CONSTRUCTIBLE NUMBERS AND GALOIS THEORY

SVANTE JANSON

Abstract. We correct some errors in Grillet [2], Section V.9.

1. Introduction

The purpose of this note is to correct some errors in Grillet [2], Section V.9 (in particular Theorem 9.3 and Lemma 9.4). See also [1].

As in Grillet [2], we define a *constructible* number to be a complex number such that the corresponding point in the Euclidean plane is constructible from 0 and 1 by ruler and compass (a.k.a. straightedge and compass). Let $\mathcal{K}$ be the set of constructible numbers. Then, as shown in [2, Proposition 9.1 and Lemma 9.2], $\mathcal{K}$ is a subfield of $\mathbb{C}$, which is closed under taking square roots (i.e., if $z \in \mathcal{K}$, then $\pm\sqrt{z} \in \mathcal{K}$); moreover, $\mathcal{K}$ is the smallest such subfield of $\mathbb{C}$.

Remark. A complex number is constructible if and only if its real and imaginary parts are constructible [2, Lemma 9.2], so it suffices to study real constructible numbers. However, for the present purpose it is simpler to allow complex numbers.

2. Main result

Theorem 2.1. *The following are equivalent, for a complex algebraic number z:*

(i) *z is constructible ($z \in \mathcal{K}$).*
(ii) *There is a chain of field extensions $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$ with $z \in F_m$ and $F_i = F_{i-1}(z_i)$ with $z_i^2 \in F_{i-1}$ for every $i \le m$.*
(iii) *There is a chain of field extensions $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$ with $z \in F_m$ and $[F_i : F_{i-1}] \le 2$ for every $i \le m$.*
(iv) *There is a chain of field extensions $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_m$ with $z \in F_m$ and $[F_i : F_{i-1}] = 2$ for every $i \le m$.*
(v) *$z \in L$, where L is some normal field extension of $\mathbb{Q}$ of degree 2^k for some $k \ge 0$.*
(vi) *The splitting field of the irreducible polynomial $\mathrm{Irr}(z : \mathbb{Q})$ has degree 2^k for some $k \ge 0$.*
(vii) *The Galois group $\mathrm{Gal}(f : \mathbb{Q})$ of the irreducible polynomial $f := \mathrm{Irr}(z : \mathbb{Q})$ has degree 2^k for some $k \ge 0$.*

Date: 8 December, 2009; reference added 30 January 2011.

Proof. (i) $\iff$ (ii): By Grillet [2].

(ii) $\implies$ (iii): For every $i \le m$, z_i is a root of $f_i(X) = X^2 - b_i$ with $b_i := z_i^2 \in F_{i-1}$ and thus $X^2 - b_i \in F_{i-1}[X]$. Either $z_i \in F_{i-1}$, and then $F_i = F_{i-1}$, or f_i is irreducible over F_{i-1}, and then $[F_i : F_{i-1}] = [F_{i-1}(z_i) : F_{i-1}] = \deg(f_i) = 2$.

(iii) $\implies$ (iv): Eliminate all repetitions in the sequence $F_0, \dots, F_m$.

(iv) $\implies$ (ii): Let $i \le m$, and take any $\alpha \in F_i \setminus F_{i-1}$. Then $F_{i-1} \subsetneq F_{i-1}(\alpha) \subseteq F_i$, and since $[F_i : F_{i-1}] = 2$, $F_{i-1}(\alpha) = F_i$. Furthermore, $\alpha^2 \in F_i$, and thus (again using $[F_i : F_{i-1}] = 2$), $\alpha^2 = a\alpha + b$ for some $a, b \in F_{i-1}$. Consequently, $\alpha = a/2 \pm \sqrt{a^2/4 + b}$. Define $z_i := \sqrt{a^2/4 + b}$. Then $\alpha = a/2 \pm z_i$, and thus $F_i = F_{i-1}(\alpha) = F_{i-1}(z_i)$, and $z_i^2 = a^2/4 + b \in F_{i-1}$.

(ii) $\implies$ (v): We prove by induction on i that every field F_i has an extension L_i such that L_i is a normal extension of $\mathbb{Q}$ whose degree $[L_i : \mathbb{Q}]$ is a power of 2. We then take $L = L_m$ and observe that $z \in F_m \subseteq L_m = L$.

To prove this claim, note first that it is trivial for $i = 0$. For the induction step, we fix $i \le m$ and assume that $F_{i-1} \subseteq L_{i-1}$ where L_{i-1} is a normal extension of $\mathbb{Q}$ of degree 2^k for some $k \ge 0$. Let $w_i := z_i^2 \in F_{i-1}$ and let $\{z_{ij}\}_{j=1}^J$ be the set of conjugates of z_i over $\mathbb{Q}$. For each j, $z_{ij} = \sigma(z_i)$ for some K-automorphism σ of the algebraic closure $\overline{\mathbb{Q}}$, and thus $z_{ij}^2 = \sigma(z_i^2) = \sigma(w_i)$ is conjugate to $w_i \in F_{i-1} \subseteq L_{i-1}$. Since L_{i-1} is a normal extension of $\mathbb{Q}$, $z_{ij}^2 \in L_{i-1}$.

