Algebra

VL: Finitismus

PD Dr. Timm Lampert

Humboldt Universität Berlin

Algebraische Formeln φ

- Im Unterschied zur Arithmetik enthalten algebraische Formeln Buchstaben.
- Erweiterung der bisherigen Sprache (arithmetische Operatoren +,-,×,÷,^,√ und natürliche Zahlen) um Buchstaben. Insbesondere:
  - algebraische Gesetze, z.B.: $(a+b)+c=a+(b+c)$
  - rationale Polynome, z.B.: $x^5-6x+3=0$
- Wie sind die neuen Ausdrücke zu verstehen? Wie kann mit ihnen gerechnet werden?

A ML: Propositionale Funktionen

- Algebraische Gleichungen sind propositionale Funktionen.

⇒ Definitionsmenge für die Variablen vorausgesetzt!

⇒ Variablen sind durch Quantoren $\forall$, $\exists$ zu binden.

⇒ Algebraisches Rechnen kann auf Axiome und logische Deduktion zurückgeführt werden.

$$\exists!5x(x^5 - 6x + 3 = 0)$$
$$D : x \in \mathcal{C}$$

$$\forall x, y, z((x + y) + z = x + (y + z))$$
$$D : x, y, z \in \mathcal{C}$$

$$\exists n, x, y, z(x > 3 \wedge x^n + y^n = z^n)$$
$$D : n, x, y, z \in \mathrm{N}$$

Satz und Beweis

WWK, S. 33:

„Es gibt in der Mathematik nicht erstens einen Satz, der schon für sich allein Sinn hätte, und dann noch zweitens die Methode, um die Wahrheit oder Falschheit eines Satzes festzustellen, sondern es gibt nur die Methode, und das, was Satz genannt wird, ist nur ein abgekürzter Name für die Methode.“

PG, S. 370:

