TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 5: Algebra

5.1. Algebra studies **structures** like "groups" in which one can add and "rings" in which one can add and multiply. The theory allows to solve polynomial equations like the **cubic equation** $x^3 + bx^2 + cx + d = 0$, characterize objects by its **symmetries** like all symmetries of an equilateral triangle and is the heart and soul of many puzzles like the **Rubik cube**. Lagrange claims **Diophantus** to be the inventor of Algebra, others argue that the subject started with solutions of **quadratic equation** by **Mohammed ben Musa Al-Khwarizmi** in the book Al-jabr w'al muqabala of 830 AD. Solutions to equation like $x^2 + 10x = 39$ are solved there by the method of **completing the squares**: add 25 on both sides go get $x^2 + 10x + 25 = 64$ and so $(x + 5) = 8$ so that $x = 3$.

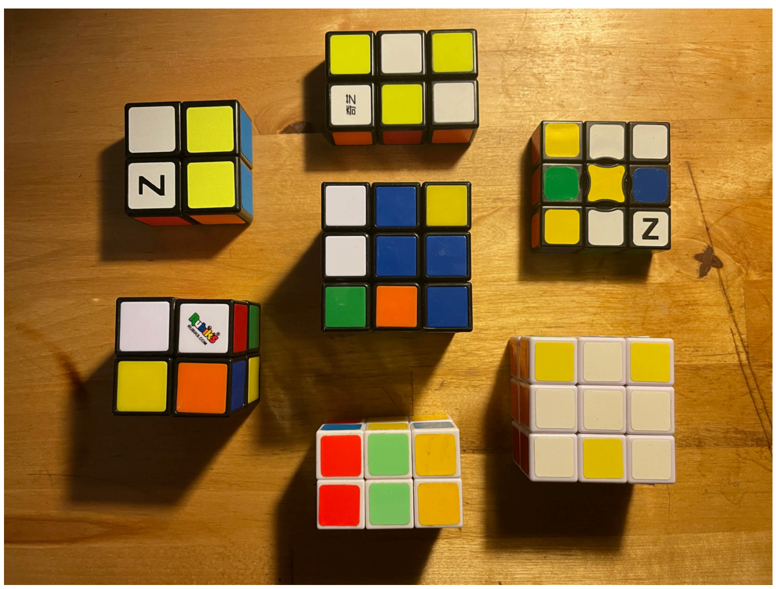

Figure 1. Rubik type puzzles.

5.2. Variables we use today in **elementary algebra** were introduced only in the 16th century. Ancient texts dealt with particular examples of equations and calculations were done with concrete numbers in the realm of **arithmetic**. It was **Francois Viete** (1540-1603) who first used letters like A, B, C, X for variables. Equations like the **quadratic equation** $x^2 + bx + c = 0$ was only written as such since 1637 with René Descartes.

5.3. The search for formulas for polynomial equations of degree 3 and 4 lasted 700 years. In the 16'th century, the cubic equation and quartic equations were solved. **Niccolo Tartaglia** and **Gerolamo Cardano** reduced the **cubic equation** $x^3 + bx^2 + cx + d = 0$ to the quadratic: first translate $X = x - b/3$ so that $X^3 + aX^2 + bX + c$ is a **depressed cubic** $x^3 + px + q$. Now substitute $x = u - p/(3u)$ to get a quadratic equation $(u^6 + qu^3 - p^3/27)/u^3 = 0$ for u^3.

5.4. **Lodovico Ferrari** shows that the quartic equation $x^4+bx^3+cx^2+dx+e=0$ can be reduced to the cubic by writing it as a product $(x^2+px+q)(x^2+ux+v)$ and solving this for p,q,u,v. For the **quintic** $x^5+bx^4+cx^3+dx^2+ex+f$ no formulas could be found. It was **Paolo Ruffini**, **Niels Abel** and **Évariste Galois** who independently realized that there are no formulas in terms of roots which allow to "solve" such equations in general. This was an amazing achievement and the birth of "group theory".

5.5. In a **group** G one has an operation $*$, an inverse a^{-1} and a **one-element** 1 such that $a*(b*c)=(a*b)*c, a*1=1*a=a, a*a^{-1}=a^{-1}*a=1$. For example, the set $\mathbb{Q}^*$ consisting of fractions p/q with non-zero p,q and multiplication operation $*$ and inverse $1/a$ form a group. The integers $\mathbb{Z}$ with addition and inverse $a^{-1}=-a$ and one-element 0 form a group too. Group operations are sometimes written in an additive way $x+y$ or in a multiplicative way $x*y$. Especially in **commutative settings**, where $a+b=b+a$, one usually uses the additive writing.

