Axiomatic Mathematics: (Un—)Decidability and (In—)Completeness

Saeed Salehi

University of Tabriz and IPM

http://SaeedSalehi.ir/

Tenth International Tbilisi Summer School in Logic and Language
Tbilisi, Georgia
22–27 September 2014

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

Some High-School Axiomatizations

L. HENKIN, *The Logic of Equality*, The American Mathematical Monthly 84 (1977) 597–612.

Every equality of $\langle \mathbb{N}, +, 0\rangle$ can be derived from the axioms:

Associativity:	$x + (y + z) = (x + y) + z$
Commutativity:	$x + y = y + x$
Identity Element:	$x + 0 = x$

The same holds for $\langle \mathbb{Z}, +, 0\rangle$, $\langle \mathbb{N}^{>0}, \cdot, 1\rangle$, $\langle \mathbb{N}, \cdot, 1\rangle$, $\langle \mathbb{Z}, \cdot, 1\rangle$, ...

For example the following (true) identity/equality can be derived (EXERCISES): $x + y = y + (0 + x)$

Some High-School Axiomatizations

L. HENKIN, *The Logic of Equality*, The American Mathematical Monthly 84 (1977) 597–612.

Equalities of $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ and $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ are axiomatized by

Associativity:	$x + (y + z) = (x + y) + z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Commutativity:	$x + y = y + x$	$x \cdot y = y \cdot x$
Identity Element:	$x + 0 = x$	$x \cdot 1 = x$
Distributivity & Zero:	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	$x \cdot 0 = 0$

Can derive all the identities such as (EXERCISES):

$$(x + y)^2 = x^2 + 2xy + y^2 \qquad (x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^n y^{n-i}$$

$$(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz$$

$$(x + a) \cdot (x + b) = x^2 + (a + b)x + ab$$

Some High-School Axiomatizations

L. HENKIN, *The Logic of Equality*, The American Mathematical Monthly 84 (1977) 597–612.

In Logic we even axiomatize the very way of reasoning:

[(REF) $u = u$]

(SYM) if $u = v$ then $v = u$

(TRA) if $u = v$ and $v = w$ then $u = w$

(REP) if $u = v$ and $u' = v'$ then $u + u' = v + v'$ ($u \cdot u' = v \cdot v'$ etc.)

(SUB) if $u = v$ then $u[x \hookleftarrow t] = v[x \hookleftarrow t]$

$w[x \hookleftarrow t]$ results from w by substituting every occurrence of x with t

This actually axiomatizes the logic of equality.

Algebraic Axiomatizing "The Laws of Thought"

Language: $\bot, \top$ $\neg$ $\wedge, \vee$ $\equiv$

Idempotence:	$p \wedge p \equiv p$	$p \vee p \equiv p$
Commutativity:	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associativity:	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	$p \vee (q \vee r) \equiv (p \vee q) \vee r$
Distributivity:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
Distributivity:	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
Tautology:	$p \wedge \top \equiv p$	$p \vee \top \equiv \top$
Contradiction:	$p \wedge \bot \equiv \bot$	$p \vee \bot \equiv p$
Negation:	$p \wedge (\neg p) \equiv \bot$	$p \vee (\neg p) \equiv \top$
Negation:		$\neg(\neg p) \equiv p$
DeMorgan:	$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$	$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$

Algebraic Axiomatizing "The Laws of Thought"

All the other laws can be proved by the above axioms; such as:

Absorption:

$$p \wedge (p \vee q) \equiv_C (p \vee \bot) \wedge (p \vee q) \equiv_D p \vee (\bot \wedge q) \equiv_C p \vee \bot \equiv_C p$$

Absorption:

$$p \vee (p \wedge q) \equiv_T (p \wedge \top) \vee (p \wedge q) \equiv_D p \wedge (\top \vee q) \equiv_T p \wedge \top \equiv_T p$$

(EXERCISES):

$$\neg\big((p \vee \neg q) \wedge (\neg p \vee q)\big) \quad \equiv \quad (p \vee q) \wedge (\neg p \vee \neg q)$$

$$\Big(p \wedge \neg\big[(q \wedge \neg r) \vee (\neg q \wedge r)\big]\Big) \bigvee \Big(\neg p \wedge \big[(q \wedge \neg r) \vee (\neg q \wedge r)\big]\Big) \quad \equiv$$

$$\equiv \quad \Big(\big[(p \wedge \neg q) \vee (\neg p \wedge q)\big] \wedge \neg r\Big) \bigvee \Big(\neg\big[(p \wedge \neg q) \vee (\neg p \wedge q)\big] \wedge r\Big)$$

Propositional Logic (LAWS)

$$\alpha \to \alpha$$

$(\alpha \wedge \beta) \to \alpha$ $\qquad$ $\alpha \to (\alpha \vee \beta)$

$(\alpha \wedge \beta) \to \beta$ $\qquad$ $\beta \to (\alpha \vee \beta)$

$(\alpha \to \beta) \to (\neg\alpha \vee \beta)$ $\qquad$ $(\neg\alpha \vee \beta) \to (\alpha \to \beta)$

$(*)\ \alpha \to (\beta \to \alpha)$ $\qquad$ $(\neg\beta) \to (\beta \to \alpha)$

$$(*)\ [\alpha \to (\beta \to \gamma)] \to [(\alpha \to \beta) \to (\alpha \to \gamma)]$$

$(*)\ (\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$ $\qquad$ $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

Propositional Logic (RULES)

$$(*)\ \frac{\alpha, \quad \alpha \to \beta}{\beta} \qquad\qquad \frac{\alpha \to \beta, \quad \beta \to \gamma}{\alpha \to \gamma}$$

Axiomatizing Propositional Logic

AX_1 $\alpha \to (\beta \to \alpha)$

AX_2 $[\alpha \to (\beta \to \gamma)] \to [(\alpha \to \beta) \to (\alpha \to \gamma)]$

AX_3 $(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$

RUL $\dfrac{\alpha, \quad \alpha \to \beta}{\beta}$

Some Theorems (EXERCISES):

$\alpha \to \alpha$

$(\neg\beta) \to (\beta \to \alpha)$

$(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

$[(\alpha \to \beta) \to \alpha] \to \alpha$

Axiomatizing Predicate Logic

Gödel's Completeness Theorem (1929)

From An Axiomatization of (Logically) Valid Formulas:

- $\alpha \to (\beta \to \alpha)$
- $(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$
- $[\alpha \to (\beta \to \gamma)] \to [(\alpha \to \beta) \to (\alpha \to \gamma)]$
- $\forall x\varphi(x) \to \varphi(t)$
- $\varphi \to \forall x\varphi$ [x is not free in φ]
- $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$

With the Modus Ponens Rule:

- $\dfrac{\varphi, \quad \varphi \to \psi}{\psi}$

All the Universally Valid Formulas CAN BE GENERATED.

