Constructions with ruler and compass.

Semyon Alesker.

1 Introduction.

Let us assume that we have a ruler and a compass. Let us also assume that we have a segment of length one. Using these tools we can construct segments of other lengths, e.g. we can construct a segment which is twice longer, or three times or any integer number of times longer; also we can divide given segment to any number of equal parts. The question we are going to discuss is: **segments of which lengths can be constructed with ruler and compass**?

From the above remarks it follows that we can construct a segment of any rational positive length. Also some irrational numbers can be constructed: for example the Pythagoras theorem implies that we can construct $\sqrt{2}$ or more generally $\sqrt{n}$ when n is a positive integer. Later on we will see that a square root of any positive rational number also can be constructed. In these lectures we will prove the following result.

Theorem 1. *One cannot construct $\sqrt[3]{2}$ using ruler and compass.*

We will see that the method of the proof allows to show that one cannot construct not only $\sqrt[3]{2}$, but many other numbers. Such results look quite exciting: how one can approach such a question? If we would require to prove that some number could be constructed using ruler and compass, we could try to invent an explicit procedure to construct it. But how to show that no arbitrarily long and complicated construction using ruler and compass leads to $\sqrt[3]{2}$?

By itself, such kind of non-existence results may sound at the first glance of moderate importance. However what turns out to be really important is *the method* of the proof. We will learn the notion of field and some basic results in linear algebra which have applications in mathematics (and other branches of science) far beyond the ruler and compass constructions.

2 Basic steps in constructions with ruler and compass.

Let us summarize precisely what kind of basic steps we are allowed to do with ruler and compass.

The basic steps are: (a) drawing a line through two given points; (b) drawing a circle with given center and radius; (c) taking intersection point of two lines, two circles, and a line and a circle.

In fact we cannot do anything else, just multiple repetition of these basic steps. As you know, these basic steps allow us to divide a given segment to any number of equal parts,

to draw a line perpendicular to a given one and passing through a given point, to divide a given angle to two equal angles, etc.

Let us show how to construct using these steps the square root of any positive rational number.

Proposition 2. *One can construct with ruler and compass $\sqrt{\frac{m}{n}}$ where m, n are positive integers.*

Proof. We have $\sqrt{\frac{m}{n}} = \frac{\sqrt{mn}}{n}$. Since we can divide a given segment to n equal parts, it suffices to construct $\sqrt{mn}$, namely square root of any positive integer l.

Let us prove it by induction. If $l = 1$ there is nothing to prove. Assume that we have constructed $\sqrt{l-1}$. Then we can construct using ruler and compass a right triangle with cathetii with lengths 1 and $\sqrt{l-1}$. By the Pythagoras theorem the length of the hypotenuse is equal to $\sqrt{1+(l-1)} = \sqrt{l}$ as necessary. The proposition is proved.

At this point it is worthwhile to emphasize that the last proposition implies in particular that we already know to construct some irrational numbers: for example $\sqrt{2}$ is irrational. Let us prove this in a somewhat more general form: $\sqrt[m]{2}$ is irrational for any integer $m > 1$ (we will need this fact below for $\sqrt[3]{2}$). Assume that for some positive integers a, b one has

$$\sqrt[m]{2} = \frac{a}{b}.$$

We also may and will assume that a and b have no common divisors. In particular they cannot be even simultaneously.

We have $a^m = 2b^m$. This implies that a is even. Thus $a = 2a_1$. Hence $2^m a_1^2 = 2b^2$, or $b^2 = 2^{m-1}a_1^2$. Hence b is also even. This is a contradiction.

3 Relations to the field theory.

In modern algebra there is an important notion of a field (in Hebrew 'sade'). It has nothing to do with the usual notion of field from the every day life, and I do not know where this term comes from. Field theory has proved to be extremely useful in many branches of mathematics, especially algebra and number theory. It will be also crucial in our approach to Theorem 1. We will need the notion of field in somewhat lesser generality than one usually defines it in modern literature.

Definition 3. A field is a subset K of complex numbers $\mathbb{C}$ which has the following properties:

(1) K contains 1;

(2) K is closed under sums and differences: namely if complex numbers a, b belong to K then $a + b$ and $a - b$ also belong to K;

(3) K is closed under product and division: namely if a, b belong to K, then $a \cdot b$ and $\frac{a}{b}$ belong to K (for the latter statement one should assume of course that $b \neq 0$).

