Constructing Algebraic Numbers

Georges Gonthier
Microsoft Research Cambridge
Cyril Cohen   Russell O'Connor

Algebraic Numbers

- Classically, complex roots of rational polynomials + algebraic transitivity
- Folklore: algebraics are in fact constructive
- Construction requirements:
  - algebraically closed
  - contains (algebraic over) rationals
  - has real (ordered) norm
  - conjugation automorphism

Fundamental Theorem of "Algebra"

- Famous conundrum and troll

  "$\mathbb{C}$ is algebraically closed"

- The main subject, the field of complex numbers $\mathbb{C}$, is constructed in Analysis
- Most (all?) proofs are based in Analysis
- Why is this a "Theorem of Algebra"?

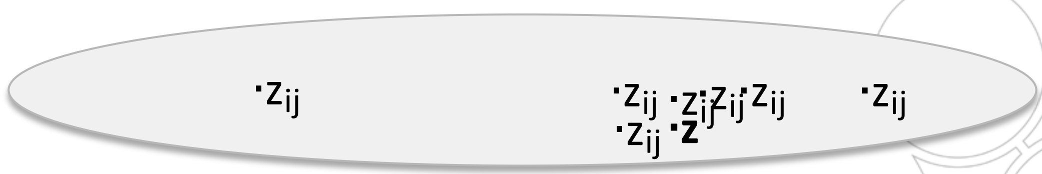
Norm, Order and Conjugates

- Order from norm (**`Num.mixin`**)
  - $a \leq b \Leftrightarrow 0 \leq b - a$
  - $0 \leq a \Leftrightarrow |a| = a$
- Norm from conjugation: $|a| = \sqrt{a\bar{a}}$
- An ordered domain has characteristic 0, so it contains a copy of , so all we need is

```
Theorem Fundamental_Theorem_of_Algebraics :
  {L : closedFieldType &
     {conj : {rmorphism L -> L} | involutive conj
                                            & ~ conj =1 id}}.
```

From Algebraics to the FTA

- Roots of a complex polynomial $P = \sum_0^n a_i X^i$ are bounded in norm by the Cauchy bound $M_P = \sum_0^n |a_i| / |a_n|$
- A complex polynomial P is a limit of algebraic polynomials Q_i.
- Roots of the Q_i lie in a compact disk of radius sup M_{Q_i} .



- Thus they have a limit point z, which is a root of P.

The Constructive Real Route

- Start with the real algebraics E
  - *discrete* subtype of the constructive reals
  - *real closed field*
- Get algebraics as E[i]
  - *explicit conjugation*
- Prove the FTA
  - algebraic, constructive proof
- Cyril Cohen’s PhD work

Carving Real Algebraics

- Start with constructive reals CR
  - “quotient” of explicit Cauchy completion
  - *not* discrete
- Use CR to interpret countable type of real algebraic specs
  - rational polynomial + sign change interval
  - bisecting root search
- Show that equality of interpretations is decidable
  - reduce to separable polynomials
  - in isolation interval compare polynomials
- Lift arithmetic and closure to RA specs
  - multivariate resultants
- Build quotient with explicit representative

The Artin Proof of the FTA

- Classical algebraic proof, uses Galois theory
- Assume R is a real closed field, p an R[i] polymomial
  - The Intermediate Value Theorem holds for R polynomials
- Take a Sylow 2-group S of Gal(C/R), where C is the splitting field of p (wlog i is in C)
  - if S < Gal(C/R) its fixed field has odd minimal polynomials
  - if Gal(C/R[i]) has a 2-group H of index 2 its fixed field has quadratic minimal polynomials solvable with R square roots.
- Getting C requires finding irreducible polynomial factors
- Cyril switched to companion matrix encoding variant.

The Countable Field Route

- First construct an algebraic closure E of $\mathbb{Q}$.
  - possible because $\mathbb{Q}$ is countable (R. O'Connor).
- Then construct (choose!) a conjugation automorphism in E.
  - E + conj is rigid so there are many choices
  - doesn't actually construct reals
  - still involves an FTA proof
  - the Primitive Element Theorem yields generator for finite extensions of $\mathbb{Q}$.
- We get algebraic closures of finite fields as a side product.

Simple Countable Extensions

- Given a K-polynomial p, construct K[z] s.t. p[z] = 0.
  - would be K[X] / (q) if we had an irreducible q | p
- If K is countable, we can still construct a decidable (q)
  - as $(q) = \bigcap(q_i)$, and $q_{i+1} = GCD(q_i, p_i)$ if $\neq 1$, else q_i
  - p_i ranges over K[X], and $p_i \in (q) \Leftrightarrow q_{i+1} \mid p_i$
- In Coq

```
pose fix d i :=
  if i isn't i1.+1 then p else
  let d1 := oapp (gcdp (d i1)) 0 (unpickle i1) in
  if size d1 > 1 then d1 else d i1.
pose I : pred {poly F} := [pred q | d (pickle q).+1 %| q].
```

Countable Field Closure

- Classically
  - (finitely) iterate simple extensions to get splitting extensions
  - (transfinitely) iterate splitting extensions for $p \in K[X]$
  - finish with algebraic transitivity
- Countably, there is no need for the double iteration, and algebraic transitivity.
  - just iterate over polynomials in the extensions as we go.

