Solutions Exercise sheet 5

Exercises marked with * go beyond the standard subject matter.

1. *(Constructions with compass and ruler)* In the Euclidean plane consider the following two operations:

(a) *(ruler)* Given two points P, Q, we can draw a straight line through them.

(b) *(compass)* Given two points P, Q draw a circle whose center is one of P,Q and whose radius is equal to the distance between the given points.

Assume we are given two distinct points P_0 and P_1 in the plane. Through translation, rotation and stretching, we can assume that $P_0 = (0, 0)$ and $P_1 = (1, 0)$.

We say a point P is **constructible** if there exists a finite sequence of points

$$P_0, P_1, \ldots, P_n = P$$

in the plane with the following property. Let

$$S_j = \{P_0, P_1, \ldots, P_j\}, \text{ for } 1 \leqslant j \leqslant n.$$

For each $2 \leqslant j \leqslant n$, P_j is either

(i) the intersection of two distinct straight lines, each joining two points of S_{j-1}, or

(ii) a point of intersection of a straight line joining two points of S_{j-1} and a circle with centre a point of S_{j-1} and radius the distance between two points of S_{j-1}, or

(iii) a point of intersection of two distinct circles, each with centre a point of S_{j-1} and radius the distance between two points of S_{j-1}.

In case (iii), the centres must be different if the circles are to intersect: the radii may or may not be different.

If $P = (x, y)$ is a constructible point, we consider the extension $\mathbb{Q}(x, y) : \mathbb{Q}$ generated by x and y. In this exercise we'll prove that if $P = (x, y)$ is a constructible point, the extension $\mathbb{Q}(x, y) : \mathbb{Q}$ is finite, and $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$, for some non-negative integer r.

Let $P_0, P_1, \ldots, P_n = P$ be a sequence of points which satisfies the requirements of the definition of P being constructible. Let $P_j = (x_j, y_j)$, and for $1 \leqslant j \leqslant n$ let

$$F_j = \mathbb{Q}\left(x_1, y_1, x_2, y_2, \ldots, x_j, y_j\right),$$

so that $F_{j+1} = F_j\left(x_{j+1}, y_{j+1}\right)$, for $1 \leqslant j < n$.

(a) Prove that $[F_{j+1} : F_j] = 1$, if (x_{j+1}, y_{j+1}) is the intersection of two distinct straight lines, each joining two points of S_j, i.e. arises from an intersection point of type (i).

(b) Prove that $[F_{j+1} : F_j] = 1$ or 2, if (x_{j+1}, y_{j+1}) is a point of intersection of an appropriate straight line and circle, i.e. arises from an intersection point of type (ii).

(c) Prove that $[F_{j+1} : F_j] = 1$ or 2, if (x_{j+1}, y_{j+1}) is a point of intersection of two circles.

(d) Show that

$$[F_n : F_1] = [F_n : \mathbb{Q}] = 2^s,$$

for some $s \in \mathbb{Z}_{\geqslant}$ and conclude

$$[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r,$$

for some non-negative integer r.

Solution: If (a_1, b_1) and (a_2, b_2) are two points in S_j, the equation of the line joining (a_1, b_1) and (a_2, b_2) is $(x - a_2)(b_1 - b_2) = (a_1 - a_2)(y - b_2)$, and therefore has the form

$$\lambda x + \mu y + v = 0,$$

where λ, μ and v are elements of F_j.

Similarly the equation of the circle, centre (a_1, b_1) and radius the distance between points (a_2, b_2) and (a_3, b_3) of S_j, is

$$(x - a_1)^2 + (y - b_1)^2 = (a_2 - a_3)^2 + (b_2 - b_3)^2,$$

and therefore has the form

$$x^2 + y^2 + 2gx + 2fy + c = 0$$

where f, g and c are elements of F_j.

(a) Assume (x_{j+1}, y_{j+1}) is the intersection of two distinct straight lines, each joining two points of S_j. In this case (x_{j+1}, y_{j+1}) is the solution of two simultaneous equations

$$\lambda_1 x + \mu_1 y + v_1 = 0$$
$$\lambda_2 x + \mu_2 y + v_2 = 0$$

with coefficients in F_j. Solving these, we find that x_{j+1} and y_{j+1} are in F_j, so that $F_{j+1} = F_j$ and $[F_{j+1} : F_j] = 1$.

