LESSON 8 - STRAIGHT-EDGE AND COMPASS CONSTRUCTIONS

ERAN ASSAF

1. Introduction

Last lesson we introduced the notion of algebraic extensions, we have shown that the finite extensions are the algebraic extensions which are generated by finitely many elements. We have shown that "algebraic over algebraic is algebraic", and that all algebraic numbers form a field. The last thing we did was to define the compositum (composite field) of two field extensions. We will start the lesson by better understanding the degree of the compositum, and move on to relate what we have learned to constructions with straight-edge and compass.

2. Composite field

Example 1. *The composite of* $K_1 = \mathbb{Q}(\sqrt{2})$ *and* $K_2 = \mathbb{Q}(\sqrt[3]{2})$ *is* $K = \mathbb{Q}(\sqrt[6]{2})$. *Indeed,* $K_1, K_2 \subseteq K$, *and conversely, any field containing* K_1 *and* K_2 *would contain* $\sqrt{2}/\sqrt[3]{2} = \sqrt[6]{2}$.

Definition 2. *Let* K_1, K_2 *be two finite extensions of* F *contained in* K. *We say that* K_1 *and* K_2 *are* **linearly disjoint** *if an* F*-basis for* K_2 *remains linearly independent over* K_1.

Proposition 3. *Let* K_1, K_2 *be two finite extensions of* F *contained in* K. *Then*

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F].$$

with equality if and only if K_1, K_2 *are linearly disjoint.*

Proof. Let $\alpha_1, \ldots, \alpha_m$ be a basis for K_1 over F and let $\beta_1, \ldots, \beta_n$ be a basis for K_2 over F. Then

$$K_1K_2 = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) = K_1(\beta_1, \ldots, \beta_n),$$

and since $\beta_1, \ldots, \beta_n$ span K_2 over F, $\beta_i\beta_j = \sum a_{ijl}\beta_l$ for some $a_{ijl} \in F$. Let $L = \{\sum c_l\beta_l : c_l \in K_1\}$. The above shows that L is closed under addition and. multiplication. Since every element $\gamma \in L$ is algebraic over F, we can write its inverse as a polynomial $\gamma^{-1} = p_\gamma(\gamma) \in L$. Therefore, L is a field which contains both K_1 and K_2, hence $L = K_1K_2$ and $\beta_1, \ldots, \beta_n$ span K_1K_2 over K_1. It follows that $[K_1K_2 : K_1] \leq n = [K_2 : F]$ with equality if and only if the β_j are linearly independent over K_1. Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$, this proves the proposition. □

Corollary 4. *The notion of linear disjointness does not depend on the choice of basis, or on the order of the fields.*

Corollary 5. *Suppose that* $[K_1 : F] = m$ *and* $[K_2 : F] = n$ *with* m, n *relatively prime. Then* $[K_1K_2 : F] = mn$.

Proof. We have $m \mid [K_1K_2 : F]$ and $n \mid [K_1K_2 : F]$, hence $mn = \text{lcm}(m, n) \mid [K_1K_2 : F]$. Together with $[K_1K_2 : F] \leq mn$, we are done. □

Example 6. $[\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6$.

3. Straightedge and compass constructions

The idea of constructions with straight-edge and compass is simple - we are only allowed to construct circles with center at a point we have constructed, passing through another point, and lines passing through two points that we have constructed. The points are constructed as intersection points of lines and circles we have constructed.

Since we need some measurement to compare to and set things to scale, constructing a number means given a segment of length 1, to construct a segment of that length.

Definition 7. *A real number $\alpha \in \mathbb{R}$ is* **constructible** *if a segment of length α can be constructed by successive iterations of*

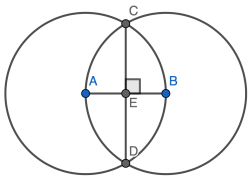
- *lines drawn through two points already constructed.*
- *circles with center a point already constructed and radius a constructed length.*
- *finding the points of intersection of lines and circles already constructed.*

given a segment of length 1.

