Lecture 5: Algebra

Algebra studies **algebraic structures** like "groups" and "rings". The theory allows to solve polynomial equations, characterize objects by its symmetries and is the heart and soul of many puzzles. 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 **completing the squares**: add 25 on both sides go get $x^2 + 10x + 25 = 64$ and so $(x + 5) = 8$ so that $x = 3$.
The use of **variables** introduced in school in **elementary algebra** were introduced later. Ancient texts only dealt with particular examples and calculations were done with concrete numbers in the realm of **arithmetic**. **Francois Viete** (1540-1603) used first letters like A, B, C, X for variables.

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 to the quadratic: [first remove the quadratic part with $X = x - a/3$ so that $X^3 + aX^2 + bX + c$ becomes the **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.] **Lodovico Ferrari** shows that the quartic equation can be reduced to the cubic. For the **quintic** however 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" equations $p(x) = 0$ for polynomials p of degree larger than 4. This was an amazing achievement and the birth of "group theory".

Two important algebraic structures are **groups** and **rings**.

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 Q^* of 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. A **ring** R has two compositions $+$ and $*$, where the plus operation is a group satisfying $a + b = b + a$ in which the one element is called 0. The multiplication operation $*$ has all group properties on R^* except the existence of an inverse. 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** or the **rational numbers** or the **real numbers**. The later two are actually **fields**, rings for which the multiplication on nonzero elements is a group too. The ring of integers are no field because an integer like 5 has no multiplicative inverse. The ring of rational numbers however form a field.

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. The set of all **similarity operations** on the plane for example form a group. An important example of a ring is the **polynomial ring** of all polynomials. 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 $(x^2 + 3x + 1) + (x - 7) = x^2 + 4x - 7$. The problem to

for example can be written as $(x+1)(x-2)$ have a number theoretical flavor. Because symmetries of some structure form a group, we also have intimate connections with geometry. But this is not the only connection with geometry. Geometry also enters through the polynomial rings with several variables. Solutions to $f(x,y) = 0$ leads to geometric objects with shape and symmetry which sometimes even have their own algebraic structure. They are called **varieties**, a central object in **algebraic geometry**.

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, fractions and reals and the addition $+$, the 1 element 0 and inverse $-g$, we have a group. Many groups are written multiplicatively where the 1 element is 1. In the case of fractions or reals, 0 is not part of the multiplicative group because it is not possible to divide by 0. The nonzero fractions or the nonzero reals form a group. In all these examples the groups satisfy the commutative law $g * h = h * g$.
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 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 $(1,2,3,4) \to (1,2,4,3)$. The rotational symmetry group of the cube happens to be the same than the group S_4. To see this "isomorphism", label the 4 space diagonals in the cube by $1,2,3,4$. Given a rotation, we can look at the induced permutation of the diagonals and 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.

Many **puzzles** are groups. A popular puzzle, the **15-puzzle** 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 15 puzzle group has 16!/2 elements and the "god number" is between 152 and 208. 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. Its still popular and the world record is to have it solved in 5.55 seconds. Cubes 2x2x2 to 7x7x7 have been solved in a total time of 6 minutes. For the 3x3x3 cube, the god number is now known to be 20: one can always solve it in 20 or less moves.

Many puzzles are groups.

A small rubik type game is the "floppy", which is a third of the rubik and which has only 192 elements. An other example is the **Meffert's great challenge**. Probably the simplest example of a Rubik type puzzle is the **pyramorphix**. It is a puzzle based on the tetrahedron. Its group has only 24 elements. It is the group of all possible permutations of the 4 elements. It is the same group as the group of all reflection and rotation symmetries of the cube in three dimensions and also is relevant when understanding the solutions to the quartic equation discussed at the

Lecture 5: Algebra

Quadratic equation

The quadratic equation $x^2 + bx + c = 0$ can be solved by **completing the square**. This idea goes back 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 with Francois Viète.

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 The quartic

Lodovico Ferrari showed that the quartic equation can be reduced to the cubic. First reduce it to the depressed quartic $x^4 + px^2 + qx + r$. Then write this as a factor $(x^2 + ax + b)(x^2 + cx + d)$. This leads to a system of equations for a,b,c,d which can be solved as it produces a cubic equation for a^2. For **quintic equations**, no formulas could be found. This opens a new chapter.

3 The quintic

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. This was a triumph of **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 $a*(b*c) = (a*b)*c, a*1 = 1*a = a, a*a^{-1} = a^{-1}*a = 1$.

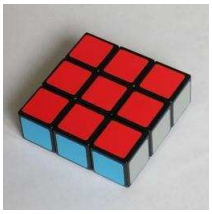
For example, the nonzero fractions p/q with multiplication operation $*$ and inverse $1/a$ form a group. The integers with addition and inverse $a^{-1} = -a$ and "1"-element 0 form a group too.

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 demonstrate this puzzle and some others during class.