5.6. A **ring** R comes with two operations, addition and multiplication $+$ and $*$. The plus operation is a group satisfying the commutativity law $a+b=b+a$ in which the one-element is called 0. The multiplication operation $*$ is required to be associative. The two operations $+$ and $*$ are glued together by the **distributive law** $a*(b+c)=a*b+a*c$. An example of a ring are the **integers** $\mathbb{Z}$ or the **rational numbers** $\mathbb{Q}$ or the **real numbers** $\mathbb{R}$. The last two are actually **fields**, rings for which the multiplication on nonzero elements is a group too.

5.7. Why is the theory of groups and rings not part of arithmetic? First of all, a crucial ingredient of algebra is the appearance of **variables** and computations with these algebras without using concrete numbers. Second, the algebraic structures are not restricted to "numbers". Groups and rings are general structures and extend for example to objects like the set of all possible symmetries of a geometric object.

5.8. Groups appear often as **symmetries** in a geometry. The set of all **similarity transformations** on the plane for example form a group. An other important ring is the **polynomial ring** of all polynomials in a variable x. Given any ring R and a variable x, the set $R[x]$ consists of all polynomials with coefficients in R. The addition and multiplication is done like in $(x^2+3x+1)+(x-7)=x^2+4x-7$.

5.9. The problem to factor a given polynomial with integer coefficients into polynomials of smaller degree: x^2-x+2 for example can be written as $(x+1)(x-2)$ have a number theoretical flavor. Because symmetries of some structure form a group, the algebra of groups has intimate connections with geometry. The importance of this manifests also in physics, where groups explain the structure of elementary particles.

5.10. Symmetries are not the only connection with geometry. Here is a link to more modern geometry. If we look at polynomial rings of several variables, we get geometric objects with shape and symmetry which sometimes even have their own algebraic structure. They are called **varieties** and are studied in **algebraic geometry**. An example of a variety is the lemniscate of Gerono given by $(x^2-1)^2+y^2=1$. Algebraic objects given by polynomial equations in have in the last century been generalized further to **schemes**, **algebraic spaces** or **stacks**. Commutative algebra continue to play a crucial role in such constructs.

5.11. Arithmetic introduces addition and multiplication of numbers. Both form a group. The operations can be written additively or multiplicatively. Lets look at this a bit closer: for integers $\mathbb{Z}$, fractions $\mathbb{Q}$ and reals $\mathbb{R}$ and the addition $+$, the one-element 0 and the inverse is $-g$, we have a group. Many groups are written multiplicatively, where the one-element is 1. In the case where we have both addition and multiplication, the number 0 is not part of the multiplicative group. It is not possible to divide by 0. But the nonzero fractions or the nonzero real numbers form a group. In all these examples $\mathbb{Z},\mathbb{Q},\mathbb{R}$, the groups satisfy the commutative law $g*h=h*g$.

5.12. Groups are in general not commutative. The set of all rotations in space is an example of a group where it matters in which order we turn things. Rotate a cube by 90 degrees around the x-axes, then by 90 degrees around the y-axes is different from doing things with the opposite order. It contains the subgroup of all rotations which leave the unit cube invariant. There are $3 * 3 = 9$ rotations around each major coordinate axes, then 6 rotations around axes connecting midpoints of opposite edges, then $4 * 2$ rotations around diagonals. Together with the identity we have a group with 24 elements. This is the group of symmetries of the cube.

5.13. An other example of a group is S_4, the set of all permutations of four numbers $(1, 2, 3, 4)$. If $g : (1, 2, 3, 4) \to (2, 3, 4, 1)$ is a permutation and $h : (1, 2, 3, 4) \to (3, 1, 2, 4)$ is an other permutation, then we can combine the two and define $h * g$ as the permutation which does first g and then h. We end up with the permutation $(1, 2, 3, 4) \to (1, 2, 4, 3)$.