„… richte Deinen Blick dorthin, wo im Beweis noch gerechnet wird.“

$\mathbb{A}_F$: Beweisabhängige Deutung von *x*

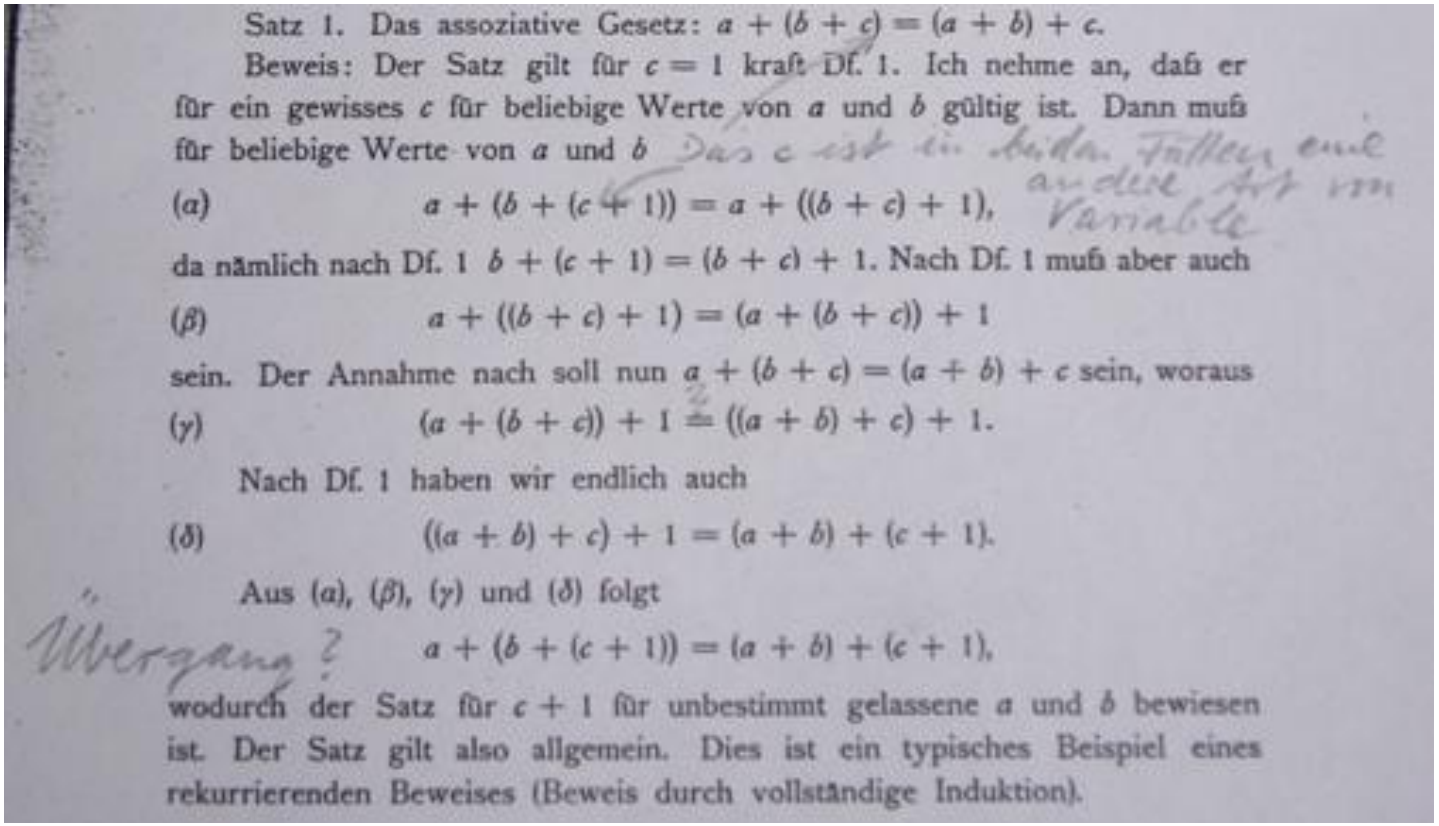
1. Algebra und Arithmetik: *x* als Variable für nat. o. rat. Zahlen
   - Algebraische Gesetze und Induktionsbeweis:
     - logisch-axiomatischer Beweis
     - rekursiver Beweis
     - struktureller Beweis
   - $\mathbb{A}$- und Ω-Kalkül
2. Algebraische Äquivalenzumformungen: *x* als Unbestimmte
   - Algebraische Beweise unter Voraussetzung von $\mathbb{A}$-Gesetzen
3. Einführung algebraischer Zahlen: *x* als Unbekannte
   - Faktorisierung (Fundamentalsatz und Kronecker-Algorithmus)
   - Darstellbarkeit durch Radikale
   - Darstellbarkeit durch kartesische Koordinaten

