The Many Lives of Lattice Theory

Gian-Carlo Rota

Introduction

Never in the history of mathematics has a mathematical theory been the object of such vociferous vituperation as lattice theory. Dedekind, Jónsson, Kurosh, Malcev, Ore, von Neumann, Tarski, and most prominently Garrett Birkhoff have contributed a new vision of mathematics, a vision that has been cursed by a conjunction of misunderstandings, resentment, and raw prejudice.

The hostility towards lattice theory began when Dedekind published the two fundamental papers that brought the theory to life well over one hundred years ago. Kronecker in one of his letters accused Dedekind of "losing his mind in abstractions," or something to that effect.

I took a course in lattice theory from Oystein Ore while a graduate student at Yale in the fall of 1954. The lectures were scheduled at 8 a.m., and only one other student attended besides me—María Wonenburger. It is the only course I have ever attended that met at 8 o'clock in the morning. The first lecture was somewhat of a letdown, beginning with the words: "I think lattice theory is played out" (Ore's words have remained imprinted in my mind).

For some years I did not come back to lattice theory. In 1963, when I taught my first course in combinatorics, I was amazed to find that lattice theory fit combinatorics like a shoe. The temptation is strong to spend the next fifty minutes on the mutual stimulation of lattice theory and combinatorics of the last thirty-five years. I will, however, deal with other aspects of lattice theory, those that were dear to Garrett Birkhoff and which bring together ideas from different areas of mathematics.

Gian-Carlo Rota is professor of applied mathematics and philosophy at MIT. His e-mail address is `rota@math.mit.edu`.

This article is based on an invited address delivered at the Garrett Birkhoff Memorial Conference, Harvard University, April 1, 1997.

Lattices are partially ordered sets in which least upper bounds and greatest lower bounds of any two elements exist. Dedekind discovered that this property may be axiomatized by identities. A lattice is a set on which two operations are defined, called join and meet and denoted by $\vee$ and $\wedge$, which satisfy the idempotent, commutative and associative laws, as well as the absorption laws:

$$a \vee (b \wedge a) = a$$
$$a \wedge (b \vee a) = a.$$

Lattices are better behaved than partially ordered sets lacking upper or lower bounds. The contrast is evident in the examples of the lattice of partitions of a set and the partially ordered set of partitions of a number. The family of all partitions of a set (also called equivalence relations) is a lattice when partitions are ordered by refinement. The lattice of partitions of a set remains to this day rich in pleasant surprises. On the other hand, the partially ordered set of partitions of an integer, ordered by refinement, is not a lattice and is fraught with pathological properties.

Distributive Lattices

A distributive lattice is a lattice that satisfies the distributive law:

$$a \vee (b \wedge c) = (a \wedge b) \vee (a \wedge c).$$

For a long time a great many people believed that every lattice is distributive. This misunderstanding was finally cleared up when Garrett Birkhoff, in the early thirties, proved a fundamental theorem, which we summarize next.

There is a standard way of constructing distributive lattices. One takes all the order ideals of a partially ordered set P. An order ideal is a subset of P with the property that if $x \in P$ and $y \leq x$, then $y \in P$. Union and intersection of order ideals are order ideals. In other words, the set of all order ideals of a partially ordered set is a distributive lattice.

Garrett Birkhoff proved the converse of this statement: every finite distributive lattice is isomorphic to the lattice of order ideals of some partially ordered set. The resulting contravariant functor from the category of partially ordered sets to the category of distributive lattices, known as the "Birkhoff transform", provides a systematic and useful translation of the combinatorics of partially ordered sets into the algebra of distributive lattices.

The definitive generalization of Birkhoff's theorem to arbitrary distributive lattices was obtained in the sixties by Ann Priestley. Briefly, there is a nontrivial extension of the notion of topological space that takes order into account, defined by Leopoldo Nachbin in his thesis. Distributive lattices are represented as lattices of closed order ideals on such ordered topological spaces. Point set topology has been nontrivially extended to ordered topological spaces, but this extension has remained largely unknown. Dieudonné was taken with it after he read the copy of Nachbin's thesis that the author, working in total isolation, sent him from Rio de Janeiro. Dieudonné tried to drum up some interest in ordered topological spaces without success.

It is a miracle that families of sets closed under unions and intersections can be characterized solely by the distributive law and by some simple identities. Jaded as we are, we tend to take Birkhoff's discovery for granted and to forget that it was a fundamental step forward in mathematics.