Remark 4. It is easy to see that any field $K \subset \mathbb{C}$ contains the rationals $\mathbb{Q}$. Indeed starting with 1 and using sums and differences we can obtain any integer number. Taking their fractions we can obtain any rational number.

Example 5. (1) The set $\mathbb{C}$ of all complex numbers is of course a field.

(2) The subsets $\mathbb{R}$ and $\mathbb{Q}$ of real and rational numbers respectively are fields.

(3) The subset $\mathbb{Z}$ of all integer numbers is *not* a field. In fact $\mathbb{Z}$ satisfies all the properties in the definition except of closeness under division.

(4) Let K be a field and let $t \in K$. Define $K(\sqrt{t})$ to be the set of all elements of the form $a + \sqrt{t}b$ with arbitrary $a, b \in K$. Then $K(\sqrt{t})$ is a field. (In particular $\mathbb{Q}(\sqrt{2})$ is a field.) Indeed closeness under sums and differences is obvious. Closeness under products:

$$(a + \sqrt{t}b)(c + \sqrt{t}d) = (ac + tbd) + \sqrt{t}(ad + bc).$$

It remains to check that if $x \in K(\sqrt{t})$ then $1/x \in K(\sqrt{t})$. Indeed

$$\frac{1}{a + \sqrt{t}b} = \frac{a}{a^2 - tb^2} - \sqrt{t}\frac{b}{a^2 - tb^2}.$$

Our problem of constructing segments of given length using ruler and compass is equivalent (in a trivial way) to the following problem of constructing complex numbers using ruler and compass. Let us fix on our plane a coordinate system. Then points on the plane will be identified with complex numbers: point with coordinates (x, y) can be identified with the complex number $x + iy$. A point with coordinates (x, y) can be constructed using ruler and compass if and only if one can construct segments of lengths $|x|$ and $|y|$. Thus instead of talking of constructing a segment of given length we will talk of complex numbers which can be constructed using ruler and compass.

Clearly the complex numbers $0, 1, i$ can be constructed. Our first non-trivial step towards proving Theorem 1 is as follows.

Theorem 6. *The set of all complex numbers which can be constructed with ruler and compass is a field.*

Proof. The closeness under sums and differences is obvious (check it!). Let us check closeness under product. Assume that $z = a + ib$ and $w = c + id$ can be constructed. Then

$$zw = (ac - bd) + i(ad + bc).$$

From this formula it is clear that it suffices to prove that if two segments of lengths u and v can be constructed then a segment of length uv can be constructed. On the axis x let us choose points A and B such that

$$|OA| = 1,\ |AB| = u.$$

On the axis y let us choose a point C such that

$$|OC| = v.$$

Using ruler and compass we can draw through the point B the line parallel to AC. Let D be the point of intersection of this line with the axis y. We have

$$\frac{|CD|}{|OC|} = \frac{|AB|}{|OA|}.$$

Namely $\frac{|CD|}{v} = \frac{u}{1}$. Hence $|CD| = uv$.

It remains to show closeness under inverses. If $z = a + ib$ then

$$\frac{1}{z} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}.$$

Since we already know closeness under sums, differences, and products, it remains to show closeness under inverses only for *positive* numbers. Thus let us assume that one can construct a segment of length u. Let us construct a segment of length $1/u$.

On the axis x let us choose points A and B such that

$$|OA| = u,\ |AB| = 1.$$

On the axis y let us choose a point C such that $|OC| = 1$. Let us draw through B the line parallel to AC. Let D be the point of intersection of it with the axis y. Then we have

$$\frac{|CD|}{|OC|} = \frac{|AB|}{|OA|} = \frac{1}{u}.$$

Hence $|CD| = 1/u$. Theorem is proved.

Once we know that the set of all complex numbers constructible with ruler and compass is a field, we will need more information about the structure of fields. This will be done in the next section.

4 Some field theory and linear algebra.

Definition 7. Let $F \subset K (\subset \mathbb{C})$ be fields. One says that K is a finite extension of F if there exist finitely many elements $k_1, \dots, k_n \in K$ such that any elements $x \in K$ can be written in the form

$$x = f_1 k_1 + \dots + f_n k_n \text{ for some } f_1, \dots, f_n \in F.$$

In this case one says that $k_1, \dots, k_n$ span K over F.