Axiomatizing Predicate Logic

Some Theorems (EXERCISES):

- $\forall x(\varphi \to \psi) \longleftrightarrow [\varphi \to \forall x\psi]$ [x is not free in φ]
- $[\neg\forall x\varphi(x) \to \forall x\psi(x)] \longrightarrow \forall x[\neg\varphi(x) \to \psi(x)]$
- $\neg\forall x\neg[\forall y\theta(x,y)] \longrightarrow \forall y\neg\forall x\neg\theta(x,y)$
- $\exists y\forall x\big(\varphi(y) \to \varphi(x)\big)$ http://en.wikipedia.org/wiki/Drinker_paradox
- $\exists y\forall x\big(\varphi(x) \to \varphi(y)\big)$
- $\neg\exists y\forall x\big[\theta(x,y) \longleftrightarrow \neg\theta(x,x)\big]$ (Russell's) Barber Paradox
- $\forall x\neg[\varphi \longleftrightarrow \neg\varphi]$ Liar Paradox
- $\forall x\exists y\forall z\big(\theta(x,y) \wedge [\theta(y,z) \to \theta(x,z)]\big) \longrightarrow$ $\neg\forall u\big(\varphi(u) \leftrightarrow \forall v[\theta(u,v) \to \neg\varphi(v)]\big)$ Yablo's Paradox

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 $\mathbb{C} \models \forall x \exists y (y \cdot y + x = 0)$.

Axiomatizing Mathematical Structures

The Theory of Order ($<$)

Cantor: Every Countable Dense Linear Order Without Endpoints Is Isomorphic to $\langle\mathbb{Q},<\rangle$.

Thus, the theory of "dense linear orders without endpoints" fully axiomatizes the theory of $\langle\mathbb{Q},<\rangle$:

- $\forall x,y(x<y\rightarrow y\not<x)$ Anti-Symmetric
- $\forall x,y,z(x<y<z\rightarrow x<z)$ Transitive
- $\forall x,y(x<y\vee x=y\vee y<x)$ Linear
- $\forall x,y(x<y\rightarrow\exists z[x<z<y])$ Dense
- $\forall x\exists y(x<y)$ No Last Point
- $\forall x\exists y(y<x)$ No Least Point

Axiomatizing Mathematical Structures

The Theory of Order ($<$)

Also $\langle\mathbb{R},<\rangle$ is a model of this theory.
So, the theories of $\langle\mathbb{Q},<\rangle$ and $\langle\mathbb{R},<\rangle$ can be axiomatized as "dense linear order without endpoints".

Though the First-Order Theories of $\langle\mathbb{Q},<\rangle$ and $\langle\mathbb{R},<\rangle$ are equal, these structures are very different: $\langle\mathbb{R},<\rangle$ is complete (every bounded subset has a supremum) while $\langle\mathbb{Q},<\rangle$ is not.

Axiomatizing Mathematical Structures

The Theory of Order ($<$)

The Theory of Order in $\mathbb{Z}$ is Characterized as:

Linear Discrete Order Without EndPoints

in the language $\{S, <\}$ where $S(x) = x + 1$ is the successor function, definable by $<$: $S(x) = z \iff \forall y(x < y \leftrightarrow z \leqslant y)$.

- $\forall x, y(x < y \to y \not< x)$ Anti-Symmetric
- $\forall x, y, z(x < y < z \to x < z)$ Transitive
- $\forall x, y(x < y \vee x = y \vee y < x)$ Linear
- $\forall x, y(x < y \leftrightarrow S(x) < y \vee S(x) = y)$ Discrete Order
- $\forall x \exists y(x = S(y))$ Predecessor

These Completely Axiomatize the Whole Theory of $\langle \mathbb{Z}, S, < \rangle$.

Axiomatizing Mathematical Structures

The Theory of Order ($<$)

Zero (0) and Successor (S) are definable in $\langle\mathbb{N},<\rangle$:
$u=0 \iff \forall x(\neg x<0)$ and $v=S(u) \iff \forall x(x<v \leftrightarrow x\leqslant u)$

H. B. ENDERTON, *A Mathematical Introduction to Logic*, 2nd ed. Academic Press 2001.

The theory of $\langle\mathbb{N},0,S,<\rangle$ can be completely axiomatized by

- $\forall x,y(x<y\rightarrow y\not<x)$ Anti-Symmetric
- $\forall x,y,z(x<y<z\rightarrow x<z)$ Transitive
- $\forall x,y(x<y\vee x=y\vee y<x)$ Linear
- $\forall x,y(x<y\leftrightarrow S(x)<y\vee S(x)=y)$ Discrete Order
- $\forall x(x\neq 0\rightarrow \exists y[x=S(y)])$ Successor
- $\forall x(x\not<0)$ Least Point

Axiomatizing Mathematical Structures

The Theory of Addition $(+)$

The structures $\langle\mathbb{Q},+\rangle$, $\langle\mathbb{R},+\rangle$ and $\langle\mathbb{C},+\rangle$ have, *surprisingly*, the same theory: Non-Trivial Torsion-Free Divisible Abelian Groups:

