The Fundamental Theorem of Algebra — Logically

Saeed Salehi

University of Tabriz and IPM

http://SaeedSalehi.ir/

28 October 2014

AmirKabir University of Technology (Tehran Polytechnic)

The Theorem

Every (non-trivial) Polynomial Has a Complex Root.

Coefficients can be real or complex.

Logically

a first-order scheme

$$\forall \mathbf{a_1}, \mathbf{a_2}, \cdots, \mathbf{a_{n-1}}, \mathbf{a_n} \exists x \big(x^n + \mathbf{a_n} x^{n-1} + \mathbf{a_{n-1}} x^{n-2} + \cdots + \mathbf{a_2} x + \mathbf{a_1} = 0 \big)$$

$$\mathbf{n} = 1, 2, 3, \cdots$$

More Logically

1. $\forall a_1 \exists x(x + a_1 = 0)$
2. $\forall a_1, a_2 \exists x(x^2 + a_2 x + a_1 = 0)$
3. $\forall a_1, a_2, a_3 \exists x(x^3 + a_3 x^2 + a_2 x + a_1 = 0)$
4. $\forall a_1, a_2, a_3, a_4 \exists x(x^4 + a_4 x^3 + a_3 x^2 + a_2 x + + a_1 = 0)$
5. $\forall a_1, a_2, a_3, a_4, a_5 \exists x(x^5 + a_5 x^4 + a_4 x^3 + a_3 x^2 + a_2 x + a_1 = 0)$

$\vdots$

(n) $\forall \bar{a} \exists x(x^n + \sum_{i=1}^{i=n} a_i x^{i-1} = 0)$

$\vdots$

Axiom / Axiomatic / Axiomaitzation

Merriam-Webster: www.merriam-webster.com

AXIOM:

a statement accepted as true as the basis for argument or inference

Postulate

AXIOMATIC:

based on or involving an axiom or system of axioms

AXIOMATIZATION:

the act or process of reducing to a system of axioms

Axiom / Axiomatic / Axiomaitze

Oxford: www.oxforddictionaries.com

AXIOM:

a statement or proposition which is regarded as being established, accepted, or self-evidently true *the axiom that sport builds character*

Math: a statement or proposition on which an abstractly defined structure is based

Origin: late 15th century: from French axiome or Latin axioma, from Greek axio-ma 'what is thought fitting', from axios 'worthy'

AXIOMATIC: self-evident or unquestionable

it is axiomatic that good athletes have a strong mental attitude

Math: relating to or containing axioms

AXIOMATIZE: express (a theory) as a set of axioms

the attempts that are made to axiomatize linguistics

Axiomatizing Mathematical Structures

Addition and Multiplication of the Complex Numbers $\langle\mathbb{C},+,\cdot\rangle$

Tarski: The (First-Order Logical) Theory of the Structure $\langle\mathbb{C},0,1,-,{}^{-1},+,\cdot\rangle$ is Decidable and CAN BE AXIOMATIZED AS an **Algebraically Closed Field** with zero characteristic.

- $x+(y+z)=(x+y)+z$
- $x+y=y+x$
- $x+0=x$
- $x+(-x)=0$
- $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- $x\cdot y=y\cdot x$
- $x\cdot 1=x$
- $x\neq 0\rightarrow x\cdot x^{-1}=1$
- $0\neq 1+\cdots+1=n$

- $\forall a_1,\cdots,a_n\exists x(x^n+\sum_{i=1}^{i=n}a_ix^{i-1}=0)$ $\qquad n=1,2,\cdots$

Some References

- G. KREISEL, J. L. KRIVINE, *Elements of Mathematical Logic: model theory*, North Holland 1967.
- Z. ADAMOWICZ, P. ZBIERSKI, *Logic of Mathematics: a modern course of classical logic*, Wiley 1997.
- J. BOCHNAK, M. COSTE, M.-F. ROY, *Real Algebraic Geometry*, Springer 1998.
- S. BASU, R. POLLACK, M.-F. COSTE-ROY, *Algorithms in Real Algebraic Geometry*, 2nd ed. Springer 2006.

Algebraic Geometry

$\mathbb{R}$ and $\mathbb{C}$ with $+$ and $\cdot$

Tarski & Chevalley:

The projection of a constructible set (in $\mathbb{C}$) is constructible.

Constructible:

Boolean ($^{\complement}$, $\cap$, $\cup$) Combinations of $\{\overline{x} \mid \mathsf{p}(\overline{x}) = 0\}$'s.

