat sich der Begriff des Ringes nur langsam und schrittweise herauskristallisiert. – In seinem Beitrag beschreibt Israel Kleiner diese Entwicklung von den Anfängen bis in die dreissiger Jahre unseres Jahrhunderts. Eng verbunden mit dem Begriff des Ringes ist derjenige des Ideals. Eingeführt von Kummer und Dedekind im Spezialfall von Ringen algebraischer Zahlen zeigte sich die Kraft des Idealbegriffs nach und nach in der gesamten Ringtheorie: bei den Polynom- und Funktionenringen der algebraischen Geometrie, bei den nichtkommutativen Ringen der Gruppen- und Darstellungstheorie, und bei den Operatoralgebren der Analysis. Es ist dies wohl charakteristisch für unsere Mathematik: Werkzeuge die an einem Spezialfall entwickelt wurden, wie hier der Begriff des Ideals, tragen in aller Regel auch zur Lösung ganz anderer Fragestellungen bei. *ust*

*) This is a much-expanded version of my paper on "The genesis of the abstract ring concept", *American Mathematical Monthly* 103 (1996), 417–424.

to extend the complex numbers to various hypercomplex number systems. The genesis of the theories of commutative and noncommutative rings dates back to the early 19th century, while their maturity was achieved only in the third decade of the 20th century.

The following is a diagrammatic sketch summarizing the above remarks. As you note, the examples come first and the abstractions later – much later. This is, of course, the historical order.



We begin our account with the "simpler" theory of noncommutative rings.

A. Noncommutative ring theory

In a strict sense, noncommutative ring theory originated from a single example – the quaternions, invented (discovered?) by Hamilton in 1843. These are "numbers" of the form $a + bi + cj + dk$ $(a, b, c, d$ real numbers) which are added componentwise and in which multiplication is subject to the relations $i^2 = j^2 = k^2 = ijk = -1$. This was the first example of a noncommutative number system, obeying all the (algebraic) laws of the real and complex numbers except for commutativity of multiplication. Such a system is now called a *skew field* or a *division algebra*. Hamilton's motivation was to extend the algebra of vectors in the plane to an algebra of vectors in 3-space. Having failed in this task, he turned successfully to quadruples of reals. The "pure" quaternions did, in fact, yield a vector algebra in 3-space. See [19].

1. Examples of hypercomplex number systems

Hamilton's invention of the quaternions was conceptually groundbreaking – "a revolution in arithmetic which is entirely similar to the one which Lobachevsky effected in geometry", according to Poincaré [15, p. 29]. Indeed, both achievements were radical violations of prevailing conceptions. Like all revolutions, however, the invention of quaternions was initially received with less than universal approbation: "I have not yet any clear view as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties", declared Hamilton's mathematician friend John Graves [16, p. 229].

Most mathematicians, however, including Graves, soon came around to Hamilton's point of view. The quaternions acted as a catalyst for the exploration of diverse "number systems", with properties which departed in various ways from those of the real and complex numbers. Among the examples of such hypercomplex number systems are the following (see [2], [15], [16], [19]):

(i) **Octonions.** These are 8-tuples of reals which include the quaternions and form a division algebra in which multiplication is nonassociative. They were introduced in 1844 by Cayley and (independently) by the very John Graves who questioned Hamilton's "imaginaries".

(ii) **Exterior algebras.** These are n-tuples of reals, added componentwise and multiplied via the "exterior product". They were introduced by Grassmann in 1844 as part of a brilliant attempt to construct a vector algebra in n-dimensional space. Grassmann's style was far from simple and his approach was ahead of its time, so his ideas were not widely accepted.

(iii) **Group algebras.** In 1854 Cayley published a paper on (finite) abstract groups, at the end of which he gave a definition of a group algebra (over the real or complex numbers). He called it a system of "complex quantities" and observed that it is analogous to Hamilton's quaternions – it is associative and noncommutative, but in general not a division algebra.

(iv) **Matrices.** In two papers of 1855 and 1858 Cayley introduced (square) matrices. He noted that they can be treated as "single quantities", added and multiplied like "ordinary algebraic quantities", but that "as regards their multiplication, there is the peculiarity that matrices are not in general convertible [commutative]".

(v) **Biquaternions.** These were introduced by Clifford in 1873 in connection with problems in geometry and physics. They are elements of the form $h_1 + h_2\alpha$, where h_1 and h_2 are quaternions, $\alpha^2 = 1$, and $\alpha h_i = h_i\alpha$.

2. Classification

Over a thirty-year period (c. 1840–1870) a stock of examples of noncommutative number systems had been established. One could now begin to construct a theory. The general concept of a hypercomplex number system (in current terminology, a finite-dimensional algebra) emerged, and work began on classifying certain types of these structures. We focus on three such developments, dealing with *associative* algebras. (An "algebra" in this paper will mean an associative algebra.)

(i) **Low-dimensional algebras.** Of fundamental importance here is the work of Benjamin Peirce of Harvard – the first important contribution to algebra in the U.S. We are referring to his groundbreaking paper "Linear Associative Algebra" of 1870. In the last 100 pages of this 150-page paper Peirce classifies algebras (i.e. hypercomplex number systems) of dimension < 6 by giving their multiplication tables. There are, he shows, over 150 such algebras! What is important in this paper, though, is not the classification but the means used to obtain it. For here Peirce introduces concepts, and derives results, which proved fundamental for subsequent developments. Among these conceptual advances are:

(a) An "abstract" definition of a finite-dimensional algebra. Peirce defines such an algebra – he calls it a "linear associative algebra" – as the totality of formal expressions of the form $\sum_{i=1}^{n} a_i e_i$, where the e_i are "basis elements". Addition is defined componentwise and multiplication by means of "structural constants" c_{ij}^k, namely $e_i e_j = \sum_{k=1}^{n} c_{ij}^k e_k$. Associativity under multiplication and distributivity are assumed, but not commutativity. This is probably the earliest explicit definition of an associative algebra.

(b) The use of complex coefficients. Peirce takes the coefficients a_i in the expressions $\sum a_i e_i$ to be *complex* numbers. This conscious broadening of the field of coefficients from $\mathbb{R}$ to $\mathbb{C}$ was an important conceptual advance on the road to coefficients taken from an arbitrary field.

(c) Relaxation of the requirement that an algebra have an identity. This, too, is a departure from past practice and gives an indication of Peirce's general, abstract approach.

(d) Introduction of nilpotent and idempotent elements. An element x of an algebra is *nilpotent* if $x^n = 0$ for some positive integer n and *idempotent* if $x^2 = x$. These concepts proved basic for the subsequent study of algebras and, still later, of rings. Peirce proved the fundamental result that any algebra contains a nonzero nilpotent or an idempotent element.

