Snapshots of modern mathematics
from Oberwolfach

№ 4/2014

What does “>” really mean?

Bruce Reznick

This Snapshot[1] is about the generalization of “>” from ordinary numbers to so-called *fields*. At the end, I will touch on some ideas in recent research.

1 Generalizing the reals

One of the favorite serious games of mathematicians is to take a familiar idea in a familiar situation, extract its essence, and then try to apply it in a broader environment.

One example is the concept of fields. It is inspired by the properties of $\mathbb{R}$, the set of real numbers. A *field* is a set of objects which can be added, subtracted, multiplied, and divided within the field,[2] in accordance with the usual calculation rules (commutativity, associativity, and distributivity). To be more precise, mathematicians also require that there exist *neutral elements* (called 0 and 1, much like in the case of real numbers) with respect to addition and multiplication.[3] Instead of saying that division must be possible, we might

[1] The author thanks Cynthia Vinzant and the editors for their careful reading of an earlier version, and useful suggestions.

[2] meaning that the product, sum, etc. of two elements of the field must itself be an element of the field,

[3] That is, there should be elements 0 and 1 such that $x + 0 = x$ and $x \cdot 1 = x$ for every element x of the field. The neutral element of the addition 0 is somewhat special in that one does not divide by 0 – just as we know it from the real numbers.

as well require that for every $x \neq 0$ in the field there is a *reciprocal* $\frac{1}{x}$, because division by an element is the same as multiplication with its reciprocal: $\frac{x}{y} = x \cdot \frac{1}{y}$.

What other fields do we know? One familiar field is $\mathbb{Q}$, the set of *rational numbers*: a rational number is any quotient of two integers (where of course the denominator must be non-zero), such as $-\frac{3}{4}$, $\frac{22}{7}$, $0 = \frac{0}{5}$, or $2 = \frac{2}{1}$.

What about $\mathbb{Z}$, the set of integers? This is *not* a field, because you usually can't divide two integers and stay in $\mathbb{Z}$: $\frac{22}{7}$ is a number, but it isn't an integer.[4]

Another field you may know is $\mathbb{C}$, the set of complex numbers. A complex number is an object of the form $a + ib$, where a and b are real numbers, and i is something else.[5] If you multiply two complex numbers, you get a complex number. Here's an example to show how it's done:

$$(1 + 2i)(3 + 4i) = 3 + 4i + 6i + 8i^2 = 3 + 10i - 8 = -5 + 10i.$$

The neutral element of the addition in $\mathbb{C}$ is $0 = 0 + 0 \cdot i$, the neutral element of the multiplication is $1 = 1 + 0 \cdot i$. What about taking reciprocals? If neither a nor b is 0, then $(a + ib)(a - ib) = a^2 - i^2 b^2 = a^2 - (-1)b^2 = a^2 + b^2$, so the reciprocal $\frac{1}{a+ib}$ of the complex number $a + ib$ is $\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}$, again a complex number.[6]

You might know from Euclid's famous proof that $\sqrt{2}$ isn't a rational number, that is, that there are no two integers a and b such that $\sqrt{2} = \frac{a}{b}$. We now use this knowledge to define a new field called $\mathbb{Q}(\sqrt{2})$: it consists of all numbers of the form $a + b\sqrt{2}$, where a and b are elements of $\mathbb{Q}$. Addition, multiplication and so work as in the field of real numbers $\mathbb{R}$. Is $\mathbb{Q}(\sqrt{2})$ really a field? It's easy to check most of the usual rules, but reciprocals need a trick. Suppose neither a nor b are zero. Then $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, so it follows that the reciprocal $\frac{1}{a+b\sqrt{2}}$ of $a + b\sqrt{2}$ is given by $\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2} \cdot \sqrt{2}$, again

---

[4] To an English speaker, the letters "$\mathbb{Q}$" and "$\mathbb{Z}$" may seem strange, but they stand for the German words "Quotient" (meaning – not surprisingly – "quotient") and "Zahlen" (meaning "numbers"). This choice seems to have been made by the French mathematical collective Nicolas Bourbaki in the 1930s and is universally used in mathematics.

[5] You sometimes see that $i = \sqrt{-1}$, but this is very confusing for several reasons: The square root symbol in $\sqrt{-1}$ does not denote the same thing as the familiar square root from $\mathbb{R}$, and there's no way to distinguish i from $-i$ as *the* square root of -1. It's better to think of i as something specific with the property that $i^2 = -1$. Once you've picked i, $-i$ has the same property, but it's defined in terms of i.

