Chapter 7
Understanding School Mathematics in Terms of Linear Measure and Discrete Real Additive Groups

Hyman Bass

Introduction

I report here on a capstone mathematics course for secondary mathematics teachers,[1] developed experimentally over the past several years. In this course I have attempted, among other things, to incorporate ideas of abstract algebra that are situated in the fundamental mathematical structures of school mathematics, and to use them to illuminate those structures, and reveal often-unseen connections. For example, rather than develop general group theory, I focus on the structure of the additive and multiplicative groups of the basic rings of school mathematics, and use the group theoretic perspective to illuminate and connect many school topics. I contend that this exposure to "abstract algebra in context" contributes significantly to mathematical knowledge for teaching (Ball, Thames, & Phelps, 2008), perhaps an aspect of "horizon knowledge." But this might be less clear, or less accessible, with other important abstract algebra topics (Sylow Theorems, Galois Theory, etc.).

In addition to making curricular connections across mathematical topics, I have designed some novel problem-solving formats to prompt making connections. These connections have, primarily, been of one of two forms: (1) connections across mathematical domains, and (2) structural connections between apparently unrelated problems. Examples of these also are presented below.

[1] Though addressed to secondary teachers, much of the course content deepens understanding of mathematics in the early grades as well. The course is also suitable for regular mathematics majors.

H. Bass (✉)
Department of Mathematics and School of Education, University of Michigan, Ann Arbor, MI, USA
e-mail: hybass@umich.edu

N. H. Wasserman (ed.), *Connecting Abstract Algebra to Secondary Mathematics, for Secondary Mathematics Teachers*, Research in Mathematics Education,
https://doi.org/10.1007/978-3-319-99214-3_7

I begin below with a brief overview of abstract algebra and its origins. Following that, I outline the structure of my course. The content of the course represents my own mathematical perspective on school mathematics, aimed at conceptual coherence. It centrally features the real number line, with its geometric and arithmetic structures. Linear measurement, expressed through division with remainder, leads directly to place value and modular congruence. Abstract algebra enters through the study of discrete additive groups of real numbers, from which multiplicative arithmetic and commensurability (irrationality) naturally emerge. Brief treatments of polynomial algebra and combinatorics then culminate in discrete calculus, the natural generalization of the “pattern generalization” activities in school mathematics. Finally, I present and discuss some problem-solving designs, which I regard as a way to cultivate important mathematical practices in the course.

What Is Abstract Algebra, and Where Did It Come from?

“Algebra” signifies many things. First, it provides a compact and efficient (but sometimes opaque) symbolic notational system to compose mathematical expressions and relations involving abstract quantities. An early appearance of this is the (x, y) Cartesian coordinate system, which supported the algebraic formulation of many geometric ideas. The origins of algebra as a substantive mathematical domain came from efforts to solve polynomial equations in one variable, for example finding higher degree analogues of the quadratic formula (degree 2, “known” already by the ancient Babylonians and Egyptians). Italian mathematicians in the sixteenth century succeeded with cubic and quartic equations (degrees 3 and 4), but the quintic (degree 5) resisted. The deep proof (by Abel) that the general quintic equation could *not* be solved by radicals ushered in some of the most fundamental ideas of modern mathematics, group theory in particular, via algebraically permissible permutations of the roots of a polynomial. This strand culminates today in Galois Theory, the capstone of some abstract algebra courses.

“Modern” or “abstract” algebra, with its emphasis on general structures (groups, rings, and fields), axiomatically defined, took hold in the twentieth century, starting with the lectures of Emmy Noether and Emil Artin, and captured in van der Waerden’s classic text, *Moderne Algebra* (van der Waerden, 1930, 1931). These structures arise from both number theory (studying generalizations of the arithmetic of integers and the rational numbers) and from efforts to understand solutions of polynomial equations (with real or complex coefficients)—eventually, several equations of arbitrary degree in several variables. One linear (i.e., degree 1) equation in one variable reduces to elementary arithmetic with the four operations (typically learned in grades 1–6); the solution of $ax + b = 0$ is $x = -b/a$. One equation in one variable of *higher degree* is a big jump in sophistication and culminates with Galois Theory (undergraduate math majors). Many *linear* equations in several variables are the core of linear algebra, for which there is a fairly complete and accessible algebraic theory (undergraduate STEM students). This is fundamental

Table 7.1 The "geography" of algebraic equations

Domain	Degree	Variables	Learners
Elementary arithmetic	1	1	Grades 1–6
Linear algebra	1	>1	STEM majors
Field and Galois theory	>1	1	Math majors
Algebraic geometry	>1	>1	Research mathematicians

since, whereas the world is mostly nonlinear; many problems are first approached by linear approximation, calculus being a preeminent example of this. The vast general case (many equations, many variables, high degree) is algebraic geometry, one of the most advanced areas of contemporary mathematics (research mathematicians) (see Table 7.1).

The power of axiomatic methods became clear in the twentieth century: mathematicians were able to solve many longstanding problems[2] that had earlier seemed intractable. As such, abstract algebra gained a prominent place in the professional training of mathematicians. This standing gradually trickled down into the curriculum of general mathematics majors, thereby affecting secondary mathematics teachers, who are required to be mathematics majors. The "New Math" reforms of the 1950s and 1960s even witnessed (eventually aborted) efforts to have abstract approaches infiltrate the early school grades.

Abstract Algebra for Secondary Teaching

The power of mathematical abstraction is its generality, thus having the potential to conceptually unify many apparently distinct mathematical contexts. But abstraction also exacts a cost for the novice learner since, by its nature, abstraction purges the concepts of the concrete individual contexts that it generalizes, and these are a main source of sense making.

Thus, one may reasonably ask, "What is the abstract algebra easily accessible to secondary teachers that deeply relates to their work as teachers?" This question is hard to manage since teachers' mathematics content courses are generally taught in mathematics departments, and it makes sense for these departments to require their majors to learn abstract algebra. At the same time, the work of teaching requires a depth and flexibility of mathematical understanding of the fundamental structures of the school curriculum (place value, the number line, algebraic equations, and

[2] For example, Hilbert's proof, using Noetherian conditions, that the ring of invariant polynomials of a reductive group action is finitely generated, thus eclipsing years of laborious, inconclusive computation.

functions) that is often not fully achieved in typical academic mathematics courses, and is even lacking among many mathematics majors.[3]

While the main ideas and constructs of abstract algebra are arguably relevant to school mathematics, their typical academic presentation contains much that is remote from the needs of K-12 teachers, in two respects. First, its generality and basic examples quickly exceed the context of school mathematics. This is a pragmatic consideration since teachers' exposure to mathematics is limited in time. Second, the rich algebraic structures already present in school mathematics (for example the algebraic (and geometric) structure of additive and multiplicative groups of real numbers and of modular rings) are often not treated, in abstract algebra courses, in sufficient detail to illuminate and add depth and coherence to related school mathematics topics.

Consider the case of group theory. In an abstract algebra course, among the first examples after cyclic groups are the symmetric groups. While they are of major mathematical importance, they are not familiar objects to school students, and computations in them are difficult and notationally complex. Non-commutative groups first arise most naturally as groups of geometric transformations (symmetries), a rich and beautiful development. While geometric transformations appear in high school curricula, they are not generally treated from a group theoretic perspective.