Modular Lattices

Modular lattices are lattices that satisfy the following identity, discovered by Dedekind:

$$(c \wedge (a \vee b)) \vee b = (c \vee b) \wedge (a \vee b).$$

This identity is customarily recast in user-friendlier ways. Examples of modular lattices are lattices of subspaces of vector spaces, lattices of ideals of a ring, lattices of submodules of a module over a ring, and lattices of normal subgroups of a group. For example, in the lattice of subspaces of a vector space the meet of two subspaces is their set theoretic intersection, and the join of two subspaces is the subspace spanned by the two subspaces. Join and meet of linear varieties in projective space are algebraic renderings of projection and section of synthetic projective geometry. Synthetic projective geometry, relying as it does on axioms of incidence and refusing any appeal to coordinates, is best understood in the language of modular lattices.

But synthetic geometry acquired a bad name after algebraic geometers declared themselves unable to prove their theorems by synthetic methods. The synthetic presentation of geometry has become in the latter half of this century a curiosity, cultivated by Italians and by Professor Coxeter. Modular lattices were dismissed without a hearing as a curious outgrowth of a curiosity.

Garrett once described to me his first meeting with von Neumann. After exchanging a few words they quickly got down to their common interest in lattice theory, and von Neumann asked Garrett, "Do you know how many subspaces you get when you take all joins and meets of three subspaces of a vector space in general position?" Garrett immediately answered, "Twenty-eight!", and their collaboration began at that moment.

The free modular lattice with three generators, which indeed has twenty-eight elements, is a beautiful construct that is presently exiled from textbooks in linear algebra. Too bad, because the elements of this lattice explicitly describe all projective invariants of three subspaces.

One of Garrett's theorems on modular lattices states that the free modular lattice generated by two linearly ordered sets (or chains) is distributive. This result has been shamelessly restated without credit in disparate mathematical languages.

The core of the theory of modular lattices is the generalization of the theory of linear dependence of sets of vectors in a vector space to sets of linear subspaces of any dimension. Dilworth, Kurosh, Ore, and several others defined an extended concept of basis, and they established invariance of dimension and exchange properties of bases. The translation of their results into coordinate language is only now being carried out.

Two recent developments in modular lattices are:

First, the discovery of 2-distributive lattices by the Hungarian mathematician Andras Huhn. A 2-distributive lattice is a lattice that satisfies the identity

$$a \vee (x \wedge y \wedge z) =$$
$$(a \wedge (x \vee y)) \vee (a \wedge (x \vee y)) \vee (a \vee (y \wedge z)).$$

This improbable identity implies that the lattice is modular and much more. It has been shown by Bjarni Jónsson, J. B. Nation, and several others that 2-distributive lattices are precisely those lattices that are isomorphically embeddable into the lattice of subspaces of a vector space over any field whatsoever, subject only to cardinality restrictions. Thus, 2-distributive lattices come close to realizing the ideal of a universal synthetic geometry, at least for linear varieties. They have a rich combinatorial structure.

Second, the theory of semiprimary lattices. These lattices were given their unfortunate name by Reinhold Baer, but, again, only recently has their importance been realized in the work of such young mathematicians as Franco Regonati and Glenn Tesler. Examples of semiprimary lattices are the lattice of subgroups of a finite Abelian group and the lattice of invariant subspaces of a nilpotent matrix. Semiprimary lattices are modular, and hence every element is endowed with a rank or dimension. However, the elements of semiprimary lattices are additionally endowed with a finer type of rank, which is a partitition of an integer, or a Young shape, as we say in combinatorics. For the lattice of subgroups of an Abelian group such a partition comes from the structure theorem for finite Abelian groups; for the invariant subspaces of nilpotent matrices the partition comes from the Jordan canonical form.

This finer notion of dimension leads to a refinement of the theory of linear dependence. One major result, due to Robert Steinberg, is the following. Consider a complete chain in a semi-primary lattice. Two successive elements of the chain differ by one dimension, but much more is true. As we wind up the chain, we fill a Young shape with integers corresponding to the positions of each element of the chain, and thus every complete chain is made to correspond to a standard Young tableau.

Now take two complete chains in a semiprimary lattice. It is easy to see that a pair of complete chains in a modular lattice determines a permutation of basis vectors. In a semiprimary lattice each of the two chains is associated with a standard Young tableau, hence we obtain the statement and proof of the Schensted algorithm, which precisely associates a pair of standard Young tableaux to every permutation.

