On the numbers which are constructible with straight edge and compass

Antoine Chambert-Loir

Université de Rennes 1, IRMAR (UMR 6625 du CNRS), Campus de Beaulieu, 35042 Rennes Cedex
Courriel : **antoine.chambert-loir@univ-rennes1.fr**

***Abstract.* —** The purpose of this note is to show that the well known criterion for a complex number to be constructible with straight edge and compass can be established without any use of Galois theory.

Throughout this note, we identify the field $\mathbf{C}$ of complex numbers with the real plane $\mathbf{R}^2$. For distinct points $a, b \in \mathbf{C}$, we denote by (ab) the line passing through a and b and by $\mathscr{C}(a,b)$ the circle with center a passing through b.

Let S be a subset of $\mathbf{C}$ containing 0 and 1. We say that a complex number z is elementarily constructible (understated, with straight edge and compass) from S if there are points a, b, a', b' in S such that one of the following assertions hold:

– the lines (ab) and $(a'b')$ are not parallel and meet in z;
– the circle $\mathscr{C}(a,b)$ and the line $(a'b')$ meet in z;
– the circles $\mathscr{C}(a,b)$ and $\mathscr{C}(a',b')$ meet in z.

We say that a complex number z is constructible (understated, with straight edge and compass) from S if there are points $z_1, \dots, z_n = z$ such that, for any integer i with $1 \leqslant i \leqslant n$, z_i is elementarily constructible from $S \cup \{z_1, \dots, z_{i-1}\}$.

We say finally that a complex number z is constructible if it is constructible from $\{0,1\}$.

The basic construction of a line parallel to a given one, and passing through a given point, together with Thales's Theorem imply easily that if z, z' are constructible numbers (from a subset S), then so are $z+z'$, $z-z'$, zz' and, if $z' \neq 0$, z/z'. Similarly, by drawing lines passing through a point and perpendicular to the coordinate axes, we see that a complex number is constructible if and only if its real and imaginary parts are constructible. The absolute value of a constructible number is constructible.

Let z be a constructible positive real number and let us draw three points B, H, C on a line, in that order, at distances $BH = 1$ and $HC = z$. Let the perpendicular to BC through H and the circle with diameter BC meet in two points, say A and A'. Then, one has $AH = \sqrt{z}$, which shows that the square root of a positive real number is constructible. Writing down the equations for the real and imaginary parts of the square roots of a complex number, it appears that the square roots of a constructible complex number are still constructible.

Writing down the equations defining the line/line, line/circle and circle/circle intersections, it appears that if a complex number z is elementarily constructible from S, then it satisfies a polynomial equation of degree $\leqslant 2$ whose coefficients lie in the field

generated by S. Conversely, the solutions of such an equation can be expressed using only one square root. Referring to standard texts on basic algebra or field theory for more details, the preceding considerations imply the following theorem.

Theorem 1. — *A complex number z is constructible if and only if there exists a sequence of subfields $\mathbf{Q} = F_0, \dots, F_n$ such that $z \in F_n$ and such that for any $i \in \{1, \dots, n\}$, F_i is a quadratic extension of F_{i-1}.*

Remark 1.1. — Let S be a subset of $\mathbf{C}$ containing $\{0, 1\}$. The set of complex numbers wich are constructible from S is the smallest subfield F of $\mathbf{C}$ containing S such that F is stable under taking square roots.

The following corollaries use basic definitions from field theory, namely that of a finite extension, as well as the multiplicativity of degrees. For these, we also refer to basic texts on algebra.

Corollary 1.2. — *If a complex number z is constructible, then it is an algebraic number and its degree is a power of 2.*

Proof. — With the notations of Theorem 1, F_n is a finite extension of $\mathbf{Q}$ of degree 2^n, in particular an algebraic extension. Since $z \in F_n$, it is an algebraic number. Moreover, $\mathbf{Q}(z)$ is a sub-extension of F_n whose degree is precisely the degree of z. By multiplicativity of degrees, the degree of z divides 2^n, hence is a power of 2. □

Corollary 1.3. — *If a complex number z is constructible, then all of its conjugates are constructible too.*

Proof. — Let z' be a conjugate of z in $\mathbf{C}$. There exists a unique field homomorphism $f_0 \colon \mathbf{Q}(z) \to \mathbf{C}$ such that $f_0(z) = z'$. We may extend it inductively to a field homomorphism $f_n \colon F_n \to \mathbf{C}$. Considering the sequence of fields $(f_n(F_i))$, we see that z' is constructible. □