The Conceptual Foundations of My Course

I take the real number line, with its combined arithmetic and geometric structures, to be a central object of in-depth study throughout. In this regard, I am influenced by the ideas of Davydov (1990), who emphasized the centrality of quantities and their measurement in the teaching and learning of mathematics, starting in the earliest grades. In particular, I feature *division with remainder* as the far-reaching *conceptual foundation of linear measurement*, not as a computational task in whole number arithmetic. It leads directly to both the detailed development of place value expansion (in any base) of a positive real number, and to modular congruence.

In the treatment of the four arithmetic operations, school mathematics emphasizes algorithmic computation in the place value, or fraction, notational systems. While concrete computation is vitally important, what is relatively neglected in school mathematics is the *conceptual geometric meaning of the operations on the number line*. For example, addition and subtraction can be interpreted in terms of translations, and multiplication in terms of 0-centered dilation and reflection. These understandings are at once intuitively accessible, *pre-computational*, and they are the foundation for proving some striking and consequential theorems about

[3] I say this from having taught the course several times to successful mathematics majors, who consistently note that they are learning things about place value, and about the number line, that they had never known before.

real additive groups, starting with division with remainder itself. Interestingly, this treatment leads naturally to the notion of commensurability, providing a deepened understanding of the distinction between rational and irrational numbers, as well as group theoretic definitions of gcd and lcm, thus making their basic properties all easily derivable, prior to prime factorization theory.

Group theory enters through the study of the additive and multiplicative groups of the basic rings of school mathematics—integers, rationals, reals, and, eventually, complex numbers, and modular rings. Many of the early theorems in arithmetic (Fermat's Little Theorem, Cauchy's Theorem, multiplicativity of the phi-function, quadratic residues, and even gcd and lcm) are essentially group theoretic in nature. Division with remainder is used to give a complete description of discrete additive groups of real numbers. The multiplicative group $\mathbb{R}^*$ (with $\mathbb{R}^* = \mathbb{R}\{0\}$) of nonzero real numbers exhibits torsion, $\{\pm 1\}$, and a direct product structure, $\mathbb{R}^* = \{\pm 1\} \times (0, \infty)$, with corresponding *homomorphisms*, *sign*, and *absolute value*. Moreover we have an order preserving group *isomorphism*, $\exp : \mathbb{R} \to (0, \infty)$, from the additive to the positive multiplicative group, with inverse log. The latter permits us to transport additive group theorems to the multiplicative group, where they would be much more difficult to discover and prove directly. So these real additive and multiplicative groups provide a direct and organic connection of significant school mathematics to some substantial, yet "familiar," abstract algebra—even prior to the axiomatic definition of a group. And this arises even before number theoretic ideas, which are captured in the study of additive and multiplicative groups of modular rings. The eventual study of additive and multiplicative groups of complex numbers leads to two-dimensional vector algebra and to two-dimensional geometric transformations.

The course also includes some fundamental "classical algebra," for example a brief treatment of the basic properties of polynomials (root theorems, Binomial Theorem, interpolation, etc.), coupled naturally with an introduction to combinatorics. The proof of the Binomial Theorem is derived from a more basic algebraic identity ("A product of sums is a sum of products" or "distributivity on steroids") that yields also a proof of the inclusion–exclusion formula, even in geometric measure settings. Combining the root theorems with group theory, we show that any finite multiplicative group of a field (e.g., the multiplicative group of a finite field) is cyclic.[4]

Many of these ideas converge in the chapter on Discrete Calculus. Many secondary curricula now introduce functions largely as an activity of "finding a pattern" in some finite sequence of numbers (or figures), on the basis of determining the next term, and, eventually, the general term. The data presented are equivalent to a table pairing the term number in the sequence with the corresponding value, or

[4] This is derived from the following theorem about a finite group G of order n. For each whole number d, let $G_d = \{x \in G | \, x^d = 1\}$. If: $(*)$ [For each divisor d of n, $\#G_d \leq d$], then G is cyclic. If G is in a field, then $(*)$ follows from the root theorem for $X^d - 1$.The theorem is proved by close comparison of G with $\mathbb{Z}/\mathbb{Z}n$.

equivalently, a finite list of points in the plane. An expression for the general term then simply defines a function whose graph passes through the given points. In other words, this is essentially an interpolation problem. The "pattern" comes into play in suggesting a simplest function solution, linear in the case of constant difference, exponential in the case of a constant ratio. If the differences are not constant, one can look at differences of differences, etc., thus reaching quadratic functions, for example.

The method of looking at successive differences is just the "differential" aspect of Discrete Calculus, a topic that is built on the basic algebraic foundations described above. It provides an elegant and accessible formal analogue of Calculus itself, and it leads quickly to a number of interesting results and connections to school mathematics—e.g., the Binomial Theorem, the formulas for sums of powers of consecutive natural numbers, etc. Above all, Discrete Calculus provides, in my view, a much more comprehensive and powerful framework for initial understanding of functions. It is perhaps a good alternative to high school calculus, one that would strengthen the often-underdeveloped algebraic skills of high school graduates, even those having taken AP Calculus.

A consistent aim of my course, as I hope can be discerned in the above overview, is conceptual coherence, building on *connections* between mathematical ideas, something I feel is often lost in the fragmentation and shallow treatments of many curricular materials.

Detailed Description of the Course

The outline of a *book project* (Chaps. 1–12) based on the course is presented in Table 7.2 below. The book's contents are more comprehensive than those of the (one term) course, and would be more suitable for a full-year course. Though oriented toward secondary teachers, the course also could be of interest to more general mathematics majors (and would not substantially duplicate their typical advanced undergraduate mathematics coursework). At the same time much of the course content is highly relevant to the elementary math curriculum, and so it could be of value to mathematically well-motivated and prepared elementary teachers. For the present, necessarily brief, discussion of the course, I will simply highlight some of the novel ideas and approaches that each of the topics (i.e., chapters) of the book offers.

Division with Remainder (DwR) and Place Value

Dividing a by b ($b \neq 0$), $a = qb + r$, yields an *integer* quotient q, and a remainder r *smaller than* b. I view the problem of dividing a by b not as a piece of integer arithmetic, but rather as the *foundation of linear measurement*, where a and b are