Tarski & Seidenberg:

The projection of a semi-algebraic set (in $\mathbb{R}$) is semialgebraic.

Semi-Algebraic:

Boolean Combinations of $\{\overline{x} \mid \mathsf{p}(\overline{x}) = 0\}$'s and $\{\overline{x} \mid \mathsf{p}(\overline{x}) > 0\}$'s.

Axiomatizing Mathematical Structures

Addition, Multiplication and Order of the Reals $\langle\mathbb{R},+,\cdot,<\rangle$

Tarski: The (First-Order Logical) Theory of the Structure $\langle\mathbb{R},0,1,-,^{-1},+,\cdot,<\rangle$ is Decidable and CAN BE AXIOMATIZED AS a **Real Closed (Ordered) Field**.

- $x+(y+z)=(x+y)+z$
- $x+y=y+x$
- $x+0=x$
- $x+(-x)=0$
- $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- $x<y<z\rightarrow x<z$
- $x<y\rightarrow x+z<y+z$
- $x<y\wedge 0<z\rightarrow x\cdot z<y\cdot z$
- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- $x\cdot y=y\cdot x$
- $x\cdot 1=x$
- $x\neq 0\rightarrow x\cdot x^{-1}=1$
- $0<1$
- $x<y\vee x=y\vee y<x$
- $x\not< x$
- $0<z\rightarrow\exists y(z=y\cdot y)$
- $\forall a_1,\cdots,a_{2n+1}\exists x(x^{2n+1}+\sum_{i=1}^{i=2n+1}a_ix^{i-1}=0)$ $n\in\mathbb{N}$

Axiomatizing Mathematical Structures

Addition and Multiplication of the Real Numbers $\langle\mathbb{R},+,\cdot\rangle$

Tarski: The (First-Order Logical) Theory of the Structure $\langle\mathbb{R},0,1,-,^{-1},+,\cdot\rangle$ is Decidable and CAN BE AXIOMATIZED BY:

- $x+(y+z)=(x+y)+z$
- $x+y=y+x$
- $x+0=x$
- $x+(-x)=0$
- $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- $x^2+y^2+z^2=0\rightarrow x=y=z=0$
- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- $x\cdot y=y\cdot x$
- $x\cdot 1=x$
- $x\neq 0\rightarrow x\cdot x^{-1}=1$
- $0\neq 1$
- $\exists y(x=y^2\vee x+y^2=0)$

- $\forall a_1,\cdots,a_{2n+1}\exists x(x^{2n+1}+\sum_{i=1}^{i=2n+1}a_ix^{i-1}=0)$ $\quad n\in\mathbb{N}$

Axiomatizing Mathematical Structures

Addition and Multiplication of Naturals, Integers and Rationals

Can We Axiomatize $\langle\mathbb{N},+,\cdot\rangle$, $\langle\mathbb{Z},+,\cdot\rangle$ or $\langle\mathbb{Q},+,\cdot\rangle$?

$$\begin{array}{ccccccccccccc}
\mathbb{N} & \subset & \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R}_{\text{Geom.Const.}} & \subset & \mathbb{R}_{\mathcal{alg}} & \subset & \mathbb{R} & \subset & \mathbb{C} \\
 & & \cap & & \cap & & \cap & & \cap & & & & \\
 & & \mathbb{Z}[i] & \subset & \mathbb{Q}[i] & \subset & \mathbb{C}_{\text{Geom.Const.}} & \subset & \mathbb{C}_{\mathcal{alg}} & & \subset & & \mathbb{C}
\end{array}$$

Any Set of Sentences Can Be Regarded As A Set of Axioms
Only When
It Is A Recursively (Computably) Enumerable Set Of Sentences!

Computably Enumerable set A: an (input-free) algorithm $\mathcal{P}$ lists all members of A; i.e., $A = \texttt{output}(\mathcal{P})$.

Computably Enumerable vs. Computably Decidable

- Computably Enumerable set A: an (input-free) algorithm $\mathcal{P}$ lists all members of A; i.e., $A = \texttt{output}(\mathcal{P})$.
- Computably Decidable set A: an algorithm $\mathcal{P}$ decides on any input x whether $x \in A$ (outputs YES) or $x \notin A$ (outputs NO).

. Post–Kleene's Theorem: A Set is Computably Decidable if and only if Both it and its Complement are Computably Enumerable.