PA-Beweis

AE	Nr.	Formel	Regel
1	(1)	$\forall x \forall y(x+(y+1) = (x+y)+1)$	Ax. 5
2	(2)	$(\varphi(1) \wedge \forall z(\varphi(z) \rightarrow \varphi(z+1)) \rightarrow \forall z\varphi(z)$	Ax. 8: IS
3	(3)	$\forall x \forall y(x+(y+c) = (x+y)+c)$	AE
3	(4)	$\forall y(a+(y+c) = (a+y)+c)$	3∀E
3	(5)	$a+(b+c) = (a+b)+c$	4∀E
1	(6)	$\forall y((a+b)+(y+1) = ((a+b)+y)+1)$	1∀E
1	(7)	$(a+b)+(c+1) = ((a+b)+c)+1$	6∀E
1,3	(8)	$(a+b)+(c+1) = (a+(b+c))+1$	7,5=E
1	(9)	$\forall y(a+(y+1) = (a+y)+1)$	1∀E
1	(10)	$a+((b+c)+1) = (a+(b+c))+1$	1∀E
1,3	(11)	$(a+b)+(c+1) = a+((b+c)+1)$	10,8=E
1	(12)	$\forall y(b+(y+1) = (b+y)+1)$	1∀E
1	(13)	$b+(c+1) = (b+c)+1$	12∀E
1,3	(14)	$(a+b)+(c+1) = a+(b+(c+1))$	13,11=E
1,3	(15)	$a+(b+(c+1))= a+(b+(c+1))$	14,14=E
1,3	(16)	$a+(b+(c+1))= (a+b)+(c+1)$	14,15=E
1,3	(17)	$\forall y(a+(y+(c+1))= (a+y)+(c+1))$	16∀I
1,3	(18)	$\forall x \forall y(x+(y+(c+1))= (x+y)+(c+1))$	17∀I
1	(19)	$\forall x \forall y(x+(y+c) = (x+y)+c) \rightarrow \forall x \forall y(x+(y+(c+1))= (x+y)+(c+1))$	3,18K
1	(20)	$\forall z(\forall x \forall y(x+(y+z) = (x+y)+z) \rightarrow \forall x \forall y(x+(y+(z+1))= (x+y)+(z+1)))$	19∀I
1	(21)	$\forall x \forall y(x+(y+1) = (x+y)+1) \wedge \forall z(\forall x \forall y(x+(y+z) = (x+y)+z) \rightarrow \forall x \forall y(x+(y+(z+1))= (x+y)+(z+1)))$	1,20∧I
1,2	(22)	$\forall x \forall y \forall z(x + (y + z) = (x + y) + z)$	2,21MPP

Skolem

Begründung der elementaren Arithmetik durch die rekurrierende Denkweise ohne Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich, S. 5



Satz 1. Das assoziative Gesetz: $a + (b + c) = (a + b) + c$.

Beweis: Der Satz gilt für $c = 1$ kraft Df. 1. Ich nehme an, daß er für ein gewisses c für beliebige Werte von a und b gültig ist. Dann muß für beliebige Werte von a und b

$$(\alpha) \qquad a + (b + (c + 1)) = a + ((b + c) + 1),$$

da nämlich nach Df. 1 $b + (c + 1) = (b + c) + 1$. Nach Df. 1 muß aber auch

$$(\beta) \qquad a + ((b + c) + 1) = (a + (b + c)) + 1$$

sein. Der Annahme nach soll nun $a + (b + c) = (a + b) + c$ sein, woraus

$$(\gamma) \qquad (a + (b + c)) + 1 = ((a + b) + c) + 1.$$

Nach Df. 1 haben wir endlich auch

$$(\delta) \qquad ((a + b) + c) + 1 = (a + b) + (c + 1).$$

Aus (α), (β), (γ) und (δ) folgt

$$a + (b + (c + 1)) = (a + b) + (c + 1),$$

wodurch der Satz für $c + 1$ für unbestimmt gelassene a und b bewiesen ist. Der Satz gilt also allgemein. Dies ist ein typisches Beispiel eines rekurrierenden Beweises (Beweis durch vollständige Induktion).

Induktionsbeweis

ASS: $a + (b + c) = (a + b) + c$ $\quad\quad$ c = Variable

Voraussetzungen:

1. $Df._R$ +: $a+(b+1) = (a+b)+1$
2. IV: $a+(b+c) = (a+b)+c$ $\quad\quad$ c = Parameter

Beweis:

Verankerung:

Nr.	Term	Regel
(1)	a+(b+1)	
(2)	(a+b)+1	$Df._R$ +

Induktionsschritt:

Nr.	Term	Regel
(1)	a+(b+(c+1))	
(2)	a+((b+c)+1)	$Df._R$ +
(3)	(a+(b+c))+1	$Df._R$ +
(4)	((a+b)+c)+1	IV
(5)	(a+b)+(c+1)	$Df._R$ +

c und damit ASS kommen im Beweis nicht vor!