Define $L_{ij} := L_{i-1}(z_{i1}, \dots, z_{ij})$, and $L_i := L_{iJ}$. Thus $L_{i0} = L_{i-1}$. For $1 \le j \le J$, we have $L_{ij} = L_{i,j-1}(z_{ij})$ and $z_{ij}^2 \in L_{i-1} \subseteq L_{i,j-1}$; hence $[L_{ij} : L_{i,j-1}] = 1$ or 2 (as in the proof of (ii) $\implies$ (iii) above). Consequently,

$$[L_i : L_{i-1}] = [L_{iJ} : L_{i0}] = \prod_{j=1}^{J} [L_{ij} : L_{i,j-1}] = 2^\ell$$

for some ℓ, and $[L_i : \mathbb{Q}] = [L_i : L_{i-1}][L_{i-1} : \mathbb{Q}] = 2^{\ell+k}$. This proves the induction step, and thus the claim.

(v) $\implies$ (vi): Let $\{z_j\}_{j=1}^J$ be the set of conjugates of z. Since L is normal, each $z_j \in L$. Define $E := \mathbb{Q}(z_1, \dots, z_J)$, the splitting field of $\operatorname{Irr}(z : \mathbb{Q})$. Then $\mathbb{Q} \subseteq E \subseteq L$, and thus $[L : E]\,[E : \mathbb{Q}] = [L : \mathbb{Q}] = 2^k$; hence $[E : \mathbb{Q}]$ is a divisor of 2^k, and thus a power of 2.

(vi) $\iff$ (vii): A splitting field is a Galois extension (in characteristic 0, at least), and the degree of a Galois extension equals the order of its Galois group.

(vii) $\implies$ (iv): Let E be the splitting field of f, and let G be the Galois group $\operatorname{Gal}(f : \mathbb{Q}) = \operatorname{Gal}(E : \mathbb{Q})$. By Sylow's first theorem (and induction), there is a chain of subgroups $G = H_0 \supset H_1 \supset \cdots \supset H_k = \{1\}$ with $|H_i| = 2^{k-i}$. The fundamental theorem of Galois theory shows that the corresponding sequence of fixed fields $F_i := \operatorname{Fix}_E(H_i)$ satisfies $F_0 \subset F_1 \subset \cdots \subset F_k$ and $[E : F_i] = |H_i| = 2^{k-i}$, which yields $[F_i : \mathbb{Q}] = 2^i$ and $[F_i : F_{i-1}] = 2$. Clearly $z \in E = F_k$. $\square$

Recall that the degree $\deg_K(\alpha)$ of an algebraic element α in an extension of a field K is the degree of its irreducible polynomial. Furthermore, $\deg_K(\alpha) = [K(\alpha) : K]$; see [2, Section V.2].

Corollary 2.2. *If z is constructible, then z is algebraic and its degree $\deg_{\mathbb{Q}}(z) = [\mathbb{Q}(z) : \mathbb{Q}]$ is a power of 2.*

However, the converse of Corollary 2.2 is *not* true, as shown by the following example.

Example 2.3. Let α be a root of an irreducible polynomial $f(X) \in \mathbb{Q}[X]$ of degree 4, such that the Galois group $\mathrm{Gal}(f : \mathbb{Q}) = S_4$ or A_4. Since $f = \mathrm{Irr}(\alpha : \mathbb{Q})$, and the order of the Galois group $\mathrm{Gal}(f : \mathbb{Q})$ is 24 or 12, and thus not a power of 2, Theorem 2.1 shows that α is not constructible. On the other hand, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4 = 2^2$.

(Such polynomials f exist. By [2, Proposition V.5.6], any polynomial of degree 4 such that its cubic resolvent is irreducible will do. $X^4 + 2X - 2$ is an explicit example.)

Remark 2.4. It is easily seen that the following properties are equivalent, for a complex number z.

(i) The degree of z over $\mathbb{Q}$ is a power of 2.
(ii) The degree $[\mathbb{Q}(z) : \mathbb{Q}]$ of $\mathbb{Q}(z)$ over $\mathbb{Q}$ is a power of 2.
(iii) z lies in an extension E of $\mathbb{Q}$ whose degree $[E : \mathbb{Q}]$ is a power of 2.

Corollary 2.2 thus says that these conditions are necessary for z to be constructible, but Example 2.3 shows that they are *not* sufficient. (Cf. Theorem 2.1(v), where the extension is assumed to be normal.)