Extension Codes

```
pose minXp (p : {poly _}) := if size p > 1 then p else 'X.
have minXp_gt1 p: size (minXp _ p) > 1 by …
have ext1 p := countable_field_extension (minXp_gt1 _ p).
pose ext1to E p : {rmorphism _ -> ext1fT E p} :=
  tag (tagged (ext1 E p)).
pose Ext := {E : countFieldType & nat -> {poly E}}.
pose MkExt : Ext := Tagged _ _.
pose EtoInc (E : Ext) i := ext1to (tag E) (tagged E i).
pose incEp E i j :=
 if decode j isn't [:: i1; k] then c else
 let v := map_poly (EtoInc E i) (tagged E j) in
 if i1 == i then odflt v (unpickle k) else v.
pose fix E_ i :=
 if i is i1.+1 then MkExt _ (incEp (E_ i1) i1) else MkExt F \0.
```

- An extension is a countable field with a polynomial enumerator.
- The enumerator decodes an index into a polynomial over a specific (current *or earlier*) extension.

The Primitive Element Theorem

- For suitable $\alpha : K \to L$, $p^\alpha(x) = 0$, $q^\alpha(y) = 0$, find $z = p_z^\alpha(x,y)$ such that $x = p_x^\alpha(z)$, $y = p_y^\alpha(z)$ (in fact $z = \alpha(t)y - x$).
- Constructive proof by Russell O'Connor
- For separable q, there is r so that any t with $r(\alpha(t)) \neq 0$ works – so in characteristic 0 we can take $t = n \in \mathbb{N}$.
- Use $\mathrm{GCD}(p^\alpha(XY + x), q^\alpha(Y + y)/(Y - y))$ – and the division annihilator of $p^\alpha(X + x)$ and $q^\alpha(X + y)/X$.
- z is algebraic over K by algebraic transitivity.
- then $\mathrm{GCD}(p^\alpha(\alpha(t)X - x), q^\alpha) = X - y$, so y is in $K^\alpha[z]$.

Building an Involution

- Using the PET, construct sequences x_n, z_n in E such that
  1) $\mathbb{Q}[x_n]$ does not contain i = $\sqrt{-1}$
  2) $\mathbb{Q}[z_n] = \mathbb{Q}[x_n, i]$
  3) $\mathbb{Q}[x_{n+1}]$ contains $\mathbb{Q}[x_n]$
  4) all z in E are in some $\mathbb{Q}[z_n]$
- By 1) and 2), conjugation is uniquely defined in $\mathbb{Q}[z_n]$, so by 4) their chain union is a conjugation for E.
- The union of the $\mathbb{Q}[x_n]$ is the real algebraics, but we never construct it.
- To ensure 4) we will need the FTA and

  4') every monic polynomial p over $\mathbb{Q}[x_m]$ with $p(0) = - c^2 \neq 0$ has a root in one of the $\mathbb{Q}[x_n]$.

Avoiding $\sqrt{-1}$

- We need to strengthen 1) to

  1') $\mathbb{Q}[x_n]$ is a real subfield.
- Use index decoding on n to find a suitable polynomial p.
- Since $p(0) < 0$ and $p(M_p) > 0$, p has a positive root x_{n+1}.
- Order $\mathbb{Q}[x_{n+1}]$ by positioning x_{n+1} as the root found by dichotomy on $[0, M_p]$.
- We can use refine the position of x_{n+1} to decide whether $r(x_{n+1}) > 0$ when $d^o\, r < d^o\, p$, since r and p are coprime, so $ur + vp = 1$.

The Artin Proof, Reordered

- We don't have the real subfield!
- No matter, we induct on $|\mathrm{Gal}(\mathbb{Q}[z, z_n]/ \mathbb{Q}[z_n])|$ instead.
- In the non 2-group case, consider $-p(X)p(-X)$
- For square roots $Y^2 = a + ib$, $b \neq 0$, consider

  $$X^4 - aX^2 - b^2/4 \text{ (then } Y = X + ib/2X).$$
- For $Y^2 = a$, $a \neq 0$, solve $(Y / (1 + i))^2 = -ia/2$.

The FTA is Analysis, after all

- It is a theorem that can be stated in Algebra,
- the construction can be done in Algebra,
- but its proof always seems to require either Analysis or Choice…
- Except for Sturm sequences, perhaps?