Lattice of Ideals

Dedekind outlined the program of studying the ideals of a commutative ring by lattice-theoretic methods, but the relevance of lattice theory in commutative algebra was not appreciated by algebraists until the sixties, when Grothendieck demanded that the prime ideals of a ring should be granted equal rights with maximal ideals. Those mathematicians who knew some lattice theory watched with amazement as the algebraic geometers of the Grothendieck school clumsily reinvented the rudiments of lattice theory in their own language. To this day lattice theory has not made much of a dent in the sect of algebraic geometers; if ever it does, it will contribute new insights. One elementary instance: the Chinese remainder theorem. Necessary and sufficient conditions on a commutative ring are known that insure the validity of the Chinese remainder theorem. There is, however, one necessary and sufficient condition that places the theorem in proper perspective. It states that the Chinese remainder theorem holds in a commutative ring if and only if the lattice of ideals of the ring is distributive.

The theory of ideals in polynomial rings was given an abstract setting by Emmy Noether and her school. Noetherian rings were defined, together with prime and primary ideals, and fundamental factorization theorems for ideals were proved. It does not seem outrageous to go one step further in Dedekind's footsteps and extend these theorems to modular lattices. This program was initiated by Oystein Ore and developed by Morgan Ward of Caltech and by his student, Bob Dilworth. Dilworth worked at this program on and off all his life, and in his last paper on the subject, published in 1961, he finally obtained a lattice theoretic formulation of the Noetherian theory of ideals. I quote from the introduction of Dilworth's paper:

> The difficulty [of the lattice theory of ideals] occurred in treating the Noether theorem on decompositon into primary ideals. … In this paper, I give a new and stronger formulation for the notion of a "principal element" and…prove a [lattice theoretic] version of the Krull Principal Ideal Theorem. Since there are generally many non-principal ideals of a commutative ring which are "principal elements" in the lattice of ideals, the [lattice theoretic] theorem represents a considerable strengthening of the classical Krull result.

Forgive my presumptuousness for making a prediction about the future of the theory of commutative rings, a subject in which I have never worked. The theory of commutative rings has been torn by two customers: number theory and geometry.

Our concern here is the relationship between commutative rings and geometry, not number theory. In the latter part of this century algebra has so overwhelmed geometry that geometry has come to be viewed as a mere "façon de parler". Sooner or later geometry in the synthetic vein will reassert its rights, and the lattice theory of ideals will be its venue. We intuitively feel that there is a geometry, projective, algebraic, or whatever, whose statements hold independently of the choice of a base field. Desargues's theorem is the simplest theorem of such a "universal" geometry. A new class of commutative rings remains to be discovered that will be completely determined by their lattice of ideals. Von Neumann found a class of noncommutative rings that are determined by their lattices of ideals, as we will shortly see, but the problem for commutative rings seems more difficult. A first step in this direction was taken by Hochster. Algebraic geometry done with such rings might be a candidate for "universal geometry".

Commutative rings set the pace for a wide class of algebraic systems in the sense of Garrett Birkhoff's universal algebra. The lattice of congruences of an algebraic system generalizes the lattice of ideals, and this analogy allows us to translate facts about commutative rings into facts about more general algebraic systems. An example of successful translation is the Chinese remainder theorem in its lattice theoretic formulation, which has been proved for general algebras. The work of Richard Herrmann and his school has gone far in this direction. In view of the abundance of new algebraic structures that are being born out of wedlock in computer science, this translation is likely to bear fruit.

Linear Lattices

Having argued for modular lattices, let me now argue against them.

It turns out that all modular lattices that occur in algebra are endowed with a richer structure. They are lattices of commuting equivalence relations. What are commuting equivalence relations?

Two equivalence relations on a set are said to be independent when every equivalence class of the first meets every equivalence class of the second. This notion of independence originated in information theory and has the following intuitive interpretation. In the problem of searching for an unknown element, an equivalence relation can be viewed as a question whose answer will tell to which equivalence class the unknown element belongs. Two equivalence relations are independent when the answer to either question gives no information on the possible answer to the other question.

Philosophers have gone wild over the mathematical definition of independence. Unfortunately, in mathematics philosophy is permanently condemned to play second fiddle to algebra. The pairs of equivalence relations that occur in algebra are seldom independent; instead, they satisfy a sophisticated variant of independence that has yet to be philosophically understood—they commute.

