An application of Galois theory: (Im-) Possibility of geometric constructions

The set up is that we are given a straightedge and compass and the points $(0,0) \in \mathbb{R}^2$ and $(1,0) \in \mathbb{R}^2$. We call these two points "known" points. Now one produces new "known" points via the following operations:

(i) Take two of the "known" points and draw a straight line through them

(ii) Take a "known" point and draw the circle centered at it whose radius is the distance between two known points (Note: one can use different assumptions here and then show that they lead to the same results)

Then we make the following definitions.

Definition. Any point of intersection of such lines and circles becomes a "known" point.

Definition. A number $a \in \mathbb{R}$ is called constructible if, starting with $(0,0)$ and $(1,0)$ we can construct by the above rules two points whose distance is $|a|$. A point $P = (x,y) \in \mathbb{R}^2$ is called constructible if x and y are constructible.

How does this have to do with algebra? It's not so hard to show the following lemma.

Lemma. The subset K of $\mathbb{R}$ given by constructible numbers is a field.

The proof of this is not difficult, and I leave it to you as an exercise. The idea is that, firstly, $0, 1 \in K$ from above. Suppose that $a, b \in K$. Then one can show $a \pm b \in K$ (we can assume that $a, b, a \pm b$ are all positive). Also, $ab \in K$ and $a/b \in K$ if $b \neq 0$ (we can assume that a, b, ab, a/b are all positive)

What is the shape of coordinates of new "known" points obtained via the geometric constructions? We answer this in the following lemma.

Lemma. Let $F \subseteq \mathbb{R}$ be a field. Suppose C_i for $i = 1, 2$ is either a line in $\mathbb{R}^2$ passing through two points in F^2 or a circle centered at a point in F^2 with radius in F. Let P be a point of intersection of C_1 and C_2. Then the coordinates of P are in $F(\sqrt{u})$ for some $u \in F$ which satisfies $u \geq 0$.

Proof. Equations for lines as above are of the form

$$ax + by + c = 0$$

with $a, b, c \in F$. Equations for circles as above are of the form

$$(x - x_1)^2 + (y - y_1)^2 = r^2$$

with $x_1, y_1, r \in F$. Let us now prove the lemma case by case:

(i) A point of intersection between two lines as above has coordinates in F.

(ii) Suppose P is a point of intersection between a line and a circle as above. Eliminating one of the variables in the quadratic equation shows that the coordinates lie in an extension of F of degree at most 2.

(iii) Suppose P is a point of intersection between two circles as above: The solution set of

$$(x - x_1)^2 + (y - y_1)^2 - r^2 = 0 = (x - x_2)^2 + (y - y_2)^2 - s^2$$

equals the solution set of

$$(x-x_1)^2+(y-y_1)^2-r^2 = 0 = (x-x_2)^2+(y-y_2)^2-s^2-[(x-x_1)^2+(y-y_1)^2-r^2]$$

Which is the intersection of a circle and a line as above.

□

From this we can derive the following crucial theorem about what kinds of number in $\mathbb{R}$ are constructible.

Theorem. *A real number $a \in \mathbb{R}$ is constructible if and only if there is a tower of fields*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

such that

(i) $a \in K_r$

(ii) $[K_{i+1} : K_i] = 2$ *for all* $0 \leq i \leq r - 1$

Proof. Suppose first that a is constructible. Then $(|a|, 0)$ is a known point and by the previous lemma there is a tower of fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

such that $|a| \in K_r$, and hence $a \in K_r$, and $[K_{i+1} : K_i] = 2$ for all $0 \leq i \leq r - 1$.

Suppose now conversely that such a sequence of fields exists. Let us prove the result by induction on r. In case that $r = 0$ we have that $a \in \mathbb{Q}$ and we have seen that a is

constructible. Hence suppose now that the result is true for $r-1$. Note that a satisfies a quadratic equation over K_{r-1} and hence is of the form

$$a = q + r\sqrt{s}$$

with $q, r, s \in K_{r-1}$ and $s \geq 0$. Hence we are done if we can show that if $s \geq 0$ is constructible then $\sqrt{s}$ is constructible. This is an elementary geometry problem which I encourage you to think about.

□

We can now prove some impossibilities of constructions considered by the ancient Greek! In these notes we include an example which does not require knowledge of Galois theory. Namely, we show the following.

Theorem. *There is no general straightedge and compass construction that trisects an angle.*

Proof. It is clearly sufficient to show that there is at least one angle that cannot be trisected by straightedge and compass. So, consider the angle

$$\theta = \pi/3$$

Then θ is constructible since $(\cos(\pi/3), \sin(\pi/3)) = (1/2, \sqrt{3}/2)$ is constructible. Hence if one could trisect θ then one could construct by straightedge and compass two lines which intersect at an angle of $\pi/9$ and hence the number $\cos(\pi/9)$ would be constructible. Let us show that this is impossible. Recall the triple angle formula

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

and let $\alpha = \cos(\pi/9)$. Since $\cos 3\alpha = 1/2$ it follows that α is a root of

$$4x^3 - 3x - 1/2 = 0$$

and hence α is a root of

$$8x^3 - 6x - 1 = 0$$

which is irreducible over $\mathbb{Q}$ by the rational root test and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and this is not a power of 2 and hence α cannot be constructed by straightedge and compass. □