- $\forall x,y,z\,\big(x+(y+z)=(x+y)+z\big)$ — Associativity
- $\forall x,y\,\big(x+y=y+x\big)$ — Commutativity
- $\forall x\,\big(x+0=x\big)$ — Additive Identity
- $\forall x\,\big(x+(-x)=0\big)$ — Additive Inverse
- $\forall x\exists y\big(\underbrace{y+\cdots+y}_{n-\text{times}}=x\big),\ \ n=2,3,\cdots$ — Divisibility
- $\forall x\,\big(\underbrace{x+\cdots+x}_{n-\text{times}}=0\longrightarrow x=0\big),\ \ n=2,3,\cdots$ — Torsion-Freeness
- $\exists x\,\big(x\neq 0\big)$ — Non-Triviality

Definability

The Theory of Addition $(+)$

Zero (0) and the minus function $(-)$ are definable in $\langle\mathbb{Q},+\rangle$, $\langle\mathbb{R},+\rangle$ and $\langle\mathbb{C},+\rangle$ (and also in $\langle\mathbb{Z},+\rangle$):

$$u=0 \iff u+u=u$$
$$u=-v \iff u+v=0 \qquad \Big(\iff (u+v)+(u+v)=u+v\Big)$$

Let us note that the above definition of 0 works also in $\langle\mathbb{N},+\rangle$.

Moreover, order $(<)$ is definable in $\langle\mathbb{N},+\rangle$ (but not in $\langle\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},+\rangle$):

$$u<v \iff \exists x(x+x\neq x \wedge x+u=v)$$

Axiomatizing Mathematical Structures

The Theory of Addition $(+)$

The Theory of $\langle \mathbb{Z}, + \rangle$ is Axiomatizable as
Non-Trivial Torsion-Free Abelian Group with Division Algorithm.
Axioms of $\langle \mathbb{Z}, 0, 1, -, + \rangle$:

- $\forall x, y, z\, \big(x + (y + z) = (x + y) + z\big)$
- $\forall x, y\, \big(x + y = y + x\big)$
- $0 \neq 1$
- $\forall x \exists y\, \big(\bigvee_{i<n} (x = n \centerdot y + i)\big)$
- $\forall x\, \big(x + 0 = x\big)$
- $\forall x\, \big(x + (-x) = 0\big)$
- $\forall x\, \big(n \centerdot x = 0 \rightarrow x = 0\big)$

$$n \centerdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{n-\text{times}}$$

G. S. BOOLOS, et. al., *Computability and Logic*, 5th ed. Cambridge University Press 2007.

C. SMORYŃSKI, *Logical Number Theory I: an introduction*, Springer 1991.

Axiomatizing Mathematical Structures

The Theory of Addition $(+)$

The Theory of $\langle\mathbb{N},+\rangle$ is Axiomatizable as Non-Trivial Discretely Ordered Abelian Monoid with Division Algorithm.

Axioms of $\langle\mathbb{N},0,1,+,<\rangle$:

- $\forall x,y,z\,\big(x+(y+z)=(x+y)+z\big)$
- $\forall x,y,z\,\big(x<y\rightarrow x+z<y+z\big)$
- $\forall x,y,z\,\big(x<y<z\rightarrow x<z\big)$
- $\forall x,y\,\big(x<y\vee x=y\vee y<x\big)$
- $\forall x,y\,\big(x<y\longleftrightarrow x+1\leqslant y\big)$
- $\forall x\exists y\,\big(\bigvee_{i<n}(x=n\centerdot y+i)\big)$

- $\forall x\,\big(x+0=x\big)$
- $\forall x,y\,\big(x+y=y+x\big)$
- $\forall x,y\,\big(x\not< x\big)$
- $\forall x\,(0\leqslant x)$
- $\forall x\,\big(n\centerdot x=0\rightarrow x=0\big)$

$n\centerdot\alpha=\underbrace{\alpha+\cdots+\alpha}_{n-\text{times}}$

Axiomatizing Mathematical Structures

The Theory of Addition and Order $(+,<)$

The structure $\langle \mathbb{Z}, 0, 1, -, +, < \rangle$ can be axiomatized as

Non-Trivial Discretely Ordered Abelian Group with Division Algorithm:

- $\forall x, y, z\, \big(x + (y + z) = (x + y) + z\big)$
- $\forall x, y\, \big(x + y = y + x\big)$
- $\forall x\, \big(x + 0 = x\big)$
- $\forall x\, \big(x + (-x) = 0\big)$
- $\forall x, y\, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z\, \big(x < y < z \rightarrow x < z\big)$
- $\forall x, y\, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y\, \big(x < y \longleftrightarrow x + 1 < y \vee x + 1 = y\big)$
- $\forall x, y, z\, \big(x < y \rightarrow x + z < y + z\big)$
- $\forall x \exists y\, \big(\bigvee_{i<n} (x = n \centerdot y + i)\big),\;\; n = 2, 3, \cdots$

Axiomatizing Mathematical Structures

The Theory of Addition and Order $(+, <)$

$\langle \mathbb{Q}, 0, -, +, < \rangle$ and $\langle \mathbb{R}, 0, -, +, < \rangle$ have, again *surprisingly*, the same theory of Non-Trivial Ordered Divisible Abelian Groups:

- $\forall x, y, z \, \big(x + (y + z) = (x + y) + z\big)$
- $\forall x, y \, \big(x + y = y + x\big)$
- $\forall x \, \big(x + 0 = x\big)$
- $\forall x \, \big(x + (-x) = 0\big)$
- $\forall x, y \, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z \, \big(x < y < z \rightarrow x < z\big)$
- $\forall x, y \, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y, z \, \big(x < y \rightarrow x + z < y + z\big)$
- $\forall x \exists y \big(n \centerdot y = x\big), \;\; n = 2, 3, \cdots$
- $\exists x \, \big(x \neq 0\big)$

So Far ...

$\{<\}$, $\{+\}$ and $\{+,<\}$

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	$\langle\mathbb{N},<\rangle$	$\langle\mathbb{Z},<\rangle$	$\langle\mathbb{Q},<\rangle$	$\langle\mathbb{R},<\rangle$	–
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{+,<\}$	$\langle\mathbb{N},+,<\rangle$	$\langle\mathbb{Z},+,<\rangle$	$\langle\mathbb{Q},+,<\rangle$	$\langle\mathbb{R},+,<\rangle$	–

Δ_1 = Axiomatizable (and so Decidable)

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–

Axiomatizing Mathematical Structures

Theory of Addition and Multiplication $(+,\cdot)$ the case of $\langle\mathbb{C},+,\cdot\rangle$

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**.