Two equivalence relations are said to commute when the underlying set may be partitioned into disjoint blocks and the restriction of the pair of equivalence relations to each of these blocks is a pair of independent equivalence relations. In other words, two equivalence relations commute when they are isomorphic to disjoint sums of independent equivalence relations on disjoint sets.

Mme. Dubreil found in her 1939 thesis an elegant characterization of commuting equivalence relations. Two equivalence relations on the same set commute whenever they commute in the sense of composition of relations, hence the name.

The lattice of subspaces of a vector space is an example of a lattice that is naturally isomorphic to a lattice of commuting equivalence relations on the underlying vector space viewed as a mere set. Indeed, if W is a subspace of a vector space V, one defines an equivalence relation on the set of vectors in V by setting $x \equiv_W y$ whenever $x - y \in W$. Meet and join of subspaces are isomorphic to meet and join of the corresponding equivalence relations in the lattice of all equivalence relations on the set V. The lattice of subspaces of a vector space V is isomorphic to a sublattice of the lattice of all equivalence relations on the set V, in which any two equivalence relations commute.

Similar mappings into lattices of commuting equivalence relations exist for the lattice of all ideals of a ring and the lattice of all submodules of a module. Mark Haiman has proposed the term "linear lattice" for lattices of commuting equivalence relations.

Schützenberger found an identity satisfied in certain modular lattices that is equivalent to Desargues's theorem. Not long afterwards, Bjarni Jónsson proved that every linear lattice satisfies Schützenberger's identity. At that time the problem arose of characterizing linear lattices by identities. This brings us to two notable theorems Garrett proved in universal algebra.

The first of Birkhoff's theorems characterizes categories of algebraic systems which can be defined by identities. These are precisely those categories of algebraic systems that are closed under the three operations of products, subalgebras, and homomorphic images. For example, groups and rings can be characterized by identities, but fields cannot, because the product of two fields is not a field. There are algebraic systems which are known to be definable by identities because they have been shown to satisfy the three Birkhoff conditions but for which the actual identities are not known.

The second of Birkhoff's theorems states that a category of algebraic systems is endowed with "free algebras" if and only if it is closed under products and subalgebras.

The category of linear lattices is closed under products and sublattices, so that the free linear lattice on any set of generators exists. A thorough study of free linear lattices, revealing their rich structure, was carried out by Gelfand and Ponomarev in a remarkable series of papers. Their results are so stated as to apply both to modular and to linear lattices. The free linear lattice in n generators is intimately related to the ring of invariants of a set of n subspaces in general position in projective space. Gelfand has conjectured that the free linear lattice in four generators is decidable. Recently an explicit set of generators for the ring of invariants of a set of four subspaces in projective space has been given by Howe and Huang; Gelfand's conjecture is the lattice theoretic analog and is thus probably true.

It is not known whether linear lattices may be characterized by identities. Haiman has proved that linear lattices satisfy most of the classical theorems of projective geometry, such as various generalizations of Desargues's theorem, and he proved that not even these generalized Desarguian conditions suffice to characterize linear lattices.

The deepest results to date on linear lattices are due to Haiman, who in his thesis developed a proof theory for linear lattices. What does such a proof theory consist of? It is an iterative algorithm performed on a lattice inequality that splits the inequality into subinequalities by a tree-like procedure and eventually establishes that the inequality is true in all linear lattices, or else it automatically provides a counterexample. A proof theoretic algorithm is at least as significant as a decision procedure, since a decision procedure is merely an assurance that the proof theoretic algorithm will eventually stop.

Haiman's proof theory for linear lattices brings to fruition the program that was set forth in the celebrated paper "The logic of quantum mechanics", by Birkhoff and von Neumann. This paper argues that modular lattices provide a new logic suited to quantum mechanics. The authors did not know that the modular lattices of quantum mechanics are linear lattices. In light of Haiman's proof theory, we may now confidently assert that Birkhoff and von Neumann's logic of quantum mechanics is indeed the long-awaited new "logic" where meet and join are endowed with a logical meaning that is a direct descendant of "and" and "or" of propositional logic.

Lattice Theory and Probability

One of the dramas of present-day mathematics is the advent of noncommutative probability. Lattice theoretically, this drama is a game played with three lattices: the lattice of equivalence relations, Boolean algebras, and various linear lattices that are threatening to replace the first two.