(e) The *Peirce decomposition*. Peirce showed that if e is an idempotent of an algebra A then $A = eAe \oplus eB_1 \oplus B_2 e \oplus B$, where $B_1 = \{x \in A : xe = 0\}$, $B_2 = \{x \in A : ex = 0\}$, and $B = B_1 \cap B_2$ ($\oplus$ indicates direct sum). This so-called Peirce decomposition of an algebra relative to an idempotent enabled Peirce to get a better hold on the algebra by studying its constituent parts. It is a central tool in the study of rings and algebras.

Peirce's work was well ahead of its time, and at first attracted little attention. Cayley, for example, who praised Peirce's work in an address in 1883 to the British Association for the Advancement of Science, called it "outside of ordinary mathematics". Even some of Peirce's admirers in the United States characterized the work as "philosophy of mathematics" rather than mathematics proper. But Peirce, of course, turned out to have been a *mathematical* pioneer.

(ii) **Division algebras.** As we mentioned, the first example of a noncommutative algebra, namely Hamilton's quaternions, was a division algebra. The question arose as to which other finite-dimensional algebras over $\mathbb{R}$ (algebras of n-tuples of real numbers) are division algebras. The answer was given, independently, by Frobenius (in 1878) and by C.S. Peirce (B. Peirce's son, in 1881), namely that the only such algebras are the real numbers, the complex numbers, and the quaternions.

(iii) **Commutative algebras.** In the 1860s Dedekind and Weierstrass proved that the only finite-dimensional commutative algebras over $\mathbb{R}$ or $\mathbb{C}$ without nonzero nilpotent elements are direct sums of copies of $\mathbb{R}$ or $\mathbb{C}$. This means that not only addition but also multiplication in such algebras is componentwise. This result was published only in the 1880s.

See [2], [16], [19] for further details of the above.

3. Structure

The first example of a noncommutative algebra was given by Hamilton in 1843. During the next forty years mathematicians introduced other examples, and began to bring some order into them and to single out certain types for special attention. The stage was (almost) set for the founding of a general theory of finite-dimensional, noncommutative, associative algebras. The task was accomplished in the last decade of the 19th century and the first decade of the 20th. Before that, however, important developments took place in a neighboring branch of mathematics which had an impact on the work in associative

algebras. This was the founding of the theory of Lie groups and Lie algebras in the 1870s and 1880s.

Lie founded the theory of continuous transformation groups (now called Lie groups) in the 1870s to facilitate the study of differential equations. Just as Galois associated a finite (discrete) group of permutations with an algebraic (polynomial) equation, so Lie associated an infinite (continuous) group of transformations with a differential equation. Lie subsequently showed that for the purposes of the differential equation it suffices to focus on the "local" structure of the Lie group – that is, on the "infinitesimal transformations" which, when multiplied using the "Lie product", form a Lie algebra. (If S, T are infinitesimal transformations, so is their Lie product $[S, T]$ which is given by $[S, T] = ST - TS$.) Just as in the case of algebraic equations, so too in this theory the objects of special interest are the "simple" Lie groups. These give rise to "simple" Lie algebras. Lie thus proposed the task of studying the structure of Lie algebras with special attention to the "simple" ones. This task was admirably accomplished in the 1880s by Killing and Cartan, who decomposed "semi-simple" Lie algebras (i.e. algebras with zero radical) into simple ones (i.e. those without ideals) and then classified the latter. See [2], [19].

(i) **Algebras over $\mathbb{R}$ or $\mathbb{C}$.** In the 1890s Cartan, Frobenius, and Molien proved (independently) the following fundamental structure theorem for finite-dimensional associative algebras over the real or complex numbers. If A is such an algebra then

(a) $A = N \oplus B$, where N is nilpotent and B is semi-simple. An algebra N is *nilpotent* if $N^k = 0$ for some positive integer k; it is *semi-simple* if it has no nontrivial nilpotent ideals – this, at least, was the initial conception of semi-simplicity.

(b) $B = C_1 \oplus C_2 \oplus \cdots \oplus C_n$, where C_i are simple algebras, that is, have no nontrivial ideals. (The nilpotent part N is intractable, even today.)

(c) $C_i = M_{n_i}(D_i)$, the algebra of $n_i \times n_i$ matrices with entries from a division algebra D_i.

The above representations are, moreover, unique; that is, the n, n_i are unique, and the N, B, C_i, D_i are unique up to isomorphism.

The immediate inspiration and motivation for this result came from the neighboring theory of Lie algebras. But there were other precedents for decomposition results in algebra – for example, the decomposition of an ideal in the ring of integers of an algebraic number field into a unique product of prime ideals, given by Dedekind in 1871 (see below), and the decomposition of a finite abelian group into a unique direct product of cyclic groups of prime-power order, proved by Frobenius and Stickelberger in 1879.

Of the work of the three mathematicians who established the above results, Cartan's proved the most influential. His proof techniques, however, were soon superseded by Wedderburn's (see below). What proved lasting, apart from the structure theorem, were the following four concepts which Cartan introduced, albeit only at the *end* of his paper, and only to *state* the structure theorems more succinctly: direct sum, ideal, simple algebra, and semi-simple algebra. Cartan was the first to introduce these explicitly in the context of noncommutative, associative algebras. (Dedekind introduced ideals for certain commutative rings more than two decades earlier (as we shall see), but there

is no reference in Cartan's work to Dedekind's ideals.) For example, Cartan defines an ideal – he calls it an "invariant system" – as follows:

> We say that a system Σ admits an invariant subsystem σ, if every element of σ belongs to Σ and if the product, on the right or on the left, of an arbitrary element of σ and an arbitrary element of Σ belongs to σ.

See [16], [19] for further details.

(ii) **Algebras over arbitrary fields.** At the end of the 19th century the theory of finite-dimensional algebras had attained a degree of maturity. All-important connections had been made with Lie's theory of continuous groups as well as with the theory of finite groups, via group representation theory. At the same time, a major structure theorem was available. The theory of finite-dimensional algebras thus became a distinct discipline for serious mathematical investigation. What was needed for further progress in the subject was a new departure. This was provided by Wedderburn's groundbreaking paper of 1907, entitled "On hypercomplex numbers" [20].

The major result in Wedderburn's paper, namely the structure theorem for finite-dimensional algebras, is essentially the same as that given by Cartan. There was "merely" an extension of the field of scalars of the algebra from $\mathbb{R}$ or $\mathbb{C}$ to an arbitrary field. This extension, however, necessitated a new approach to the subject – a rethinking and reformulation of its major concepts and results.

Cartan's methods relied heavily on the vector-space structure of the algebra and on the field of scalars ($\mathbb{R}$ or $\mathbb{C}$). He associated a characteristic and minimal polynomial with each algebra – these are fundamental tools in his development of the theory. Their factors are related to the structure of the given algebra. For example, he defined a "pseudo-null" element of an algebra as one whose characteristic polynomial has only the zero root. It can be shown that this notion is equivalent to that of a nilpotent element, defined almost thirty years earlier by Benjamin Peirce. See [16].