Example 8. (1) $\mathbb{C}$ is finite extension of $\mathbb{R}$ (spanned by 1 and i).

(2) $\mathbb{Q}(\sqrt{t})$, $t \in \mathbb{Q}$, is a finite extension of $\mathbb{Q}$ (spanned by 1 and $\sqrt{t}$).

(3) One can show that $\mathbb{R}$ and $\mathbb{C}$ are not finite extensions of $\mathbb{Q}$. We will not prove this result and will not use it.

(4) One can show that the set of all complex numbers constructible with ruler and compass is not a finite extension of $\mathbb{Q}$. However we will prove that any element of it is contained in a finite extension of $\mathbb{Q}$ (which might be rather large though).

Now we come to the central notion of this section.

Definition 9. Let a field K be a finite extension of a field F. The minimal number of elements of K spanning K over F is called *the degree of K over F*. The degree is denoted by $[K : F]$.

Exercise. Show that

$$[\mathbb{C} : \mathbb{R}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

The main result of this section is the following.

Theorem 10. *Let $F \subset K \subset L$ be fields such that K is a finite extension of F and L is a finite extension of K. Then L is a finite extension of F and*

$$[L : F] = [L : K] \cdot [K : F].$$

To prove this theorem we will need some preparations. This material is usually proved in courses of linear algebra in a greater generality.

Definition 11. Let K be a finite extension of F. A sequence of elements $x_1, \dots, x_n \in K$ is called *linearly dependent* over F if there exist $f_1, \dots, f_n \in F$, not all equal to 0, such that

$$f_1 x_1 + \cdots + f_n x_n = 0.$$

Otherwise the sequence $x_1, \dots, x_n$ is called *linearly independent* over F.

Notice that in a linearly independent sequence all elements must be different from 0. Indeed otherwise if say $x_1 = 0$ then $1 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n = 0$.

Exercise. Show that $1, i \in \mathbb{C}$ are linearly independent over $\mathbb{R}$, and that $1, \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ are linearly independent over $\mathbb{Q}$.

Theorem 12. *If a field K is spanned over F by n elements then any linearly independent sequence in K contains at most n elements.*

To prove Theorem 12 let us prove first a technical lemma.

Lemma 13. *Let K be spanned over F by $z_1, \dots, z_s$ which are linearly dependent. Assume moreover that the first t elements of this sequence are linearly independent. Then from the initial sequence one can delete one element z_i with $i > t$ such that the remaining sequence still spans K over F.*

Proof of Lemma. Since our sequence is linearly dependent then there exist $f_1, \dots, f_s \in F$ not all 0, such that

$$f_1 z_1 + \cdots + f_s z_s = 0.$$

Let i be the maximal index such that $f_i \neq 0$ (thus $f_{i+1} = \cdots = f_s = 0$). Since by assumption the first t elements are linearly independent, $i > t$. Let us show that z_i can be deleted from the sequence. For simplicity of the notation only we will assume that $i = s$ (this may be assumed by changing the numeration). We have

$$z_s = -\frac{f_1}{f_s} z_1 - \cdots - \frac{f_{s-1}}{f_s} z_{s-1}. \tag{1}$$

For any $x \in K$ there exists a presentation

$$x = a_1 z_1 + \cdots + a_{s-1} z_{s-1} + a_s z_s \text{ with } a_j \in F.$$

Substituting (1) into the last formula we get

$$x = (a_1 - \frac{a_s f_1}{f_s}) z_1 + \cdots + (a_{s-1} - \frac{a_s f_{s-1}}{f_s}) z_{s-1}.$$

Hence $z_1, \ldots, z_{s-1}$ span K over F. Lemma is proved.

Proof of Theorem 12. Let K be spanned by $x_1, \ldots, x_n$. Let a sequence $y_1, \ldots y_m \in K$ be linearly independent. We have to show that $m \leq n$. Assume in the contrary that $m > n$.