Table 7.2 Outline of a book developed from the capstone course

Chapter	Topics
1	**Division with Remainder and Place Value** Division with Remainder (*DwR*): Given $a, b \in \mathbb{R}, b \neq 0, \exists\,!\, q \in \mathbb{Z}, r \in \mathbb{R}, 0 \leq r < \lvert b\rvert$ such that $a = qb + r$ $q = q_b(a)$, $r = r_b(a)$. The case $b = 1$: $[a] = q_1(a)$, $a = r_1(a)$ Place value: $b \in \mathbb{Z}, b \geq 2, a \in \mathbb{R}$: $a = \sum\limits_h d_h(a)b^h$, with $d_h(a) = r_b([ab^{-h}])$ Order of magnitude
2	**Modular Congruence** Given $a, b, m \in \mathbb{R} : a =_m b$ means $a - b \in \mathbb{Z}m \iff r_m(a) = r_m(b)$ Divisibility tests; "Fast track to the remainder" Base-*b* representation of a fraction, $N/D : d_{-h}(N/D) = q_D(r_D(Nb^{h-1})b)$; eventually periodic; Wait time *t*; period *p*; Write $D = D_0D_1$, so that D_0 divides b^e for some *e*, $gcd(D_1, b) = 1$. Then $t =$ least *e* such that $b^e =_{D_0} 0$, and $p =$ least *e* such that $b^e =_{D_1} 1$
3	**Rules of Arithmetic: Commutative Rings** Quick axiomatic definitions of (semi-)groups, rings, commutativity. Unit groups, zero divisors, etc. Examples, including modular rings and polynomials. Some geometric series polynomial identities. It is shown that for positive relatively prime integers *a*, *b*, the largest integer <u>not</u> in the semi-group $\mathbb{N}a + \mathbb{N}b$ is $ab - a - b$.
4	**Geometry of the Number Line** Metric spaces (*X*, *d*). Ball and spheres. Isolated points. Discrete sets. Closure; density. Detailed study of (often arithmetic) examples on the number line
5	**(Discrete) Additive Groups of Real Numbers** Let *A* be an additive group of real numbers. Theorems: I. If 0 is isolated in *A* then *A* is uniformly discrete; II. *A* is either discrete or dense in $\mathbb{R}$; III. If *A* is discrete then $A = \mathbb{Z}a$ for a unique $a \geq 0$
6	**Commensurability: gcd and lcm** Theorem IV. $\mathbb{Z}a + \mathbb{Z}b$ is discrete iff *a* and *b* are commensurable. In this case, $d = \text{gcd}\,(a, b)$ and $m = \text{lcm}\,(a, b)$ are defined to be the nonnegative generators of $\mathbb{Z}a + \mathbb{Z}b$ and $\mathbb{Z}a \cap \mathbb{Z}b$, respectively. Chinese Remainder Theorem
7	**Primes and Factorization** Definition; infinitely many. Prime (Power) Factorization: $a = \pm \Pi p^{e(p,a)}$. Mersenne, perfect, and Fermat numbers. Appendices: Multiplicative groups of modular rings; applications to cryptography
8	**Combinatorics** Brief introduction. "*n*-choose-*d*," ${}_nC_d$; Pascal's Triangle
9	**Polynomials** Degree, leading term, roots. $f(a) = 0$ iff $(x - a)$ divides *f*. *f* has $\leq \deg(f)$ roots Interpolation. Cor. $f(\mathbb{Q}) \subseteq \mathbb{Q}$ iff all coefficients of *f* are in $\mathbb{Q}$. Binomial Theorem. A finite multiplicative group in a field is cyclic. Appendix: Inclusion–Exclusion Formula
10	**Discrete Calculus** Sequences as (the ring $\mathcal{F}$ of) functions $f : \mathbb{N} \to \mathbb{R}$. The discrete derivative Δ and integral *S*, as linear operators $\Delta, S{:}\mathcal{F} \to \mathcal{F}$. Fundamental Theorem: $\Delta Sf = f$ and $S\Delta f = f - f(0)$. Binomial polynomials $B_d(x) = {}_xC_d$. Polynomials $f = \sum a_dB_d$. $f(\mathbb{Z}) \subseteq \mathbb{Z}$ iff all $a_d \in \mathbb{Z}$. Formulas for sums of consecutive *d*th powers

(continued)

Table 7.2 (continued)

Chapter	Topics
11	**Complex Numbers** Beyond the course
12	**Plane Transformation Geometry Using Complex Numbers** Beyond the course
	Appendix: Some Problem-Solving Activity Designs
	1. Finding a structure common to a diverse set of problems 2. Showing that a diverse set of problems are all modeled by the same equation

real numbers, with b the unit of measure. Note that q (but not r in general) is still an integer. Thus, Division with Remainder (*DwR*) is a theorem about linear measure, and whose meaning is easily pictured on the number line, partitioned by the integer multiples of b, between two of which a lies. The uniqueness of *DwR* says that $q = q_b(a)$ and $r = r_b(a)$ are multivariate functions of (a, b). Here, dividing by 1 is interesting! $q_1(a) = [a]$ is the "integer part of a," and $r_1(a) = \langle a \rangle$ is the "fractional part of a." If a is a whole number, written in base-10, then $r_{10}(a)$ is the unit (or ones) digit of a. This observation leads to the following explicit formula for the coefficient d_h of b^h in the base-b expansion (with b an integer greater than 1) of a real number $a \geq 0$: $d_h = r_b([ab^{-h}])$. We also define the order of magnitude of an integer N as the number of significant digits of N, and show that this is sub-multiplicative. I pose questions showing that bases $b \neq 10$ commonly and naturally occur, for example: (1) What is a base-1000 representation of 48,279,506,371,817? Answer: You're staring at one! In fact, we recite the number in base-1000! (2) Calculating a^{89} from the definition requires 88 multiplications. How many multiplications are required using iterated squaring? This depends on the base-2 expansion of 89, and needs only nine multiplications. (3) The best time ever in the NY marathon is: 2:05:06 = 2 h, 5 min, 6 s. Maria ran her first NY marathon in 3:05:02. How much longer than the record was her time? This is a problem of 3-digit subtraction in base 60.

Modular Congruence

"$a =_m b$" is my notation for what is usually written in the more cumbersome form, "$a \equiv b \pmod{m}$."[5] Importantly, I allow a, b, m to be *real numbers*, and take the congruence to mean that $a - b$ is an *integer multiple* of m; equivalently, $r_m(a) = r_m(b)$. (This is the equivalence relation corresponding to the additive group $\mathbb{R}/\mathbb{Z}m$.) It is shown that modular congruence preserves sums, but it preserves products in general only when a, b, m, etc. are integers. This chapter also includes a systematic discussion of so called "divisibility tests," such as "casting out nines"

[5] After 6 years of use, this notation has not encountered any mathematical difficulties or conflicts.

(N is divisible by 9 iff the sum of its (base-10) digits is so). Instead, for a given divisor D, we show more generally how one can construct a function $S(N)$ with two properties: (1) $S(N)$ is, in general, much smaller than N; and (2) $S(N){=}_D N$. It follows that iterating S gives "a fast track to $r_D(N)$."

Base-b Expansion of a Proper Reduced Fraction $N/D = \sum_{h>0} d_{-h} b^{-h}$

It is shown that $d_{-h} = q_D(r_D(Nb^{h-1})b)$. Note that this involves quotients and remainders only of division by the denominator D (not N or b). This formula essentially encodes base-b long division of N by D. From this, one shows that for some "wait time t," and "period p," we have $d_{-h} = d_{-k}$ whenever $t < h < k$ and $h{=}_p k$. Write $D = D_0 D_1$ so that D_0 divides some power of b, and $\gcd(D_1, b) = 1$. Then t is the least e such that $b^e =_{D_0} 0$, and p is the least e such that $b^e =_{D_1} 1$.

Rules of Arithmetic: Commutative Rings

Commutative rings are introduced at this point, presented as formalizing the "Rules of Arithmetic," accompanied by numerous examples. Starting with one binary operation, I define semi-groups and groups, particularly the group of units of a semi-group. Among the interesting (additive) examples are: the set of fractions with square-free denominator; and the set of periods of a function of a real variable. We also derive the "Frobenius number," $ab - a - b$, of the additive semi-group generated by relatively prime integers $a, b > 0$. Next come rings, with the distributive law linking multiplication and addition. In this general context we prove familiar identities, like $0 \bullet a = 0$, $-(-a) = a$, $(-a) \bullet (-b) = a \bullet b$, etc. Then we construct the modular rings $\mathbb{Z}/\mathbb{Z}m$, and polynomial rings $A[x]$.