[6] This was the hardest part of checking that $\mathbb{C}$ is truly a field – why not have fun trying to check the rest of the requirements on your own!

an element of $\mathbb{Q}(\sqrt{2})$. This will work as long as the denominator $a^2 - 2b^2$ isn't zero. Conveniently, $a^2 - 2b^2 = 0$ if and only if $2 = \left(\frac{a}{b}\right)^2$, and this is the case if and only if $\sqrt{2} = \pm\frac{a}{b}$, which, as was earlier noted, is impossible by Euclid.[7]

Here's another way to make more complicated fields. Real polynomials[8] behave much like integers: they obey the algebraic rules of the real numbers, but you can't necessarily divide them. We say that $\mathbb{R}(x)$, the *field of rational functions over* $\mathbb{R}$, is the set of quotients of real polynomials in x.[9] Here are some examples of rational functions: $p(x) = 1 + 2x$, $p(x) = \frac{1}{x}$, $p(x) = \frac{1+2x}{3+\pi x}$, and $p(x) = \frac{1+x^{1000}}{17-3x^6}$. This idea also works for polynomials with more than one variable. Here are some examples of rational functions in $\mathbb{R}(x, y)$, $\mathbb{R}(x_1, x_2, x_3)$, and $\mathbb{R}(x_1, \ldots, x_n)$ for any integer n: $p(x, y) = \frac{1+x^2+y^2}{1+x^4+7y^{100}}$, $p(x_1, x_2, x_3) = x_1^7 + x_2^7 - 13x_3^5$, $p(x_1, \ldots, x_n) = \frac{(1+x_1+\ldots+x_n)^6}{\pi^2+x_1^2+\ldots+x_n^2}$.

2 Generalizing "$>$"

Two mathematicians working in the 1920s, Emil Artin (1898 – 1962) and Otto Schreier (1901 – 1929) generalized "$>$" to fields. Since "$a > b$" is the same thing as "$a - b > 0$", defining "$>$" is the same as saying which elements should be positive. When you add or multiply positives the result should be positive, and you want decisiveness: if $a \neq 0$, then either a is positive or a is negative (that is, $-a$ is positive), but not both.

Formally, an *order* on a field F is a set P (the "positive" elements in F) so that

(1) if $x \in F$, exactly one of these statements is true: $x = 0$ or $x \in P$ or $-x \in P$,
(2) if $x, y \in P$, then $x + y \in P$,
(3) if $x, y \in P$, then $xy \in P$.

Artin and Schreier also found a very useful property which follows from (1)-(3):

(4) if $x \in F$ and $x \neq 0$, then $x^2 \in P$; if $x_1, ..., x_n \in F$ and every $x_i \neq 0$, then $x_1^2 + \ldots + x_n^2 \in P$.

---

[7] We can similarly define $\mathbb{Q}(\sqrt{n})$ for any integer n which isn't a "perfect square".
[8] that is, polynomials with real numbers as coefficients
[9] It's okay for the denominator to be 1, so a polynomial is a rational function too.

Proof of (4): If $x \neq 0$, then either $x \in P$ or $-x \in P$. But $x^2 = x \cdot x = (-x) \cdot (-x)$, so (3) implies that $x^2 \in P$ in either case, and if each x_i^2 is in P (for $i = 1, \ldots, n$), then so is $x_1^2 + \ldots x_n^2$. How would we know that we have a good definition? The simplest requirement is that it should lead back to the familiar "$>$" when $F = \mathbb{R}$. Fortunately, this is the case:

Suppose P is an order on $\mathbb{R}$. If $a \in \mathbb{R}$ and $a > 0$ (">" meaning the usual order on $\mathbb{R}$), then we have no way of knowing whether $a \in P$ directly. But we already know that we can define the real number $x = \sqrt{a}$, and it follows from (4) that $a = x^2 \in P$. From (1), if $a < 0$, then $-a > 0$, hence $-a \in P$, and this classifies all the elements of $\mathbb{R}$ as to whether they belong to P. We have shown that $P = \{a \in \mathbb{R} : a > 0\}$. This is the only possibility for P. We don't get anything new, but this is precisely what we wanted – it just means our definition seems robust.[10]

What about $\mathbb{C}$? It turns out that it is impossible to define an order on $\mathbb{C}$! The reason is that if P were an order in $\mathbb{C}$, then since $i \neq 0$, condition (4) would imply that $0 = 1 - 1 = 1^2 + i^2 \in P$, which is impossible.[11]

More surprises occur in $\mathbb{Q}(\sqrt{2})$. There are exactly two different ways to define an order on $\mathbb{Q}(\sqrt{2})$, one in which $\sqrt{2} \in P$ and one in which $-\sqrt{2} \in P$. The proofs need more space than I've been allowed. Call those two orders P_1 and P_2. We have $a + b\sqrt{2} \in P_1$ exactly when $a + b\sqrt{2} > 0$, and $a + b\sqrt{2} \in P_2$ exactly when $a - b\sqrt{2} > 0$.[12]