Wedderburn's approach to the study of the structure of finite-dimensional algebras, which are important examples of noncommutative rings, was conceptual rather than computational. "It is remarkable", he wrote toward the end of the paper, "that the properties of a field with regard to division are not used in many of the theorems of the preceding sections." Among the ideas which he either introduced for the first time or made central in the study of algebras, ideas now (ninety years later) still recognized by students of algebra as basic, are the notions of ideal, quotient algebra, nilpotent algebra, radical, semi-simple and simple algebra, direct sum, and tensor product. His work served as a model for other ring-theoretic structure theorems.

B. Commutative ring theory

Commutative ring theory originated in algebraic number theory, algebraic geometry, and invariant theory, and has in turn been applied mainly to these subjects.

1. Algebraic number theory

Several of the central areas of number theory, principally Fermat's Last Theorem, reciprocity laws, and binary quadratic forms, were instrumental in the emergence of algebraic

number theory. Although the main problems in these areas were expressed in terms of integers, it gradually became apparent that the solutions called for embedding the integers in domains of what came to be known as algebraic integers.

(i) **Fermat's Last Theorem.** Euler in the 18th century and several mathematicians in the early 19th century realized that to prove Fermat's Last Theorem (FLT) – the unsolvability in integers of $x^n + y^n = z^n$ $(n > 2)$ – even for small values of n, it is necessary to use "complex integers". For example, $x^3+y^3 = z^3$ is written as $(x+y)(x+\rho y)(x+\rho^2 y) = z^3$, where $\rho = \frac{-1+\sqrt{3}i}{2}$ is a primitive cube root of 1, and this is now an equation in the domain $D_3 = \{a + b\rho : a, b \in Z\}$. Assuming the solvability of $x^3 + y^3 = z^3$, and given that D_3 is a unique factorization domain (UFD), one can arrive at a contradiction. If we write $x^p + y^p = z^p$ as $(x + y)(x + \omega y)(x + \omega^2 y) \cdots (x + \omega^{p-1} y) = z^p$, ω a primitive pth root of 1 (it suffices to prove FLT for $n = p$, a prime) and consider now the domain $D_p = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in Z\}$, we could similarly prove FLT, were the domain D_p of *cyclotomic integers* a UFD for all p. Of course it is not (failing for all $p \geq 23$). But viewing $x^p + y^p = z^p$ as an equation in D_p is nevertheless an important idea in dealing with FLT. See [9].

An elementary example of the utility of "complex integers" in solving problems about ordinary integers is the problem of finding all integer solutions of the diophantine equation $x^2 + 2 = y^3$, a special case of the famous "Bachet equation" $x^2 + k = y^3$. (This is an example of an elliptic curve; these proved important in Wiles' solution of FLT.) It is easy to see that $x = \pm 5$, $y = 3$ are solutions. To find *all* solutions we write $x^2 + 2 = y^3$ as $(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3$. This is now an equation in the domain $D = \{a + b\sqrt{2}i : a, b \in Z\}$. We can show that D is a UFD and that $x + \sqrt{2}i$ and $x - \sqrt{2}i$ are relatively prime in D. Since their product is a cube, each factor must be a cube (in D). In particular, $x + \sqrt{2}i = (a + b\sqrt{2}i)^3$, $a, b \in Z$. Cubing and equating coefficients we can easily show that $x = \pm 5$, $y = 3$ are the *only* solutions of $x^2 + 2 = y^3$ – no easy feat to accomplish without the use of complex integers.

(ii) **Reciprocity laws.** Just as solving polynomial equations is important in algebra, solving polynomial congruences, notably $a_0 + a_1 x + \cdots + a_m x^m \equiv 0 \pmod{n}$, $a_i \in Z$, is important in number theory. The case of arbitrary m is intractable, but the quadratic case, $a_0 + a_1 x + a_2 x^2 \equiv 0 \pmod{n}$, was dealt with by Gauss in the *Disquisitiones Arithmeticae* of 1801. It suffices to consider the congruence $x^2 \equiv q \pmod{p}$, p and q odd primes (the case of even primes has to be considered separately). Gauss proved the celebrated *quadratic reciprocity law*, namely that $x^2 \equiv q \pmod{p}$ is solvable if and only if $x^2 \equiv p \pmod{q}$ is solvable, unless $p \equiv q \equiv 3 \pmod{4}$, in which case $x^2 \equiv q \pmod{p}$ is solvable if and only if $x^2 \equiv p \pmod{q}$ is not.

What about higher reciprocity laws? That is, is there a "reciprocity relation" between the solvability of $x^m \equiv q \pmod{p}$ and $x^m \equiv p \pmod{q}$ for $m > 2$? Gauss took the view that such laws cannot even be properly *conjectured* within the context of natural numbers: "The previously accepted laws of arithmetic are not sufficient for the foundations of a general theory .... Such a theory demands that the domain of higher arithmetic be endlessly enlarged" [13, p. 108].

A prophetic statement, indeed. Gauss was calling for the founding of an arithmetic theory of algebraic numbers. In fact, Gauss himself began to enlarge the domain of arithmetic

by introducing what came to be known as the *Gaussian integers*,

$$Z[i] = \{a + bi : a, b \in Z\},$$

and showing that they form a UFD. This he did in two papers in 1829 and 1831, in which he used $Z[i]$ to *formulate* the law of *biquadratic reciprocity*. At about the same time, Jacobi and Eisenstein (as well as Gauss in unpublished papers) formulated the *cubic reciprocity law*. Here one needed to consider the domain

$$Z[\rho] = \{a + b\rho : a, b \in Z\},$$

ρ a primitive cube root of 1, which was also shown to be a UFD. The search was on for higher reciprocity laws. But as in the case of Fermat's Last Theorem, here too one needed new methods to deal with cases beyond the first few, for unlike $Z[i]$ and $Z[\rho]$, other domains of higher arithmetic needed to formulate such laws are not UFDs. See [4], [13].

(iii) **Binary quadratic forms.** An (integral) binary quadratic form is an expression of the form $f(x, y) = ax^2 + bxy + cy^2, a, b, c \in Z$. The major problem of the theory of quadratic forms was: given a form f, find all integers m which can be represented by f, that is, for which $f(x, y) = m$. For example, Fermat considered the representation of integers as sums of two squares. Gauss in the *Disquisitiones* developed a comprehensive and beautiful theory of binary quadratic forms. Most important was his definition of the *composition* of two forms and his proof that the (equivalence classes of) forms with a given discriminant $D = b^2 - 4ac$ form (in modern terms) a commutative group under this composition. See [8].