Consider the longer sequence

$$y_1, x_1, \ldots, x_n.$$

Clearly it spans K. Moreover it is linearly dependent (since $y_1 = a_1 x_1 + \cdots + a_s x_s$ and hence $(-1) \cdot y_1 + a_1 x_1 + \cdots + a_s x_s = 0$). The beginning of this sequence y_1 is linearly independent. Hence by Lemma 13 one can delete from this sequence one of the x_i's and get again a spanning sequence. After rearranging indices we may assume that we delete x_n. Then the sequence

$$y_1, x_1, \ldots, x_{n-1} \tag{2}$$

spans K over F. Let us add to it y_2:

$$y_2, y_1, x_1, \ldots, x_{n-1}. \tag{3}$$

This sequence spans K, its beginning y_2, y_1 is linearly independent. Moreover this sequence is linearly dependent since y_2 can be expressed via the others (since (2) spans K). Hence again by Lemma 13 we can delete one of the remaining x_i's and get a spanning sequence. We will proceed in this way: at each step we add a new y_k and delete one of the x's till we delete all the x's after n steps. Thus we will obtain that the sequence $y_n, \ldots, y_1$ spans K over F. But then y_{n+1} is a linear combination of the first n y's, and hence as previously the whole sequence $y_{n+1}, y_n, \ldots, y_1$ is linearly dependent. This is a contradiction. Theorem 12 is proved.

Definition 14. Let a field K be a finite extension of a field F. A sequence $k_1, \ldots, k_n \in K$ is called a *basis* of K over F if it is linearly independent and spans K over F.

Theorem 15. *Let a field K be a finite extension of a field F. Then*

(1) K has a basis over F;

(2) any basis has the same number of elements equal to $[K : F]$.

Proof. Denote for brevity $n = [K : F]$. First let us prove part (1). Let $k_1, \ldots, k_n$ be a shortest spanning sequence. We will show that it is linearly independent, and hence is a basis. If it is linearly dependent, then by Lemma 13 we can delete one of its elements and still get a spanning sequence (in order to apply this lemma formally, we just take the initial

linearly independent sequence to be the empty one). But this contradicts the minimality of $n = [K : F]$. Part (1) is proved.

Let us prove part (2). Let $x_1, \dots, x_m$ be another basis. We want to show that $m = n$. Since the basis $k_1, \dots, k_n$ constructed in the previous step spans K and $x_1, \dots, x_m$ are linearly independent, Theorem 12 implies that $m \leq n$. But m cannot be strictly smaller than n since then we would have a spanning sequence shorter than n in contradiction to the definition of n. Hence $m = n$. Theorem 15 is proved.

Proof of Theorem 10. Recall that we have $F \subset K \subset L$. Let $k_1, \dots, k_n \in K$ be a basis of K over F, and let $l_1, \dots, l_m \in L$ be a basis of L over K. Thus $n = [K : F]$, $m = [L : K]$. We will show that all mn pairwise products $k_i \cdot l_j$ with $i = 1, \dots, n$, $j = 1, \dots, m$ form a basis of L over F. Clearly this will imply the theorem immediately.

Let us prove first that these elements span L over F. Let $x \in L$ be an arbitrary element. Then

$$x = a_1 l_1 + \cdots + a_m l_m \text{ with } a_i \in K. \tag{4}$$

But each a_j can be expressed via k_i's with coefficients from F:

$$a_j = f_{j1} k_1 + \cdots + f_{jn} k_n \text{ with } f_{ji} \in F. \tag{5}$$

Substituting (5) to (4) we obtain

$$x = \sum_{i,j} f_{ji}(k_i l_j).$$

Since $x \in L$ was arbitrary, all $k_i l_j$ span L over F.

It remains to show that all $k_i l_j$ are linearly independent over F. Assume that there exist $f_{ji} \in F$ such that

$$\sum_{ij} f_{ji} k_i l_j = 0. \tag{6}$$

But we have

$$0 = \sum_{ij} f_{ji} k_i l_j = \sum_i (\sum_j f_{ji} k_i) l_j.$$

But $\sum_j f_{ji} k_i$ belong to K for all i. Then they must vanish since the l_j's are linearly independent over K:

$$\sum_j f_{ji} k_i = 0.$$

Now since the k_i's are linearly independent over F we conclude that $f_{ji} = 0$ for all i, j. Theorem 10 is proved.

Let us deduce an application from the above results which we will need later. Let us denote by $\mathbb{Q}(\sqrt[3]{2})$ the set of all numbers of the form $a + \sqrt[3]{2} b + \sqrt[3]{4} c$ with $a, b, c \in \mathbb{Q}$.

