LESSON 1 - WELCOME TO ABSTRACT ALGEBRA

ERAN ASSAF

1. introduction

Welcome to Abstract Algebra 81/111! What is this course about?

In one word - Symmetry. In two words - Galois theory.

The main theorem of the class is the jewel on the crown of thousands of years of mathematical thinking - the main theorem of Galois theory. It has far reaching applications to problems that people have been thinking about for a long long time. The history of Galois theory is unusually interesting. It certainly goes back to 1600 BC, where the ancient Babylonians worked out how to solve a quadratic equation.

Who was Galois?

Évariste Galois was a colorful and tragic figure - a youthful genius, one of the thirty or so greatest mathematicians who have ever lived, but also a political revolutionary during one of the most turbulent periods in he history of France. At the age of 20 he was killed in a duel, ostensibly over a woman and quite possibly with a close friend, and his work was virtually lost to the world; only some smart thinking by Joseph Liouville rescued it. Galois's story is one of the most memorable among the lives of the great mathematicians, even when the more excessive exaggerations and myths are excised.

However, the way in which we will learn this theory is the way it was presented by Emmy Noether in her treatise on the theory of ideals, published at 1920.

What is our goal this term?

Our goal is to settle (once and for all) questions that have haunted mathematicians throughout centuries and even millennia, such as solving equations in one variable and constructions with straight-edge and compass. Once this is done, towards the end of the term, we will learn that there are many more questions to be asked, and wonder around us to think about a few.

2. Constructions with Straight-Edge and Compass

According to Plato, the only perfect geometrical figures are the straight line and the circle. As a result, Greek geometers restricted their constructions to constructions with a straight-edge (a ruler with no markings, allowing one to draw a line between two points) and a compass (allowing one to draw a circle with center at one point, and passing through another. There is an advantage to not using measurements, as the constructions turn out to be very exact, not suffering from measurement inaccuracies.

One such simple construction is the construction of a perpendicular bisector. Given a segment AB, we can draw the circle O_A with center A and radius AB, and the circle O_B

with center B and radius O_B. Then the line passing through the intersection points of the two circles is the perpendicular bisector to AB (Why?).

3. Solving equations

I'll remind you that when we learned how to solve a quadratic equation such as $x^2 - x - 1 = 0$, we would multiply by 4 and complete the square to have $(2x-1)^2 = 5$. At this point, we can extract a square root and obtain $2x - 1 = \pm\sqrt{5}$, whence $x = \frac{1\pm\sqrt{5}}{2}$. That is, we could find a solution to this equation by using the four arithmetic operations, and extraction of a square root.

Equations that can be solved by using the four arithmetic operations and extraction of (not necessarily square) roots are called **solvable by radicals**.

4. Activity

10 minutes discussion in groups.

Now that you are all more familiar with the problems and the difficulties that arise, let's discuss how our predecessors dealt with them.

5. History of solving equations

All the material presented here was taken from the main sources [1–3].

Since the solution of a linear equation $ax = b$ does not use anything more than division, one can start with quadratic equations. The first known solution of a quadratic equation dates from (2003 BCE - 1595 BCE). It reads: "I have subtracted from the area the side of my square: 870. Take 1, the coefficient. Divide 1 into two parts: $\frac{1}{2}$. Multiply $\frac{1}{2}$ and $\frac{1}{2}$: $\frac{1}{4}$. You add to 870, and $870\frac{1}{4}$ has the root $29\frac{1}{2}$. You add to $29\frac{1}{2}$ the $\frac{1}{2}$ which you have multiplied by itself: 30, and this is the side of the square."

First, we see that the text solves the problem $x^2 - x = 870$, and obtains the positive solution $x = 30$. Moreover, it seems that the author applies a general method to solve an equation of the form $x^2 - ax = b$, where a is the "coefficient". You divide the coefficient into two parts - $\frac{a}{2}$, multiply it by itself to obtain $\left(\frac{a}{2}\right)^2$, and add it to b to obtain $\left(\frac{a}{2}\right)^2 + b$, from which one extracts a square root, and then add $\frac{a}{2}$ to obtain

$$x = \frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 + b}.$$

The Babylonians did not have negative numbers (all the numbers are actually lengths or areas), therefore they discard the negative solution. They have also considered various types of quadratic equations, depending on the sign of the coefficients. There are three types: (Why not four?)