5.14. The rotation symmetry group of the cube turns out to be the same than the group S_4. To see this "isomorphism", label the 4 space diagonals in the cube by numbers $1, 2, 3, 4$. Given a rotation, we can look at the induced permutation of the diagonals. Every rotation corresponds to exactly one permutation. The symmetry group can be introduced for any geometric object. For shapes like the triangle, the cube, the octahedron or tilings in the plane. Symmetry groups describe geometric shapes by algebra.

5.15. Many **puzzles** are groups. A popular puzzle is the **15-puzzle**. It was invented in 1874 by **Noyes Palmer Chapman** in the state of New York. If the hole is given the number 0, then the task of the puzzle is to order a given random start permutation of the 16 pieces. To do so, the user is allowed to transposes 0 with a neighboring piece. Since every step changes the signature s of the permutation and changes the taxi-metric distance d of 0 to the end position by 1, only situations with even $s + d$ can be reached. It was **Sam Loyd** who suggested to start with an impossible solution and as an evil plot to offer 1000 dollars for a solution. The group of the 15 puzzle has $16!/2$ elements. Strangely enough the "God number" of the puzzle is not known exactly. It is between 152 and 208.

5.16. The **Rubik cube** is an other famous puzzle, which is a group. Exactly 100 years after the invention of the 15 puzzle, the Rubik puzzle was introduced in 1974. It still popular and some can solve it in 5 seconds. For the $3x3x3$ cube, the **God number**, is is now known to be 20: this means that one can always solve it in 20 or less moves, in principle.

5.17. A small Rubik type game is the $3 \times 3 \times 1$ Rubik cube called the "floppy" which is a third of the Rubik and which has only 192 elements.

5.18. The smallest Rubik cube of interest is the $2 \times 2 \times 1$ Rubik. If we allow all the cubes to move, then this group has 24 elements. It is again the same group than the rotation symmetry group of the cube. It is also the symmetry group the roots of the quartic equation $x^4 + bx^3 + cx^2 + dx + e = 0$.

Work problems

5.19. The solution of the **quadratic equation** $x^2 + bx + c = 0$ is one of the major achievements of early algebra. It relies on the method of **completion of the square** and is due to the Persian mathematician **Al Khwarizmi**. The **completion of the square** is the idea to add $b^2/4$ on both sides of the equation and move the constant to the right. Like this $x^2 + bx + b^2/4$ becomes a square $(x + b/2)^2$. Geometrically, one has added a square to a region to get a square. From $(x+b/2)^2 = -c+b^2/4$ we can solve x and get the famous formula for the solution of the quadratic equation

$$x = \pm\sqrt{\frac{b^2}{4} - c} - \frac{b}{2} .$$

There are two solutions. An other point of view is to plug in $x = y - b/2$. **Problem 1)** Write down the solution in the more general case $ax^2 + bx + c = 0$.

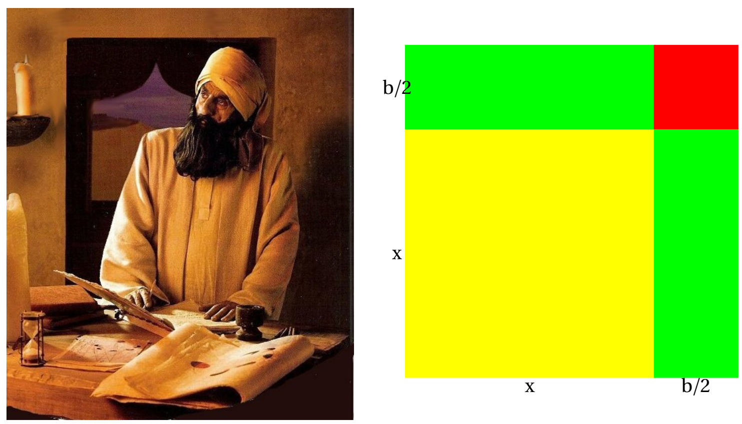

FIGURE 2. Al Kharizmi and the completion of the square.

5.20. Here are some SAT tricks. Why do they work?
Problem 2)
a) If x_1, x_2 are the two solutions to $x^2+bx+c = 0$, then the sum of the two solutions is $x_1+x_2 = -b$.
b) If x_1, x_2 are the two solutions of $x^2 + bx + c$, then the product of the solutions is $x_1x_2 = c$.

5.21. Problem 3) Find the solutions to the following equations

a) $x^4 - 4x^2 + 3 = 0$? b) $x^6 - 4x^4 + 3x^2 = 0$.