Proposition 16. $\mathbb{Q}(\sqrt[3]{2})$ *is a field. Moreover* $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Proof. The closeness of $\mathbb{Q}(\sqrt[3]{2})$ under sums and differences is obvious. Let us prove now the closeness under the products. We have by a straightforward computation

$$\begin{aligned}(a + \sqrt[3]{2}b + \sqrt[3]{4}c)(u + \sqrt[3]{2}v + \sqrt[3]{4}w) = \\ au + 2bw + 2cv + \\ \sqrt[3]{2}(av + bu + 2cw) + \\ \sqrt[3]{4}(aw + bv + cu).\end{aligned}$$

To prove the closeness under the inverse is tricky. You can try to prove it directly. We will use some of the above linear algebra. Let $x \in \mathbb{Q}(\sqrt[3]{2})$. Since $\mathbb{Q}(\sqrt[3]{2})$ is spanned over $\mathbb{Q}$ by 3 elements $1, \sqrt[3]{2}, \sqrt[3]{4}$, Theorem 12 implies that any sequence of length 4 is linearly dependent over $\mathbb{Q}$. In particular the sequence $1, x, x^2, x^3$ is linearly dependent. Hence there exist $a, b, c, d \in \mathbb{Q}$, not all 0, such that

$$ax^3 + bx^2 + cx + d = 0.$$

If $d = 0$ we can divide by x and get a similar equation on x of lower degree. If still the free coefficient vanishes, we can divide again by x. In any case, eventually we get for some $1 \leq l \leq 3$ and rational coefficients $u, \ldots, v, w$

$$ux^l + \cdots + vx + w = 0$$

with $w \neq 0$. Hence moving w to the right and dividing by $-w$ we get

$$x(-\frac{u}{w}x^{l-1} - \cdots - \frac{v}{w}) = 1.$$

Thus the expression in brackets is x^{-1} and it clearly belongs to $\mathbb{Q}(\sqrt[3]{2})$.

It remains to show that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. The above discussion implies that this degree is at most 3. Let us assume that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 2$. Then by Theorem 12 any sequence of length 3 is linearly dependent. Hence there exist $a, b, c \in \mathbb{Q}$, not all 0, such that

$$a\sqrt[3]{4} + b\sqrt[3]{2} + c = 0.$$

If $a = 0$ then we get that $\sqrt[3]{2}$ is a rational number which is false as we have seen. Thus $a \neq 0$, and dividing by a we may assume that $a = 1$. Thus $\sqrt[3]{2}$ is a root of the polynomial $f(x) = x^2 + bx + c$. But $\sqrt[3]{2}$ is also a root of the polynomial $g(x) = x^3 - 2$. We also have the following identity

$$x^3 - 2 = (x^2 + bx + c)(x - b) + \left((b^2 - c)x + bc - 2\right). \tag{7}$$

You can check this identity directly, but it was obtained as a result of division of g by f with a remainder (for those of you who know what it is). This identity implies that $\sqrt[3]{2}$ must be a root of the polynomial of first degree $(b^2 - c)x + bc - 2$. But if this polynomial is not identically zero it would follow again that $\sqrt[3]{2}$ is a rational number which is false. Hence this polynomial must vanish. Thus we get

$$x^3 - 2 = (x^2 + bx + c)(x - b) \text{ with } b, c \in \mathbb{Q}. \tag{8}$$

Let us show that this is impossible. We readily have

$$(x^2 + bx + c)(x - b) = x^3 + (-b^2 + c)x - bc.$$

Comparing the coefficients with (8) we deduce

$$-b^2 + c = 0,\ bc = 2.$$

Thus $c = b^2$, and hence $b^3 = 2$. Thus $b = \sqrt[3]{2}$ is a rational number, this is again a contradiction. Proposition 16 is proved.

Exercise. Show that $\mathbb{Q}(\sqrt[3]{3})$, $\mathbb{Q}(\sqrt[3]{5})$ are fields and they are finite extensions of $\mathbb{Q}$ of degree 3.

5 A necessary condition of constructibility of a complex number with ruler and compass. Proof of the main result.

In this section we will obtain a strong general restriction on any complex number which can be constructed using ruler and compass, and then we will check that this restriction is not satisfied by $\sqrt[3]{2}$; this will prove Theorem 1. Here is the condition:

Theorem 17. *Any complex number which can be constructed with ruler and compass is contained in a finite extension of $\mathbb{Q}$ of degree which is a power of 2.*

Before we will prove this interesting result let us see how it implies our main result that $\sqrt[3]{2}$ cannot be constructed with ruler and compass.