What about the field of rational functions $\mathbb{R}(x)$? There are infinitely many orders! The proof is a little tricky, but here is the main idea: For each real number $r \in \mathbb{R}$, we want to define a specific order P_r depending on r. For each $f = \frac{p}{q}$ (where p and q are both polynomials), we need to decide whether f should be called positive. First try the rule that $f \in P_r$ if $f(r) > 0$. This makes (2) and (3) work, but (1) fails: what if $p(r) = 0$ or $q(r) = 0$? So we modify our definition to say that $f \in P_r$ if $f(x) > 0$ for every x just a little to the right

[10] You can also try to prove that every order P on $\mathbb{Q}$ is the usual order. It is not possible to use the last proof because we can't always take square roots in $\mathbb{Q}$, as we saw with "2". Hint: first try to prove that 1 is in P, then prove that positive integers are in P. Then try to write a fraction $\frac{m}{n}$ as the product of a positive integer and a square.

[11] If you know anything about finite fields, the same argument shows that they have no orders either.

[12] To an algebraist, there is no fundamental difference between $\sqrt{2}$ and $-\sqrt{2}$ (or i and $-i$.)

of r.[13] If $f(x) \geq 0$ for every $x \in \mathbb{R}$, then f will belong to P_r for every r. Are the orders P_s and P_r really different for every $r \neq s$? First of all, note that if $f(r) > 0$ and $f(s) < 0$, then $f \in P_r$ and $-f \in P_s$. We need to find such a rational function f for each pair r, s. To simplify things, we may assume that $r < s$. If we set $t = \frac{r+s}{2}$, then $-(x-t) \in P_r$ and $(x-t) \in P_s$; that is, the polynomial $x - t$ is negative in P_r and positive in P_s. This is true for any such r and s, so $\mathbb{R}(x)$ has (at least) as many orders as there are real numbers – infinitely many! Things get even more complicated when you look at $\mathbb{R}(x, y)$ or $\mathbb{R}(x_1, \ldots, x_n)$, but the same ideas can be made to work.

3 Serious mathematics

In 1888, the great mathematician David Hilbert (1862 – 1943) proved that there exists a polynomial p in two variables with the property that $p(x, y) \geq 0$ for all $x, y \in \mathbb{R}$ that at the same time can't be written in the form $p(x, y) = h_1(x, y)^2 + \ldots + h_k(x, y)^2$ for any k and any polynomials $h_1, \ldots, h_k$, see [2]. Interestingly, Hilbert never found an explicit example. The first such example was discovered in 1967 by Theodore S. Motzkin (1908 – 1970); it is $p(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$.

In 1893, Hilbert proved that for polynomials p in two variables, if $p(x, y) \geq 0$ for all $x, y \in \mathbb{R}$, then there must exist polynomials $f_1(x, y), \ldots, f_k(x, y)$ and $g_1(x, y) \neq 0, \ldots, g_k(x, y) \neq 0$ so that $p(x, y) = \left(\frac{f_1(x,y)}{g_1(x,y)}\right)^2 + \ldots + \left(\frac{f_k(x,y)}{g_k(x,y)}\right)^2$, see [3]. It's important that if p is a sum of squares of rational functions in this way, then necessarily $p(x, y) \geq 0$ for every x and y, so a representation of p as a sums of squares gives a "certificate" that p takes only non-negative values. In conclusion: for a polynomial p, taking only non-negative values is equivalent to being a sum of squares of rational functions.

Does the same thing hold for polynomials in more than two variables? In 1900, Hilbert gave his famous list of 23 questions which he expected to occupy

[13] Technically, we choose $\epsilon > 0$ small enough that $f(x) > 0$ for every $x \in (r, r + \epsilon)$. It can be proved that if $f \neq 0$, there exists an $\epsilon > 0$ so that either $f(x) > 0$ for every $x \in (r, r + \epsilon)$ or $-f(x) > 0$ for every $x \in (r, r + \epsilon)$.

mathematicians for the 20th century, and the following question is known as Hilbert's 17th Problem [4]:

If p is a real polynomial and $p(x_1, \ldots, x_n) \geq 0$ for all real numbers $x_1, \ldots, x_n$, must there exist polynomials $f_1, \ldots, f_k$ and $g_1, \ldots, g_k$ so that $p(x_1, \ldots x_n) = \left(\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)}\right)^2 + \ldots + \left(\frac{f_r(x_1,\ldots,x_n)}{g_r(x_1,\ldots,x_n)}\right)^2$?