The *idea* behind composition of forms is simple: if forms f and g represent integers m and n, respectively, then their composition $f * g$ should represent the product mn. The *implementation* of this idea is subtle and very difficult to describe. Attempts to gain conceptual insight into Gauss' theory of composition of forms inspired the efforts of some of the best mathematicians of the time, among them Dirichlet, Kummer, and Dedekind. The key idea here, too, was to extend the domain of higher arithmetic and view the problem in a broader context. Here is perhaps the simplest illustration:

If m_1 and m_2 are sums of two squares, so is m_1m_2. Indeed, if $m_1 = x_1^2 + y_1^2$ and $m_2 = x_2^2 + y_2^2$, then $m_1m_2 = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$. In terms of the composition of quadratic forms this can be expressed as $f(x_1, y_1) * f(x_2, y_2) = f(x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$, or $f * f = f$, where $f(x, y) = x^2 + y^2$. But even this "simple" law of composition seems mysterious and ad hoc until one introduces Gaussian integers, which make it transparent:

$$\begin{aligned}
&(x_1^2 + y_1^2)(x_2^2 + y_2^2) \\
&\quad = (x_1 + y_1 i)(x_1 - y_1 i)(x_2 + y_2 i)(x_2 - y_2 i), \\
&\quad = (x_1 + y_1 i)(x_2 + y_2 i)\overline{(x_1 + y_1 i)(x_2 + y_2 i)} \quad (\overline{\alpha} \text{ denotes the conjugate of } \alpha) \\
&\quad = [(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i][(x_1x_2 - y_1y_2) - (x_1y_2 + x_2y_1)i] \\
&\quad = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2.
\end{aligned}$$

In general, $ax^2 + bxy + cy^2 = m$ can be written as

$$\frac{1}{a}\left(ax + \frac{b+\sqrt{D}}{2}y\right)\left(ax + \frac{b-\sqrt{D}}{2}y\right) = m,$$

where $D = b^2 - 4ac$ is the discriminant of the quadratic form. We have thus expressed the problem of representation of integers by binary quadratic forms in terms of the domain

$$R = \left\{\frac{u+v\sqrt{D}}{2} : u, v \in Z,\ u \equiv v \pmod 2\right\}.$$

Since such domains do not, in general, possess unique factorization, the development of their arithmetic theory became an important goal. See [4], [9].

To summarize: We have seen that in dealing with central problems in number theory, namely Fermat's Last Theorem, reciprocity laws, and binary quadratic forms, it was found important to formulate them as problems in domains of algebraic integers. The study of unique factorization in such domains became the major problem of a newly emerging subject – algebraic number theory. Kummer dealt with it by means of ideal numbers, Dedekind by means of ideals, and Kronecker by means of divisors. We consider below the contributions of Kummer and of Dedekind.

(iv) **Kummer's ideal numbers.** We recall that the domains of cyclotomic integers, $D_p = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in Z,\ \ \omega$ a primitive pth root of $1\}$, were central in the study of Fermat's conjecture. They also proved important in the investigation of higher reciprocity laws. Both problems were of great interest to Kummer (the latter apparently more than the former), and to make significant progress it was essential to establish unique factorization (of some type) in the domains D_p. This Kummer accomplished in the 1840s. As he put it in a letter to Liouville, unique factorization in D_p "can be saved by the introduction of a new kind of complex numbers that I have called ideal complex numbers". Kummer's major result was that every element in the domain of cyclotomic integers is a unique product of "ideal primes".

Kummer's theory of ideal numbers was vague and computational. In fact, the central notions of ideal number and ideal prime were only *implicitly* defined in terms of their divisibility properties (see [8]). Kummer noted that in adopting the implicit definitions he was guided by the idea of a "free radical" in chemistry, a substance whose existence can only be discerned by its effects.

To give the reader a sense of Kummer's theory of ideal numbers, we adduce a standard example, due to Dedekind, of a (noncyclotomic) domain $D = \{a + b\sqrt{5}i : a, b \in Z\}$, in which factorization is not unique. We have, for example, $6 = 2 \times 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$, where 2,3, and $1 \pm \sqrt{5}i$ are primes (indecomposables) in D. To restore unique factorization of $6 \in D$, adjoin the "ideal numbers" $\sqrt{2}, (1+\sqrt{5}i)/\sqrt{2}$, and $(1-\sqrt{5}i)/\sqrt{2}$. These are, in fact, *ideal primes*. We then have

$$6 = 2 \times 3 = \sqrt{2} \times \sqrt{2} \times \frac{1+\sqrt{5}i}{\sqrt{2}} \times \frac{1-\sqrt{5}i}{\sqrt{2}}, \text{ and}$$

$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) = \sqrt{2} \times \frac{(1+\sqrt{5}i)}{\sqrt{2}} \times \sqrt{2} \times \frac{(1-\sqrt{5}i)}{\sqrt{2}}; \text{ that is,}$$

the decomposition of 6 into ideal primes is now unique. Moreover, the choice of the ideal primes $\sqrt{2}, (1 \pm \sqrt{5}i)/\sqrt{2}$, which seems ad hoc, will come to seem natural after ideals are introduced. See [8], [9].

(v) **Dedekind's ideals.** Kummer's ideas were brilliant but difficult and not clearly formulated. The fundamental concepts of ideal number and ideal prime were not intrinsically defined. Moreover, Kummer's decomposition theory applied only to cyclotomic integers. What was needed was a decomposition theory which would apply to arbitrary domains of algebraic integers. This was devised, independently and in different ways, by Dedekind and Kronecker. We will focus on Dedekind's formulation, which is the one that has generally prevailed.

The main result of Dedekind's groundbreaking 1871 work is that every nonzero ideal in the domain of integers of an algebraic number field is a unique product of prime ideals. Before one could state this theorem one had, of course, to define the concepts in its statement, namely "the domain of integers of an algebraic number field", "ideal", and "prime ideal". It took Dedekind about twenty years to formulate them.

The number-theoretic domains studied at the time, such as the Gaussian integers, the integers arising from cubic reciprocity, and the cyclotomic integers, are all of the form $Z[\theta] = \{a_0 + a_1\theta + \cdots + a_n\theta^n : a_i \in Z\}$, where θ satisfies a polynomial with integer coefficients. It was therefore tempting to define the domains to which Dedekind's theorem would apply as objects of this type. But Dedekind showed that these were the wrong objects. For example, he showed that Kummer's theory of unique factorization could *not* be extended to the domain $Z[\sqrt{3}i] = \{a + b\sqrt{3}i : a, b \in Z\}$, and of course, Dedekind's objective was to try to extend Kummer's theory to *all* domains of algebraic integers.