Geometry of the Number Line

The geometry of the number line is treated in the context of general *metric spaces*, a topic initially independent of the preceding material (except for the examples used), but then merged with the algebra in the next chapter. Though metric spaces may seem excessively general, I find this context both mathematically and pedagogically advantageous. Mathematically, it is natural and useful to understand the line as a (one-dimensional) case of Euclidean geometry. Pedagogically, geometric ideas (like the "neighborhood" of a point) are intuitively easier to process in dimensions greater than 1. Also, the geometry of $\mathbb{R}$ is defined by its order structure, but this feature, unique to dimension 1, does not convey a general geometric intuition. This is a territory notorious for definitions with multiple quantifiers, which are often difficult for students to manage. To mitigate this, I have found it helpful to use the concept of a point being *isolated* in a metric space (having “room of its own,” or having “its private space”). For example, a point $x \notin Y$ is in the *closure* of Y (in a metric space X) if x is not isolated in $Y \cup \{x\}$. The main concepts we need for our applications are *discreteness* of a metric space (all points are isolated), and *density* of one metric space Y in another space X (X is the closure of Y). Here is a sample problem: If a sequence of fractions converges to an irrational number, show that their denominators go to infinity.

(Discrete) Additive Groups of Real Numbers

The (discrete) additive groups of real numbers are a central, but, at this point, deceptively easy part of the course. We prove the following three important theorems about any additive group A of real numbers, as relatively simple applications of *DwR* (division with remainder). (I) If 0 is isolated in A, then A is uniformly discrete. (II) A is either discrete or dense in $\mathbb{R}$. (III) If A is discrete, then $A = \mathbb{Z}a$ for a unique $a \geq 0$.

Commensurability: gcd and lcm

Real numbers a and b are commensurable if $b = 0$ or if a/b is rational. Also using *DwR*, we prove the following theorem: (IV) (Commensurability Theorem) $\mathbb{Z}a + \mathbb{Z}b$ is discrete iff a and b are commensurable. In this case, $d = \text{gcd}\,(a, b)$ and $m = \text{lcm}\,(a, b)$ are defined to be the nonnegative generators of $\mathbb{Z}a + \mathbb{Z}b$ and $\mathbb{Z}a \cap \mathbb{Z}b$, respectively. From this, one can directly develop extensive properties of gcd and lcm, all prior to prime factorization (see Appendix 2).

Primes and Prime Factorization

Here I emphasize the uniqueness of the factorization, which gives rise to the functions $e_p(a)$, which is the exponent of p in the *prime power factorization* of an integer $a \neq 0$. These functions extend to rational numbers $a \neq 0$, and define homomorphisms from the multiplicative group of $\mathbb{Q}$ to the additive group of $\mathbb{Z}$. This easily gives the traditional characterizations of gcd and lcm, the divisor function, and the Euler phi function, as well as the criteria for a dth root of a rational number to be rational. There is also discussion of Mersenne, perfect, and Fermat numbers.

Combinatorics

The formula ${}_nC_d = n(n - 1)\dots(n - d + 1)/d!$, for the number of d-sets in an n-set, is derived by first showing that the numerator counts the number of *ordered* d-sets, while the denominator counts the number of orderings of a d-set. I emphasize that it is worth noting the non-obvious fact that this fraction is an integer. In the next class I ask the class to show that the product of d consecutive integers is always divisible by $d!$, to find out if they see the connection between this question and the formula. We also verify several identities that lead to Pascal's Triangle.

Polynomials

After the basics on the degree and leading term of polynomials, the "root theorems" are proved; in particular, f has at most deg(f) roots if the coefficient ring is an integral domain. This, combined with some group theory and combinatorics, is used to show that *a finite multiplicative group in a field is cyclic*. We then demonstrate *interpolation*: Given a_j, b_i $(1 \leq i \leq n)$, with the a_j twice distinct, there is a unique f of degree less than n such that $f(a_i) = b_i$, $(1 \leq i \leq n)$. It follows that if, for an infinite field $Q, f(Q) \subseteq Q$, then the coefficients of f belong to Q. The analogue for $\mathbb{Z}$ in place of a field is false, but this situation is precisely analyzed later using Discrete Calculus. We also prove the Binomial Theorem using combinatorial arguments. Similar arguments give a proof of the Inclusion–Exclusion Formula.

Discrete Calculus

The section on "Discrete Calculus" vastly generalizes the part of the high school curriculum focused on "finding patterns" in a partially given sequence. I view the set of (infinite) sequences as the ring $\mathcal{F}$ of functions $f : \mathbb{N} \to \mathbb{R}$. The discrete derivative Δ (where $\Delta f(x) = f(x + 1) - f(x)$) and the discrete integral S (where $S(x) = f(0) + f(1) + \dots + f(x - 1)$) are linear operators (i.e., Δ, $S : \mathcal{F} \to \mathcal{F}$). The Fundamental Theorem of Discrete Calculus is then a pair of simple algebraic identities: $\Delta Sf = f$, and $S\Delta f = f - f(0)$. Then I introduce the Binomial Polynomials $B_d(x)=$ "x-choose-d." These are perfectly suited for discrete calculus, because: $\Delta B_d = B_{d-1}$ (Pascal's Relation), and $SB_d = B_{d+1}$. Any polynomial f can be uniquely written as $f = \sum a_d B_d$, and it is shown that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ iff all $a_d \in \mathbb{Z}$. By expressing x^n as a linear combination of $B_d(0 \leq d \leq n)$, and integrating, we obtain formulas for the sums of consecutive nth powers.

Problem-Solving Activities that Emphasize Connections

Complementary to the topical connections developed in the construction of the course curriculum, I have tried to design instructional problem-solving activities that explicitly involve seeing and using (sometimes subtle) mathematical connections. In this section, I discuss two different types of activities: (1) connections across mathematical domains, and (2) structural connections between apparently unrelated problems.

Connections Across Mathematical Domains

A simple example of connecting across mathematical domains would be the problem discussed above, about a base-1000 representation of 48,217,589,625,903. Another example asks for a description of all real functions $f(x)$ of a real variable such that $|f(x) - f(y)| = |x - y|$ for all x and y, to see if students recognize that this is asking for all isometries of the line.

For another example, one that spans several topics of the book, after deriving the combinatorial formula, $n(n - 1)(n - 2)\ldots(n - d + 1)/d!$, for ${}_nC_d$, in the next class I ask students to show that any product of d consecutive integers is divisible by d! The exercise is intended to prompt them to see this connection between combinatorics and arithmetic. Relatedly, the ${}_xC_d$ (note, x in place of n) function gives examples of polynomials (with non-integer coefficients) that have integer values at integers. In our later discussion of Discrete Calculus, we show that integer linear combinations of the ${}_xC_d$ function are, in fact, the only such polynomials. This contrasts with our earlier conclusion, from the interpolation formula, that a polynomial taking rational values at rational numbers must have rational coefficients. All of these examples provide an opportunity for students to identify and reflect on mathematical connections that span different areas of mathematics—discrete mathematics, arithmetic, algebra, etc.

Structural Connections Between Apparently Unrelated Problems

In a more structured design activity, I focus deliberately on the goal of "seeing and using mathematical structure" (one of the eight mathematical practices in the Common Core State Standards of the United States (CCSSM, 2010)). Here, I use some designs and examples also presented in Bass (2017). The general idea is to give the class sets of diverse problems for which the task is to seek, or to discover, unexpected connections between them. This work is done collaboratively in small groups, over a period of two or more classes.