(b) Assume (x_{j+1}, y_{j+1}) is a point of intersection of an appropriate straight line and circle. In this case (x_{j+1}, y_{j+1}) satisfies equations

$$\lambda x + \mu y + \nu = 0,$$
$$x^2 + y^2 + 2gx + 2fy + c = 0$$

with coefficients in F_j. Suppose that $\lambda \neq 0$. We can then eliminate x, and obtain a monic quadratic equation in y. If this factors over F_j as

$$(y - \alpha)(y - \beta) = 0$$

then $y_{j+1} = \alpha$ or β, so that $y_{j+1} \in F_j$; substituting in the linear equation, $x_{j+1} \in F_j$, so that $F_{j+1} = F_j$, and $[F_{j+1} : F_j] = 1$. If the quadratic is irreducible, it must be the minimal polynomial for y_{j+1} : thus, $[F_j(y_{j+1}) : F_j] = 2$. As $x_{j+1} = -\lambda^{-1}(\mu y_{j+1} + v)$, $x_{j+1} \in F_j(y_{j+1})$ and so $F_{j+1} = F_j(x_{j+1}, y_{j+1}) = F_j(y_{j+1})$. If $\lambda = 0$, then $\mu \neq 0$, and we can repeat the argument, interchanging the roles of x_{j+1} and y_{j+1}.

(c) Assume (x_{j+1}, y_{j+1}) is a point of intersection of two suitable circles. In this case (x_{j+1}, y_{j+1}) satisfies equations

$$x^2 + y^2 + 2g_1 x + 2f_1 y + c_1 = 0$$
$$x^2 + y^2 + 2g_2 x + 2f_2 y + c_2 = 0$$

with coefficients in F_j. Subtracting, (x_{j+1}, y_{j+1}) satisfies the equation

$$2(g_1 - g_2)x + 2(f_1 - f_2)y + (c_1 - c_2) = 0$$

We cannot have $g_1 = g_2$ and $f_1 = f_2$, for then the circles would be concentric, and would not intersect. Thus this case reduces to the previous one.

(d) By part (a) - (c), we have that $[F_{j+1}; F_j] = 1$ or 2. Then, by the tower law, $[F_n : F_1] = [F_n : \mathbb{Q}] = 2^s$ for some non-negative integer s. But $\mathbb{Q}(x, y) = \mathbb{Q}(x_n, y_n)$ is a subfield of F_n containing $\mathbb{Q}$, so by the tower law again,

$$[F_n : \mathbb{Q}(x, y)]\,[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^s,$$

and so $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$, for some non-negative integer r.

2. *(Trisecting the angle)* It is not possible to construct the angle $\alpha/3$ for every angle α by using only a finite number of steps with a compass and ruler.

Hint: Consider $\cos(\frac{\pi}{9})$ and find its minimal polynomial.

Solution: We will show that we can not trisect $\alpha = \frac{\pi}{3}$.

Using a ruler and compass it is possible to construct the angle $\frac{\pi}{3}$. If we could trisect α, this would mean we could construct the angle $\pi/9$. This would then imply that we could construct a point P which is in the intersection of the line given by

$$x \sin\frac{\pi}{9} = y \cos\frac{\pi}{9};$$

and the circle with center P_0 and radius $P_0P_1 = 1$. It would follow that $(\cos\frac{\pi}{9}, \sin\frac{\pi}{9})$ would be constructible, which would in return mean

$$\left[\mathbb{Q}\left(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}\right) : \mathbb{Q}\left(\cos\frac{\pi}{9}\right)\right]\left[\mathbb{Q}\left(\cos\frac{\pi}{9}\right) : \mathbb{Q}\right] = 2^t,$$

for some non-negative t.

Note that $\cos(\alpha) = \frac{1}{2} \in \mathbb{Q}$. Let $w := 2\cos\frac{\pi}{9}$. Then the degree of the minimal polynomial of w over $\mathbb{Q}$ is 3: by the triple angle identity,

$$\frac{1}{2} = \cos\left(3 \cdot \frac{\pi}{9}\right) = 4\cos\left(\frac{\pi}{9}\right)^3 - 3\cos\left(\frac{\pi}{9}\right),$$

so that $w^3 - 3w - 1 = 0$. Since the polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, it is the minimal polynomial of w over $\mathbb{Q}$. Then $[\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$, so by Exercise **1**.d, $\frac{\pi}{9} = \frac{\alpha}{3}$ is not constructible.