One had to begin the search for the appropriate domains, Dedekind contended, within an "algebraic number field" – a finite field extension $Q(\alpha) = \{q_0 + q_1\alpha + \cdots + q_s\alpha^s : q_i \in Q\}$ of the rationals, α an algebraic number, that is, a root of a polynomial with integer coefficients. The notion of "algebraic number" was well known at the time, but not that of "algebraic integer". Dedekind showed that, in fact, *all* elements of $Q(\alpha)$ are algebraic numbers. But what is the appropriate subdomain of $Q(\alpha)$ in which to do number theory – "the integers of $Q(\alpha)$"? Dedekind defined them to be the elements of $Q(\alpha)$ which are roots of *monic* polynomials with integer coefficients. (Note that under this definition the "ordinary" integers Z – "the integers of Q" – are the roots of *linear* monic polynomials.) He showed that these elements "behave" like integers – they are closed under addition, subtraction, and multiplication; in our terminology, they form a ring – a subring of $\mathbb{C}$.

Having defined the domain of algebraic integers of $Q(\alpha)$ in which he would formulate and prove his result on unique decomposition of ideals, Dedekind considered, more generally, sets of integers of $Q(\alpha)$ closed under addition, subtraction, and multiplication. He called them "orders". (The domain of integers of $Q(\alpha)$ is the largest order.) Here, then, was an algebraic first for Dedekind – an essentially axiomatic definition of a (commutative) ring, albeit in a concrete setting.

The second fundamental concept of Dedekind's theory, that of ideal, derived its motivation (and name) from Kummer's ideal numbers. Dedekind wanted to characterize them *internally*, within the domain D_p of cyclotomic integers. Thus, for each ideal number σ he considered the set of cyclotomic integers divisible by σ. These, he noted, are closed

under addition and subtraction, as well as under multiplication by all elements of D_p. Conversely, he proved (and this is a difficult theorem) that every set of cyclotomic integers closed under these operations is precisely the set of cyclotomic integers divisible by some ideal number τ. Thus there is a one-one correspondence between ideal numbers and subsets of the cyclotomic integers closed under the above operations. Such subsets of D_p Dedekind called *ideals*. These subsets, then, characterized ideal numbers internally, and served as motivation for the introduction of ideals in arbitrary domains of algebraic integers. Dedekind defined them abstractly as follows [8]:

> A subset I of the integers R of an algebraic number field K is an *ideal* of R if it has the following two properties:
>
> (i) If $\beta, \gamma \in I$ then $\beta \pm \gamma \in I$.
>
> (ii) If $\beta \in I, \mu \in R$ then $\beta\mu \in I$.

Dedekind then defined a prime ideal – perhaps the most important notion of commutative algebra – as follows: An ideal P of R is *prime* if its only divisors are R and P. Given ideals A and B, A was said to divide B if $A \supseteq B$. In later versions of his work Dedekind showed that A divides B if and only if $B = AC$ for some ideal C of R. Having defined the notion of prime ideal, Dedekind proved his fundamental theorem that every nonzero ideal in the ring of integers of an algebraic number field is a unique product of prime ideals. See [7], [8] for details.

How did Dedekind's ideas apply to (say) the nonunique factorization of 6 into primes in the domain $D = \{a + b\sqrt{5}i : a, b \in Z\} : 6 = 2 \times 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$? If we let $P = \langle 2, 1 + \sqrt{5}i\rangle = \{2\alpha + (1 + \sqrt{5}i)\beta : \alpha, \beta \in D\}$ – the ideal of D generated by 2 and $\sqrt{5}i$, $Q = \langle 3, 1 + \sqrt{5}i\rangle$, $R = \langle 3, 1 - \sqrt{5}i\rangle$, then we can verify that $P^2 = \langle 2\rangle, PQ = \langle 1 + \sqrt{5}i\rangle, QR = \langle 3\rangle$, and $PR = \langle 1 - \sqrt{5}i\rangle$ ($\langle\alpha\rangle$ denotes the ideal generated by α; if A and B are ideals of a ring R, their product is the ideal $AB = \{\sum_{\text{finite}} a_i b_i : a_i \in A,\ b_i \in B\}$.)

The factorizations $6 = 2 \times 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$ now yield the following factorizations of ideals: $\langle 6\rangle = \langle 2\rangle\langle 3\rangle = P^2(QR)$ and $\langle 6\rangle = \langle 1+\sqrt{5}i\rangle\langle 1-\sqrt{5}i\rangle = (PQ)(PR) = P^2QR$. One can readily verify that the ideals P, Q, R are prime. Thus the *ideal* $\langle 6\rangle$ (if not the *element* 6) has been factored uniquely into prime ideals. Paradise regained via ideals.

Let us compare the factorization of $\langle 6\rangle$ into *prime ideals* with the factorization of 6 into *ideal primes* (à la Kummer) that we gave earlier:

$$6 = 2 \times 3 = \sqrt{2} \times \sqrt{2} \times \frac{1 + \sqrt{5}i}{\sqrt{2}} \times \frac{1 - \sqrt{5}i}{\sqrt{2}},$$

and

$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i) = \sqrt{2} \times \frac{1 + \sqrt{5}i}{\sqrt{2}} \times \sqrt{2} \times \frac{1 - \sqrt{5}i}{\sqrt{2}}.$$

Performing some 18th-century symbolic callisthenics, we obtain the following: Since $P^2 = \langle 2\rangle$, $P \sim \sqrt{2}$ (where "$\sim$" stands for "corresponds to", "captures", "represents"). In fact, P is the ideal consisting of all elements of D divisible by the ideal number $\sqrt{2}$

(that is, such that the quotient is an algebraic integer). We also have $PQ = \langle 1 + \sqrt{5}i \rangle$, hence $PQ/P \sim (1 + \sqrt{5}i)/\sqrt{2}$, so that the ideal Q corresponds to the ideal number $(1 + \sqrt{5}i)/\sqrt{2}$. And since $PR = \langle 1 - \sqrt{5}i \rangle, PR/P \sim (1 - \sqrt{5}i)/\sqrt{2}$, hence $R \sim (1 - \sqrt{5}i)/\sqrt{2}$. This removes the mystery associated with our earlier introduction of the ideal numbers $\sqrt{2}$ and $(1 \pm \sqrt{5}i)/\sqrt{2}$.

Dedekind's work was the culmination of seventy years of investigations of problems related to unique factorization. It created, in one swoop, a new subject – algebraic number theory. It introduced, albeit in a concrete setting, some of the most fundamental concepts of commutative algebra, such as ring, ideal, and prime ideal. His work also established one of the central results of algebraic number theory, namely the representation of ideals in domains of integers of algebraic number fields as unique products of prime ideals. The theorem was soon to play a fundamental role in the study of algebraic curves (see below).