$\therefore$ So, if the theory of a structure $\mathrm{Th}(\mathfrak{A}) = \{\psi \mid \mathfrak{A} \models \psi\}$ is computably enumerable then so is its complement:
$\mathrm{Th}(\mathfrak{A})^{\complement} = \{\theta \mid \mathfrak{A} \not\models \theta\} = \{\theta \mid \mathfrak{A} \models \neg\theta\} = \{\neg\varphi \mid \varphi \in \mathrm{Th}(\mathfrak{A})\}$, whence it is decidable. Thus

$$\mathrm{Th}(\mathfrak{A}) \text{ is decidable} \iff \mathfrak{A} \text{ is axiomatizable (in a c.e. way)}$$

First–Order Logic (SEMANTICS)

Fix a domain: a set to whose members the variables refer.
We will use the sets of numbers:

Natural ($\mathbb{N}$), Integer ($\mathbb{Z}$), Rational ($\mathbb{Q}$), Real ($\mathbb{R}$), Complex ($\mathbb{C}$).

Tarski's Definition of Truth defines satisfiability of a formula in a structure (by induction).

Examples:

- ▷ $\mathbb{N} \not\models \forall x \exists y (x + y = 0)$ but $\mathbb{Z} \models \forall x \exists y (x + y = 0)$.
- ▷ $\mathbb{Z} \not\models \forall x \exists y (x \neq 0 \rightarrow [x \cdot y = 1])$ but $\mathbb{Q} \models \forall x \exists y (x \neq 0 \rightarrow [x \cdot y = 1])$.
- ▷ $\mathbb{Q} \not\models \forall x \exists y (0 \leqslant x \rightarrow [y \cdot y = x])$ but $\mathbb{R} \models \forall x \exists y (0 \leqslant x \rightarrow [y \cdot y = x])$.
- ▷ $\mathbb{R} \not\models \forall x \exists y (y \cdot y + x = 0)$ but $\mathbb{C} \models \forall x \exists y (y \cdot y + x = 0)$.

Axiomatizability of Mathematical Structures

Addition and Multiplication $\langle\mathbb{N},+,\cdot\rangle,\langle\mathbb{Z},+,\cdot\rangle,\langle\mathbb{Q},+,\cdot\rangle$

Gödel's First Incompleteness Theorem:

$\mathrm{Th}(\mathbb{N},+,\cdot)$ is Not Computably Enumerable.

An Immediate Corollary:

$\mathrm{Th}(\mathbb{Z},+,\cdot)$ is Not Computably Enumerable.

Because $\mathbb{N}$ is definable in it: for $m\in\mathbb{Z}$ we have

$$m\in\mathbb{N}\iff\exists a,b,c,d(\in\mathbb{Z})\,(m=a^2+b^2+c^2+d^2),$$

by Lagrange's Four Square Theorem.

Neither is $\mathrm{Th}(\mathbb{Q},+,\cdot)$. Since, $\langle\mathbb{Q},+,\cdot\rangle$ can define $\mathbb{Z}$:

J. ROBINSON, *Definability and Decision Problems in Arithmetic*, JSL 14 (1949) 98–114.

B. POONEN, *Characterizing integers among rational numbers with a universal-existential formula*, American Journal of Mathematics 131 (2009) 675–682.

J. KOENIGSMANN, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, arXiv:1011.3424 [math.NT] (Nov. 2010) (Nov. 2013)

Axiomatizability of Mathematical Structures

Addition and Multiplication

$$
\begin{array}{ccccccccccc}
\mathbb{N} & \subset & \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R}_{\rm Geom.Const.} & \subset & \mathbb{R}_{\alpha\ell g} & \subset & \mathbb{R} \\
 & & \cap & & \cap & & \cap & & \cap & & \cap \\
 & & \mathbb{Z}[i] & \subset & \mathbb{Q}[i] & \subset & \mathbb{C}_{\rm Geom.Const.} & \subset & \mathbb{C}_{\alpha\ell g} & \subset & \mathbb{C}
\end{array}
$$

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}_{\rm G}$	$\mathbb{R}_{\alpha\ell g}$	$\mathbb{R}$
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	¿?	Δ_1	Δ_1

		$\mathbb{Z}[i]$	$\mathbb{Q}[i]$	$\mathbb{R}_{\rm G}[i]$	$\mathbb{R}_{\alpha\ell g}[i]$	$\mathbb{R}[i]$
$\{+,\cdot\}$		$\not\Delta_1$	$\not\Delta_1$	¿?	Δ_1	Δ_1