Struktureller Beweis

Nr.	Ausdruck	Regel
(1)	$S^{\mu_a}0 + (S^{\mu_b}0 + S^{\mu_c}0)$	l.S
(2)	$S^{\mu_a}0 + (S^{\mu_b}S^{\mu_c}0)$	Def.+
(3)	$S^{\mu_a}0 + (S^{\mu_x})0$	Def.^{S}, Def.^{0}
(4)	$S^{\mu_a}0 + S^{\mu_x}0$	R1
(5)	$S^{\mu_a}S^{\mu_x}0$	Def.+
(6)	$S^{\mu_a}S^{\mu_b}S^{\mu_c}0$	Def.^{S}, Def.^{0}
(7)	$(S^{\mu_a}S^{\mu_b})S^{\mu_c}0$	R1
(8)	$(S^{\mu_a}0 + S^{\mu_b}0) + S^{\mu_c}0$	Def.+, r.S.

Variablen kommen in Form von $S^{\mu}0$ vor!

Gegenüberstellung

Beweisart	Def. x	Voraussetzung	Was bewiesen wird
logisch-axiomatisch	$\Im(x) = x \in \mathrm{N}$	Mengenlehre	$PA \vdash$ $\forall x \forall y \forall z (x + (y + z) \rightarrow (x + y) + z)$
rekursiv	$x := [1, \mathrm{x}, \mathrm{x} + 1]$	rekursive Def.	$a + (b + 1) = (a + b) + 1,$ $a + (b + (c + 1)) = (a + b) + (c + 1)$
strukturell	$x := S^{\mu_z} 0$	Ω-Kalkül	$S^{\mu_a} 0 + (S^{\mu_b} 0 + S^{\mu_c} 0) =$ $(S^{\mu_a} 0 + S^{\mu_b} 0) + S^{\mu_c} 0$

A-Gesetze

ASS1: $a + (b + c) = (a + b) + c$

ASS2: $a \times (b \times c) = (a \times b) \times c$

KOM1: $a + b = b + a$

KOM2: $a \times b = b \times a$

DIS1: $a \times (b + c) = a \times b + a \times c$

DIS2: $a \div (b + c) = a \div b + a \div c$

Für $a = S^{\mu a \overline{\nu a}}0$, $b = S^{\mu b \overline{\nu b}}0$, $c = S^{\mu c \overline{\nu c}}0$ lassen sich diese Gesetze aus dem Ω-Kalkül herleiten.

Erweiterung

- Wir brauchen die algebraischen Gesetze *nicht* zum Rechnen mit rationalen Zahlen, sondern zum Rechnen mit Buchstaben.
- In der Algebra stehen die Buchstaben *nicht* für rationale Zahlen.
- Algebra: „regula della *cosa*“: Variable *r („res“) – keine spezifische Form!*
- Es bedarf algebraischer Gesetze, da die Buchstaben *nicht* notwendigerweise von der Form $S^{\mu\bar{\nu}}0$ sind.
- Die Beweise der algebraischen Gesetze beweisen nur, dass die algebraischen Gesetze aus denen für die rationalen Zahlen folgen.
- Sie beweisen nicht, dass sie darüber hinaus gelten: Diese Erweiterung ist eine Erweiterung der Regeln, die keines Beweises fähig ist.
  - Dies ermöglicht neue, rein algebraische Beweise, in denen die Buchstaben wie Konstante verwendet werden.
  - Dies wiederum führt zu neuen Zahlen (Unbestimmte $\Rightarrow$ Unbekannte).

E1: Algebraische Strukturen

Beweis von

$(a+b)^2 = a^2 + 2a \times b + b^2$

Nr.	Ausdruck	Regel
(1)	$(a+b)^2$	l.S.
(2)	$(a+b) \times (a+b)$	Def.^
(3)	$(a+b) \times a + (a+b) \times b$	DIS1
(4)	$a \times (a+b) + b \times (a+b)$	KOM2
(5)	$a \times a + a \times b + b \times a + b \times b$	DIS1
(6)	$a^2 + a \times b + b \times a + b^2$	Def.^
(7)	$a^2 + a \times b + a \times b + b^2$	KOM2
(8)	$a^2 + 2a \times b + b^2$	Def.+, r.S.