Proof of Theorem 1. Let us assume the contrary. Then there exists a finite extension K of $\mathbb{Q}$ which contains $\sqrt[3]{2}$ and such that $[K : \mathbb{Q}] = 2^n$. Then evidently $\mathbb{Q}(\sqrt[3]{2}) \subset K$: indeed $\sqrt[3]{2} \in K$, hence $\sqrt[3]{4} = (\sqrt[3]{2})^2 \in K$ since K is closed under products, hence any sums of their rational multiples also belong to K.

By Theorem 10 we have

$$2^n = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})] \cdot 3$$

where the last equality is due to Proposition 16. Thus 3 divides 2^n which is impossible! Theorem 1 is proved.

Proof of Theorem 17. Now we have to recall all the basic steps in constructions with ruler and compass which we have listed at the beginning of Section 2. Let a be a complex number which can be constructed with ruler and compass. In principle the number of basic steps necessary to construct a could be very large. We can also list all the complex numbers which has been constructed in the intermediate steps. Thus there exist complex numbers $a_0, a_1, a_2, \ldots, a_N$ such that the last number a_N is just a (N is the number of basic steps which can be very large), $a_0 = 0$, $a_1 = 1$, and each subsequent number a_i is obtained from the previously constructed numbers $a_0, \ldots, a_{i-1}$ using one of the following operations:

(1) a_i is the point of intersection of two lines, each one passing through some of two points among $a_0, \dots, a_{i-1}$;

(2) a_i is a point of intersection of a line passing through two points among $a_0, \dots, a_{i-1}$ and a circle whose center and radius are among $a_0, \dots, a_{i-1}$;

(3) a_i is a point of intersection of two circles whose centers and radii are among $a_0, \dots, a_{i-1}$.

We will prove the theorem by induction in N, but for technical reasons it will be convenient to prove also that such a filed K can be chosen to be invariant under the complex conjugation and moreover K contains all other a_i's. The advantage of working with fields invariant under the complex conjugation is that with any complex number it contains also its real and imaginary parts (prove it!).

If $N = 1$ there is nothing to prove since we can take $K = \mathbb{Q}$. Let us assume now that the numbers $a_0, \dots, a_{N-1}$ are contained in a field F which is an extension of $\mathbb{Q}$ of degree 2^n and is invariant under the complex conjugation. Now we will make the induction step. We will consider separately each of the cases (1)-(3) above.

Case (1). Let us recall that equation of a line passing through two points on the plane (u_1, v_1) and (u_2, v_2) is

$$y = \frac{v_2 - v_1}{u_2 - u_1} \cdot (x - u_1) + v_1. \tag{9}$$

(Here we ignore the case when the denominator may vanish. This special case can be considered separately in an entirely similar way. We leave it to a reader as a simple exercise.)

In our case all the real coefficients u_i, v_i belong to the field F since F is invariant under the complex conjugation. Hence all the ratios of coefficients in (9) also belong to F. Thus $a_N = a$ is a point of intersection of two lines

$$y = k_1 x + b_1,$$
$$y = k_2 x + b_2$$

where the coefficients k_1, k_2, b_1, b_2 belong to F. Let us show that the point of intersection of two lines with coefficients in F also belongs to F. There is an explicit formula for the point of intersection, you can obtain it by yourself:

$$\left(\frac{b_1 - b_2}{k_2 - k_1}, \frac{b_1 k_2 - k_1 b_2}{k_2 - k_1} \right).$$

We see that the coordinates belong to the same field F due to its closeness under the algebraic operations. Thus eventually $a_N = a$ belongs to the same field F.

Case (2). In this case a in an intersection point of a line whose coefficients belong to F (as in the previous case, we have used the invariance of F under the complex conjugation) and a circle whose center and radius belong to F:

$$y = kx + b, \tag{10}$$
$$(x - u)^2 + (y - v)^2 = R^2 \tag{11}$$

where $k, b, u, v, R \in F$. Substituting (10) to (11) and solving the quadratic equation we get

$$x = \frac{a - k(b-v) \pm \sqrt{(-u + k(b-v))^2 - (1+k^2)(u^2 + (b-v)^2 - R^2)}}{1+k^2},$$
$$y = kx + b.$$

Notice that the sign before the square root corresponds to two points of intersection of line and circle. Now this expression may not belong to F since F may not be closed under taking square roots. The only thing we will use from this complicated formula is that x, y have the form

$$x = \alpha + \beta\sqrt{\gamma},\ y = kx + b$$

with $\alpha, \beta, \gamma, k, b \in F$. Also we assume that $\gamma \geq 0$ since otherwise the line and the circle do not intersect. This formula implies that $a_N = a \in K := F(\sqrt{\gamma})$.