Table 7.3 An elementary sorting task (from Bass, 2017)

1. What are all three-digit numbers that you can make using each of the digits 1, 2, 3, and using each digit only once?
2. Angel, Barbara, and Clara run a race. Assuming there is no tie, what are all possible outcomes of the race (first, second, third)?
3. You are watching Angel, Barbara, and Clara playing on a merry-go-round. As the merry-go-round spins, what are all the different ways that you see the three of them from left to right?
4. You want to choose from among Angel, Barbara, and Clara, a two-person rowing team, one for the bow, the other for the stern. What are all ways to do this?
5. In a 3 × 3 grid square, color three of the (unit) squares blue, in such a way that there is at most (or at least) one blue square in each row and in each column. What are all ways of doing this?
6. Find all of the symmetries of an equilateral triangle

In one format for these problems, *sorting*, I provide students with a list of diverse problems and ask them to group together problems which are "essentially" the same, and also indicate other significant but perhaps weaker connections, using a "connection network" representation. In another format, *common structure*, I provide a set of problems that, although quite diverse, all share a common mathematical structure. The students are asked not only to solve the problems, but also to identify and articulate the common structure, and to demonstrate how it is involved in each of the problems. The problems in these common structure sets often seem, on the surface, to be unrelated. This is a challenging and engaging activity that is best enacted over several class sessions. Students have reacted quite positively to these activities, noting specifically the elements of "mathematical surprise" involved.

Tables 7.3 and 7.4 present two examples. (Other examples can be found in Bass (2017).)

It is easy to see that problems 1 and 3 are "isomorphic." And problem 5 is likewise, though the connection is more subtle. Problems 2 and 6, though giving the same kind of answer, are fundamentally different from the others, and from each other. One way to see this is to replace the "3" in these problems by an $n > 3$. Problem 4 is an outlier, essentially unrelated to the other problems.

The next example is an expansion of a set of six problems (Ar1-4, R1, and G1) published by Usiskin (1968). The thirteen problems are grouped into four different subject areas. I formed my class into small groups, each one assigned to solve, and relate, the problems in a single one of the subject areas, and to prepare a class presentation of its work the following week. In the course of these collective presentations, the class discovers, to their great surprise, that in fact *all* of the problems are modeled by a simple variant of the same Diophantine equation, $1/n + 1/m = 1/2$ (Ar1). I have used this activity in professional development settings, with teachers and mathematics educators, with the same effect. As a follow up to this activity, it can be shown how the combinatorial classification of Platonic solids reduces, using Euler's formula, to finding all solutions (V, E, F

Table 7.4 The expanded Usiskin set

ARITHMETIC
Ar1 Find all ways to express 1/2 as the sum of two unit fractions (i.e., fractions of the form 1/n, n a positive integer)
Ar2 Find all rectangles with integer side lengths whose area and perimeter are numerically equal
Ar3 The product of two integers is positive and twice their sum. What can these integers be?
Ar4 For which integers $n > 1$ does $(n - 2)$ divide $2n$?
RATES
R1 Which pairs of positive integers have harmonic mean equal to 4? [The harmonic mean h of n numbers $a_1, a_2, \ldots, a_n$ is defined so that $1/h$ is the average of the reciprocals, $\frac{1}{a_1}, \frac{1}{a_2} \cdots \frac{1}{a_n}$]
R2 Nina can paint a house in n days, and Maria can paint it in m days (n and m positive integers). Working together they can paint the house in 2 days. What are the possible values of n and m?
R3 A turtle travels up a hill at n miles per hour, and returns down the hill at m miles per hour ($n \leq m$, n and m positive integers). The average speed for the round trip is 4 miles per hour. What are the possible values of (n, m)?
GEOMETRY
G1 Given a point P in the plane, find all n such that a small circular disk centered at P can by covered by nonoverlapping congruent tiles shaped like regular n-gons that have P as a common vertex.
G2 Two vertical poles, N and M, have heights n meters and m meters, respectively, with n and m being integers. A wire is stretched from the top of pole N to the base of pole M, and another wire is stretched from the top of pole M to the base of pole N. These wires cross at a point 2 m above the ground. What are the possible values of (n, m)?
G3 The base b and corresponding height h of a triangle are integers. A square is inscribed in the triangle with one side on the given base. Suppose that the side length of the square is 2. What are the possible values of (b, h)?
ALGEBRA
Al1 For which numbers s does $p(x) = x^2 - sx + 2s$ have positive integer roots?
Al2 Let u be a positive real number. Find all solutions (n, m, v) with n and m positive integers, and $v > 0$, of the equations: $(uv)^2 = u^n = v^m$
A13 Let (r, b) be positive integers. In a bin containing $r \bullet b$ balls, r of them are red and b of them are blue. For which (r, b) is there a 50–50 chance that a randomly chosen ball will be either red or blue?

being integers greater than or equal to 3) of the (related) Diophantine equation: $1/V + 1/F = 1/2 + 1/E$. Analysis of these problems can be found in Appendix 1.

Conclusion

The course I have described aims to achieve coherence by emphasizing mathematical *connections*, in two ways: *curricular*, by making explicit some often undeveloped connections among different topics; and *cognitive*, through the design of novel cross-domain and common structure problem-solving activities. Abstract algebra fundamentally enables both aspects of this mathematical coherence, via the group theoretic study of the additive and multiplicative groups of the basic rings of school mathematics: integers, rationals, reals, complex numbers, and modular rings. The connections are most dramatic in the last chapters, which exhibit a confluence of ideas from combinatorics, number theory, algebra, and calculus.

The course provides a number of useful enlargements of the topics of typical school curricula that would likely be new for both school students and their teachers. But these could enrich and deepen their understanding of the basic structures of school mathematics, while still being mathematically accessible, and also challenging. I regard a pedagogy that features collaboration and group work, and emphasizes mathematical exposition, explanation, and justification, as an important component of this course. In addition to a course structure, various units could also be adapted and used in professional development settings. In sum, the course provides one example of how ideas from abstract algebra—and other areas of mathematics—can be developed from and connected to the mathematics of the school curriculum.

Appendix 1: Analysis of the Extended Usiskin Problem Set

Problems **Ar1**, **Ar2**, **Ar3**, **Ar4**, in order, lead directly to the following Diophantine equations ("Diophantine" because one seeks (positive) *integer* solutions):

$$1/n + 1/m = 1/2 \tag{7.1}$$

$$2\,(n+m) = nm \tag{7.2}$$

$$2n = m\,(n-2) \tag{7.3}$$

$$\text{For which } n > 1 \text{ does } n-2 \text{ divide } 2n \tag{7.4}$$

Version (7.4) is essentially a verbal expression of the Eq. (7.3). Moreover, it is not difficult to see how Eqs. (7.1–7.3) are algebraically equivalent. For example, multiply (7.1) by $2nm$ to get (7.2); and subtract $2m$ from (7.2) to get (7.3). Hence, solving any one of them provides solutions to the others.

My students generally preferred to use (7.3) to express m in terms of n:

$$m = 2n/(n-2). \tag{7.5}$$

They then did numerical experiments to find those n for which $2n/(n-2)$ is an integer. (Some students even graphed m in (7.5) as a function of $n > 0$, and highlighted the integer points on the graph.) The solutions they found were:

$$(n, m) = (4, 4)\,, (3, 6)\,, \text{or } (6, 3)\,. \tag{7.6}$$

None of the students tried to work directly with (7.1), which is my preferred approach. Using the symmetric roles of m and n, we can assume that $n \leq m$. Then $n \geq 3$; otherwise $1/n \geq 1/2$. Also $n \leq 4$; otherwise $1/n + 1/m < 1/2$. Thus either $n = 3$ (and so $m = 6$) or $n = 4$ (and so $m = 4$).