As important as his concepts and results were Dedekind's methods. In fact, "his insistence on philosophical principles was responsible for many of his important innovations" [8, p. 349]. One of his philosophical principles was a focus on intrinsic, conceptual properties over formulas, calculations, or concrete representations. Another was the acceptance of nonconstructive procedures (definitions, proofs) as legitimate mathematical methods. Dedekind's great concern for teaching also influenced his mathematical thinking. His two very significant methodological innovations were the use (outside of geometry) of the axiomatic method and the institution of set-theoretic modes of thinking.

The axiomatic method was just beginning to resurface after 2000 years of near dormancy. Dedekind was instrumental in pointing to its mathematical power and pedagogical value. In this he inspired (among others) David Hilbert and Emmy Noether. His use of set-theoretic formulations (recall, for example, his definition of an ideal as the set of elements of a domain satisfying certain properties), including the use of the completed infinite – taboo at the time – preceded by about ten years Cantor's seminal work on the subject.

2. Algebraic geometry

Algebraic geometry is the study of algebraic curves and their generalizations to n dimensions, algebraic varieties. An algebraic curve is the set of roots of an algebraic function; that is, a function $y = f(x)$ defined implicitly by the polynomial equation $P(x, y) = 0$. It is natural to study algebraic curves in complex projective space.

Several approaches were used in the study of algebraic curves, notably the analytic, the geometric-algebraic, and the algebraic-arithmetic. In the analytic approach, to which Riemann (in the 1850s) was the major contributor, the main objects of study were algebraic functions $f(w, z) = 0$ (of a complex variable) and their integrals, the so-called abelian integrals, which are closely related to the important notion of the genus of an algebraic curve. It was in this connection that Riemann introduced the fundamental notion of a Riemann surface, on which algebraic functions become single-valued. Riemann's methods were, however, nonrigorous, relying heavily on the physically obvious, but mathematically questionable, Dirichlet Principle.

In the 1860s and 1870s Clebsch, Gordan, Brill, and especially M. Noether introduced geometric-algebraic methods to study algebraic functions and curves. A major problem,

solved by Noether, was: given algebraic curves $f(x,y)=0, g(x,y)=0$, to find conditions under which a polynomial $F(x,y)$ is representable in the form $F=Af+Bg$, A and B polynomials in x and y. In modern terms: under what conditions is F an element of the ideal (in the polynomial ring $\mathbb{R}[x,y]$) generated by f and g? The ideas of the geometric school can be thought of as the starting point of the theory of polynomial ideals. See [2], [10], [12] for details.

(i) **Algebraic function fields.** Neither the transcendental methods of Riemann, nor the geometric-algebraic ideas of M. Noether et al, provided a rigorous foundation for algebraic function theory. This was accomplished by Dedekind and Weber in their groundbreaking 1882 paper "Theory of algebraic functions of a single variable", in which they proposed to "provide a basis for the theory of algebraic functions, the major achievement of Riemann's researches, in the simplest and at the same time rigorous and most general manner". The fundamental idea of their algebraic-arithmetic approach was to carry over to algebraic function fields the ideas which Dedekind had earlier introduced for algebraic number fields.

Just as an algebraic number field is a finite extension $Q(\alpha)$ of the field Q of rationals, so an algebraic function field is a finite extension $K=\mathbb{C}(z)(w)$ of the field $\mathbb{C}(z)$ of rational functions (in the indeterminate z). That is, w is a root of a polynomial $a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n$, where $a_i\in\mathbb{C}(z)$ (we can take $a_i\in\mathbb{C}[z]$). Thus $w=f(z)$ is an algebraic function defined implicitly by the polynomial equation $P(z,w)=a_0+a_1w+a_2w^2+\cdots+a_nw^n=0$. In fact, all elements of $K=\mathbb{C}(z,w)$ are algebraic functions.

Let now A be the "ring of integers" of K over $\mathbb{C}(z)$; that is, A consists of the elements of K which are roots of *monic* polynomials over $\mathbb{C}[z]$. As for algebraic numbers, here too every nonzero ideal of A is a unique product of prime ideals. Incidentally, the meromorphic functions on a Riemann surface form a field of algebraic functions, with the entire functions as their "ring of integers".

Dedekind and Weber were now ready to give a rigorous, algebraic definition of a Riemann surface S of the algebraic function field K: it is (in our terminology) the set of nontrivial discrete valuations on K. (The finite points of S correspond to ideals of A; to deal with points at infinity of S Dedekind and Weber introduced the notions of "place" and "divisor".) Many of Riemann's ideas about algebraic functions were here developed algebraically and rigorously. In particular, a rigorous proof was given of the important Riemann-Roch theorem. See [2], [10].

Beyond Dedekind's and Weber's technical achievements in putting major parts of Riemann's algebraic function theory on solid ground, their conceptual breakthrough lay in pointing to the strong analogy between algebraic number fields and algebraic function fields, hence between algebraic number theory and algebraic geometry. This analogy proved extremely fruitful for both theories. For example, the use of power series in algebraic geometry inspired Hensel in 1897 to introduce p-adic numbers ("power series" in the prime p). The resulting idea of p-adic completion proved important in both algebraic number theory and algebraic geometry. Another noteworthy aspect of Dedekind's and Weber's work was its generality and applicability to arbitrary fields, in particular Q and Z_p, which were important in number-theoretic contexts. Thus ideas from algebraic geometry could be applied to number theory. See [10], [17].

(ii) **Polynomial rings and their ideals.** As we noted, polynomial ideals in algebraic geometry had their implicit beginnings in M. Noether's work (c. 1870). Important advances were made by Kronecker in the 1880s and especially by Hilbert, Lasker, and Macauley in 1890, 1905, and 1913, respectively.

The need for polynomial ideals in the study of algebraic varieties is manifest. An algebraic variety V is defined as the set of points in $\mathbb{R}^n$ (or $\mathbb{C}^n$) satisfying a system of polynomial equations $f_i(x_1, \ldots, x_n) = 0$, $i = 1, 2, 3, \ldots$. The Hilbert Basis Theorem implies that finitely many equations will do. But different systems of polynomial equations may give rise to the same set of roots. For example, the circle V in $\mathbb{R}^3$ of radius 2 lying in the plane parallel to the (x, y) plane and two units above it may be described as $V = \{(x, y, z) : x^2 + y^2 - 4 = 0, z - 2 = 0\}$, as $V = \{(x, y, z) : x^2 + y^2 + z^2 - 8 = 0,\ z - 2 = 0\}$, or as $V = \{(x, y, z) : x^2 + y^2 - 4 = 0,\ x^2 + y^2 - 2z = 0\}$ ([1]). Is there a canonical set of polynomials which describes the variety (circle) V?

It is easy to see that if $f_1, \ldots, f_m$ are polynomials which vanish on the points of V, then so do all polynomials of the set $I = \{g_1 f_1 + \cdots + g_m f_m : g_i \in \mathbb{R}[x, y, z]\}$. But I is an ideal of the polynomial ring $\mathbb{R}[x, y, z]$. In fact, the set of *all* polynomials of $\mathbb{R}[x, y, z]$ which vanish on the points of V is also an ideal – and it is evidently the "canonical" set of polynomials to describe V.