Let us show that $F(\sqrt{\gamma})$ is exactly the field we need. First it is spanned over F by two elements $1, \sqrt{\gamma}$. Hence $[K : F] \leq 2$, namely this degree is either 1 or 2 (depending whether $\sqrt{\gamma}$ belongs to F or not respectively). Hence by Theorem 10

$$[K : \mathbb{Q}] = [K : F] \cdot [F : \mathbb{Q}] = [K : F] \cdot 2^n = 2^n \text{ or } 2^{n+1}.$$

Also K contains all the a_i's. To finish the induction step it remains to show that K is invariant under the complex conjugation. This is easy: if $z = a + \sqrt{\gamma}b \in K$ then $\bar{z} = \bar{a} + \sqrt{\gamma}\bar{b} \in K$. Case (2) is proved.

Case (3). Now $a_N = a$ is a point of intersection of two circles. We will see that this case follows from the previous one.

Thus let $a_N = a$ be a point of intersection of two circles

$$(x - a_1)^2 + (y - b_1)^2 = R_1^2, \tag{12}$$
$$(x - a_2)^2 + (y - b_2)^2 = R_2^2 \tag{13}$$

where a_i, b_i, R_i belong to F. After subtracting (12) from (13) we obtain the following equivalent system of equations:

$$(x - a_1)^2 + (y - b_1)^2 = R_1^2, \tag{14}$$
$$(a_1 - a_2)(2x - a_1 - a_2) + (b_1 - b_2)(2y - b_1 - b_2) = R_2^2 - R_1^2. \tag{15}$$

The second equation is an equation of a line. Thus we are reduced to the Case (2). Hence Theorem 17 is proved.

6 Further results and exercises.

The methods we have described can be used to prove that some other numbers cannot be constructed with ruler and compass.

Exercise. Show that $\sqrt[3]{3}, \sqrt[3]{5}$ cannot be constructed with ruler and compass.

The method of these lectures can be generalized much further. For example inspection of the proof of Theorem 17 shows that any complex number is contained in a field K of degree 2^n over $\mathbb{Q}$ with an extra property which is called *Galois extension*, named after the famous French mathematician Évariste Galois (1811-1832) who died at the age 21. These is another restriction on numbers constructible with ruler and compass. We will not describe here what it is, and refer an interested reader to the book "Galois theory" by E. Artin. This book is rather elementary, and can be read by high school pupils, perhaps with some minor advice of more senior friends at the vary beginning. Here we state only a necessary and sufficient condition for constructibility of a complex number with ruler and compass.

Theorem 18. *A complex number can be constructed with ruler and compass if and only if it is contained in a Galois extension of $\mathbb{Q}$ of degree which is a power of 2.*

A consequence of this theorem is that the unit circle *can be* divided to 17 equal parts with ruler and compass. (This result was first discovered by the great German mathematician Carl Friedrich Gauss (1777-1855) and in fact in a more general form when he was 19 years old, before creation of the Galois theory.) For this is suffices to show that the complex 17-th root of unity $e^{\frac{2\pi i}{17}}$ is contained in a Galois extension of $\mathbb{Q}$ of degree which is a power of 2. This is indeed the case. More precisely it follows from some general results in Galois theory that the field $\mathbb{Q}(e^{\frac{2\pi i}{17}})$ is a Galois extension of $\mathbb{Q}$ of degree $16 = 2^4$.

Numbers which belong to some finite extension of $\mathbb{Q}$ (without any restriction on the degree of the extension) are called algebraic. (Perhaps some of have heard an equivalent definition of them: algebraic numbers are precisely roots of polynomials with rational coefficients.) In particular all numbers constructible with ruler and compass are algebraic. However not all numbers are algebraic. They are called transcendental. It can be shown (and these are non-trivial theorems) that the numbers π and e are transcendental.