1. Buchstaben werden als *Unbestimmte* („res“, „irgendetwas“) verwendet.
2. Arithmetische Operatoren werden ineinander übersetzt, nicht beseitigt.
3. Keine Umformung in ideale Repräsentanten von Zahlen, sondern Umformung algebraischer Strukturen zum Zwecke der Identifikation formaler Eigenschaften / Beziehungen zwischen algebraischen Strukturen.

E2: Algebraische Gleichungen

Nr.	Ausdruck	Regel
(1)	$x^2 + 2x = 0$	
(2)	$x^2 + 2x + 1 = 1$	+1
(3)	$(x+1)^2 = 1$	1. BF
(4)	$\mathbf{x+1 = \sqrt{1}}$	√
(5)	$x = \{-1,1\}$ -1	-1
(6)	$x_1 = 0, x_2 = -2$	Def.-

Nr.	Ausdruck	Regel
(1)	$x^2 + 2x = 0$	
(2)	$x^2 + 2x + 1 = 1$	+1
(3)	$(x+1)^2 = 1$	1. BF
(4)	$\mathbf{\lvert x+1 \rvert = 1}$	√
(5)	$\pm(x+1) = 1$	|E
(6)	$x_1 + 1 = 1$ $-x_2 - 1 = 1$	KE KE
(7)	$x_1 = 0$ $-x_2 = 2$	-1 +1
(8)	$x_1 = 0, x_2 = -2$	*-1

Nr.	Ausdruck	Regel
(1)	$x^2 + 2x = 0$	
(2)	$x \cdot (x+2) = 0$	DIS
(3)	$x = 0,$ $x + 2 = 0$	FU
(4)	$x_1 = 0$ $x_2 = -2,$	 -2

1. Dieselbe Operation / bijektive Funktion wird rechts und links der Gleichung angewendet.
2. Keine Termumformung, sondern Umformung von Gleichungen
3. Im Gegensatz zu *x als Unbestimmte* steht *x als Unbekannte* für bestimmte Lösungen: $x \Rightarrow x_1, x_2$ (Individuierung)

Mehrdeutige Radikale

Bewersdorff, *Von der Gleichungsauflösung zur Galois-Theorie*, S. 82:

„[…] $x = \sqrt[n]{1}$ […] ein solches Symbol [lässt] algebraisch unterschiedliche Deutungen zu. Das heißt, dieses Symbol besitzt Interpretationen, die in Bezug auf die Grundrechenarten voneinander abweichende Eigenschaften aufweisen. Beispielsweise umfasst die Mehrdeutigkeit des Wurzelausdruckes $\sqrt[4]{1}$ die vier komplexen Zahlen 1, -1, i und –i, …“

E3: Quadrieren auf beiden Seiten

$$\sqrt{8-2x} = 1+\sqrt{5-x}$$

$$\left(\sqrt{8-2x}\right)^2 = \left(1+\sqrt{5-x}\right)^2$$

$$2-x = 2\sqrt{5-x}$$

$$(2-x)^2 = \left(2\sqrt{5-x}\right)^2$$

$$x^2 = 16$$

$$x_1 = 4; \quad x_2 = -4$$

$\sqrt{8-2\cdot 4} = \sqrt{8-8} = \sqrt{0} = 0$
$1+\sqrt{5-4} = 1+\sqrt{1} = 1+1 = 2$

$\sqrt{8-2\cdot(-4)} = \sqrt{8-(-8)} = \sqrt{16} = 4$

$1+\sqrt{5-(-4)} = 1+\sqrt{9} = 1+3 = 4$

$L = \{-4\}$

$\{\mathbf{0}\} <= \{\mathbf{0},2\}$

$\{-4,\mathbf{4}\} <=> \{-2,\mathbf{4}\}$

Polynome

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n, \quad n \geq 0$$

rationales Polynom: Polynom mit rationalen Koeffizienten, P$\in \mathbb{Q}$

Algebraische Zahlen: „Lösungen“ von P(x) = 0 mit P $\in \mathbb{Q}$

1. Inwieweit können Lösungen rationaler Polynome durch Radikale dargestellt werden?
2. Inwieweit kann x in Polynomen in Unbekannte überführt werden?