Note that the above remarks point to a correspondence between ideals of $\mathbb{R}[x_1, \ldots, x_n]$ (or of $\mathbb{C}[x_1, \ldots, x_n]$) and varieties in $\mathbb{R}^n$ (or $\mathbb{C}^n$): If V is a variety, let $I(V) = \{f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}$, and if J is an ideal of $\mathbb{R}[x_1, \ldots, x_n]$, let $V(J) = \{(b_1, \ldots, b_n) \in \mathbb{R}^n : g(b_1, \ldots, b_n) = 0 \text{ for all } g \in J\}$. The Hilbert Nullstellensatz (in one of its incarnations) says that $V(J) \neq \emptyset$ if the variety is in $\mathbb{C}^n$ (or K^n for any algebraically closed field K). This correspondence is central in algebraic geometry. It is, in fact, a one-one correspondence between varieties over an algebraically closed field K and their largest defining ideals, the so-called radical ideals. Under this correspondence prime ideals correspond to irreducible varieties. See [5], [10], [12].

Hilbert, Lasker, and Macauley exploited the above correspondence in the late 19th and early 20th centuries by undertaking a thorough study of ideals in polynomial rings in order to shed light on algebraic varieties. Lasker's major result was the "primary decomposition" of ideals: Every ideal in a polynomial ring $F[x_1, \ldots, x_n]$ is a finite intersection of primary ideals. (Primary ideals, first defined by Lasker, are generalizations of prime ideals; the former are to the latter what prime powers are to primes in the ring of integers.) Translated into the language of algebraic geometry, the result says that every variety is a finite union of *irreducible varieties*, that is, those that cannot be nontrivially decomposed as finite unions of other varieties. Macauley proved the *uniqueness* of the primary decomposition, which implied that every variety can be expressed uniquely as a union of irreducible varieties – a sort of "Fundamental Theorem of Arithmetic" for varieties. (By the way, it is no easy matter to determine *geometrically* when a curve is irreducible; it is the *algebra* that comes to a geometer's aid here.) Hilbert's important contributions to the subject were made in the context of his work on invariants (see below). See [5], [10], [12].

3. Invariant theory

Invariant theory had its roots in both number theory and geometry. Given two quadratic forms $f = ax^2 + 2bxy + cy^2$ and $f_1 = a_1x_1^2 + 2b_1x_1y_1 + c_1y_1^2$ over the integers, Gauss defined them to be *equivalent* if f can be changed into f_1 by a linear transformation given by $x = px_1 + qy_1$, $y = rx_1 + sy_1$, where $ps - qr = 1$. Equivalent quadratic forms represent the same set of integers. Moreover, the discriminants $D = b^2 - ac$ and $D_1 = b_1^2 - a_1c_1$ of f and f_1, respectively, are equal. The discriminant is thus said to be an *invariant* of the quadratic form under a linear transformation of the variables with determinant 1.

The first half of the 19th century saw the rise of new geometries – projective, hyperbolic, Riemannian, algebraic, and others. Efforts were undertaken to distinguish among the different types of geometry by pinpointing the characteristics of each. Invariance of properties under various transformations was an important tool in these studies, leading in time to Klein's Erlangen Program. For example, projective properties of geometric figures are those which are invariant under linear transformations, while algebraic-geometric properties are those invariant under birational transformations.

In the mid-19th century invariant theory became an independent field of study, divorced from its number-theoretic and geometric connections. In fact, between the 1860s and the 1880s it became a major branch of *algebra*. Two problems engaged mathematicians' interest: To find specific invariants of various forms and to find "complete systems" of invariants.

Specifically, given a binary form $f(x_1, x_2) = a_0x_1^n + a_1x_1^{n-1}x_2 + \cdots + a_nx_2^n$ (the a_i now taken in $\mathbb{R}$ or $\mathbb{C}$) which is changed by a linear transformation of the variables $x_1, x_2, \ldots, x_n$ into the form $F(X_1, X_2) = A_0X_1^n + A_1X_1^{n-1}X_2 + \cdots + A_nX_2^n$, then any function I of the coefficients which satisfies the relation $I(A_0, \ldots, A_n) = r^kI(a_0, \ldots, a_n)$ (r in $\mathbb{R}$ or $\mathbb{C}$) is called an *invariant* of f (under linear transformations). Cayley, Sylvester, Gordan, and others found specific invariants (e.g. the Jacobian, the Hessian) for specific forms (e.g. binary quartic forms, cubic forms). Attention turned, in time, to finding a *complete system of invariants* for a given form, namely a minimal set of invariants such that any other invariant of the form could be expressed as a linear combination of the system. The existence of a *finite* complete system – a basis – for *binary* forms of any degree was first established by Gordan in 1868. His proof was long and difficult and showed how to *compute* the basis. Bases for a number of other forms (e.g. ternary quadratic and cubic forms) were obtained during the next twenty years.

Hilbert, who wrote a thesis on invariants in 1885, and in 1888 gave a much simpler, but noncomputational, proof of Gordan's result on binary forms, astonished the mathematical community in 1890 by showing that any form, of any degree, in any number of variables, has a basis. Hilbert adopted a new, conceptual, approach to the subject. The idea was to consider, instead of invariants, expressions in a finite number of variables – in short, the polynomial ring in those variables. Hilbert then proved what came to be known as *Hilbert's Basis Theorem*, namely that every ideal in the ring of polynomials in finitely many variables has a finite basis. The existence of a basis for an arbitrary form now followed (see [10], p. 29). "This is not mathematics, it is theology", protested Gordan in response to Hilbert's abstract, nonconstructive proof [14, p. 930]. The theology of the 1890s, however, became the mathematical gospel of the 1920s. See [6], [10], [14].

C. The abstract definition of a ring

In the first decade of the 20th century there were well established, flourishing, concrete theories of both commutative and noncommutative rings and their ideals (the noncommutative theory dealt with algebras, which are of course rings). Their roots were in algebraic number theory, algebraic geometry, invariant theory, and the theory of hypercomplex numbers. Moreover, abstract (axiomatic) definitions of groups, fields, and vector spaces had then been in existence for about two decades. The time was ripe for the abstract ring concept to emerge.

The first abstract definition of a ring was given by Fraenkel (of set-theory fame) in a 1914 paper entitled "On zero divisors and the decomposition of rings" [11]. Fraenkel's definition meant to encompass both commutative and noncommutative rings, for the examples of rings he gave included integers modulo n, matrices, p-adic integers, and hypercomplex number systems. But his work was not grounded in the major concrete theories which had earlier been established.