$$x^2 + ax = b, \quad x^2 - ax = b, \quad \text{and } x^2 + b = ax.$$

How did they argue to get these solutions? We don't know, but we guess that they have first solved the system

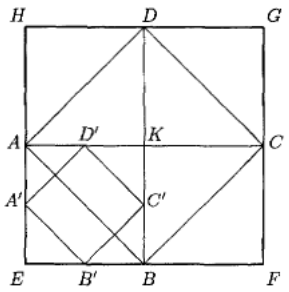
$$\begin{cases} x - y & = a \\ xy & = b \end{cases}$$

using geometry. By introducing $z = y + \frac{a}{2}$, one sees that $z^2 - \left(\frac{a}{2}\right)^2 = b$, hence the solution.

Looking at the examples of quadratic equations solved by the Babylonians, one notices a curious fact - the third type $x^2 + b = ax$ does not explicitly appear. This is even more puzzling given the frequent occurrence in the tablets of problem such as to find the length and breadth of a rectangle given its area and perimeter, which amounts to the same thing. The suggested explanation is that the Babylonians explicitly avoided this type because it admits two positive solutions. However, this observation that algebraic equations of degree higher than 1 have several interchangeable solutions is of fundamental importance - it is the cornerstone of Galois theory, and we shall have the opportunity to see to what clever use it will be put by Lagrange and other mathematicians.

As André Weil commented in relation to another topic: "This is very characteristic in the history of mathematics. When there is something that is really puzzling and cannot be understood, it usually deserves the closest attention because some time or other some big theory will emerge from it.".

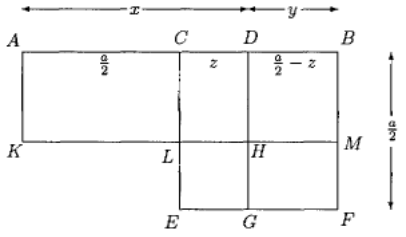
While the Babylonians knew how to solve quadratic equations, their algebra can be characterized as numerical, for it made no use of symbols. The second stage of the evolution of algebra coincides with the flourishing of classical Greek mathematics (5th cen. BCE - 2nd cen. BCE). One important change is the change of focus to the concept of proof. Another is the discovery that the naive idea of a number (an integer or a rational number) is not sufficient to account for geometric magnitudes. For instance, no line segment could be used as a length unit to measure the diagonal and the side of the square by integers - the ratio $(\sqrt{2})$ is not a rational number. You might have seen some proof of other of that fact (if not, try to think about it!). But the ancient greeks considered this problem geometrically.



If we assume both AB and AC are integers, then the areas of $ABCD$ and $EFGH$ are both squares, an $EFGH = 2ABCD$ is even, hence its side length is even, so EB is an integer, so $EBKA$ is a square, and as $ABCD = 2EBKA$, AB is even, so $A'B'$ is an

integer. Iterate the process to see that both AB and AC are infinitely divisible by 2 to get a contradiction.

Prompted by this discovery, the greeks developed new techniques to operate with ratios of geometric magnitudes - a "geometric algebra", which is methodically explained by Euclid in "The Elements". Although Euclid does not explicitly deal with quadratic equations, we can detect them camouflaged in geometry, e.g. Book II, Prop. 5: "If a straight line be cut into equal and unequal segments, the rectangle contained by the unequal segments of the whole together with the square on the straight line between the points of section is equal to the square on the half."



6. History of geometric constructions

Before we move on with the times, let us just note that the 5th century BCE is also the time when three important problems of geometric construction (with straight-edge and compass) became well-known.

(1) The duplication of a cube.
(2) Trisecting an angle.
(3) Constructing a regular n-gon, for any n.
(4) Squaring the circle.

The first three were solved only in the 1830s, and the fourth one only at the end of the 19th century. (In a few weeks time, you will also be able to solve these). The first problem was so popular that a legend was made up about it. Athens was afflicted by the plague, and the pronouncement of the oracle at Delos was that the plague would cease if the cubical alter to Apollo were doubled in size. Hence the name Delian problem.

