A constructive version of Laplace's proof on the existence of complex roots

Cyril Cohen, Thierry Coquand

A constructive version of Laplace's proof on the existence of complex roots

Cyril Cohen and Thierry Coquand

December 19, 2012

Introduction

Gauss presented several proofs that the field complex numbers is algebraically closed. His second proof [3] is sometimes described as a rigorous version of a previous proof due to Laplace [6]. Both proofs indeed can be seen as arguments showing that if R is a real closed field then the field $C = R[i]$ obtained by adding a root of $i^2 + 1 = 0$ is algebraically closed. Theses two proofs are however different: the proof of Gauss for instance refers to the notion of discriminant of a polynomial, which is not used in Laplace's proof. Laplace's argument is interesting from the point of view of constructive mathematics since it relies on the existence of a splitting field of an arbitrary nonconstant polynomial in $C[X]$. The existence of such a splitting field does not raise any problem from a classical point of view, and it is interesting that Gauss criticizes Laplace's argument on the fact that he uses this existence without justification[1]. One analysis of the notion of splitting field from a constructive point of view can be found in Edwards' book [2]. But this analysis relies on a factorization algorithm, which exists only in special (but important) cases: for instance over rational numbers, or over fields of the form $\mathbb{Q}(X_1, \ldots, X_n)$ or over algebraic extensions of such fields. The classic book of van der Waerden [11] presents such algorithms, and the reference [9] refines this analysis. For a general discrete field, however, we cannot hope for a factorization algorithm [11, 8]. We apply here a different constructive analysis, inspired by some remarks of A. Joyal [5]. We use this to present a constructive version of Laplace's proof, different from the proof of Gauss. As we said, this is an application of a general method for making constructive sense of the notion of a splitting field of a nonconstant polynomial over an arbitrary field, and we present this method in the second part of this paper.

1 Laplace's argument

We recall briefly Laplace's proof of the fundamental theorem of algebra [6]. If $m > 0$ is a natural number, we let $v_2(m)$ be the greatest k such that 2^k divides m. Let R be a real closed field and $C = R[i]$ with $i^2 + 1 = 0$. Let P be a monic polynomial of degree m in $R[X]$. We show by induction on $v_2(m)$ that P has a root in C. For $v_2(m) = 0$ the polynomial P has a root in R since R is real closed. Otherwise let L be a splitting field of P over C. (We use classical logic at this point.) In L, the polynomial P has m roots $x_1, \ldots, x_m$. For each u in R we can

[1] It is enough to show that there is an extension where a given polynomial P has a root. If P is irreducible it is enough to take $C[X]/\langle P \rangle$. Classically one can always reduce to this case by considering an irreducible factor of P. Constructively however, it may not be possible to find an irreducible factor: to decide if $X^2 + 1$ is irreducible for instance is in general undecidable. This classical argument seems simple, but requires the notion of irreducible polynomial, notion that appears only explicitely in the work of Abel and Galois [2], 15 years after the second proof of Gauss [3].

form a polynomial $Q_u = \Pi_{i<j}(X - x_i - x_j - ux_ix_j)$ of degree $m' = m(m-1)/2$. Since Q_u is symmetric in $x_1, \ldots, x_m$ we have Q_u in $R[X]$. Since $v_2(m') = v_2(m) - 1$ we have by induction hypothesis an element y_u in C such that $Q_u(y_u) = 0$ and then $y_u = x_i + x_j + ux_ix_j$ for some $i < j$. We consider $l = m' + 1$ different values of u. By the pigeon-hole principle, we have two values $u_1 < u_2$ corresponding to the same pair $i < j$: we have both both $y_{u_1} = x_i + x_j + u_1x_ix_j$ and $y_{u_2} = x_i + x_j + u_2x_ix_j$. It follows that we have both $x_i + x_j$ and x_ix_j in C. Since x_i and x_j are the roots of the polynomial $T^2 - (x_i + x_j)T + x_ix_j$ of degree two with coefficients in C, it suffices to show the existence of square roots in C to conclude that x_i and x_j are in C, using the quadratic formula. This entails that P has a root in C, as desired. The existence of square roots in C follows from the existence of square roots of positive elements[2] of R, which in turn comes from the fact R is a real closed field.

The only place where classical logic appears in this argument is in the use of the splitting field L of the polynomial P. The next section will contain a constructive reading of Laplace's proof. This follows a general method of explaining constructively the existence of a splitting field, and we explain this method in the following section.

