Constructible numbers

Define recursively a set of numbers in the complex plane as follows.

$$S_0 = \{0, 1\} \tag{0.1}$$

$$S_{n+1} = S_n \cup A_{n+1} \tag{0.2}$$

where A_{n+1} consists of all points occurring in the intersection of two distinct lines, two distinct circles, or a circle and a line constructed from S_n. That is, these circles and lines are subject to the conditions that
(1) the lines must go through two points in S_n;
(2) and the circles must have centres in S_n and radii the distance between two points in S_n.
As an easy exercise, you should check that

$$S_1 = \{0, 1, -1, 2, (1 + \sqrt{3}i)/2, (1 - \sqrt{3}i/2\}. \tag{0.3}$$

Now define

$$S = \cup_{n=0}^{\infty} S_n \subset \mathbb{C}. \tag{0.4}$$

It might be useful to have notations also for the set L_n of lines constructed from S_n and the set C_n of circles constructed from S_n. And then

$$L = \cup_{n=0}^{\infty} L_n \tag{0.5}$$

and

$$C = \cup_{n=0}^{\infty} C_n. \tag{0.6}$$

To warm up, let us check

Lemma 0.1. *We have $\bar{S}_n = S_n$, where the bar refers to complex conjugation. So $\bar{S} = S$.*

Proof. This is clearly true for S_0. Assume it for S_n. Then $\bar{L}_n = L_n$ and $\bar{C}_n = C_n$. So $\bar{A}_{n+1} = A_{n+1}$ and hence, $\bar{S}_{n+1} = S_{n+1}$. This finishes the proof by induction. □

We note that the x-axis is in L_0, while the y-axis is in L_2. By drawing circles centered at the origin, we see that if the real number x is in S_n, then $ix \in S_{n+1}$. Similarly, if the purely imaginary number iy is in S_n, then $y \in S_{n+1}$. Also, using intersections between the x-axis and suitable circles, we see that if the real numbers x and y are in S_n, then $x \pm y \in S_{n+1}$. It will be convenient now to forget the indices and refer to the whole set S, even though it is an interesting exercise to keep track of the day of creation for any give number, line, or circle. By drawing a circle centered at the origin, we see that If r is the distance between two points in S, then $r \in S$.

Using three suitable circles, we can construct the vertical line $x = a$ going through any $a \in S \cap \mathbb{R}$. Similarly, we can construct a horizontal line through any $iy \in S \cap i\mathbb{R}$. Combined with the lemma on complex conjugation, this gives us

Lemma 0.2. *We have $z \in S$ if and only if $Re(z), Im(z) \in S$.*

Proof. Wejhave just explained why $Re(z), Im(z) \in S$ implies $z \in S$. It remains only to explain how to extract the real and imaginary parts from z. But $Re(z)$ is the intersection point between the real axis and the line connecting z with $\bar{z}$. $Im(z)$ is the plus or minus the distance from $Re(z)$ to z, which can then by marked off on the real line with a circle having this radius. □

We now apply the addition property for real numbers to see that if $z, w \in S$, then $z \pm w \in S$. Given a real number $a \in S$, by using the points 1 and ia, it is easy to construct the line l_a of slope a going through the origin. Similarly, if $a \neq 0$, by using the points a and i, we can construct the line $l_{1/a}$ with slope $1/a$. But then, by marking off the intersection point of l_a and the vertical line through

$b \in S \cap \mathbb{R}$, we see that if $a, b \in S \cap \mathbb{R}$, then $ab \in S \cap \mathbb{R}$. Similarly, if $a \neq 0$, then $b/a \in S \cap \mathbb{R}$. Since multipication and division of complex numbers can be expressed entirely in terms of multiplication and division for the real and imaginary parts, we see that if $z, w \in S$, then $zw \in S$, while if $z \neq 0$, then $w/z \in S$. So we have proved:

Proposition 0.3. *S is a subfield of $\mathbb{C}$.*

In particular, $\mathbb{Q} \subset S$.

We wish to describe S in a manner familar to standard field theory. We start by noting the following key property of S.

Proposition 0.4. *Suppose $z \in S$. Then $\sqrt{z} \in S$.*

Clearly, the statement doesn't depend on which square root is chosen.