Lösungsformeln

$$ax^2 + bx + c = 0 \qquad (a \neq 0).$$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x^3 = bx + c$$

$$x = \sqrt[3]{\frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 - \left(\frac{b}{3}\right)^3}} + \sqrt[3]{\frac{c}{2} - \sqrt{\left(\frac{c}{2}\right)^2 - \left(\frac{b}{3}\right)^3}}$$

- Es gibt Lösungsformeln bis zum 4. Grade.

⇒ Radikale sind Lösungen, aber sind auch alle Lösungen Radikale?

$$x^5 - 6x + 3 = 0$$

Galois-Theorie

1. Bildung von *Beziehungen* zwischen Lösungen, z.B. $x_1 = -x_2$ und $x_2 = -x_1$ gelten, wenn $x_1 = \alpha_1$ und $x_2 = -\alpha_1$ (Beziehungs-Polynome).
2. Bildung der Galois-Gruppe (diejenigen der n! Permutationen der Indices, die jedes Beziehungs-Polynom in ein Beziehungs-Polynom überführen).
3. Entscheidung über Auflösbarkeit der Gleichung anhand der Galois-Gruppe (z.B. über Gruppen-Tafel).

$\Rightarrow$ Algorithmische Entscheidung über Lösbarkeit in Radikale, ohne Lösungen vorauszusetzen.

$\Rightarrow$ Entscheidung über die Möglichkeit, Lösungen in Radikalen auszudrücken, durch Reduktion auf rein *formale* Eigenschaften!

$$x^4 - 4x^3 - 4x^2 + 8x - 2 = 0\,.$$

	1	2	3	4
σ_0	1	2	3	4
σ_1	3	2	1	4
σ_2	1	4	3	2
σ_3	3	4	1	2
σ_4	2	1	4	3
σ_5	4	1	2	3
σ_6	2	3	4	1
σ_7	4	3	2	1

	1	2	3	4
erst σ_1 ...	3	2	1	4
... und dann σ_6	4	3	2	1

σ \ τ	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
σ_1	σ_1	σ_0	σ_3	σ_2	σ_6	σ_7	σ_4	σ_5
σ_2	σ_2	σ_3	σ_0	σ_1	σ_5	σ_4	σ_7	σ_6
σ_3	σ_3	σ_2	σ_1	σ_0	σ_7	σ_6	σ_5	σ_4
σ_4	σ_4	σ_5	σ_6	σ_7	σ_0	σ_1	σ_2	σ_3
σ_5	σ_5	σ_4	σ_7	σ_6	σ_2	σ_3	σ_0	σ_1
σ_6	σ_6	σ_7	σ_4	σ_5	σ_1	σ_0	σ_3	σ_2
σ_7	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1	σ_0

$$x^4 - 4x^3 - 4x^2 + 8x - 2 = 0\,.$$

$$x_{1,3} = 1 + \sqrt{2} \pm \sqrt{3 + \sqrt{2}}$$

$$x_{2,4} = 1 - \sqrt{2} \pm \sqrt{3 - \sqrt{2}}$$

Schritte zur Auflösung der Gleichung	Körper der jeweils aktuell "bekannten Größen"	Galois-Gruppe der Gleichung
$\sqrt{3-\sqrt{2}}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}}, \sqrt{3-\sqrt{2}})$	σ_0
↑ Quadratwurzel		
$\sqrt{3+\sqrt{2}}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}})$	σ_0, σ_2
↑ Quadratwurzel		
$\sqrt{2}$	$\mathbb{Q}(\sqrt{2})$	$\sigma_0, \sigma_1, \sigma_2, \sigma_3$
↑ Quadratwurzel		
Koeffizienten der Gleichung	$\mathbb{Q}$	$\sigma_0, \sigma_1, \sigma_2, \sigma_3$ $\sigma_4, \sigma_5, \sigma_6, \sigma_7$

Fundamentalsatz

- „Jedes *komplexe* Polynom *n*-ten Grades hat - Vielfachheiten mitgezählt - genau *n komplexe* Nullstellen.“

- Voraussetzungen:
  - komplexe Ebene *C*
  - Analysis (Vollständigkeitsaxiom)

- Der Fundamentalsatz sagt nur, dass es komplexe Lösungen x_1, … x_n gibt, nicht, wie man diese bestimmt.