Problem **R1** corresponds to the equation,

$$1/4 = (1/2)\,(1/n + 1/m)\,, \tag{7.7}$$

which is (7.1) multiplied by 1/2.

For Problem **R3**: If one travels distance d at speed v in time t, then: $d = vt$ and $t = d/v$. Now suppose that one travels distance d at speed v_1 in time t_1, and then returns at speed v_2 in time t_2. What is the average speed for the whole trip? It is

$$\begin{aligned} v_{ave} &= (\text{total distance}) \,/\, (\text{total time}) \\ &= 2d / \,(t_1 + t_2) \\ &= \frac{2d}{\frac{d}{v_1} + \frac{d}{v_1}} = \frac{2}{\frac{1}{v_1} + \frac{1}{v_2}} \end{aligned}$$

Thus,

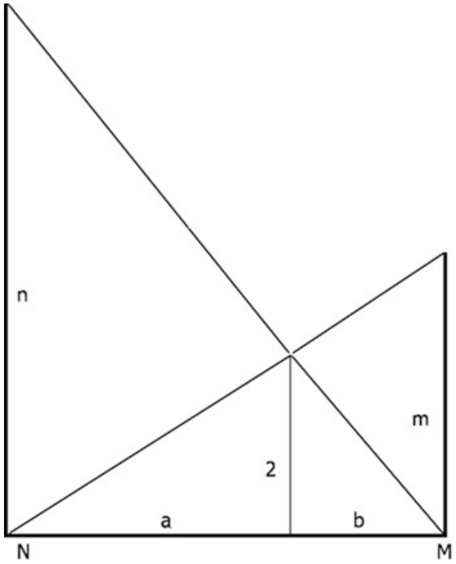
$$\frac{1}{v_{\text{ave}}} = \frac{1}{2}\left(\frac{1}{v_1} + \frac{1}{v_2}\right).$$

In other words, v_{ave} is the harmonic mean of v_1 and v_2. In problem **R2**, d would be the work of painting the house, and n and m are the rates at which Nan and her Mom do that job. The rate of doing it together (analogous to average speed) is the harmonic mean of the two rates.

The **geometry problems** are less obviously related, but they too lead to the same Diophantine equations. In Problem **G1**, let $\alpha(n)$ denote the (equal) interior angle(s) of a regular n-gon: then it is known that $\alpha(n) = \frac{n-2}{n} \cdot 180^{\circ}$. For some number, say m, of these regular n-gons to fit together to cover the area around a point P, we would need: $m \cdot \frac{n-2}{n} \cdot 180^{\circ} = 360^{\circ}$, i.e.,

$$m\,(n-2) = 2n, \text{ as in } \mathbf{Ar3}. \tag{7.8}$$

For **G2** (also framed as the “crossing ladders problem”), consider the diagram:



Using similar triangles we have:

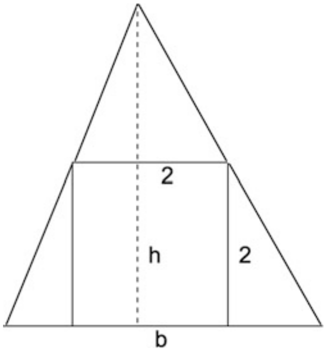
$$(a + b) / n = a/2, \text{ and}$$

$$(a + b) / m = b/2$$

Adding these equations, and then dividing by $a + b$, gives

$$1/n + 1/m = 1/2, \text{ as in } \mathbf{Ar1}. \tag{7.9}$$

For **G3**, consider the diagram:



The big triangle and the one above the square are similar (corresponding sides are parallel), and so $h/b = (h - 2)/2$, whence, multiplying this by $2b$, the equation

$$2h = b\,(h - 2)\,, \text{ as in } \mathbf{Ar3}. \tag{7.10}$$

In **Al1**, if we formally factor p:
$p(x) = x^2 - sx + 2s = (x - n)(x - m) \ldots (n, m$ being integers)
we find that

$$n + m = s, \text{ and}$$

$$nm = 2s$$

whence n and m are positive, since s is, and so we have the equation

$$nm = 2\,(n + m)\,, \text{ as in } \mathbf{Ar2}. \tag{7.11}$$

Then s (=$n + m$) = 8 (=4 + 4) or 9 (=3 + 6).
In **Al2**, the mathematics is mainly happening in the exponents: $(uv)^2 = u^n = v^m$
We first get, from $(uv)^2 = v^m$, that $u^2 = v^{m-2}$, so

$$v = u^{2/(m-2)}.$$

Then, substituting for v in $(uv)^2 = u^n$ gives: $(u \bullet u^{2/(m-2)}) = u^n$
Equating exponents then gives:

$$n = 2\,[1 + 2/\,(m - 2)] = 2m/\,(m\text{–}2)\,,$$

whence, again, equation

$$2m = n\,(m - 2)\,. \tag{7.12}$$

In **Al3**, the conditions on (r, b) are that, $r + b = rb/2$. Dividing this by rb gives,

$$1/b + 1/r = 1/2, \text{ as in } \mathbf{Ar1}. \tag{7.13}$$

Appendix 2: Group Theoretic Derivation of Properties of gcd and lcm

Note that all of what follows precedes, and does not depend on, prime factorization.

(**DM0**): Let a and b be real numbers. Then we have proved that:

$\mathbb{Z}a + \mathbb{Z}b$ is discrete $\Longleftrightarrow$ a and b are commensurable

In what follows we shall assume that a and b are commensurable, unless the contrary is indicated. In this case we define

$d =$ gcd $(a, b) \geq 0$ and $m =$ lcm $(a, b) \geq 0$

by

$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ and $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$

Note that a and b are integers if and only if d is an integer. When $d = 1$, we say that a and b are "relatively prime." We say that a fraction a/b is "reduced" if gcd$(a, b) = 1$.

To ease writing we shall here abbreviate:

$(a, b) =$ gcd (a, b) and $[a, b] =$ lcm (a, b)

We now record some basic properties. We omit proofs if they follow easily from the definitions. We have bolded the items that are especially important and/or useful.

(**DM1**): There exist integers r, s such that $d(=(a, b)) = ra + sb$.

(**DM2**): (d) $d \mid a$ and $d \mid b$. If $d^{'} \mid a$ and $d^{'} \mid b$, then $d^{'} \mid d$

"d is the greatest common divisor of a and b"

(m) $a \mid m$ and $b \mid m$. If $a \mid m^{'}$ and $b \mid m^{'}$, then $m \mid m^{'}$

"m is the least common multiple of a and b"

(**DM3**): Suppose that $a \mid A$ and $b \mid B$. Then $(a, b) \mid (A, B)$ and $[a, b] \mid [A, B]$.

Put $d = (a, b)$ and $D = (A, B)$. Then $d \mid a$ and $a \mid A$, so $d \mid A$. Similarly $d \mid B$, and so $d \mid D$, by (DM3(a)). In similar fashion one shows that $[a, b] \mid [A, B]$.