2 A constructive version of Laplace's proof

2.1 A combinatorial lemma

Lemma 2.1 *Let A be a commutative ring. Let I and J be two finite sets, and let $a_{p,q}$ be a family of elements of A such that $\Pi_{p\in I} a_{p,q} = 0$ for all q in J. For $f \in J \to I$, let $M(f)$ be the ideal generated by the elements $a_{f(q),q}$. We have $\Pi_{f\in J\to I} M(f) = 0$.*

Proof. We have to show

$$\forall F \in (J \to I) \to J.\exists q \in J.\forall p \in I.\exists f \in J \to I.F(f) = q \wedge f(F(f)) = p$$

which is equivalent to

$$\forall F \in (J \to I) \to J.\forall g \in J \to I.\exists q \in J..\exists f \in J \to I.F(f) = q \wedge f(F(f)) = g(q)$$

and for this, we can take $q = F(g)$ and $f = g$. □

As we shall see later, this combinatorial Lemma is "extracted" from Laplace's classical proof described in the previous section.

2.2 Laplace's argument, constructively

We proceed as in the classical proof, replacing the splitting field, whose constructive existence is problematic in general, by the universal decomposition algebra. Let P be a monic polynomial of degree m in $R[X]$. We show by induction on $v_2(m)$ that P has a root in C. For $v_2(m) = 0$ the polynomial P has a root in R since R is real closed. Otherwise let A be the universal decomposition algebra of P over C. The universal decomposition algebra of a polynomial

[2]Indeed, let a and b be in R, let ρ be $\sqrt{a^2 + b^2}$ and ε be the sign of b, where $\sqrt{x}$ denotes the positive square root of a positive element x of R. Now,

$$a + ib = \left(\sqrt{\frac{\rho + a}{2}} + i\varepsilon\sqrt{\frac{\rho - a}{2}}\right)^2$$

$P = X^n - a_1X^{n-1} + \ldots$ can be described as $C[x_1, \ldots, x_n] = C[X_1, \ldots, X_n]/I$ where I the ideal generated by

$$\sigma_1 - a_1,\ \sigma_2 - a_2,\ \ \ldots,\ \sigma_n - a_n$$

The crucial property that we use is that the canonical map $C \to A$ is an embedding [7][3]. (We shall recall the argument in the next section.) In the C-algebra A, the polynomial P has m roots $x_1, \ldots, x_m$. For each u in R we can form a polynomial $Q_u = \Pi_{i<j}(X - x_i - x_j - ux_ix_j)$ of degree $m' = m(m-1)/2$. The polynomial Q_u is in $R[X]$ since it is symmetric in $x_1, \ldots, x_m$. Since $v_2(m') = v_2(m) - 1$ we have by induction hypothesis an element y_u in C such that $Q_u(y_u) = 0$. For any $u_1 < u_2$ in R we can find two elements r, s in C such that

$$r + s + u_1rs = y_{u_1} \qquad r + s + u_2rs = y_{u_2}$$

We write r_{u_1,u_2}, s_{u_1,u_2} such elements.

We claim that the element in C

$$S = \Pi_{q_1<q_2} P(r_{q_1,q_2})$$

is 0. This will show that P has a root in C, which is what we want to establish. For this it is enough to show that S is nilpotent in A.

We let then I be the set of pairs i, j with $1 \leqslant i < j \leqslant m$. We take for J a finite subset of R with more elements than in I. (Notice that R being real closed field contains $\mathbb{Q}$.) We can now use Lemma 2.1. Indeed for $p = (i, j)$ in I and q in J we define

$$a_{p,q} = y_q - x_i - x_j - qx_ix_j$$

We then have $\Pi_p a_{p,q} = 0$ for all q in J. For showing that S is nilpotent it is thus enough by Lemma 2.1 to show that S is in each ideal $M(f)$ generated by the elements $a_{f(q),q}$ for each $f \in J \to I$. By the pigeon-hole principle, for each f in $J \to I$ we can find (i, j) in I and $q_1 < q_2$ in J such that both elements

$$a_{p,q_1} = y_{q_1} - x_i - x_j - q_1x_ix_j \qquad a_{p,q_2} = y_{q_2} - x_i - x_j - q_2x_ix_j$$

are in $M(f)$. We then have that

$$P(r_{q_1,q_2}) = \Pi(r_{q_1,q_2} - x_l)$$

is in $M(f)$ because already $(r_{q_1,q_2} - x_i)(r_{q_1,q_2} - x_j)$ is in $M(f)$. This follows from the fact that we have, writing $r = r_{q_1,q_2}, s = s_{q_1,q_2}$

$$(r - x_i)(r - x_j) = r^2 - (x_i + x_j)r + x_ix_j = (-x_i - x_j + r + s)r + x_ix_j - rs$$