- $x+(y+z)=(x+y)+z$
- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- $x+y=y+x$
- $x\cdot y=y\cdot x$
- $x+0=x$
- $x\cdot 1=x$
- $x+(-x)=0$
- $x\neq 0\rightarrow x\cdot x^{-1}=1$
- $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- $0\neq 1$
- $\exists x\big(x^n+\mathbf{a_1}x^{n-1}+\mathbf{a_2}x^{n-2}+\cdots+\mathbf{a_{n-1}}x+\mathbf{a_n}=0\big)$

Axiomatizing Mathematical Structures

Theory of Addition and Multiplication $(+,\cdot)$ the case of $\langle\mathbb{R},+,\cdot\rangle$

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**.

- $x+(y+z)=(x+y)+z$
- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- $x+y=y+x$
- $x\cdot y=y\cdot x$
- $x+0=x$
- $x\cdot 1=x$
- $x+(-x)=0$
- $x\neq 0\rightarrow x\cdot x^{-1}=1$
- $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
- $0\neq 1$
- $x<y<z\rightarrow x<z$
- $x<y\vee x=y\vee y<x$
- $x<y\rightarrow x+z<y+z$
- $x\not< x$
- $x<y\wedge 0<z\rightarrow x\cdot z<y\cdot z$
- $0<z\rightarrow\exists y(z=y\cdot y)$
- $\exists x\big(x^{2n+1}+\mathbf{a_1}x^{2n}+\cdots+\mathbf{a_{2n}}x+\mathbf{a_{2n+1}}=0\big)$

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.

Axiomatizing Mathematical Structures

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{\cdot\}$	$\langle\mathbb{N},\cdot\rangle$	$\langle\mathbb{Z},\cdot\rangle$	$\langle\mathbb{Q},\cdot\rangle$	$\langle\mathbb{R},\cdot\rangle$	$\langle\mathbb{C},\cdot\rangle$
$\{\cdot,<\}$	$\langle\mathbb{N},\cdot,<\rangle$	$\langle\mathbb{Z},\cdot,<\rangle$	$\langle\mathbb{Q},\cdot,<\rangle$	$\langle\mathbb{R},\cdot,<\rangle$	–
$\{+,\cdot\}$	$\langle\mathbb{N},+,\cdot\rangle$	$\langle\mathbb{Z},+,\cdot\rangle$	$\langle\mathbb{Q},+,\cdot\rangle$	$\langle\mathbb{R},+,\cdot\rangle$	$\langle\mathbb{C},+,\cdot\rangle$
$\{+,\cdot,<\}$	$\langle\mathbb{N},+,\cdot,<\rangle$	$\langle\mathbb{Z},+,\cdot,<\rangle$	$\langle\mathbb{Q},+,\cdot,<\rangle$	$\langle\mathbb{R},+,\cdot,<\rangle$	–
E	$\langle\mathbb{N},\exp\rangle$	–	–	$\langle\mathbb{R},+,\cdot,e^x\rangle$	$\langle\mathbb{C},+,\cdot,e^x\rangle$

In $\langle\mathbb{N},\exp\rangle$ we have

$$u\cdot v=w \iff \forall x\Big[\exp(x,w)=\exp\big(\exp(x,u),v\big)\Big] \qquad x^w=(x^u)^v$$

$$u+v=w \iff \forall x\Big[\exp(x,w)=\exp(x,u)\cdot\exp(x,v)\Big] \qquad x^w=x^u\cdot x^v$$

Axiomatizability of Mathematical Structures

We study the Axiomatizability Problem for the Following Structures:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	$\langle\mathbb{N},<\rangle$	$\langle\mathbb{Z},<\rangle$	$\langle\mathbb{Q},<\rangle$	$\langle\mathbb{R},<\rangle$	–
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{\cdot\}$	$\langle\mathbb{N},\cdot\rangle$	$\langle\mathbb{Z},\cdot\rangle$	$\langle\mathbb{Q},\cdot\rangle$	$\langle\mathbb{R},\cdot\rangle$	$\langle\mathbb{C},\cdot\rangle$
$\{+,<\}$	$\langle\mathbb{N},+,<\rangle$	$\langle\mathbb{Z},+,<\rangle$	$\langle\mathbb{Q},+,<\rangle$	$\langle\mathbb{R},+,<\rangle$	–
$\{+,\cdot\}$	$\langle\mathbb{N},+,\cdot\rangle$	$\langle\mathbb{Z},+,\cdot\rangle$	$\langle\mathbb{Q},+,\cdot\rangle$	$\langle\mathbb{R},+,\cdot\rangle$	$\langle\mathbb{C},+,\cdot\rangle$
$\{\cdot,<\}$	$\langle\mathbb{N},\cdot,<\rangle$	$\langle\mathbb{Z},\cdot,<\rangle$	$\langle\mathbb{Q},\cdot,<\rangle$	$\langle\mathbb{R},\cdot,<\rangle$	–
$\{+,\cdot,<\}$	\	\	\	\	–
E	$\langle\mathbb{N},\exp\rangle$	–	–	$\langle\mathbb{R},+,\cdot,e^x\rangle$	$\langle\mathbb{C},+,\cdot,e^x\rangle$

Definability of $<$ By $+$ and $\cdot$

Order Is Definable By Addition And Multiplication.

Why not consider $\{+,\cdot,<\}$?
The Order Relation $<$ is Definable by $+$ and $\cdot$ as

- in $\mathbb{N}$: $a \leqslant b \iff \exists x\,(x + a = b)$.
- in $\mathbb{R}$: $a \leqslant b \iff \exists x\,(x \cdot x + a = b)$.

for $\mathbb{Z}$ Use Lagrange's Four Square Theorem; Every Natural (Positive) Number Can Be Written As A Sum Of Four Squares.