(**DM4**): $(a, b) = (b, a) = (|a|, |b|)$, and

$[a, b] = [b, a] = [|a|, |b|]$ "**Absolute Symmetry**"

(**DM5**): $(a, 0) = |a|$ and $[a, 0] = 0$.

(**DM6**): For any real number c, $(\boldsymbol{ac}, \boldsymbol{bc}) = (\boldsymbol{a}, \boldsymbol{b}) \cdot |\boldsymbol{c}|$, and

$[\boldsymbol{ac}, \boldsymbol{bc}] = [\boldsymbol{a}, \boldsymbol{b}] \cdot |\boldsymbol{c}|$ "**Multiplicative scaling**"

This follows from the easily verified relations:

$$\mathbb{Z}ac + \mathbb{Z}bc = (\mathbb{Z}a + \mathbb{Z}b) \cdot \text{c, and}$$

$$\mathbb{Z}ac \cap \mathbb{Z}bc = (\mathbb{Z}a \cap \mathbb{Z}b) \cdot c$$

Multiplicative scaling is a very useful property. For example, when a and b are commensurable, we know that there is a nonzero number c such that ca and cb are integers. Then, for example, $(a, b) = |c^{-1}|(ca, cb)$, so this reduces the calculation of (a, b) to the case of integers. Similarly for $[a, b]$.

(**DM7**): Let $d = (a, b)$ and $a = a^{'}d$ and $b = b^{'}d$. Then $(a^{'}, b^{'}) = 1$.

In fact, $d = (a, b) = (a^{'}d, b^{'}d) = (a^{'}, b^{'}) \cdot d$, by (DM6), and so $(a^{'}, b^{'}) = 1$.

(**DM8**): If $(a, b) = 1$ then $[a, b] = |a \cdot b|$

Proof. Write $1 = ra + sb$, r, $s \in \mathbb{Z}$. Let $m^{'}$ be a common multiple of a and b: $m^{'} = ua = vb$, with $u, v \in \mathbb{Z}$. Then $m^{'} = m^{'}ra + m^{'}sb = vbra + uasb = (vr + us)ab$, so $ab \mid m^{'}$. Since ab is visibly a common multiple of a and b, it follows that $|ab| = [a, b]$.

(**DM9**): $|\boldsymbol{a} \cdot \boldsymbol{b}\ | \ = (\boldsymbol{a}, \boldsymbol{b}) \cdot [\boldsymbol{a}, \boldsymbol{b}]$.

Proof. $m = [a^{'}d, b^{'}d] = [a^{'}, b^{'}] \cdot d$ by (DM7)
$=| \ a' \cdot b' \ | \cdot d\, by$ (DM8 and 9)
so

$$d \cdot m =| \ a' \cdot b' \cdot d^2 \ |=| \ a'd \cdot b'd \ |=| \ a \cdot b \ | \ .$$

(**DM10**): If $(a, b) = 1 = (a, c)$, then $(a, bc) = 1$.

Proof. Note that a, b, $c \in \mathbb{Z}$. Write $1 = ra + sb = ua + vc$, with r, s, u, $v \in \mathbb{Z}$. Then

$$1 = (ra + sb)\,(ua + vc) = (rua + rvc + sbu)\,a + (sv)bc.$$

(**DM11**): Given $a_1a_2, \ \ldots, a_n$ and $b_1b_2, \ \ldots, b_m$ with
$(a_ib_j) = 1$ for $1 \leq i \leq n$ and $1 \leq j \leq m$,
it follows that $(a_1a_2 \ldots a_n, b_1b_2 \ldots b_m) = 1$.

This follows from (DM10) by induction on $max(n, m)$, as follows. In the case $n = m = 1$ there is nothing to prove. Suppose that $m \geq 2$. Then, by induction, we have that
$(a_1a_2 \ldots a_n, b_1b_2 \ldots b_{m-1}) = 1 = (a_1a_2 \ldots a_n, b_m)$
and so the result follows from (DM11).

(**DM12**): Suppose that $(a, b) = 1 = (c, d)$. Then $(ad, bc) = (a, c) \cdot (b, d)$.

Proof. Let $=\mathbb{Z}ad + \mathbb{Z}bc$. We want to show that:

$$A = (\mathbb{Z}a + \mathbb{Z}c) \cdot (\mathbb{Z}b + \mathbb{Z}d) = \mathbb{Z}ab + \mathbb{Z}ad + \mathbb{Z}bc + \mathbb{Z}bd$$

Clearly the right side contains the left side. For the reverse inclusion, we must show that ab, $bd \in A$. Write $1 = ra + sb$ and $1 = uc + vd$ with r, s, u, $v \in \mathbb{Z}$. Then

$$ab = abuc + abvd = (au)(bc) + (bv)(ad) \in A.$$

Similarly, $bd \in A$.

(**DM13**): Suppose that a/b and c/d are <u>reduced</u> fractions.
Then $(\boldsymbol{a}/\boldsymbol{b}, \boldsymbol{c}/\boldsymbol{d}) = (\boldsymbol{a}, \boldsymbol{c}) \,/\, [\boldsymbol{b}, \boldsymbol{d}]$
= gcd (**numerators**) /lcm (**denominators**) $^{\cdot}$

Proof. $|bd \mid (a/b, c/d) = (ad, bc)$ by (DM7)
$= (a, c) \cdot (b, d)$ by (DM13)
so

$$(a/b, c/d) = (a, c) \cdot (b, d) \,/ \mid b \cdot d \mid$$

$= (a, c) \cdot (b, d)/(b, d) \cdot [b, d]$ by (DM9)

$$= (a, c) \,/\, [b, d]$$

For the next items, we shall use the following notation: If a and b are real numbers we shall write: $\mathbb{Z}(a, b) = \mathbb{Z}a + \mathbb{Z}b$. If a and b are commensurable, then $\mathbb{Z}(a, b)$ is a discrete additive group, generated by (a, b). If a and b are incommensurable then we have shown that $\mathbb{Z}(a, b)$ is dense in $\mathbb{R}$.

(**DM14**): Let a and b be real numbers, and let t be an integer. Then

$$\mathbb{Z}\,(a, b + ta) = \mathbb{Z}\,(a, b)$$

In case a and b are commensurable, it follows that:
$(\boldsymbol{a}, \boldsymbol{b} + \boldsymbol{ta}) = (\boldsymbol{a}, \boldsymbol{b})$ "**Additive translation**"

Proof. Let $A = \mathbb{Z}(a, b)$, and $B = \mathbb{Z}(a, b + ta)$. We want to show that $A = B$. Since a, $(b + ta) \in A$, it follows that $B \subseteq A$. Writing $b = (b + ta) - ta$, we see that a, $b \in B$, and so $A \subseteq B$. Hence, $A = B$, as claimed.

Example. The Fibonacci sequence F_n is defined recursively by: $F_0 = 0$, $F_1 = 1$, and, for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$ (i.e., 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...)

It follows from (DM14) that, for all $n \geq 1$, $\gcd(F_n, F_{n+1}) = 1$.

(**DM15**): Given real numbers $a \geq b > 0$, put $c = r_b(a) < b$. Then $\mathbb{Z}(b, c) = \mathbb{Z}(a, b)$.
Hence, if a and b are commensurable, then so also are b and c, and
$(b, c) = (a, b)$.