Fraenkel's aim in this paper was to do for rings what Steinitz had just (1910) done for fields, namely to give an abstract and comprehensive theory of commutative and noncommutative rings. Of course he was not successful (he did admit that the task here is not as "easy" as in the case of fields) – it was too ambitious an undertaking to subsume the structure of both commutative and noncommutative rings under one theory.

Among the main concepts introduced in Fraenkel's paper are "zero divisors" and "regular elements". Fraenkel deals only with rings which are not integral domains (i.e. rings with zero divisors) and discusses divisibility for such rings. Much of the paper deals with decomposition of rings as direct products of "simple" rings (not the usual notion of simplicity). See [3].

Fraenkel's definition of a ring is in today's style. He defines a ring as "a system" with two abstract operations, to which he gives the names addition and multiplication. Under one of the operations (addition) the system forms a group – he gives its axioms. The second operation (multiplication) is associative and distributes over the first. Two axioms give the closure of the system under the operations, and there is the requirement of an identity in the definition of the ring. Commutativity under addition does *not* appear as an axiom but is proved! So are other elementary properties of a ring such as $a \times 0 = 0$, $a(-b) = (-a)b = -(ab)$, and $(-a)(-b) = ab$. There are two "extraneous" axioms, dealing with "regular" elements in the ring, which depart from an otherwise modern definition. The latter was given by Sono in a 1917 paper entitled "On congruences" [18]. Sono's is a very modern, abstract work, discussing cosets, quotient rings, maximal and minimal ideals, simple rings, the isomorphism theorems, and composition series. See [3].

Although Fraenkel's and Sono's works were not in the mainstream of contemporary ring-theoretic studies, their significance 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 (algebras) of hypercomplex numbers.

D. Emmy Noether and Emil Artin

Yet rings of polynomials, rings of algebraic integers, and rings of hypercomplex numbers remained central in ring theory. In the hands of the master algebraists Noether and Artin their study was transformed in the 1920s into powerful, abstract theories. Noether's two seminal papers of 1921 and 1927 extended and abstracted the decomposition theories of polynomial rings on the one hand and of the rings of integers of algebraic number fields and algebraic function fields on the other, to abstract commutative rings with the ascending chain condition – now called *Noetherian rings*.

More specifically, Noether showed in the 1921 paper, entitled "Ideal theory in rings", that the results of Hilbert, Lasker, and Macauley on primary decomposition in polynomial rings hold for any (abstract) ring with the ascending chain condition. Thus results which seemed inextricably connected with the properties of polynomial rings were shown to follow from a single axiom! In her 1927 paper, "Abstract development of ideal theory in algebraic number fields and function fields", she discussed the Dedekind and Dedekind-Weber results on decomposition of ideals as unique products of prime ideals in, respectively, rings of integers of algebraic number fields and function fields, in the setting of abstract rings. In particular, she characterized abstract commutative rings in which every nonzero ideal is a unique product of prime ideals. Such rings are now called *Dedekind domains*.

Artin, inspired by Noether's work on (commutative) rings with the ascending chain condition, generalized Wedderburn's structure theorems in his 1927 paper, "On the theory of hypercomplex numbers", to (noncommutative) rings with the descending chain condition. In particular, he showed that such rings, with zero radical – now called *Artinian rings* – can be decomposed into direct sums of simple rings, and these are matrix rings over division rings.

While with Fraenkel and Sono we witness the birth of the abstract ring *concept*, with Noether and Artin we see the birth of abstract ring *theory*. Noether and Artin made the abstract ring concept central in algebra by framing in an abstract setting the theories which were its major inspirations. In this context they introduced, and gave prominence to, such fundamental algebraic notions as ideal (including one-sided ideal), module, and chain conditions – both ascending and descending. Ring theory now took its rightful place along the by then well established theories of groups and fields as one of the pillars of abstract algebra. See [2], [10], [19].

E. Epilogue

The importance of ring theory in algebra and beyond has anything but diminished in the seventy or so years since Noether's and Artin's works. To illustrate, we quote from a 1991 book on the subject, *A First Course in Noncommutative Rings*, by the prominent algebraist T.Y. Lam:

> Today, ring theory is a fertile meeting ground for group theory (group rings), representation theory (modules), functional analysis (operator algebras), Lie theory (enveloping algebras), algebraic geometry (finitely generated algebras, differential operators, invariant theory), arithmetic (orders, Brauer groups), universal algebra

(varieties of rings), and homological algebra (cohomology of rings, projective modules, Grothendieck and higher K-groups).

As a final comment, the recent paper of Richard Taylor and Andrew Wiles, filling a gap in Wiles' previously announced proof of Fermat's Last Theorem, is entitled "Ring-theoretic properties of certain Hecke algebras" (see *Ann. Math* 141 (1995), 553–572).

References

[1] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, Macmillan, 1941.

[2] N. Bourbaki, *Elements of the History of Mathematics*, Springer-Verlag, 1994.

[3] D.M. Burton and D.H. Van Osdol, "Toward the definition of an abstract ring", in: *Learn from the Masters*, ed. by F. Swetz et al, Mathematical Association of American, 1995, pp. 241–251.

[4] H. Cohn, *Advanced Number Theory*, Dover, 1980.

[5] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[6] T. Crilly, "Invariant Theory", in: *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, ed. by I. Grattan-Guinness, Routledge, 1994, pp. 787–793.

[7] H.M. Edwards, "Dedekind's invention of ideals", *Bull. Lond. Math. Soc.* 15(1983), 8–17.

[8] ___, "The genesis of ideal theory", *Arch. Hist. Ex. Sci.* 23(1980), 321–378.

[9] ___, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1977.

[10] D. Eisenbud, *Commutative Algebra, with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.

[11] A. Fraenkel, "Über die Teiler der Null und die Zerlegung von Ringen", *Jour. für die Reine und Angew. Math.* 145(1914), 139–176.

[12] J.J. Gray, "Early modern algebraic geometry", in: *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, ed. by I. Grattan-Guinness, Routledge, 1994, pp. 920–926.

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1982.

[14] M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, 1972.

[15] C.C. MacDuffee, "Algebra's debt to Hamilton", *Scripta Math.* 10(1944), 25–35.

[16] K.H. Parshall, "H.M. Wedderburn and the structure theory of algebras", *Arch. Hist. Ex. Sci.* 32(1985), 223–349.

[17] J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[18] M. Sono, "On Congruences I–IV", *Mem. Coll. Sci. Kyoto.* 2(1917), 203–226, 3(1918), 113–149, 189–197, and 299–308.

[19] B.L. Van der Waerden, *A History of Algebra*, Springer-Verlag, 1985.

[20] J.H.M. Wedderburn, "On hypercomplex numbers", *Proc. Lond. Math. Soc.* 6(1907), 77–118.

Israel Kleiner
Department of Mathematics and Statistics
York University
North York, Ontario
Canada M3J 1P3
kleiner@yorku.ca