- in $\mathbb{Z}$: $a \leqslant b \iff \exists \alpha, \beta, \gamma, \delta\,(a + \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = b)$.

for $\mathbb{Q}$ Lagrange's Theorem Holds Too: $0 \leqslant r = m/n = (mn)/n^2 = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)/n^2 = (\alpha/n)^2 + (\beta/n)^2 + (\gamma/n)^2 + (\delta/n)^2$.

- in $\mathbb{Q}$: $a \leqslant b \iff \exists \alpha, \beta, \gamma, \delta\,(a + \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = b)$.

$\boxed{a < b \iff a \leqslant b \wedge a \neq b}$ $\boxed{a \leqslant b \iff a < b \vee a = b}$

The Theory of Multiplication

Mainly Missing ...

Skolem Arithmetic $\langle \mathbb{N}, \cdot \rangle$:

PATRICK CEGIELSKI, *Théorie Élémentaire de la Multiplication des Entiers Naturels*, in C. Berline, K. McAloon, J.-P. Ressayre (eds.) *Model Theory and Arithmetics*, LNM 890, Springer 1981, pp. 44–89.

$\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$?

Missing in the literature. Maybe because:

– almost the same proofs can show the decidability of $\langle \mathbb{Z}, \cdot \rangle$ (?)

– the decidability of $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$ follows from the decidability of $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ (Tarski's Theorems)

but an axiomatization for their theories $\cdots$ still missing!

– and $\langle \mathbb{Q}, \cdot \rangle$? $\cdots$ again missing!

The Theory of Multiplication and Order

- The Theory of $\langle\mathbb{R},\cdot,<\rangle$ Is Decidable by Tarski's Result (1931).

  Still No Axiomatization In the Literature $\cdots$

- The Theory of $\langle\mathbb{N},\cdot,<\rangle$ Is Equivalent to that of $\langle\mathbb{N},+,\cdot\rangle$, and The Theory of $\langle\mathbb{Z},\cdot,<\rangle$ Is Equivalent to that of $\langle\mathbb{Z},+,\cdot\rangle$: by Robinson's Result (1949) $+$ is Definable in $\langle\mathbb{N},\mathbb{Z},\cdot,<\rangle$ by Tarski's Identity:

$$x+y=z \iff \big[S(x\cdot y)=S(x)\cdot S(y)\wedge z\cdot S(z)=z\big]\bigvee \big[S(x\cdot z)\cdot S(y\cdot z)=S(z\cdot z\cdot S(x\cdot y))\wedge z\cdot S(z)\neq z\big].$$

Recall S is definable by $<$ in $\mathbb{N}$ (and in $\mathbb{Z}$)

- and $\langle\mathbb{Q},\cdot,<\rangle$? $\cdots$ still missing!

Axiomatizability of Mathematical Structures

State of the Art — so far ...

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	?	$\Delta_1^?$	$\Delta_1^?$
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	■	■	■	Δ_1	Δ_1
$\{\cdot,<\}$	■	■	?	$\Delta_1^?$	–
E	■	–	–	¿?	■

Definability

and Interpretability

- By Gödel's result $\langle \mathbb{N}, +, \cdot \rangle$ can define $\exp$.
- $\langle \mathbb{N}, +, \cdot \rangle$ can interpret $\langle \mathbb{Z}, +, \cdot \rangle$: $\mathbb{Z} = \mathbb{N} \cup \{x \mid \exists y \in \mathbb{N}(y + x = 0)\}$,
- and also $\langle \mathbb{Q}, +, \cdot \rangle$: $\mathbb{Q} = \{x \mid \exists y \in \mathbb{Z}, z \in \mathbb{N}(z \neq 0 \wedge z \cdot x = y)\}$.
- $\langle \mathbb{Z}, +, \cdot \rangle$ can define $\mathbb{N}$ (=$\{\sum_{i=1}^{4} x_i^2 \mid x_1, x_2, x_3, x_4 \in \mathbb{Z}\}$.)
- So can $\langle \mathbb{Q}, +, \cdot \rangle$ (Robinson's Theorem 1949).
- $\langle \mathbb{C}, +, \cdot, e^x \rangle$ defines $\mathbb{Z}$ (=$\{x \mid \forall y, z[y^2 + 1 = 0 \wedge e^{y \cdot z} = 1 \rightarrow e^{x \cdot y \cdot z} = 1]\}$) and also $\mathbb{N}$ and $\mathbb{Q}$.

Problem (Open)

Can $\langle \mathbb{C}, +, \cdot, e^x \rangle$ *define* $\mathbb{R}$ *?*

Axiomatizing Mathematical Structures

The Theory of Multiplication $(\cdot)$

An Axiomatization for The Multiplicative Theory of $\mathbb{C}$:
Let $\omega_k = \cos(2\pi/k) + i\sin(2\pi/k)$ be a $k-$th root of the unit;
so $1, \omega_k, (\omega_k)^2, \cdots, (\omega_k)^{k-1}$ are all the $k-$th roots of the unit.

The Structure $\langle \mathbb{C}, 0, \omega_1, \omega_2, \omega_3, \omega_4, \ldots, ^{-1}, \cdot\rangle$ Is Axiomatized By:

- $\forall x, y, z\, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x\, \big(x \neq 0 \rightarrow x \cdot x^{-1} = 1\big)$
- $\forall x\, \big(x^n = 1 \longleftrightarrow \bigvee_{i<n} x = (\omega_n)^i\big)$
- $\bigwedge_{i\neq j<n} (\omega_n)^i \neq (\omega_n)^j$
- $\forall x\, \big(x \cdot 1 = x\big)$
- $\forall x, y\, \big(x \cdot y = y \cdot x\big)$
- $\forall x\, \big(x \cdot 0 = 0 \neq 1\big)$

Axiomatizing Mathematical Structures

The Theory of Multiplication $(\cdot)$

The Real Numbers $\mathbb{R}$:

Indeed, $\langle \mathbb{R}^{>0}, 1, ^{-1}, \cdot \rangle$ is a non-trivial torsion-free divisible abelian group:

- $\forall x, y, z\, (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- $\forall x\, (x \cdot x^{-1} = 1)$
- $\forall x\, (x^n = 1 \rightarrow x = 1)$
- $\exists x\, (x \neq 1)$
- $\forall x\, (x \cdot 1 = x)$
- $\forall x, y\, (x \cdot y = y \cdot x)$
- $\forall x \exists y\, (x = y^n)$