Proof. By *DwR*, $a = qb + r$ with q an integer and $0 \leq r = r_b(a) < b$. Thus, $0 \leq r = a - qb = c < b$, and it follows then from Additive Translation ($DM14$) that: $\mathbb{Z}b + \mathbb{Z}c = (a - qb) = \mathbb{Z}a + \mathbb{Z}b$.

(DM16): **The Euclidean Algorithm (EA)**. Let a and b be commensurable real numbers, not both equal to 0. The Euclidean Algorithm (**EA**) is an algorithm to produce $(a, b) =$ gcd (a, b). Without loss of generality (DM5), we can assume that $a \geq b \geq 0$, and we shall then write $a_0 = a$ and $a_1 = b$. Then there is an integer $n = n(a_0, a_1) \geq 0$, and a sequence, $a_0 \geq a_1 > a_2 > \ldots > a_n > a_{n+1} = 0$ such that $(a_j, a_{j+1}) = (a_0, a_1)$ for all $j \leq n$. In particular, $(a_0, a_1) = (a_n, a_{n+1}) = a_n$.

Proof. If $a_1 = 0$, we set $n = 0$, and all is clear. So suppose that $a_1 > 0$. Suppose that $j \geq 1$, and that we have constructed $a_0 > a_1 > a_2 > \ldots > a_j > 0$.

Then, with the notation (of DM16), we set $a_{j+1} = r_{aj}(a_{j-1})$ and we have $(a_j,$ $a_{j+1}) = (a_{j-1}, a_j)$.

We continue in this fashion if $a_{j+1} > 0$. If $a_{j+1} = 0$, then we set $n = j$, and stop. All of the properties above follow from (DM16). The process must stop in a finite number of steps since $\mathbb{Z}(a, b)$ is uniformly discrete, so it cannot contain an infinite decreasing sequence of positive numbers.

(DM17): Suppose that $a > b > 0$ are incommensurable real numbers. Then we can still apply the Euclidean Algorithm process, but it won't stop in finitely many steps. Explicitly, set $a_0 = a$ and $a_1 = b$. Then we can produce an infinite sequence of positive numbers $a_0 > a_1 > a_2 > \ldots > a_n > a_{n+1} > \ldots$ such that $\mathbb{Z}(a_j, a_{j+1}) = \mathbb{Z}(a_0, a_1)$ for all $j \geq 0$.

This follows inductively from (DM16). We can't have $a_{j+1} = 0$ since $\mathbb{Z}(a_0, a_1)$ is not discrete, in fact it is dense in $\mathbb{R}$. It can further be shown that $a_n \to 0$ as $n \to \infty$.

(DM18): Multiple gcds and lcms. Define commensurability for a sequence $(a_1, a_2, \ldots, a_n)$ of real numbers to mean that $\mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n$ is discrete.

Then, as above, we can define $\gcd(a_1, a_2, \ldots, a_n)$ and $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$ to be the nonnegative generators of $\mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n$ and of $\mathbb{Z}a_1 \cap \mathbb{Z}a_2 \cap \ldots \cap \mathbb{Z}a_n$, respectively. These are clearly symmetric functions of their n variables. Moreover, we have recursive descriptions,

$\gcd(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n) = \gcd(a_1, a_2, \ldots, a_n)$

$\operatorname{lcm}(\operatorname{lcm}(a_1, a_2, \ldots, a_{n-1}), a_n) = \operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

To simplify writing we shall put

$$\delta(a_1, a_2, \ldots, a_n) = \gcd(a_1, a_2, \ldots, a_n), \text{ and}$$

$$\mu(a_1, a_2, \ldots, a_n) = \operatorname{lcm}(a_1, a_2, \ldots, a_n)$$

Note that the a_j are all integers if and only if $\delta(a_1, a_2, \ldots, a_n)$ is an integer. Moreover, $\delta(a_1, a_2, \ldots, a_n)$ and $\mu(a_1, a_2, \ldots, a_n)$ satisfy the analogue of multiplicative scaling (DM7).

(DM19): Writing $d = \delta(a_1, a_2, \ldots, a_n)$ and $a_j = a_j' \cdot d$ for each j, we have

$$\delta\left(a_1', a_2', \ldots, a_n'\right) = 1.$$

(DM20): Assume that all $a_j \neq 0$. If $\delta(a_1, a_2, \ldots, a_n) = 1$, then $\mu\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_n}\right) = 1$. (i.e., if $\mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n = \mathbb{Z}$, then $\mathbb{Z}{a_1}^{-1} \cap \mathbb{Z}{a_2}^{-1} \cap \ldots \cap \mathbb{Z}{a_n}^{-1} = \mathbb{Z}$.)

Proof. Put $G = \mathbb{Z}{a_1}^{-1} \cap \mathbb{Z}{a_2}^{-1} \cap \ldots \cap \mathbb{Z}{a_n}^{-1}$. Clearly G contains $\mathbb{Z}$. It remains to show that any a in G is an integer. For each j we can write $a = s_j/a_j$ with s_j an integer. By hypothesis we can write $1 = r_1a_1 + r_2a_2 + \ldots + r_na_n$, with all r_j integers. Then

$$a = r_1a_1a + r_2a_2a + \cdots + r_na_na$$

$$= \frac{r_1a_1s_1}{a_1} + \frac{r_2a_2s_2}{a_2} + \cdots + \frac{r_na_ns_n}{a_n}$$

$$= r_1s_1 + r_2s_2 + \cdots + r_ns_n \in \mathbb{Z}.$$

(DM21): Put $A = a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Then $A = \delta(a_1, a_2, \ldots, a_n) \cdot \mu\left(\frac{A}{a_1}, \frac{A}{a_2}, \ldots, \frac{A}{a_n}\right)$.

This is a nice, but nonobvious, generalization of the case $n = 2$, which is just (DM10): $a \cdot b = \text{ gcd } (a, b) \cdot \text{ lcm } (a, b)$.

Proof. Writing $a_j = a_j^{'} d$, with the notation of (DM20), we can apply (DM21) to obtain:

$\delta\left({a_1}', {a_2}', \ldots, {a_n}'\right) = 1 = \mu\left(\frac{1}{{a_1}'}, \frac{1}{{a_2}'}, \ldots, \frac{1}{{a_n}'}\right)$.

Multiplying the right side by $\frac{A}{d}$, and using multiplicative scaling, we get $\mu\left(\frac{A}{a_1}, \frac{A}{a_2}, \ldots, \frac{A}{a_n}\right) = \frac{A}{d}$, whence the result.

References

Ball, D. L., Thames, M. H., & Phelps, G. (2008). Content knowledge for teaching: What makes it special? *Journal of Teacher Education, 59*(5), 389–407.

Bass, H. (2017). Designing opportunities to learn mathematics theory-building practices. *Educational Studies in Mathematics, 95*(3), 229–244.

Common Core State Standards Initiative (CCSS-M). (2010). *Common core state standards for mathematics.* Retrieved from http://www.corestandards.org/math

Davydov, V.V. (1990). *Types of generalization in instruction: Logical and psychological problems in the structuring of school curricula* (*Soviet Studies in Mathematics Education* (Vol. 2)) (J. Teller, Trans.). Reston, VA: National Council of Teachers of Mathematics.

Usiskin, Z. (1968). Six nontrivial equivalent problems. *The Mathematics Teacher, 61*(4), 388–390.

van der Waerden, B. L. (1930). *Moderne algebra (I)*. New York, NY: Springer-Verlag.

van der Waerden, B. L. (1931). *Moderne algebra (II)*. New York, NY: Springer-Verlag.