  $\Rightarrow$Definitionsbereich gegeben, nicht konstruiert.
- Wie können Lösungen konstruiert werden, ohne *C* vorauszusetzen?

Kronecker-Duval Philosophy

„The most effective way for solving polynomial equation systems is just to interpret such a system as a tool for solving itself, by building programs which use this tool to manipulate its own roots.

Therefore, the best way of solving is to return the equations (well, perhaps after some massaging) shouting sufficiently loudly that *that* is the solution.

This really means that instead of working hard to build programs which *compute* the solutions, one should work hard to build programs which use the given equations in order to manipulate the solutions, without even computing them.

That is the Kronecker-Duval Philosophy."

R.F.Ree, *The foundational crisis, a crisis of computability?*

Körpererweiterung

Kronecker: Für jedes Polynom P mit Koeffizienten aus einem Körper K existiert eine Körpererweiterung L von K, über der P vollständig in Linearfaktoren zerfällt:

$$P(X) = c\,(X - x_1)(X - x_2)\ldots(X - x_n)$$

x_i aus L.

Beweis durch konstruktives Verfahren, über das x_i eingeführt werden.

„Der sogenannte Fundamentalsatz der Algebra […] verliert, wenigstens in seiner üblichen Form, die Gültigkeit. Er wird durch einen von Kronecker stammenden Satz ersetzt, der für ein gegebenes Polynom in K die Existenz eines Erweiterungskörpers gewährleistet, in dem das Polynom Wurzeln besitzt.“

Artin, *Galoische Theorie*, 1988, S. 19

Lokalisierbarkeit

- Der Fundamentalssatz sagt nicht nur, dass jedes rationale (komplexe) Polynom n-ten Grades – Vielfachheiten mitgezählt – genau n Nullstellen hat, sondern dass diese Nullstellen komplex sind.

$\Rightarrow$ Wie kann konstruktiv gezeigt werden, dass die x_i's stets auf die algebraische Form $a + bi$ gebracht werden können (= in Form cartesischer Koordinaten der komplexen Ebene interpretiert werden können)?

Lokalisierung durch Newton-Iteration

1. Gegeben:
   1. Polynom
   2. irreduzible Polynome
   3. Linearfaktorzerlegung der irreduziblen Polynome
2. Gesucht: n Darstellungen in algebraischer Form
3. Newton-Verfahren für irreduzible Polynome
   1. Iterative Annäherung der Nullstellen, wenn Startwert im Attraktorbereich liegt.
   2. Algorithmische Bestimmung der Startwerte

- Rechtfertigung der Lokalisierung durch *formale* Eigenschaften irreduzibler Polynome.
- Nur *rationale Approximation* der komplexen Koordinaten!

Konstruktion algebraischer Zahlen

1. Def. natürlicher Zahlen über Zähloperation.
2. Def. rationaler Zahlen über elementare arithmetische Operationen; Erweiterung jeweils durch Umkehroperationen.
3. Def.der Radikale über Umkehrung der Potenzoperation.
4. Def. algebraischer Zahlen als Lösungen rationaler Polynome.

$\Rightarrow$ Zahlen definiert über das Rechnen mit Termen und Gleichungen, nicht umgekehrt!

	eplizite Def.	Lokalisierung
Rationale Zahlen	+	+
Algebraische Zahlen	-	Ohne $\mathfrak{I}$: - mit $\mathfrak{I}$: +