SOLUTIONS TO WORKSHEET #1

Let $Q \neq R$ be two distinct points "drawn" in an infinite piece of paper, which we think of as the plane $\mathbf{R}^2$. A point $P \in \mathbf{R}^2$ is **constructible from** Q **and** R if $P \in \{Q, R\}$ or else P lies at the intersection of a pair of lines, of a line and a circle, or of a pair of circles that you can draw using only a straightedge and a compass following the two rules below:

(i) you can draw the line (using the straightedge) through any two points that are already drawn,

(ii) you can open the compass to span the distance $r := d(P, \tilde{P})$ between any two points P and $\tilde{P}$ that you have already drawn, place the base at a third already drawn point, say O, and draw the circle centered at O with radius r.

Identify the field of complex numbers $\mathbf{C}$ with $\mathbf{R}^2$ in the usual way. A complex number $z = x + iy$ is **constructible** if and only if the point $P = (x, y)$ is constructible from $Q = (0, 0) \simeq 0_{\mathbf{C}}$ and $R = (1, 0) \simeq 1_{\mathbf{C}}$ as above.

Problem 1. — *Use induction to prove that every integer is constructible.*

Solution. Induct on the integer $n \geq 0$ that the integers $n_{\mathbf{C}} = (n, 0)$ and $-n_{\mathbf{C}} = (-n, 0)$ are constructible starting from the two points $0_{\mathbf{C}} = (0, 0)$ and $1_{\mathbf{C}} = (1, 0)$, the base case $n = 0$ be given. Assume now that $n > 0$ and that we have constructed all integers $k_{\mathbf{C}} = (k, 0)$ satisfying $|k| < n$. To construct $n_{\mathbf{C}}$, draw a circle centred at $(n-1)_{\mathbf{C}}$—which we have constructed by the inductive hypothesis!—of radius $r = d(0_{\mathbf{C}}, 1_{\mathbf{C}}) = 1$. This circle intersects x-axis—this is the line between $0_{\mathbf{C}}$ and $1_{\mathbf{C}}$—at two points: once at the known point $(n-2)_{\mathbf{C}}$ and once at a new point, and this is none other than $n_{\mathbf{C}}$. The integer $-n_{\mathbf{C}}$ is constructed analogously by drawing a unit circle centred at $(-n+1)_{\mathbf{C}}$. ■

Problem 2. — *Use the two claims below to prove that the set F of all constructible complex numbers forms a field such that $\mathbf{Q}(i) \subset F \subset \mathbf{C}$.*

(i) *If L is a line and P is a point that have already been drawn, then we can draw the unique line containing P that is parallel to L.*

(ii) *If α and β are constructible, then so are $\alpha \cdot \beta$ and α/β (if $\beta \neq 0$).*

Solution. In view of (ii), to show that F is a field, it remains to check that it has additive inverses and is closed under addition: If $\alpha, \beta \in F$, then $-\alpha \in F$ and $\alpha + \beta \in F$. To construct $-\alpha$, consider the circle of radius $r = d(0, \alpha)$ centred at 0. This intersects the line between 0 and α at the two points $\pm\alpha$. For the sum of α and β, use (i) to draw the line L through α which is parallel the line through 0 and β; similarly, let M be the line through β which is parallel to that through 0 and α. Then the point of intersection between L and M is $\alpha + \beta$.

It remains to see that F contains the field $\mathbf{Q}(i)$. Since we know F is a field—so it is closed under addition and multiplication, for instance—it is enough to show that $i = (0, 1)$ is constructible, so that it lies in F. Construct this in two steps: First, we can construct the y-axis by choosing any integer $n \geq 1$ and drawing the two circles C_+ and C_- of radius $n+1$ centred at n and $-n$, respectively. By symmetry, C_+ and C_- intersect at two points of the form $(0, \pm y)$ for some y—in fact, an easy computation shows that $y = \sqrt{2n+1}$. In any case, the line between these points of intersection provides the y-axis. At this point, we can construct $\pm i = (0, \pm 1)$ by drawing a unit circle at centred at 0 and taking its intersection points with the y-axis. ■

Date: September 18, 2025.

Problem 3. — *Prove that the field F is closed under taking square roots.*

Solution. Thinking of $\alpha \in F$ as a complex number, we may write it in polar coordinates as

$$\alpha = re^{i\theta} \text{ for some } r \in \mathbf{R} \text{ and } \theta \in [0, 2\pi).$$

Since $\sqrt{\alpha} = \sqrt{r}e^{i\theta/2}$, it suffices to show that we can take square roots of lengths and bisect angles. If we are able to construct a length $r \in \mathbf{R}$, we can construct the length $\sqrt{r}$ by forming the circle C centred at $r - \frac{1}{4}$ with radius $r + \frac{1}{4}$. Its intersection with the y-axis has y-coordinates solving

$$(r - 1/4)^2 + y^2 = (r + 1/4)^2 \iff y^2 = (r + 1/4)^2 - (r - 1/4)^2 = r,$$

that is, at the points $(0, \pm\sqrt{r})$. This constructs the length $\sqrt{r}$.

Now suppose the angle θ is given in the unit circle C centred at the origin $Q = (0, 0)$ as PQR where $R = (1, 0)$ and P is some other point on the circumference. If $\theta = \pi$, meaning $P = (-1, 0)$, then we can bisect θ by intersecting C with the y-axis. Next, if $\theta \in (\pi, 2\pi)$, write it as $\theta = \pi + \phi$ for some $\phi \in (0, \pi)$ and note that $\theta/2 = \pi/2 + \phi/2$, so that if we know how to bisect ϕ, then we know how to bisect θ. Thus it remains to consider $\theta \in (0, \pi)$, so that P is in the upper half plane. In this case, elementary geometry shows that $\theta/2$ is the angle formed by P, $(-1, 0)$, and R. A bisector for θ can be constructed drawing the line through Q parellel to the line between $(-1, 0)$ and P. ■

Problem 4. — *Prove that you cannot construct the real number $\sqrt[3]{2}$ by proving that if $\alpha \in \mathbf{R}$ is constructible, then α is algebraic over $\mathbf{Q}$ and the degree of the field extension $\mathbf{Q} \subset \mathbf{Q}(\alpha)$ is a power of two.*

Solution. Constructible numbers arise by taking intersections of

(i) pairs of lines through constructible points, or

(ii) a line through constructible points with a circle with constructible radius and centre, or

(iii) pairs of circles with constructible radius and centre.

Since all constructible numbers are obtained by performing a finite number of such operations starting from lines or circles defined by rational numbers, it suffices to show that the output points in each construction above may be algebraically expressed in terms of the constructible input points. But each case involves solving two equations of degrees ≤ 2, and the solutions may be computed in each case to be either linear in the inputs, or else possibly involving a square root of the inputs. In all cases, the output points are algebraic in the inputs.

Now let α be constructible. To see that the degree d of the field extension $\mathbf{Q} \subseteq \mathbf{Q}(\alpha)$ is of the form 2^n for some integer $n \geq 0$, observe that α may be constructed from rational numbers by successively taking linear combinations and square roots. But this means that α satisfies some rational polynomial $f(t)$ of degree 2^N for some $N \geq 0$. The degree d is the degree of the minimal polynomial $f_{\min}(t)$ of α over $\mathbf{Q}$, and it has the property that $f_{\min}(t) \mid f(t)$. Thus $d \mid 2^N$ and so it must be of the form $d = 2^n$ for some $0 \leq n \leq N$.

■