and both $r + s - x_i - x_j$ and $x_ix_j - rs$ are in $M(f)$. Indeed we have

$$y_{q_1} = r + s + q_1rs \qquad y_{q_2} = r + s + q_2rs$$

and so

$$(q_1 - q_2)(x_ix_j - rs) = a_{p,q_2} - a_{p,q_1}$$

is in $M(f)$. This shows that $x_ix_j - rs$ is in $M(f)$. Similary

$$(q_1 - q_2)(x_i + x_j - r - s) = q_2a_{p,q_1} - q_1a_{p,q_2}$$

and so $x_i + x_j - r - s$ is also in $M(f)$.

The next section explains how we extracted this argument from Laplace's proof.

[3]The importance of the universal decomposition algebra for constructive mathematics is also stressed in the note [9].

3 Splitting field

In general let C be a commutative field and P in $C[X]$ be a nonconstant monic polynomial. We write $P = X^n - a_1X^{n-1} + a_2X^{n-2} - \ldots$. We can form the universal decomposition C-algebra A [1, 7] which is the quotient algebra $C[x_1, \ldots, x_n] = C[X_1, \ldots, X_n]/I$ where I the ideal generated by

$$\sigma_1 - a_1,\ \sigma_2 - a_2,\ \ \ldots,\ \sigma_n - a_n$$

Proposition 3.1 *The canonical map $C \to A$ is injective: if u in C becomes 0 in A then $u = 0$ in C.*

Proof. It is possible, and elementary, to show [7] that the ideal I used above in the definition of A is also generated by the so-called Cauchy modules $f_1(X_1),\ f_2(X_1, X_2), \ldots$ where

$$f_1 = P,\ f_2(X_1, X) = P - P(X_1)/X - X_1,\ f_3(X_1, X_2, X) = f_2(X_1, X) - f_2(X_1, X_2)/X - X_2,\ \ldots$$

It follows from this that A is a C-vector space of dimension $n!$ with a basis formed by the polynomials $X_1^{d_1} \ldots X_n^{d_n}$ with $d_i \leqslant n - i$. An important corollary is that if u in C becomes 0 in A then we have already $u = 0$ in C. □

In particular, if u is nilpotent in A then it is already nilpotent in C and so $u = 0$ in C, since C is a field.

This corollary is the core of the argument (as formulated in [9] it establishes that "there is some non-trivial C-algebra over which P splits"), and it might be appropriate to give another proof of it closer to the proof of Gauss, using only the fact that the polynomial $\sigma_1, \ldots, \sigma_n$ are algebraically independent in $C[X_1, \ldots, X_n]$. We show that if we have r in C which is in the ideal $\langle \sigma_1 - a_1,\ \sigma_2 - a_2,\ \ \ldots,\ \sigma_n - a_n \rangle$ then we have $r = 0$. Indeed we have a relation

$$r = p_1(\sigma_1 - a_1) + \ldots + p_n(\sigma_n - a_n)$$

with $p_1, \ldots, p_n$ in $C[X_1, \ldots, X_n]$. By averaging this relation over the symmetric group, we can assume that these polynomial are symmetric, and hence are in $C[\sigma_1, \ldots, \sigma_n]$. (Here we use the fact that R, and C, are of characteristic 0, since R is real closed.) Since $\sigma_1, \ldots, \sigma_n$ are algebraically independent it follows that $r = 0$ in C.

The C-algebra A is 0-dimensional, and to have a splitting field of P is the same as to have a prime/maximal ideal of A. Constructively, such a prime ideal may fail to exist, but we can always form the Zariski lattice $Zar(A)$ and the Boolean algebra it generates[4]. The Zariski lattice can be described as the free distributive lattice generated by symbols $D(a)$ and relations

$$D(1) = 1, \quad D(0) = 0, \qquad D(ab) = D(a) \wedge D(b), \qquad D(a + b) \leqslant D(a) \vee D(b)$$

Any element of the Zariski lattice is a finite disjunction of the form $D(a_1) \vee \ldots \vee D(a_n)$ which is also written $D(a_1, \ldots, a_n)$. For the constructible lattice we add the generators $V(a)$ and relations $D(a) \vee V(a) = 1$ and $D(a) \wedge V(a) = 0$. This is the free Boolean lattice generated by the Zariski lattice of A.

The key observation is that there is an effective realization of the Zariski lattice by taking $D(a_1, \ldots, a_n)$ to be the radical ideal generated by $a_1, \ldots, a_n$. It follows from this that we have $D(a) = 0$ iff $V(a) = 1$ iff a is nilpotent in A.