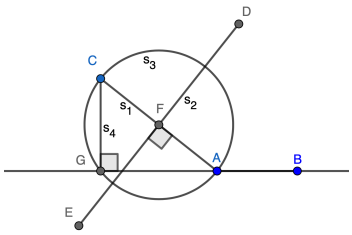
Example 8. 2 *is constructible. Given a segment of length* 1 *- AB, we draw the circle with center at A and passing through B, and we draw the line passing through A and B. Denote its second intersection with the circle by C. Then BC is of length* 2.

Some simple constructions -

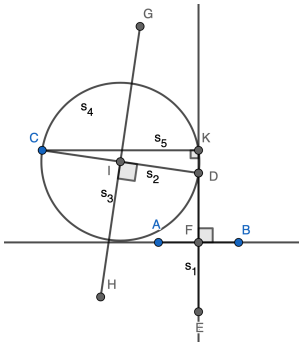
(1) can construct a perpendicular bisector of a segment. (intersect two circles).



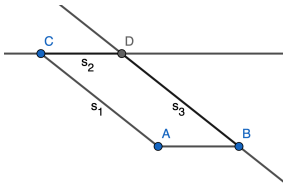
(2) can construct a line passing through a point and perpendicular to another line. (choose a point on the line, construct the segment connecting the two points, bisect it, and construct the circle whose diameter is the segment. The other intersection point of the circle with the line gives the altitude).



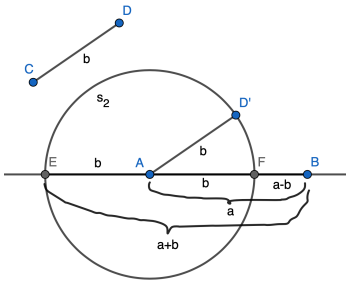
(3) can construct a line parallel to a given line through another point. (construct an altitude not passing through the point, and then an altitude from the point to it).



(4) can construct a translate of a segment through a given point. (draw the line parallel to the segment through the point, connect one of the endpoints to it, and draw the line parallel to it through the other endpoint, to form a parallelogram).



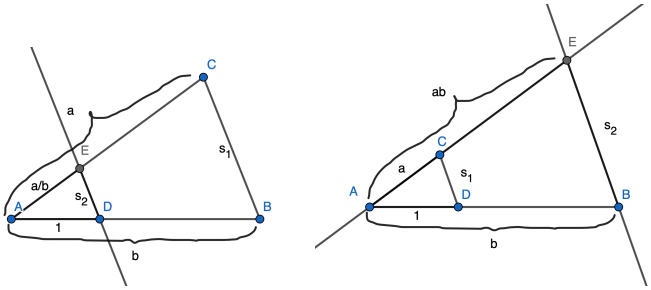
In particular, if we have two segments of length a, b we can translate one of them so they will have a common endpoint, and by drawing a circle with this point as center, obtain segments of length $a + b$ and $a - b$.



Corollary 9. *All integers $\mathbb{Z}$ are constructible.*

Proposition 10. *The constructible numbers form a field.*

Proof. Thales's theorem.

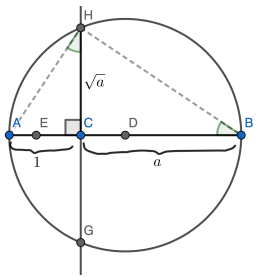


□

Corollary 11. *All rationals $\mathbb{Q}$ are constructible.*

Proposition 12. *If a is constructible, so is $\sqrt{a}$.*

Proof. Construct a circle with diameter $1 + a$ and erect the perpendicular to the diameter at the point separating $1 : a$.