Furthermore, the set S of $z \in \mathbb{C}$ that satisfy (i) (or (ii) or (iii)) is *not* a field. For example, let α be as in Example 2.3, and let its conjugates be $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$. Then the splitting field of f is $E := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. For every j, $\deg(\alpha_j) = \deg(\alpha) = 4$ and thus $\alpha_j \in S$. If S were a field, thus $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subseteq S$. However, E is a finite and separable extension of $\mathbb{Q}$, and thus it is a simple extension: $E = \mathbb{Q}(\beta)$ for some $\beta \in E$. Since E, being a splitting field, is a Galois extension of $\mathbb{Q}$,

$$\deg_{\mathbb{Q}}(\beta) = [\mathbb{Q}(\beta) : \beta] = [E : \mathbb{Q}] = |\,\mathrm{Gal}(E : \mathbb{Q})| = 12 \text{ or } 24,$$

which is not a power of 2; hence $\beta \notin S$, and thus $E \not\subseteq S$. This contradiction shows that S is not a field.

Remark 2.5. Example 2.3 gives an example of a field extension $E = \mathbb{Q}(\alpha) \supset \mathbb{Q}$ of degree 4 such that there is no intermediate field $\mathbb{Q}(\alpha) \supsetneq F \supsetneq \mathbb{Q}$. (If there were such an F, then $[\mathbb{Q}(\alpha) : F] = [F : \mathbb{Q}] = 2$, and α would satisfy Theorem 2.1(iv) and thus be constructible, a contradiction.)

3. Some classical applications

The results above are easily applied to the classical problems of construction by ruler and compass. (See also [2, Section V.9].)

3.1. **Squaring the circle.** In modern terms, the problem is to construct $\sqrt{\pi}$ by ruler and compass. Since π, and therefore also $\sqrt{\pi}$, is transcendental and not algebraic, this is impossible by Corollary 2.2. (The transcendence of π is not so easy to prove; see e.g. [3, Section 11.14].)

3.2. **Doubling the cube.** The problem is to construct $\sqrt[3]{2}$. This is a root of the irreducible polynomial $X^3 - 2 = 0$, so its degree is 3 and Corollary 2.2 shows that $\sqrt[3]{2}$ is not constructible.

3.3. **Trisecting the angle.** The problem is to construct $e^{\mathrm{i}\theta/3}$ from $e^{\mathrm{i}\theta}$. We choose $\theta = 60^\circ = \pi/3$; then $e^{\mathrm{i}\theta} = (1 + \mathrm{i}\sqrt{3})/2$ is constructible, so the task is equivalent to constructing $\alpha := e^{\mathrm{i}\theta/3} = e^{\mathrm{i}\pi/9} = e^{2\pi\mathrm{i}/18}$ from scratch. However, α is a primitive 18th root of unity, so its irreducible polynomial is the cyclotomic polynomial $\Phi_{18}(X)$, and thus

$$\deg_{\mathbb{Q}}(\alpha) = \deg(\Phi_{18}) = \varphi(18) = 6.$$

By Corollary 2.2, α is not constructible. Hence trisecting an angle by ruler and compass is in general not possible. (In particular, it is not possible for a 60° angle.)

3.4. **Constructing a regular n-gon.** This is equivalent to constructing the n:th root of unity $\omega_n := e^{2\pi\mathrm{i}/n}$. The irreducible polynomial of ω_n is the cyclotomic polynomial $\Phi_n(X)$, which has degree $\varphi(n)$. The splitting field of $\Phi_n(X)$ is $\mathbb{Q}(\omega_n)$ (since all other roots are powers of ω_n, and thus belong to $\mathbb{Q}(\omega_n)$). Consequently, Theorem 2.1(vi) shows that ω_n is constructible if and only if the degree $\varphi(n)$ of $\Phi_n(X)$ is a power of 2.

By simple number theory, see e.g. [3, Section 5.5], if n has the prime factorization $n = \prod_k p_k^{a_k}$, for some distinct primes p_k and exponents $a_k \geq 1$, then $\varphi(n) = \prod_k p_k^{a_k-1}(p_k - 1)$, which is a power of 2 if and only if $a_k = 1$ for every k with $p_k \neq 2$, and $p_k - 1$ is a power of 2 for every i. This implies that each p_k is either 2 or a Fermat number $F_j = 2^{2^j} + 1$ for some $j \geq 0$, see e.g. [2, Section V.9] or [3, Section 2.5]. Consequently:

Theorem 3.1. *A regular n-gon is constructible by ruler and compass if and only if n is a product of a power of 2 and distinct Fermat primes.*

The first 5 Fermat numbers $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are primes, but no others are known, and it seems likely (but unproven) that these are the only Fermat primes.

We see that, for example, a regular n-gon is constructible for $n = 3$, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, but not for $n = 7$, 9, 11, 13, 14, 18, 19.

References

[1] D. A. Cox, *Galois Theory.* Wiley-Interscience, Hoboken, NJ, 2004.
[2] P. A. Grillet, *Abstract Algebra.* 2nd ed., Springer, New York, 2007.
[3] G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers.* 4th ed., Oxford Univ. Press, Oxford, 1960.

Department of Mathematics, Uppsala University, PO Box 480, SE-751 06 Uppsala, Sweden

E-mail address: svante.janson@math.uu.se

URL: http://www.math.uu.se/∼svante/