Lecture 5: Algebra

Quadratic equation

The quadratic equation $x^2 + bx + c = 0$ can be solved by completing the square. This idea is due to **Mohammed ben Musa Al-Khwarizmi**:

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

Example: : $x^2 - 4x - 5$ has the root $(4 + \sqrt{16 + 20})/2 = 5$ or $(4 - \sqrt{16 + 20})/2 = -1$.
The use of **variables** and so **elementary algebra** was introduced only in the 16'th century.

1 The cubic equation

Niccolo Tartaglia and **Gerolamo Cardano** have shown how to solve the cubic equation $X^3 + aX^2 + bX + c = 0$.

Write $X = x - a/3$ to get the **depressed cubic** $x^3 + px + q$. With $x = u - p/(3u)$, we get the quadratic equation $(u^6 + qu^3 - p^3/27) = 0$.

Example: : Start with $X^3 + 2X^2 - 13X + 10 = 0$. With $X = x - 2/3$ we get $x^3 - 43x/3 + 520/27$. With $x = u + 43/(9u)$ we end up with $u^6 + 520u^3/27 + 79507/729 = 0$ which is a quadratic equation for u^3.

2 Higher order equations

Lodovico Ferrari shows that the quartic equation can be reduced to the cubic. For **quintic equations**, no formulas could be found. It was **Paolo Ruffini**, **Niels Abel** and **Évariste Galois** who realized that there are no formulas in general in terms of roots if the degree of the polynomial is 5 or higher.
The main tool to show this was **group theory**.

There are no formulas in general for the solution of polynomial equations of degree 5 or higher.

Symmetry groups

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 nonzero fractions p/q with multiplication operation $*$ and inverse $1/a$ form a group. The integers with addition and inverse $a^{-1} = -a$ and "1"-element 0 form a group too.

Here is a group which is not commutative: let G be the set of all rotations in space, 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 2*4 rotations around diagonals. Together with the identity rotation e, these are 24 rotations. The group operation is the composition of these transformations.

An other example of a group is 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 $(1, 2, 3, 4) \to (1, 2, 4, 3)$.

Puzzles

The first really popular puzzle was 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 K be reached. It was **Sam Loyd** who suggested to start with an impossible solution and offer 1000 dollars for a solution.

The **Rubik cube** is an other famous puzzle, which is a group too. Exactly 100 years after the invention of the 15 puzzle, the Rubik puzzle was introduced in 1974.

Many puzzles are groups.

One of the simplest example of a Rubik type puzzle is the **floppy cube**. It was invented by Katsuhiko Okamoto and consists of just one layer of the usual Rubik cube. We can permute both the edges and also their orientation. If we disregard rotations of the object in space, the puzzle has $4! * 8 = 192$ positions. We will look at this puzzle in class.