MATHEMATICS
under the Microscope

Notes on Cognitive Aspects of Mathematical Practice

Alexandre V. Borovik

AMS
AMERICAN MATHEMATICAL SOCIETY
Providence, Rhode Island

2009

pp. 264 – 267:

12.6.3 Snooks, snowflakes, Kepler, and Pálfy

By varying the defining identities for snooks, we can get an infinite multitude of algebraic structures, each different from the others and each having the same right to exist. This is a classical example of a "bad", unstructured, uncontrolled infinity. When encountering such situations, mathematicians professionally try to introduce some structure into the disorder and to find general principles governing the universe of snooks.

The paradigm for such an approach is set in Kepler's classical work on snowflakes [55]. Of the myriads of snowflakes, there are no two of the same shape; however, almost all of them exhibit the strikingly precise sixfold symmetry. Kepler's explanation is breathtakingly bold: the symmetry of snowflakes reflects the sixfold symmetry of the packing of tiny particles of ice (what we would now call atoms or molecules) from which the snowflake is composed. In 1611, when the book was written, it was more than a scientific conjecture—it was a prophecy.

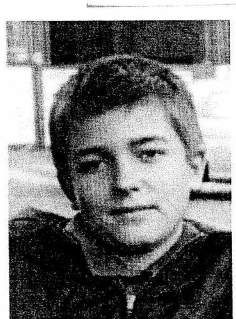
Of the infinitely many possible algebraic laws defining generalized snooks, some may allow for the existence of a finite structure. I will now outline a "snowflake" theory of arbitrary finite algebras,[9] which will of course cover the case of finite snooks. The theory belongs to David Hobby and Ralph McKenzie [365]; to avoid excessive detail, I will concentrate on its key ingredient, a theorem by Péter Pál Pálfy [394] on the structure of "minimal" algebras ([365, Theorem 4.7]).

The key idea is that we study finite algebras up to *polynomial equivalence*: we associate with every algebra $\mathbb{A}$ with ground set A the set of *all polynomial functions* on A, that is, all functions from A to A expressible by combination of basic algebraic operations of $\mathbb{A}$, with arbitrary elements from A being allowed to be used as constant "coefficients". For example, if $\mathbb{S}$ is a finite snook with the set S of elements and s is a fixed element of S, then

$$A(s,x)$$

is a polynomial function of a single variable x, while

$$T(x, A(s,y), x)$$



Péter Pál Pálfy, aged 13

is a polynomial function of two variables x and y. Two algebras are said to be *polynomially equivalent* if they have the same ground set and the same sets of polynomial functions. In particular, this means that every basic algebraic operation of the first algebra is expressed in terms of the operations of the second algebra, and vice versa. If we ignore the computational complexity of these expressions (which is not always possible in problems of a practical nature; see Section 12.5), the two algebras are in a sense mutually interchangeable.

Given a finite algebra $\mathbb{A}$, a polynomial function $f(x)$ in a single variable induces a map from A to A. Since A is finite, either $f(x)$ is a permutation of A, or it maps A to a strictly smaller subset $B \subset A$. In the second case, some iteration

$$g(x) = f(f(\cdots f(x)\cdots))$$

is an idempotent map:

$$g(g(x)) = g(x)$$

for all x. The idempotency of g allows us to "deform" and squeeze the basic operations of $\mathbb{A}$ to the set $C = g[A]$. If, for example, $T(\cdot,\cdot,\cdot)$ were an operation of $\mathbb{A}$, $T' = g(T(\cdot,\cdot,\cdot))$ becomes an operation on C. Adding all polynomial operations of $\mathbb{A}$ which preserve C, we get a new algebra $\mathbb{C}$ (we shall call it a *retract* of $\mathbb{A}$) which carries in itself a considerable amount of information about $\mathbb{A}$. For example, every homomorphic image of $\mathbb{C}$ is a retract of a homomorphic image of $\mathbb{A}$ [395].

But what happens if a finite algebra $\mathbb{A}$ has no proper retracts (that is, with C being a proper subset of A) and is therefore unsimplifiable? Pálfy calls such algebras *permutational*. Assuming that the algebra has at least three elements[10], we have a further division:

1. Every polynomial function defined in terms of $\mathbb{A}$ effectively depends on just one variable. Then all polynomial functions on A are permutations, and $\mathbb{A}$ is polynomially equivalent to a set A with an action of a finite group G, where the action of each element $g \in G$ is treated as a unary operation. This case is not at all surprising.
2. In the remaining case, when $\mathbb{A}$ is sufficiently rich for the presence of polynomial functions which really depend on at least two variables, the result is astonishing: *$\mathbb{A}$ is polynomially equivalent to a vector space over a finite field!*

So finite fields appear to be more important, or more basic, than finite snooks. Pálfy's theorem is a partial explanation of the mystery which we have already discussed in this chapter: *why are finite fields so special*? Mathematics needs more results of this nature, which help to clarify and explain the hierarchy of mathematical objects. Without a rigorous metamathematical study of the relations between various classes of mathematical objects and without the understanding of the reasons why some mathematical structures have richer theories than other structures, it is too easy to exaggerate the role of history and fashion in shaping mathematics as we know it now. I do not believe that the ideas of social constructivism can be really fruitful in the philosophy of mathematics. However, I have no space in this book to get into a detailed discussion.