Axiomatizability of Mathematical Structures

Addition and Multiplication of the Complex Numbers $\langle \mathbb{C}, +, \cdot \rangle$

THEORY OF FIELDS WITH ZERO CHARACTERISTIC

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + 0 = x$
- $x + (-x) = 0$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot 1 = x$
- $x \neq 0 \rightarrow x \cdot x^{-1} = 1$
- $0 \neq 1 + \cdots + 1 = n$

+ SOMETHING ELSE ...

which should also prove

- $\forall a_1, \cdots, a_n \exists x (x^n + \sum_{i=1}^{i=n} a_i x^{i-1} = 0)$ FTA

Axiomatizing the Field of Complex Numbers

Another Way ...

$\texttt{Fields}_0 + \Psi = \mathrm{Th}(\mathbb{C}, +, \cdot)$

$\texttt{Fields}_0 + \Psi \vdash \mathrm{FTA}$

$\texttt{Fields}_0 + \mathrm{FTA} \vdash \Psi$

So,

$$\Psi \equiv_{\texttt{Fields}_0} \mathrm{FTA}$$

One Man's Axiom is Another Man's Theorem.

One Man's Theorem is Another Man's Axiom.

story of the Parallel Postulate equivalents

Axiomatizing or Theoremizing

One Man's Meat is Another Man's Poison.

http://idioms.thefreedictionary.com/

One Man's Loss is Another Man's Gain.

http://dictionary.cambridge.org/

One Man's Trash is Another Man's Treasure.

http://idioms.thefreedictionary.com/

One Man's Ceiling is Another Man's Floor.

http://vimeo.com/55169787

One Man's Magic is Another Man's Engineering.

—Robert A. Heinlein

Axiomatizing or Theoremizing

One Man's Mistake is Another Man's Opportunity.

—Steven Brust

One Man's Home is Another Man's Uranium Dump.

http://mg.co.za/

One Man's Hate is Another Man's Faith.

http://fullcomment.nationalpost.com/

One Man's Terrorist is Another Man's Freedom Fighter. ...

—Kayode Olatunbosun (Author House 2011)

One Man's Tall is Another Man's Small: ...

Health Economics 23:7 (2014) 776–791

Algebraic Geometry vs. Mathematical Logic

One Man's Theorem is Another Man's Principle.

Tarski & Chevalley:

$$\exists x\big(\bigwedge_i p_i(x,\bar{y})=0 \wedge \bigwedge_j q_j(x,\bar{y})\neq 0\big) \equiv_{\mathbb{C}}$$
$$\equiv_{\mathbb{C}} \bigvee_{l,n}\big(\bigwedge_k P_{k,l}(\bar{y})=0 \wedge \bigwedge_m Q_{m,n}(\bar{y})\neq 0\big)$$

Tarski & Seidenberg:

$$\exists x\big(\bigwedge_i p_i(x,\bar{y})=0 \wedge \bigwedge_j q_j(x,\bar{y})> 0\big) \equiv_{\mathbb{R}}$$
$$\equiv_{\mathbb{R}} \bigvee_{l,n}\big(\bigwedge_k P_{k,l}(\bar{y})=0 \wedge \bigwedge_m Q_{m,n}(\bar{y})> 0\big)$$

Axiomatizing the Field of Real Numbers

Another Way ...

So, any proof of $\texttt{Fields}_0 \vdash_{\mathbb{C}} \mathrm{FTA}$ should give away another axiomatization of $\langle \mathbb{C}, +, \cdot \rangle$. But most of the proofs are in $\mathbb{R}$.

Another Way of Axiomatizing the Real Field?

THEORY OF FORMALLY REAL FIELDS WITH SQUARE ROOTS

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + 0 = x$
- $x + (-x) = 0$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $x^2 + y^2 + z^2 = 0 \to x = y = z = 0$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot 1 = x$
- $x \neq 0 \to x \cdot x^{-1} = 1$
- $0 \neq 1$
- $\exists y (x = y^2 \vee x + y^2 = 0)$

+ SOMETHING ELSE ...

Axiomatizing the Field of Real Numbers

Another Way ...