Proof. First we prove this for real non-negative $a \in S$. One way to do this is to recall that the parbola $y = x^2$ can be described as the locus of points whose distance to the point $(0, 1/4)$ is the same as the distance to the line $y = -1/4$. We wish to find the x-coordinate of the intersection point between this parabola and the line $y = a$. Unforuntately, we can't construct the parabola. However, we know that the distance from any point on the line $y = a$ to the line $y = -1/4$ is $a + 1/4$. So if we draw the circle of radius $a + 1/4$ with center at $(0, 1/4)$. Then the intersection points with the line $y = a$ will be $(\pm\sqrt{a}, a)$. Taking the real part gives us what we want. In general, if $z = x + iy$, then there is the formula

$$\sqrt{z} = \sqrt{\frac{r+x}{2}} + \mathrm{sign}(y)\sqrt{\frac{r-x}{2}}i, \tag{0.7}$$

where $r = \sqrt{x^2 + y^2}$. (Note that r is very easily constructed from z even without square roots). So $\sqrt{z}$ can be constructed. $\square$

Define a sequence of fields as follows.

$$F_0 = \mathbb{Q}. \tag{0.8}$$

$$F_{n+1} = F_n(\sqrt{F_n}). \tag{0.9}$$

The notation here is that if F is a subfield of $\mathbb{C}$ and $S \subset F$, then $F(\sqrt{S})$ is the smallest subsfield of $\mathbb{C}$ containing F and the square roots of elements of S. Thus, if S is countable and we enumerate its elements as $S = \{a_1, a_2, a_3, \ldots, \}$, then $F(\sqrt{S})$ is constructed as the union of a tower

$$F \subset F(\sqrt{a_1}) \subset F(\sqrt{a_1}, \sqrt{a_2}) \subset \cdots \tag{0.10}$$

Now put

$$F = \cup_{n=0}^{\infty} F_n. \tag{0.11}$$

Since $F_0 \subset S$, we see that $F \subset S$.

Proposition 0.5. *In fact, $F = S$.*

Proof. First, note by induction on n that F_n is preserved by complex conjugation. (Use the formula for the complex square root given above.) So F is preserved by complex conjugation. Next, we observe that $\sqrt{F} \subset F$, by construction.

It suffices to show $S_n \subset F$ by induction as well. This is true for S_0, so assume it for S_n. But L_n will consist of lines $ax + by = 0$ with $a, b \in F$, while C_n will consist of circles

$$(x-a)^2 + (y-b)^2 = r^2$$

with $a, b, r \in F$. Considering intersections of any of these will involve solving for x a quadratic equation ith coefficients in F. The only case that requires a moment's pause is the intersection of two distinct circles:

$$(x-a)^2 + (y-b)^2 = r^2;$$

$$(x-c)^2+(y-d)^2=s^2.$$

For them to intersection, we must have $(a,b)\neq(c,d)$. Subtracting one equation from the other will give us

$$2(c-a)x+2(d-b)y=r^2-a^2-b^2-s^2+c^2+d^2,$$

which is the equation of the line that passes through the two points. Substituting for x or y back into the equation of one of the circles shows that the solutions x,y are also in F. □

If it was't evident before, this shows that S is an algebraic extension of $\mathbb{Q}$.

For F, a little thought will reveal that any given element α is contained in a field K_n obtained as the last term in a finite tower

$$\mathbb{Q}=K_0\subset K_1\subset K_2\subset\cdots\subset K_n \tag{0.12}$$

with $K_{i+1}=K_i(\sqrt{a_i})$ for some $a_i\in K_i^*\setminus(K_i^*)^2$. Therefore, the same is true of S. In particular, we have $\mathbb{Q}(\alpha)\subset K_n$ and hence, $[\mathbb{Q}(\alpha):\mathbb{Q}]$ divides $[K_n:\mathbb{Q}]=2^n$.

Proposition 0.6. *If $\alpha\in S$, then $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^r$ for some $r\in\mathbb{N}$.*

We will see later that the converse is also true, that is, if $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^r$, then $\alpha\in S$. For now we deduce one simple consequence.

Proposition 0.7. *Given a prime number $p>2$, a necessary condition for the constructibility of the number*

$$\zeta_p:=e^{2\pi i/p}$$

is that $p=2^r+1$ for some r.

Proof. We have

$$0=\zeta_p^p-1=(\zeta_p-1)(\zeta_p^{p-1}+\zeta_p^{p-2}+\cdots+\zeta_p+1)$$

so

$$\zeta_p^{p-1}+\zeta_p^{p-2}+\cdots+\zeta_p+1=0.$$

That is, ζ_p is a root of $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$. On the other hand, $f(x)$ is irreducible. To see this, we need only show that $g(x)=f(x+1)$ is irreducible. But

$$f(x+1)=((x+1)^p-1)/x=x^{p-1}+px^{p-2}+\binom{p}{2}+\cdots+\binom{p}{2}x+p.$$

So it is irreducible by Eisenstein's criterion.

Therefore, we see that $f(x)$ is the irreducible polynomial of ζ_p. This implies that $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$. Thus, $\zeta_p\in S$ only if $p-1=2^r$. □

A little geometry will show that ζ_p is constructible if and only if the regular p-gon can be constructed with straightedge and compass. So we see that the regular 7-gon, 11-gon, and 13-gon cannot be constructed. However, $17-1=2^4$, so the regular 17-gon is a possibility. We will see later that it can in fact be constructed.