7. Algebra

The next landmark in the theory of equations is the book "Al-jabr w'al muqabala" (830 AD) due to Mohammed ibn Musa al-Khowarizmi. Although Al-Khowarizmi did not use algebraic symbolism (that was already introduced before by Diophantus), he employed consistently three words for the symbols $1, x, x^2$, classified the different six types of quadratic equations, and used the modern "completing the square" method to solve them (including, of course, a geometrical justification). This is the first treatise whose explicit goal is to solve equations.

The second half of the 15th century saw a revival of algebra aided by the fall of Constantinopole and the migration of greek scholars to Europe and the invention of the printing press. In 1494, Luca Pacioli published his "Summa de arithmetica, geometria, proportioni et proportionalia". This was one of the first printed books. It contains a table for the notations for the unknown and its powers (x^i), and the notion of a negative number. (Yes! until now they were all positive!).

It is not until 1489 that the "-" sign has been introduced to denote negative numbers by Johannes Widman, and not until 1544 that we see a notational system of powers given by numbers as exponents. The algebraic part of the above book ends with the statement that just as there is no method for effecting the quadrature of a circles so, too, there is no general method for the solution of cubic equations of the form $x^3 = ax+b$ and $x^3+ax = b$. Pacioli wrote this the day before such a method was found...

The history of the solution of the cubic equation is a detective story. It began when Scipione del Ferro (1456-1526) solved by radicals the equation $x^3 + px = q, \quad p, q > 0$, but kept his method and results secret. Keeping a method secret at the time was common practice. The owner of a method could challenge his rival to a mental duel and set him problems solvable by this method the rival was ignorant of. Victory in such a "tournament" brought one fame and placed one at an advantage when it came to filling a desirable position. Before his death, del Ferro disclosed his method to his student Fiore who, in 1535, challenged to a duel the well known Italian mathematician Niccolò Tartaglia. Tartaglia knew that Fiore had the solution to the cubic equation, and made efforts to discover it himself. He succeeded the night before the duel. (Feb. 12, 1535).

In solving the equation, Tartaglia assumed that one its roots is of the form $x = u - v$. Then the equation takes the form

$$u^3 - v^3 + (u - v)(p - 3uv) = (u - v)^3 + p(u - v) = q.$$

If one imposes in addition $3uv = p$, we get $u^3 - v^3 = q$. Substituting $v = \frac{p}{3u}$, we get a biquadratic equation. Letting $z = u^3$, this is

$$z^2 - qz - \left(\frac{p}{3}\right)^3 = 0.$$

Solving this quadratic yields $z_{1,2} = \frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$, hence

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

A few days after the duel, Tartaglia was able to solve the equation $x^3 = px+q, \quad p, q > 0$ by using the substitution $x = u + v$. The corresponding formula was

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

This involved fundamental difficulties. Indeed, if $(q/2)^2 < (p/3)^3$, there is a negative number under the square root, i.e the formula becomes meaningless. On the other hand,

examples sowed that in this case the equation could have real roots (in fact, this is precisely the case when all three roots are real!). For example, the equation $x^3 = 15x + 4$ has the root $x = 4$ in spite of the fact that $(4/2)^2 < (15/3)^3$.

This case was called "irreducible", and troubled Tartaglia a lot. He delayed the publication of his results trying to resolve this difficulty. Mathematician Girolamo Cardano was in the process of writing a book on algebra when he found out that Tartaglia knew the secret of the solution of the cubic equation. Thereupon he made every effort to ferret out the secret. In 1539 he as finally successful, swearing to Tartaglia that he would not disclose it, only to publish it in his 1545 book "Ars magna sive de Regulis algebraicis", together with the solution of the quartic equation, discovered by his student, Luigi Ferrari.

Rather to continue with the personal drama, a la "the Borgias", we follow the math. In 1572, Bombelli publishes the book "L'Algebra" in which he introduces complex numbers, describes a mechanism to extract a cubic root of a complex number and solves instances of the "irreducible case".