$\texttt{Fields}_{\sqrt{+}} + \Psi = \mathrm{Th}(\mathbb{R}, +, \cdot)$ So,

$$\Psi \equiv_{\texttt{Fields}_{\sqrt{+}}} \mathrm{FTA}_{\texttt{odd}} = \Big\{\forall \bar{a} \exists x (x^{2n+1} + \sum_{i=1}^{2n+1} a_i x^{i-1} = 0)\Big\}_n$$

Suggestions:

$\mathrm{FTA}_{\mathbb{R}} = \forall \bar{a} \exists \bar{b}, \bar{c} \forall x \Big((x^{2n} + \sum_{i=1}^{2n} a_i x^{i-1}) = \prod_{j=1}^{n} (x^2 + b_j x + c_j) \Big)$

$\mathrm{IVT} = \forall P \forall u, v \exists x \Big[u < v \wedge P(u) \cdot P(v) < 0 \longrightarrow u < x < v \wedge P(x) = 0 \Big]$

Intermediate Value Theorem $\forall P = \forall \bar{a},\ P(y) = y^m + \sum_{i=1}^{m} a_i y^{i-1}$

Alternative Axiomatizations for the Field of Real Numbers

Two Beautiful Proofs

Theorem

$\texttt{Fields}_{\sqrt{+}} + \mathrm{FTA}_{\mathbb{R}} \vdash \mathrm{FTA}_{\texttt{odd}}$

Proof.

$\forall\bar{a}\exists\bar{b}\exists\bar{c}\Big[\big(x^{2n+2}+\sum_{i=1}^{2n+1}a_ix^i\big)=\prod_{j=1}^{n+1}(x^2+b_jx+c_j)\Big]$. Since, $\prod_{j=1}^{n+1}c_j=0$, for some j, $c_j=0$. Put $c_{n+1}=0$. Whence $x\cdot\big(x^{2n+1}+\sum_{i=1}^{2n+1}a_ix^{i-1}\big)=x\cdot(x+b_{n+1})\cdot\prod_{j=1}^{n}(x^2+b_jx+c_j)$. Thus $(-b_{n+1})^{2n+1}+\sum_{i=1}^{2n+1}a_i(-b_{n+1})^{i-1}=0$. □

Question

A Nice (First–Order) Proof For $\texttt{Fields}_{\sqrt{+}} + \mathrm{FTA}_{\texttt{odd}} \vdash \mathrm{FTA}_{\mathbb{R}}$*?*

Theorem

$\texttt{Fields}_{\sqrt{+}} + \mathrm{FTA}_{\mathbb{R}} \vdash \mathrm{IVT}$

Proof.

For $P(y)=\sum_{i=1}^{m} a_i y^{i-1}$ with $u<v$ and $P(u)\cdot P(v)<0$, put $Q(y)=\frac{1}{P(u)}(1+y^2)^m P(u+\frac{v-u}{1+y^2})$. Then $Q(y)=y^{2m}+R(y^2)$ with $\deg(R)<m$ and $Q(0)=\frac{P(v)}{P(u)}=\frac{P(u)P(v)}{P(u)^2}<0$. For some $\bar{b}$ and $\bar{c}$ we have $Q(y)=\prod_{j=1}^{m}(y^2+b_j y+c_j)$. Then $\prod_{j=1}^{m} c_j<0$ and so some $c_j<0$. Whence, $Q(\mathfrak{z})=0$ for $\mathfrak{z}=\frac{1}{2}(-b_j+\sqrt{b_j^2-4c_j})$ and for $\mathfrak{x}=u+\frac{v-u}{1+\mathfrak{z}^2}$ we have $u<\mathfrak{x}<v$ and $P(\mathfrak{x})=0$. □

Question

A Nice (First–Order) Proof For $\texttt{Fields}_{\sqrt{+}} + \mathrm{IVT} \vdash \mathrm{FTA}_{\mathbb{R}}$ *?*

The Fundamental Theorem of Algebra — Logically

The Fundamental Theorem of Algebra

is then really FUNDAMENTAL

For Algebra, Analysis on Polynomials, Algebraic Geometry, First–Order Logical Axiomatization of Addition and Multiplication in Real (algebraic) and (algebraic) Complex Numbers, etc.

The Fundamental Theorem of Algebra

equivalent of other axiomatizations for reals

- Order Completeness of $\mathbb{R}$
- Induction on $\mathbb{R}$
- etc.

Thank You!

Thanks to

The Participants ....For Listening...

and

The Organizers ....For Taking Care of Everything...

SAEEDSALEHI.ir