Axiomatizing Mathematical Structures

The Theory of Multiplication $(\cdot)$

The Real Numbers $\mathbb{R}$:
The Structure $\langle \mathbb{R}, -1, 0, 1, {}^{-1}, \cdot, \mathscr{P} \rangle$ $\quad [\mathscr{P}(x) \equiv \text{“}x > 0\text{”}]$
Can Be Axiomatized By:

- $\forall x, y, z\,(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- $\forall x\,(x \neq 0 \rightarrow x \cdot x^{-1} = 1)$
- $\forall x\,(\mathscr{P}(x) \longleftrightarrow \exists y\,[y \neq 0 \wedge x = y^{2n}])$
- $\forall x\,(x^{2n} = 1 \longleftrightarrow x = 1 \vee x = -1)$
- $\forall x\,(x^{2n+1} = 1 \rightarrow x = 1)$
- $\forall x\,(x \neq 0 \rightarrow [\neg \mathscr{P}(x) \leftrightarrow \mathscr{P}(-x)])$
- $\forall x\,(x \cdot 1 = x)$
- $\forall x, y\,(x \cdot y = y \cdot x)$
- $\forall x \exists y\,(x = y^{2n+1})$
- $\forall x\,(x \cdot 0 = 0 \neq 1)$
- $\neg \mathscr{P}(0) \wedge \mathscr{P}(1) \wedge \neg \mathscr{P}(-1)$

$-x = (-1) \cdot x$

- $\forall x, y\,(\mathscr{P}(x \cdot y) \longleftrightarrow [\mathscr{P}(x) \wedge \mathscr{P}(y)] \vee [\mathscr{P}(-x) \wedge \mathscr{P}(-y)])$

Axiomatizing Mathematical Structures

The Theory of Multiplication $(\cdot)$

The Rational Numbers $\mathbb{Q}$:

The Theory of $\langle \mathbb{Q}^{>0}, 1, ^{-1}, \cdot \rangle$ Can Be Axiomatized By:

- $\forall x, y, z \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x, y \big(x \cdot y = y \cdot x\big)$
- $\forall x \big(x \cdot 1 = x\big)$
- $\forall x \big(x \cdot x^{-1} = 1\big)$
- $\forall x \big(x^n = 1 \longrightarrow x = 1\big)$
- $\forall y_1, \ldots, y_k \exists x \forall z \bigwedge_{i=1}^{k} (x^n \cdot y_i \neq z^{m_i})$ $\qquad m_1, \ldots, m_k \nmid n$

Axiomatizing Mathematical Structures

The Theory of Multiplication $(\cdot)$

The Rational Numbers $\mathbb{Q}$:

The structure $\langle \mathbb{Q}^{\geqslant 0}, 0, 1, {}^{-1}, \cdot \rangle$ can be axiomatized by axiomatizing $\langle \mathbb{Q}^{>0}, 1, {}^{-1}, \cdot \rangle$ plus $\forall x (x \cdot 0 = 0 \neq 1)$.

The structure $\langle \mathbb{Q}, 0, 1, {}^{-1}, \cdot, \mathscr{P} \rangle$ can be axiomatized by axiomatizing $\langle \mathbb{Q}^{>0}, 1, {}^{-1}, \cdot \rangle$ plus $\forall x (x \cdot 0 = 0 \neq 1)$, and

- $(-1) \cdot (-1) = 1$
- $\neg\mathscr{P}(0) \wedge \mathscr{P}(1) \wedge \neg\mathscr{P}(-1)$
- $\forall x \left(x \neq 0 \longrightarrow [\neg\mathscr{P}(x) \leftrightarrow \mathscr{P}(-x)] \right)$ $\qquad -x = (-1) \cdot x$
- $\forall x, y \left(\mathscr{P}(x \cdot y) \longleftrightarrow [\mathscr{P}(x) \wedge \mathscr{P}(y)] \vee [\mathscr{P}(-x) \wedge \mathscr{P}(-y)] \right)$

Axiomatizing Mathematical Structures

The Theory of Multiplication and Order $(\cdot, <)$

The Rational Numbers $\mathbb{Q}$:

$\langle \mathbb{Q}^{>0}, 1, ^{-1}, \cdot, < \rangle$ Can Be Axiomatized By:

- $\forall x, y, z \, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x, y \, \big(x \cdot y = y \cdot x\big)$
- $\forall x \, \big(x \cdot 1 = x \wedge x \cdot x^{-1} = 1\big)$
- $\forall x, y \, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z \, \big(x < y < z \rightarrow x < z\big)$
- $\forall x, y \, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y, z \, \big(x < y \rightarrow x \cdot z < y \cdot z\big)$
- $\forall y_1, \ldots, y_k \exists x \forall z \bigwedge_{i=1}^{k} (x^n \cdot y_i \neq z^{m_i})$ $\qquad m_1, \ldots, m_k \nmid n$
- $\forall x, y \big(x < y \rightarrow \exists z [x^n < z < y^n]\big)$ $\qquad n = 1, 2, 3, \cdots$

Axiomatizing Mathematical Structures

The Theory of Multiplication and Order $(\cdot, <)$

The Rational Numbers $\mathbb{Q}$: Axiomatizing $\langle \mathbb{Q}, -1, 0, 1, {}^{-1}, \cdot, < \rangle$:

- $\forall x, y, z\, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x\, \big(x \cdot 1 = x\big)$
- $\forall x\, \big(x \neq 0 \longrightarrow x \cdot x^{-1} = 1\big)$
- $\forall x, y\, \big(x \cdot y = y \cdot x\big)$
- $\forall x\, \big(x^{2n} = 1 \longleftrightarrow x = 1 \vee x = -1\big)$
- $\forall x\, \big(x \cdot 0 = 0 \neq 1\big)$
- $\forall x\, \big(x^{2n+1} = 1 \longrightarrow x = 1\big)$
- $-1 < 0 < 1$
- $\forall x\, \big(x \neq 0 \longrightarrow [x \not< 0 \leftrightarrow 0 < -x]\big)$