Hilbert's problem was solved by Artin in the 1920s, using the following beautiful and hard theorem about ordered fields [1]:

Suppose F is a field.

(1) If there exist nonzero elements $x_1, \ldots, x_k \in F$ such that $x_1^2 + \ldots + x_k^2 = 0$, then F has no order.

(2) If there are no *nonzero elements $x_1, \ldots, x_k \in F$ such that $x_1^2 + \ldots + x_k^2 = 0$, then F has at least one order P. Furthermore, x belongs to every possible order on F if and only if x is a sum of squares in F.*[14]

Artin then solved Hilbert's 17th Problem – the answer is "yes"! He showed that if $p(x_1, \ldots, x_n) \geq 0$ for all $x_1, \ldots, x_n$ and P is an order on $\mathbb{R}(x_1, \ldots, x_n)$, then $p \in P$. It follows by (2) that p is a sum of squares of elements of $\mathbb{R}(x_1, \ldots, x_n)$ (There's a lot of work hidden in these sentences!). Unfortunately, there's no known non-numerical algorithm [15] for finding $f_1, \ldots, f_k$ and $g_1, \ldots, g_k$.

Mathematicians, both pure and applied, are extremely interested in determining the circumstances under which a real polynomial only takes non-negative values. This is a very hard problem, both theoretically and in practice, so certificates are valuable. If $p = \left(\frac{f_1}{g_1}\right)^2 + \ldots + \left(\frac{f_k}{g_k}\right)^2$, we can clear the denominator and find H so that $H^2 p$ is a sum of squares of polynomials. If $H^2 p$ only takes non-negative values, then so does p. Finding such an H for p leads to a certificate. There now are algorithms (from an area called "semidefinite programming") which make it easy to check numerically whether any polynomial is a sum of squares of polynomials. Many mathematicians around the world have worked hard in recent years on the questions discussed in this section. I am one of them, and this has been my Snapshot.

---

[14] For fun, note that $17 + 12\sqrt{2} \approx 33.9706$ and $17 - 12\sqrt{2} \approx .0294$, so $x = 17 + 12\sqrt{2}$ is in both P_1 and P_2 for $\mathbb{Q}(\sqrt{2})$. Try to write $x = x_1^2 + \ldots + x_k^2$ for $x_1, \ldots, x_k \in \mathbb{Q}(\sqrt{2})$. Hint: start with $x_1 = q + \frac{6}{q}\sqrt{2}$ for the "right" $q = \frac{m}{n} \in \mathbb{Q}$.

[15] meaning there are only algorithms which give an approximation, not an exact solution

References

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **5** (1927), no. 1, 100–115, http://dx.doi.org/10.1007/BF02952513.

[2] D. Hilbert, *Über die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann. **32** (1888), 342–350.

[3] ———, *Über ternäre definite Formen*, Acta Math. **17** (1893), 169–197.

[4] ———, *Mathematische Probleme*, Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse **3** (1900), 253–297.

[5] T.Y. Lam, *An introduction to real algebra*, Rocky Mountain J. Math. **14** (1984), 767–814.

[6] V. Powers, *Hilbert's 17th problem and the Champagne problem*, American Mathematical Monthly **103** (1996), 879–997.

[7] B. Reznick, *Some concrete aspects of Hilbert's 17th problem*, Publ. Équipe de Logique, Univ. Paris VII, 1996.

[8] ———, *Some concrete aspects of Hilbert's 17th problem*, Real Algebraic Geometry and Ordered Structures, Cont. math., no. 253, AMS, 2000, Revised version. http://www.math.uiuc.edu~reznick/Paper34.pdf.

[9] Wikipedia, *Field (mathematics) — Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Field_%28mathematics%29, 2014, [Online; accessed 08-July-2014].

[10] ———, *Ordered field — Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Ordered_field, 2014, [Online; accessed 08-July-2014].

[11] ———, *Total order — Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Total_order, 2014, [Online; accessed 08-July-2014].

Bruce Reznick *is a professor of mathematics at the University of Illinois at Urbana-Champaign.*

Mathematical subjects
Algebra and Number Theory

Connections to other fields
Computer Science, Reflections on Mathematics

DOI
10.14760/SNAP-2014-004-EN

Snapshots of modern mathematics from Oberwolfach are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the general public worldwide. It is part of the mathematics communication project "Oberwolfach meets IMAGINARY" funded by the Klaus Tschira Foundation and the Oberwolfach Foundation. All snapshots can be found on www.imaginary.org and on www.mfo.de/snapshots.

Junior Editor
Sophia Jahns
junior-editors@mfo.de

Senior Editor
Carla Cederbaum
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9–11
77709 Oberwolfach
Germany

Director
Gerhard Huisken