3. *(Doubling the cube)* It is impossible to construct the number $\sqrt[3]{2}$ by using only a finite number of steps with a compass and ruler.

Solution: Note that the polynomial $X^3 - 2$ is irreducible over $\mathbb{Q}$. Then

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

so by Exercise **1**.d, we have $\sqrt[3]{2}$ is not constructible..

4. *(Squaring the circle)* It is impossible to construct a square with the area of a given circle by using only a finite number of steps with a compass and ruler.

Solution: W.l.o.g. we consider a circle with radius $r = 1$.

Then the degree $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is infinite, since $\sqrt{\pi}$ is transcendental (since π is transcendental). Hence it is not constructible by Exercise **1**.d.

5. * *(Classical geometric constructions)* For any set A of points, let $Cons(A)$ be the set of all points that can be constructed from A (by iterated application of the operations in Exercise **1**.).

We identify the Euclidean plane with $\mathbb{C}$ with the usual distance $d(P, Q) := |P - Q|$. To be able to construct new points, we assume that A contains at least two different points. Through translation, rotation and stretching, we can assume that A contains at least the points 0 and 1.

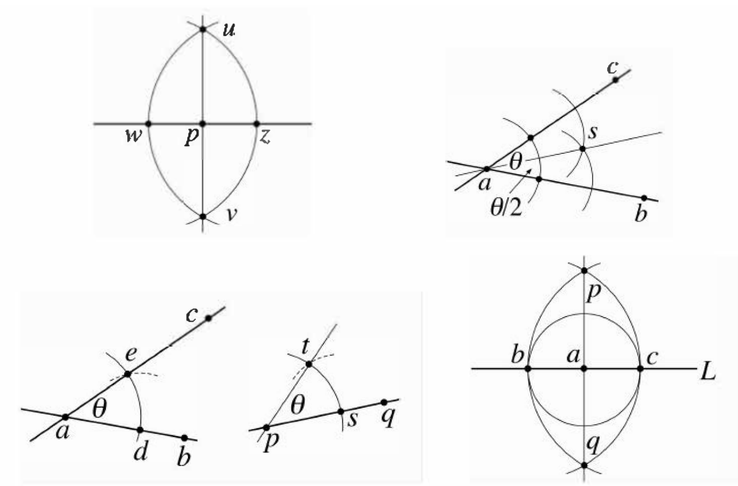
Let $K = Cons(A)$. Prove that

(i) K is a subfield of $\mathbb{C}$

(ii) $\forall z \in K : \overline{z} \in K$

(iii) $\forall z \in \mathbb{C} : z^2 \in K \rightarrow z \in K$

Solution: Using a compass and ruler we can do the following basic constructions: copy a length, copy an angle, bisect lines, bisect angles and construct a perpendicular. Below we demonstrated the following constructions: (top left) bisecting a line; (top right) bisecting an angle; (bottom left) copying an angle; (bottom right) constructing a perpendicular (picture taken from Chap. 7.3, Galois theory, I. Stewart).



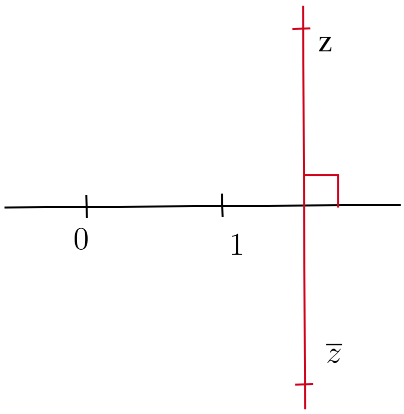
Now that we have these basic constructions, we can use them to construct more involved objects.

(a) Claim: $\forall z \in K : -z \in K$.

For $z = 0$ this is clear. Otherwise, we are given different points 0 and z on the plane. Draw a line through those two points. Then using a compass copy the length $|z - 0|$ starting from 0 on the opposite side of the point z. Hence we have the point $-z$.

(b) Claim: $\forall z \in K : \overline{z} \in K$.

Construct a perpendicular as in the picture below:

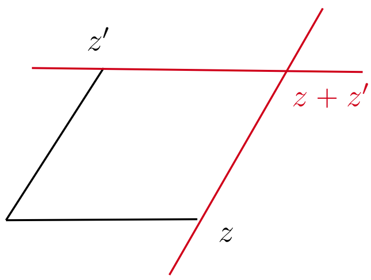


(c) Claim: if the angles α, β are constructible, then also $\alpha \pm \beta$ are constructible.