Classical probability is a game of two lattices defined on a sample space: the Boolean σ-algebra of events and the lattice of Boolean σ-subalgebras.

A σ-subalgebra of a sample space is a generalized equivalence relation on the sample points. In a sample space the Boolean σ-algebra of events and the lattice of σ-subalgebras are dual notions, but whereas the Boolean σ-algebra of events has a simple structure, the same cannot be said of the lattice of σ-subalgebras. For example, we understand fairly well measures on a Boolean σ-algebra, but the analogous notion for the lattice of σ-subalgebras—namely, entropy—is poorly understood.

Stochastic independence of two Boolean σ-subalgebras is a strengthening of the notion of independence of equivalence relations. Commuting equivalence relations also have a stochastic analog, which is best expressed in terms of random variables. We say that two σ-subalgebras, Σ_1 and Σ_2, commute when any two random variables X_1 and X_2 defining the σ-subalgebras Σ_1 and Σ_2 are conditionally independent. Catherine Yan has studied the probabilistic analog of a lattice of commuting equivalence relations: namely, lattices of nonatomic σ-subalgebras, any two of which are stochastically commuting. There are stochastic processes where all associated σ-subalgebras are commuting in Yan's sense, for example, Gaussian processes.

In a strenuous tour de force, Catherine Yan has developed a proof theory for lattices of nonatomic commuting σ-subalgebras. Her theory casts new light on probability. It is also a vindication of Dorothy Maharam's pioneering work in the classification of Boolean σ-algebras.

The portrait of noncommutative probability is at present far from complete. Von Neumann worked hard at a probabilistic setting for quantum mechanics. His search for a quantum analog of a sample space led him to the discovery of continuous geometries. These geometries are similar to projective spaces, except that the dimension function takes all real values between zero and one. Von Neumann characterized continuous geometries as modular lattices and showed that noncommutative rings can be associated with continuous geometries which share properties of rings of random variables, in particular that there is the analog of a probability distribution.

Sadly the applications of continuous geometries have hardly been explored; allow me to stick my neck out and mention one possible such application. It is probable that some of the attractive q-identities that are now being proved by representation theoretic methods can be given a "bijective" interpretation in continuous geometries over finite fields. I have checked this conjecture only for the simplest q-identities.

The triumph of von Neumann's ideas on quantum probability is his hyperfinite factor, which unlike Hilbert space has a modular lattice of closed subspaces. For a long time I have wondered why quantum mechanics is not done in the hyperfinite factor rather than in Hilbert space. Philosophically, probability in a hyperfinite factor is more attractive than ordinary probability, since the duality between events and σ-subalgebras is replaced by a single modular lattice that plays the role of both. On several occasions I have asked experts in quantum mechanics why the hyperfinite factor has been quietly left aside, and invariably I received evasive answers. Most likely, physicists and mathematicians needed some fifty years of training to grow accustomed to noncommutative probability, and only now are the tables beginning to turn after the brilliant contributions to noncommutative geometry and noncommutative probability by Alain Connes and Dan Virgil Voiculescu.

Other Directions

It is heartening to watch every nook and cranny of lattice theory coming back to the fore after a long period of neglect. One recent instance: MacNeille, a student of Garrett's, developed a theory of completion by cuts of partially ordered sets, analogous to Dedekind's construction of the real numbers. His work was viewed as a dead end until last year, when Lascoux and Schützenberger, in their last joint paper, showed that MacNeille's completion neatly explains the heretofore mysterious Bruhat orders of representation theory.

Two new structures that generalize the concept of a lattice should be mentioned in closing. First, Tits buildings. It is unfortunate that presentations of buildings avoid the lattice theoretic examples, which would display the continuity of thought that leads from lattices to buildings.

Second, Δ-matroids, due to Kung, and developed by Dress, Wentzel, and several others. Garrett Birkhoff realized that Whitney's matroids could be cast in the language of geometric lattices, which Garrett first defined in a paper that appeared right after Whitney's paper in the same issue of the *American Journal*. Roughly, Δ-matroids are to Pfaffians as matroids are to determinants. Δ-matroids call for a generalization of lattices that remains to be explored.

These developments, and several others that I have not mentioned, are a belated validation of Garrett Birkhoff's vision, which we learned in three editions of his *Lattice Theory*, and they betoken Professor Gelfand's oft-repeated prediction that lattice theory will play a leading role in the mathematics of the twenty-first century.