5.22. Problem 4) Sometimes we can find the solution of a equation by guessing.

a) Can you find the solutions to the cubic equation $x^3 - 7x + 6$? b) Can you find the solution to the equation $x^4 + 4x^3 + 6x^2 + 4x + 1$? c) What are the solutions to $x^4 - 2x^2 + 1 = 0$?

5.23. Problem 5) Verify that if a, b, c are solutions to a cubic equation and $a + b + c = 0$, then it is depressed: $x^3 + px + q = 0$. Hint: Write $(x - a)(x - b)(x - c)$.

5.24. We look at all the **rotational symmetries** of a square and realize it as a group. Given a square in the plane centered at the origin. We can rotate the square by 90, 180 or 270 degrees and get the same shape. Given two such rotations, we can perform one after the other and get an other rotation. All the rotations leaving the square invariant form a **group**: one can "add" these operations and get a new operation. here is the **multiplication table**:

+	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

Problem 6) For the equilateral triangle, there are 3 rotations and 3 reflections. Can you write the multiplication table of the symmetries of the equilateral triangle?

5.25. If we look at all rotations and reflections which leave the square invariant, there are 8 group elements. Beside the four rotations, we have 2 reflections at the diagonals and 2 reflections at the main axes.
Problem 7: Can you write down the multiplication table of the symmetries of the square? This is a large 8×8 multiplication table.

The 15 puzzle

5.26. The **15 puzzle** was invented by **Noyes Palmer Chapman** in 1874. Chapman was a post-master from Canastota in New York. From there the puzzle moved over to Syracuse, Watchhill, Hartfort and was first seriously sold in Boston. **Sam Loyd** offered a 1000 dollar prize for the solution of the case, when two pieces are switched.

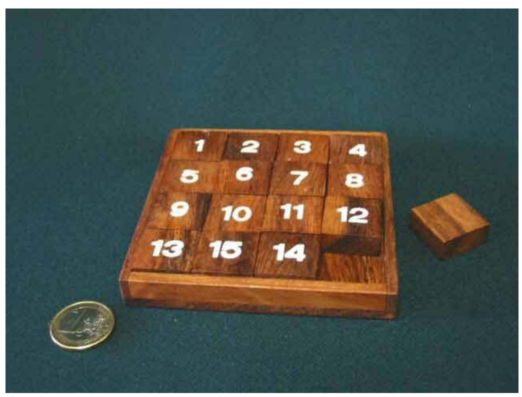

FIGURE 3. The 15 puzzle.

5.27. It is a bit harder to see that there are exactly 16!/2 group elements with the whole at the end. It is better to not assume that the hole as to be at the end since otherwise, one has no group. The god number is still not known. It between 152 and 208 for single tile moves.

Problem 8: Find and write down the argument why there we can not solve the 15 puzzle if two elements are switched.

The floppy

5.28. The **floppy cube** was designed by Katsuhiko Okamoto. With 192 possible positions, it is much less complex than the Rubik cube. We will learn how to solve it in class.

The Rubik's cube

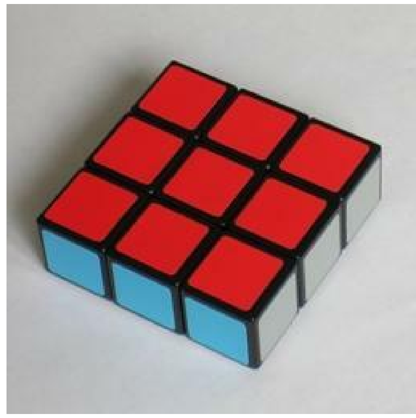

FIGURE 4. The Floppy

5.29. The **Rubik's cube** is quite a large puzzle. Argue that the Rubic cube has less than $8! \cdot 12! \cdot 3^8 \cdot 2^{12}$ group elements.

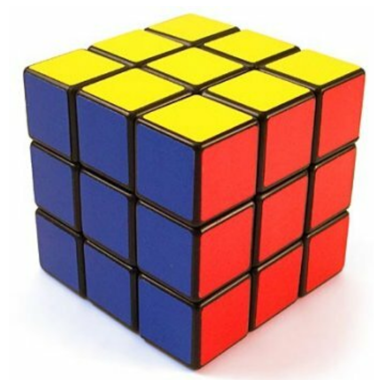

FIGURE 5. The Rubik cube

OLIVER KNILL, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022