We can then make constructive sense of Laplace's reasoning by taking the equality to be valued in the constructible lattice. (This is similar to the use of Boolean valued model in set

[4]Since A is 0-dimensional, $Zar(A)$ is already a Boolean algebra, but our argument will not use this fact.

theory. This general method was suggested by A. Joyal [5].) We read $V(a)$ as the truth value that the element a is 0. The equality

$$V(ab) = V(a) \vee V(b)$$

for instance can be interpreted as the fact that A is an integral domain for this equality. Indeed it expresses that if $ab = 0$ then $a = 0$ or $b = 0$. This is also expressed by the equality $D(ab) = D(a) \wedge D(b)$ in the Zariski lattice. Laplace's reasoning shows that we have $D(S) = 0$ where $S = \Pi_{q_1<q_2} P(r_{q_1,q_2})$. Hence, we get a constructive proof that S is nilpotent in A. The argument is as follows, using the same notations as above. For any q in R we have

$$0 = \bigwedge_{i<j} D(y_q - x_i - x_j - q x_i x_j)$$

(In Laplace's argument, this corresponds to the fact that for any q in R there exists $i < j$ such that $y_q - x_i - x_j - q x_i x_j$ is 0.) Let us write $l(q, i, j)$ the element $D(y_q - x_i - x_j - q x_i x_j)$. It follows from the pigeon-hole principle, that if we consider $m' + 1$ values of q we have

$$\bigwedge_{i<j} \bigwedge_{q_1<q_2} l(q_1, i, j) \vee l(q_2, i, j) \leqslant \bigvee_{q} \bigwedge_{i<j} l(q, i, j)$$

and so

$$0 = \bigwedge_{i<j} \bigwedge_{q_1<q_2} l(q_1, i, j) \vee l(q_2, i, j) \tag{1}$$

On the other hand, for each $q_1 < q_2$, we have[5]

$$D(r_{q_1,q_2} - x_i) \wedge D(r_{q_1,q_2} - x_j) \leqslant l(q_1, i, j) \vee l(q_2, i, j)$$

and so

$$D(S) \leqslant D(y_{q_1} - x_i - x_j - q_1 x_i x_j) \vee D(y_{q_2} - x_i - x_j - q_2 x_i x_j) \tag{2}$$

It follows from (1) and (2) that we have $D(S) = 0$ and so S is nilpotent in A and so $S = 0$ in C as desired. The previous section presents exactly this proof, where we eliminate the explicit use of the Zariski lattice of A.

What we have presented gives a proof that complex algebraic numbers are algebraically closed. The arguments in [10] explain then how to extend this to prove that any non constant polynomial with complex coefficients has a complex root.

References

[1] N. Bourbaki. Algebra II, Chapters 4-7. Springer-Verlag, 1990.

[2] H. Edwards. *Essays in Constructive Mathematics.* Springer, 2005.

[3] C.F. Gauss Another new proof of the theorem that every integral rational algebraic function of one variable can be resolved into real factors of the first or second degree. 1815, translated by P. Taylor and B. Leak (1983).

[5] Notice that this expresses that the product $(r_{q_1,q_2} - x_i)(r_{q_1,q_2} - x_j)$ is in the *radical* of the ideal generated by $y_{q_1} - x_i - x_j - q_1 x_i x_j$ and $y_{q_2} - x_i - x_j - q_2 x_i x_j$. When we unfold the argument, we find that this product is actually in this ideal, and not only in its radical.

[4] C. Gilain. L'histoire du théorème fondamental de l'algèbre. Archive for History of Exact Sciences, 42, (1991), 91-136.

[5] A. Joyal. Le théorème de Chevalley-Tarski et remarques sur l'algèbre constructive. Cah. Topol. Géom. Différ. 16 (1975), 256-258.

[6] P.S. Laplace. Leçons de mathématiques données à l'École normale en 1795. in *Oeuvres* XIV, 10-177.

[7] H. Lombardi and C. Quitté. *Algèbre Commutative. Méthodes constructives.* to appear, 2011.

[8] R. Mines, F. Richman and W. Ruitenburg. A Course in Constructive Algebra. Springer-Verlag, 1987.

[9] F. Richman. Van der Waerden's construction of a splitting field. *Comm. Algebra*, 34 (2006), 2351-2356.

[10] F. Richman. The fundamental theorem of algebra: a constructive development without choices. *Pacific Jour. Math.*, 196 (2000), 213-230.

[11] B.L. van der Waerden. *Modern Algebra.* Springer, 1970