This can be done by copying one angle right next to the other one; either on the outside (if we want to contruct $\alpha + \beta$) or on the inside (if constructing $\alpha - \beta$).

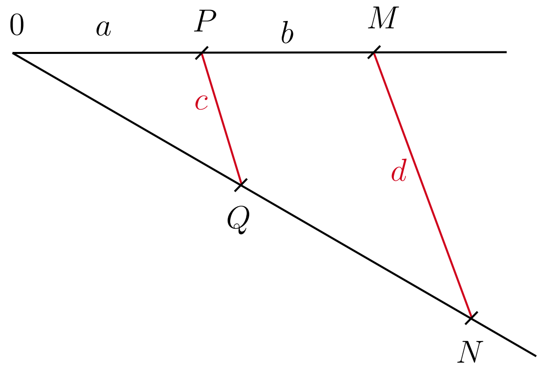
(d) Claim: $\forall z, z' \in K : z + z' \in K$.

If $z = 0$ or $z' = 0$ this is clear. Assume $z \neq 0$ and $z' \neq 0$. Draw the points $0, z, z'$ on the plane. If all those points lie on the same line, we can simply transfer the lengths on that same line to add them together. Otherwise construct a parallelogram as below:



(e) Claim: If the lengths $a, b, c > 0$ are constructible, then also $\frac{bc}{a}$ is constructible.

Draw a straight line starting at the point 0 and transfer the length a starting from the point 0. We will denote this line segment by $\overline{0P}$. Then transfer the length b starting at the point P and denote this line segment $\overline{PM}$. Then, we draw a straight line through the point P (which does not lie on the initial line) and transfer the length c onto it, starting from the point P. Denote this line segment with length c by $\overline{PQ}$. Next, draw a line parallel to $\overline{PQ}$, which goes through the point M. Finally, draw a line through the point 0 and Q as demonstrated in the picture below.

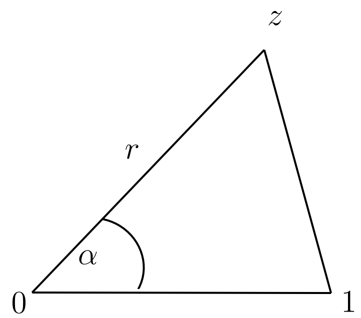


The length of the line segment $\overline{0N}$ (as in the picture above) denoted by d will be the length $\frac{bc}{a}$: we have for the lengths a, b, c, d

$$a : c = b : d$$

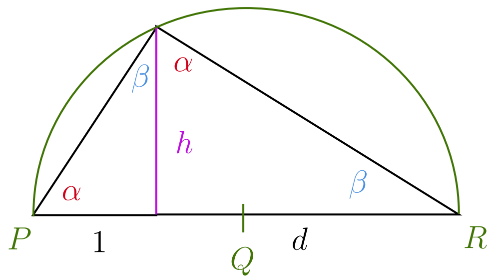
so that $d = \frac{bc}{a}$.

(f) Claim: $z = re^{i\alpha}$ is constructible $\iff$ the length r and the angle α are constructible. Consider:



(g) From the constructions above we obtain: $z, z' \in K \Rightarrow z \cdot z' \in K$, and if $z' \neq 0$, then $z/z' \in K$.

(h) Claim: If d is constructible, then also $\sqrt{d}$ is constructible.
First we draw a line with length d and then we extend that line by 1 on one side. We will denote the length of the new line $d+1$ with $\overline{PR}$. Then bisect the line $\overline{PR}$ and denote the middle point by Q. Draw a circle with radius $\overline{QR}$ with center Q. Then draw a perpendicular line through the point between the line d and 1 and have it intersect the circle. We will denote this height by h (see picture below).



Since the two smaller triangles on the picture are similar, we have

$$1 : h = h : d,$$

so $h = \sqrt{d}$.

(i) Claim: for $z \in K, w \in \mathbb{C} : w^2 = z \Rightarrow w \in K$.
We can write $z = re^{i\alpha}$, so that $w = \sqrt{r} \cdot e^{i\frac{\alpha}{2}}$. Then our claim follows from the constructions above, as we can bisect an angle and construct the square-root of a length.

Hence we have showed that K is a subfield of $\mathbb{C}$ with the properties (i)-(iii).