Similarity of triangles yields the result. □

4. Impossibility of constructions

Introducing coordinates to the plane $(x, y) \in \mathbb{R}^2$, we can equivalently ask what are all constructible points in $\mathbb{R}^2$. Assume we have constructed some number by performing N constructions. Let $F_n \subseteq \mathbb{R}$ be the subfield generated by the numbers we have constructed after n steps. Passing two lines and intersecting them gives us a linear equation, whose solution will have coordinates in F_n. An intersection of a line with a circle will construct points in a quadratic extension of F_n, and so will an intersection of two circles. Therefore, $[F_{n+1} : F_n] \leq 2$, hence if $\alpha \in \mathbb{R}$ is constructible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ for some m.

Theorem 13. *If $\alpha \in \mathbb{R}$ is constructible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ for some m.*

Corollary 14. *It is impossible to double the cube, trisect an angle or square the circle.*

Proof. Doubling the cube implies constructing a segment of length $\sqrt[3]{2}$, but it is of degree 3. Constructing an angle θ is equivalent to constructing $\cos\theta$, so trisecting the angle is the same as constructing $\cos\theta/3$ given $\cos\theta$. To see that this is not always possible, consider $\theta = 60^\circ = \pi/3$. Then from $\cos\theta = 4\cos\theta/3^3 - 3\cos\theta/3$, if we write $\beta = \cos 20^\circ$ we get $4\beta^3 - 3\beta - 1/2 = 0$. Let $\alpha = 2\beta$, then $\alpha^3 - 3\alpha - 1 = 0$, so α is the unique root in $[0, 2]$ of $x^3 - 3x - 1$. In particular, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Finally, squaring the circle is equivalent to constructing $\sqrt{\pi}$, but π is transcendental. □

Proposition 15. *Let p be a prime. A regular p-gon is constructible only if $p = 2^{2^n} + 1$ for some n is a Fermat prime.*

Proof. To construct a regular p-gon, we need to construct an angle of $2\pi/p$, hence $\cos(2\pi/p) = (\zeta_p + \zeta_p^{-1})/2$. Note that $\mathbb{Q}[\cos(2\pi/p)] \subseteq \mathbb{Q}(\zeta_p)$, and that

$$(2\cos(2\pi/p))\zeta_p = (\zeta_p + \zeta_p^{-1})\zeta_p = \zeta_p^2 + 1 \implies \zeta_p^2 - 2\cos(2\pi/p)\zeta_p + 1 = 0,$$

so that $f(x) = x^2 - 2\cos(2\pi/p)x + 1$ has ζ_p as a root. Since $\zeta_p \notin \mathbb{R}$, it follows that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\cos(2\pi/p))] = 2$. From the identity $\Phi_p(x) = x^{p-1} + \ldots + x + 1 = (x^p - 1)/(x - 1)$, we see that $\Phi_p(\zeta_p) = 0$, and we have seen that $\Phi_p(x)$ irreducible over $\mathbb{Q}$, hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Using the tower law, we obtain $[\mathbb{Q}(\cos 2\pi/p) : \mathbb{Q}] = \frac{p-1}{2}$. If the regular p-gon is constructible, then $\frac{p-1}{2} = 2^{m-1}$ for some m, hence $p = 2^m + 1$. Moreover, note that if $m = dr$ with r odd, we have

$$2^m + 1 = (2^d + 1)(2^{(r-1)d} - 2^{(r-2)d} + 2^{(r-3)d} - \ldots - 2^d + 1).$$

Therefore, if m has an odd factor $r > 1$, then it is composite. In particular, the fact that $p = 2^m + 1$ is prime, implies m does not have any odd prime factors, hence $m = 2^n$. □

5. summary

We have seen how field theory solves some centuries-old problems that mathematicians have grappled with (!!) We have seen a necessary condition for numbers to be constructible using straight-edge and compass, and applied it to a variety of problems - doubling the cube, trisecting the angle, squaring the circle. We still haven't completely solved the problem of

which regular n-gons can be constructed, although we do have a necessary condition for prime ones, showing for example that it is impossible to construct a regular heptagon(!)