$-x = (-1) \cdot x$

- $\forall x, y\, \big(0 < x \cdot y) \longleftrightarrow [0 < x \wedge 0 < y] \vee [0 < -x \wedge 0 < -y]\big)$
- $\forall x, y\, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z\, \big(0 < z \wedge x < y \rightarrow x \cdot z < y \cdot z\big)$
- $\forall x, y\, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y, z\, \big(x < y < z \rightarrow x < z\big)$
- $\forall y_1, \ldots, y_k \exists x \forall z \bigwedge_{i=1}^{k} (x^n \cdot y_i \neq z^{m_i})$ $\qquad m_1, \ldots, m_k \nmid n$
- $\forall x, y\big(x < y \rightarrow \exists z[x^{2n+1} < z < y^{2n+1}]\big)$ $\qquad n = 1, 2, 3, \cdots$
- $\forall x, y\big(0 < x < y \rightarrow \exists z[x^{2n} < z < y^{2n}]\big)$ $\qquad n = 1, 2, 3, \cdots$

Axiomatizing Mathematical Structures

The Theory of Multiplication and Order $(\cdot, <)$

The Real Numbers $\mathbb{R}$:

$\langle \mathbb{R}^{>0}, 1, ^{-1}, \cdot, < \rangle$ is a Non-Trivial Ordered Divisible Abelian Group.

- $\forall x, y, z\, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x, y\, \big(x \cdot y = y \cdot x\big)$
- $\forall x\, \big(x \cdot 1 = x\big)$
- $\forall x\, \big(x \cdot x^{-1} = 1\big)$
- $\forall x, y\, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z\, \big(x < y < z \rightarrow x < z\big)$
- $\forall x, y\, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y, z\, \big(x < y \rightarrow x \cdot z < y \cdot z\big)$
- $\forall x \exists y \big(y^n = x\big),\ \ n = 2, 3, \cdots$
- $\exists x\, \big(x \neq 1\big)$

Axiomatizing Mathematical Structures

The Theory of Multiplication and Order $(\cdot, <)$

The Real Numbers $\mathbb{R}$: Axiomatizing $\langle \mathbb{R}, -1, 0, 1, ^{-1}, \cdot, < \rangle$:

- $\forall x, y, z \, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x \, \big(x \neq 0 \longrightarrow x \cdot x^{-1} = 1\big)$
- $\forall x \, \big(0 < x \longleftrightarrow \exists y \, [y \neq 0 \wedge x = y^{2n}]\big)$
- $\forall x \, \big(x^{2n} = 1 \longleftrightarrow x = 1 \vee x = -1\big)$
- $\forall x \, \big(x^{2n+1} = 1 \rightarrow x = 1\big)$
- $\forall x \, \big(x \neq 0 \rightarrow [x \not< 0 \leftrightarrow 0 < -x]\big)$
- $\forall x \, \big(x \cdot 1 = x\big)$
- $\forall x, y \, \big(x \cdot y = y \cdot x\big)$
- $\forall x \exists y \, \big(x = y^{2n+1}\big)$
- $\forall x \, \big(x \cdot 0 = 0 \neq 1\big)$
- $-1 < 0 < 1$

$-x = (-1) \cdot x$

- $\forall x, y \, \big(0 < x \cdot y) \longleftrightarrow [0 < x \wedge 0 < y] \vee [0 < -x \wedge 0 < -y]\big)$
- $\forall x, y \, \big(x < y \longrightarrow y \not< x\big)$
- $\forall x, y, z \, \big(x < y < z \longrightarrow x < z\big)$
- $\forall x, y \, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y, z \, \big(0 < z \wedge x < y \longrightarrow x \cdot z < y \cdot z\big)$

Axiomatizability of Mathematical Structures

State of the Art — so far ...

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	■	■	■	Δ_1	Δ_1
$\{\cdot,<\}$	■	■	Δ_1	Δ_1	–
E	■	–	–	¿?	■

Axiomatizability of Mathematical Structures

Addition and Multiplication — Separately and Together

Axiomatizability of $\langle\mathbb{N},+\rangle$ (called Presburger Arithmetic) and $\langle\mathbb{Z},+\rangle$ was proved by Presburger in 1929 ($\&$ Skolem 1930).

Axiomatizability of the Theories $\langle\mathbb{N},\cdot\rangle$ (called Skolem Arithmetic) and $\langle\mathbb{Z},\cdot\rangle$ was announced by Skolem in 1930.

So, an axiomatization was expected for $\langle\mathbb{N},+,\cdot\rangle$...

(First–Order) Induction Principle (for a predicate formula φ)

$$\texttt{Ind}_\varphi: \quad \varphi(0)\wedge\forall x[\varphi(x)\rightarrow\varphi(Sx)]\longrightarrow\forall x\varphi(x)$$

Axiomatizability of Mathematical Structures

Addition and Multiplication — Separately and Together

An Axiomatization for Presburger Arithmetic $\langle \mathbb{N}, 0, 1, + \rangle$:

- $x + 1 \neq 0$
- $x + 1 = y + 1 \rightarrow x = y$
- $x + 0 = x$
- $x + (y + 1) = (x + y) + 1$
- $\varphi(0) \wedge \forall x[\varphi(x) \rightarrow \varphi(x+1)] \longrightarrow \forall x \varphi(x)$ $\varphi \in \mathrm{Formulas}(0, 1, +)$.

So, a candid axiomatization for $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$ is

A Set of Basic Axioms on $0, 1, +, \cdot, <$ Plus
Induction Scheme for all $\varphi \in \mathrm{Formulas}(0, 1, +, \cdot, <)$.