Encouraged by the success of Italian mathematicians in solving cubic and quartic equations, they now (18th century) tried hard to solve the quintic equation. The problem attracted many eminent mathematicians, including Euler, Bézout, Lagrange, and Vandermonde. Euler was able to deal with some special cases, and Bézout came up with new solutions to cubic and quartic equations, but for the quintic he obtained "frightful formulas" that led nowhere. A turning point in the history of solution of equations by radicals was the appearance in 1770-1771 of Lagrange's famous memoir "Réflexions sur la résolution algébrique des équations". In the first two parts Lagrange analyzes all methods of solution of cubic and quartic equations invented up to his time and shows why none of them is applicable to the general quintic. In the third part he analyzes some classes of solvable equations of higher degree. Finally, in the fourth part, Lagrange makes theoretical deductions based on the whole of the investigated material and concludes that all existing methods reduce to the construction of a lower-degree auxiliary equations (resolvents) whose roots are rational functions of the roots of the initial equation. Lagrange calls two functions of the roots of an equation similar if all permutations of the roots that leave one invariant also leave the other invariant and vice versa. He shows that similar functions are rationally expressible in terms of one another and of the coefficients of the equation. Examples include, for quadratic, the discriminant $\delta = (\alpha_1 - \alpha_2)^2$, for the cubic, the expression

$$u = (\alpha_1 + \zeta_3\alpha_2 + \zeta_3^2\alpha_3)^3,$$

where $\zeta_3 = e^{\frac{2\pi i}{3}}$ is a cube root of unity, and for a quartic the expression

$$(\alpha_1 + i\alpha_2 + i^2\alpha_3 + i^3\alpha_4)^3.$$

For example, in the cubic case, even permutations of the roots leave u unchanged, while odd permutations take it to $v = (\alpha_1 + \zeta_3^2\alpha_2 + \zeta_3\alpha_3)^3$. Therefore, the expressions $u + v$ and uv are fixed by all permutations, hence rational, so u, v are solutions of a quadratic equation.

Here already lies the idea that the solution of an equation by radicals depends on the group of permutations of its roots and its subgroups. However, a complication occurs at

degree 5 - considering the corresponding expression, it only satisfies a polynomial of degree 24... Other expressions can be found, the best of which leads to a root of a polynomial of degree 6. Nevertheless, all these methods fail.

Following Lagrange's analysis, Paolo Ruffini published in 1799 a proof that it is actually impossible to provide a solution by radicals to the general quintic. Ruffini's proof was long and complicated, and contained a significant gap, and in 1824 Niels-Henrik Abel found a new, independent proof, which essentially settled the issue of solvability of general equations. Abel's approach was very methodical - he argued that in order to show that it is impossible to write down a solution, we cannot continue as before, looking for a clever way, but instead we should work in a framework in which there is a solution, and then show it cannot be written in a certain way.

8. Galois

Although Abel proved that the general quintic is not solvable by radicals, the question remained - which equations are solvable by radicals? This problem was completely settled by Evariste Galois. Among other concepts, Galois introduces the concept "domain of rationality" of the coefficients of the equation (polynomial), which we now call a "field". He emphasizes that the notion of irreducibility of an equation make sense only relative to a given domain of rationality. Then he introduces the notion of a "group of substitutions", now known as a "group". He reduces the question of solvability to the study of the structure of a field, and whether it can be obtained by successively adjoining roots (radicals) to our given domain of rationality? Finally, he reduces this question to the study of the structure of a finite group, known today as the Galois group.

9. summary

This term we will investigate these "domains of rationality", known as fields, and develop a comprehensive theory of them. This will be done by considering "equations", i.e. polynomials, and their roots. When the time is ripe, we will relate these concepts to constructions with straight-edge and compass, as well as to group theory, and prove the main theorem of Galois theory. In particular, we will deduce Ruffini-Abel's theorem, and Galois criterion for solvability by radicals. We will conclude by exploring some other applications.

By the end of the term you will know:

- Given a number, tell whether it is constructible using a straight-edge and compass.
- Given a polynomial, tell whether it is solvable by radicals.

References

[1] I. G. Bashmakova and G. S. Smirnova, *The beginnings and evolution of algebra*, The Dolciani Mathematical Expositions, vol. 23, Mathematical Association of America, Washington, DC, 2000. Translated from the Russian by Abe Shenitzer with the editorial assistance of David A. Cox.

[2] Ian Stewart, *Galois Theory*, 3rd ed., Chapman & Hall/CRC Mathematics, Chapman & Hall/CRC, Boca Raton, FL, 2004.

[3] Jean-Pierre Tignol, *Galois' theory of algebraic equations*, World Scientific Publishing Co., Inc., River Edge, NJ, 2001.