Corollary 1.4. — *If a complex number z is constructible, the field generated by its conjugates is a finite extension of $\mathbf{Q}$ whose degree is a power of 2.*

Proof. — Let z be a constructible complex numbers, with conjugates $z_1, \dots, z_d$, where d is the degree of z. The field generated by the z_i is the compositum of all fields $\mathbf{Q}(z_i)$ in $\mathbf{C}$. Its degree divides the product of all the degrees $[\mathbf{Q}(z_i) : \mathbf{Q}]$. It is therefore a power of 2. □

The last corollary allows to show that the converse of Cor. 1.2 does not hold. There are polynomials $P \in \mathbf{Q}[X]$ of degree 4, irreducible over $\mathbf{Q}$, whose cubic resolvant Q is still irreducible over $\mathbf{Q}$; one may for example take $P = X^4 - X - 1$. The field F_P generated by the complex roots of P will contain the roots of Q, each of which generates an extension of degree 3 of $\mathbf{Q}$. Consequently, the degree of F_P is a multiple of 3, hence is not a power of 2.

However, it is well known that the converse to Cor. 1.4 actually holds, giving rise to a necessary and sufficient criterion for a complex number to be constructible:

Theorem 2. — *A complex number is constructible if and only if it is algebraic and the field generated by its conjugates is a finite extension of* $\mathbf{Q}$ *whose degree is a power of* 2.

The remaining part is usually proved using Galois theory. The following proof is however more elementary. It is inspired by a classical proof of the (so called) Fundamental theorem of algebra, see, *e.g.*, [**2**]. It appears as an Exercise in [**1**].

Proof. — Let z be an algebraic number, of degree d, with conjugates $z_1, \dots, z_d$. Let us assume that the field $F = \mathbf{Q}(z_1, \dots, z_d)$ is an extension of $\mathbf{Q}$ of degree a power of 2. Since this field contains $\mathbf{Q}(z_1)$, whose degree is d, this already implies that d is a power of 2. We shall now argue by induction on d.

Let $c \in \mathbf{Q}$. For $1 \leqslant i < j \leqslant d$, let us set $z_{i,j,c} = z_i + z_j + c z_i z_j$ and let Q_c be the polynomial $\prod_{i<j}(X - z_{i,j,c})$. The coefficients of Q_c are symmetric polynomial functions of the z_i, with coefficients in $\mathbf{Q}$; therefore, they are polynomial functions in the coefficients of the minimal polynomial of z_1, hence belong to $\mathbf{Q}$. Any root of Q_c generates an extension of $\mathbf{Q}$ contained in F; its degree must therefore be a power of 2. Consquently, the degrees $d_1, \dots, d_e$, of the irreducible factors $Q_{c,1}, \dots, Q_{c,e}$ of Q_c are powers of 2.

One has $d_1 + \cdots + d_e = \frac{1}{2} d(d-1)$. Necessarily, one of the degrees, say d_s divides $d/2$. The roots of $Q_{c,s}$ are of the form $z_{i,j,c}$; their degree is a power of 2 dividing $d/2$ and they generate a subfield of F, so that its degree is also a power of 2. We now apply the induction hypothesis to some $z_{i,j,c}$, so that there exist integers i, j with $1 \leqslant i < j \leqslant d$ such that $z_{i,j,c}$ is constructible.

Up to now, the rational number c was fixed, but what precedes holds for any c. Since the field of rational numbers is infinite, but there are only finitely many couples (i, j), there are two distinct rational numbers c and c', and a couple (i, j) as above, such that $z_{i,j,c}$ and $z_{i,j,c'}$ are both constructible.

Since the constructible numbers form a field, it follows that $z_i + z_j$ and $z_i z_j$ are constructible. Then, z_i and z_j, being the roots of the quadratic polynomial $(X - z_i)(X - z_j)$ with constructible coefficients, are constructible too (Theorem 1).

Since $z_1, \dots, z_d$ are conjugates of z_i, Corollary 1.3 implies that they are all constructible, as was to be shown. □

References

[1] Antoine Chambert-Loir. *A Field guide to Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[2] Pierre Samuel. *Théorie algébrique des nombres*. Méthodes. Hermann, 1971.