Axiomatizability of Mathematical Structures

Addition and Multiplication $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$

Peano's Axiomatic System (Peano's Arithmetic—PA)

- $x + 1 \neq 0$
- $x + 1 = y + 1 \longrightarrow x = y$
- $x + 0 = x$
- $x + (y + 1) = (x + y) + 1$
- $x \cdot 0 = 0$
- $x \cdot (y + 1) = (x \cdot y) + x$
- $x \neq 0 \longrightarrow \exists y[x = y + 1]$
- $\varphi(0) \wedge \forall x[\varphi(x) \rightarrow \varphi(x+1)] \longrightarrow \forall x \varphi(x)$ $\varphi \in \text{Formulas}(0, 1, +, \cdot, <)$
- $x \leqslant y \iff \exists z(z + x = y)$

Axiomatizability of Mathematical Structures

Addition and Multiplication $\langle\mathbb{N},0,1,+,\cdot\rangle$

Second Candidate:
Can True Arithmetic $\mathrm{Th}(\langle\mathbb{N},0,1,+,\cdot\rangle)$
be regarded as an axiomatization for the theory of $\langle\mathbb{N},0,1,+,\cdot\rangle$?

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., $A = \mathtt{output}(\mathcal{P})$.

Axiomatizability of Mathematical Structures

Addition and Multiplication $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$

Gödel's First Incompleteness Theorem:

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

In Particular, $PA \subsetneqq \mathrm{Th}(\mathbb{N}, +, \cdot)$*!*

An Immediate Corollary:

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

Neither is $\mathrm{Th}(\mathbb{Q}, +, \cdot)$.

and for that matter

$\mathrm{Th}(\mathbb{C}, +, \cdot, e^x)$ is not computably enumerable, either.

Axiomatizability of Mathematical Structures

A Rather Complete Picture

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1
$\{\cdot,<\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1	–
E	$\cancel{\Delta}_1$	–	–	¿?	$\cancel{\Delta}_1$

Exponentiation

Tarski's Exponential Function Problem

http://en.wikipedia.org/wiki/Tarski's_exponential_function_problem

D. MARKER, *Model Theory and Exponentiation*, Notices AMS 43 (1996) 753–759.

A. MACINTYRE, A. J. WILKIE, *On the Decidability of the Real Exponential Field*, in P. Odifreddi (ed.) Kreiseliana: about and around Georg Kreisel, A. K. Peters (1996) pp. 441–467.

is equivalent to Weak Schanuel's Conjecture:

there is an effective procedure that, given $n \geqslant 1$ and exponential polynomials in n variables with integer coefficients $f_1, \cdots, f_n, g$ produces an integer $\eta \geqslant 1$ that depends on $n, f_1, \cdots, f_n, g$ and such that if $\alpha \in \mathbb{R}^n$ is a non-singular solution of the system $\bigwedge_{1 \leqslant i \leqslant n} f_i(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$ then either $g(\alpha) = 0$ or $|g(\alpha)| > \eta^{-1}$.

Problem (Open)

Can The Theory Of $\langle \mathbb{R}, +, \cdot, e^x \rangle$ Be Axiomatized? (In A Computably Enumerable Way)?

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 $\texttt{YES}$) or $x \notin A$ (outputs $\texttt{NO}$).

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

If the theory of a structure $\mathrm{Th}(\mathfrak{A})$ is computably enumerable then so is its complement: $\mathrm{Th}(\mathfrak{A})^{\complement} = \{\neg\varphi \mid \varphi \in \mathrm{Th}(\mathfrak{A})\}$, whence it is decidable. Thus

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

A High-School Axiomatization Problem — Again

Tarski's High School Algebra Problem:

http://en.wikipedia.org/wiki/Tarski's_high_school_algebra_problem

Can Every Equality of $\langle\mathbb{N}, 1, +, \cdot, \exp\rangle$ Be Derived From:

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x \cdot 1 = x$
- $x^1 = x$
- $x^{y+z} = x^y \cdot x^z$
- $x^{y \cdot z} = (x^y)^z$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $1^x = 1$
- $(x \cdot y)^z = (x^z) \cdot (y^z)$

?

J. DONER & A. TARSKI, *An Extended Arithmetic of Ordinal Numbers*, Fundamenta Mathematicæ 65 (1969) 95–127.

A High-School Axiomatization Problem — Again

sparked a lot of interest across the science community ...

- D. RICHARDSON, *Solution of the Identity Problem for Integral Exponential Functions,* Zeitschr. Math. Log. Grund. Math. 15 (1969) 333–340.
- A. MACINTYRE, *The Laws of Exponentiation,* Model Theory and Arithmetic, LNM 890 (1981) 185–197.
- A. WILKIE, *On Expatiation—A Solution to Tarski's High School Algebra Problem* (1981), Connections b. Model Theory & Algebraic & Analytic Geometry (2000) 107–129.
- C. W. HENSON & L. A. RUBEL, *Some Applications of Nevanlinna Theory to Mathematical Logic: Identities of Exponential Functions*, Trans. AMS 282 (1984) 1–32.
- R. GUREVIČ, *Equational Theory of Positive Numbers with Exponentiation,* Proc. AMS 94 (1985) 135–141.
- R. GUREVIČ, *Equational Theory of Positive Numbers with Exponentiation Is Not Finitely Axiomatizable*, Ann. Pure App. Logic 49 (1990) 1–30.
- S. N. BURRIS & S. LEE, *Small Models of the High School Identities,* J. Alg. Comput. 2 (1992) 139–178.
- S. N. BURRIS & S. LEE, *Tarski's High School Identities,* The American Mathematical Monthly 100 (1993) 231–236.

A High-School Axiomatization Problem — Again

- S. N. Burris & K. A. Yeats, *The Saga of the High School Identities,* Algebra Universalis 52 (2005) 325–342.
- R. Di Cosmo & T. Dufour, *The Equational Theory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ Is Decidable, but Not Finitely Axiomatisable*, LPAR 2004, LNAI 3452 (2005) 240–256.

So, the set of all the equalities of $\langle \mathbb{N}, 1, +, \cdot, \exp \rangle$ is decidable, whence *axiomatizable* (but we know of no nice axiomatization.)

It is proved that no finite set can axiomatize it.

The equalities of $\langle \mathbb{N}, \cdot, \exp \rangle$ is already axiomatized by

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $(x \cdot y)^z = (x^z) \cdot (y^z)$
- $x^{y \cdot z} = (x^y)^z$

Thank You!

Thanks to

The Participants ....For Listening...

and

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

SaeedSalehi.ir