

# Constructive Algebra

---

Daniel Wessel, Università di Verona, Dip.to di Informatica

Autumn School *Proof & Computation*

Fischbachau, September 16–22, 2018

[github.com/danielwessel/pc18](https://github.com/danielwessel/pc18)

# Introduction

## “Reunion of broken parts”

- Kronecker vs. Dedekind: advent of ideal theory
- Passing from potential to actual infinity
- Rise of modern algebra
- Topology enters, Grothendieck revolutionizes
- Development of point-free methods
- Call for a revised Hilbert programme in abstract algebra

# Varieties of constructive algebra

- Operative mathematics (Lorenzen)
- Bishop-style constructive algebra (Mines, Richman, Ruitenburg)
- Topos-valid algebra (Wraith, Banaschewski, Johnstone, ... )
- Dynamical algebra (Lombardi, Roy, Coste, Yengui, ... )
- Integrated development in type theory (Coquand, Persson)
- Formal topology  $\bowtie$  comm. algebra (Coquand, Schuster, ... )

*“What would have happened if topologies without points had been discovered before topologies with points, or if Grothendieck had known the theory of distributive lattices?”*

G.-C. Rota  
*Indiscrete Thoughts*

## Key instruments

*“What would have happened if topologies without points had been discovered before topologies with points, or if Grothendieck had known the theory of distributive lattices?”*

G.-C. Rota

*Indiscrete Thoughts*

Modern constructive algebra makes extensive use of **lattice theory** (sometimes in disguise).

Important example

Constructive Krull dimension (Joyal, Lombardi)

*“When we say that we have a constructive version of an abstract algebraic theorem, this means that we have a theorem the proof of which is constructive, which has a clear computational content, and from which we can recover the usual version of the abstract theorem by an immediate application of a well classified non-constructive principle.”*

T. Coquand and H. Lombardi

*Hidden constructions in abstract algebra*

- Preliminaries
- Examples and counterexamples
- Constructive proofs from ideal objects
- Entailment relations
- Around Hilbert's 17th problem
- Abstract ideal theory in commutative rings
- Injective modules and Baer's criterion (w.i.p.)



- Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra*. Universitext. New York: Springer-Verlag, 1988
- Harold M. Edwards. *Essays in Constructive Mathematics*. New York: Springer, 2005
- Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*. Dordrecht: Springer Netherlands, 2015
- Ihsen Yengui. *Constructive commutative algebra. Projective modules over polynomial rings and dynamical Gröbner bases*. Vol. 2138. Lecture Notes in Mathematics. Cham: Springer, 2015

## **Rudiments of ring theory**

## Basic notions

We work in constructive set theory **CZF**.

A set  $S$  is said to be **discrete** if

$$\forall x, y \in S (x = y \vee x \neq y)$$

A subset  $T$  of  $S$  is **detachable** if

$$\forall x \in S (x \in T \vee x \notin T)$$

$\text{Fin}(S)$  consists of the **finitely enumerable** subsets of  $S$ , i.e.,  
 $U \in \text{Fin}(S)$  iff

$$\exists n \in \mathbb{N} \exists f (f : \{1, \dots, n\} \twoheadrightarrow U)$$

Caveat: subsets of f.e. sets need not be f.e.!

## Basic notions

Throughout, let  $\mathbf{R}$  be a commutative ring with 1.  
We will incur only few and basic concepts.

$\mathbf{R}$  is **integral** if, for all  $a \in \mathbf{R}$ ,

$$a = 0 \vee \forall b \in \mathbf{R} (ab = 0 \rightarrow b = 0)$$

$\mathbf{R}$  is a **discrete field** if, for all  $a \in \mathbf{R}$ ,

$$a = 0 \vee \exists b \in \mathbf{R} (ab = 1)$$

E.g., the trivial ring is a discrete field!

A discrete field  $\mathbf{R}$  is a discrete set iff  $1 =_{\mathbf{R}} 0$  is decidable.

## Basic notions

Recall that an **ideal**  $I$  of  $\mathbf{R}$  is an additive subgroup s.t.  $R I \subseteq I$ .

If  $U \in \text{Pow}(\mathbf{R})$ , then  $\langle U \rangle$  denotes the ideal **generated** by  $U$ .

An ideal  $I$  is **prime** if

$$ab \in I \rightarrow a \in I \vee b \in I$$

and **maximal** if, for all  $a \in \mathbf{R}$ ,

$$a \in I \vee \exists b \in \mathbf{R} (1 - ab \in I)$$

Every maximal ideal is prime.

$I$  is maximal iff the quotient ring  $R/I$  is a discrete field.

## Basic notions

Let  $I$  be an ideal of  $\mathbf{R}$ .

The **radical** of  $I$  is

$$\sqrt{I} = \{ a \in \mathbf{R} : \exists n \in \mathbb{N} ( a^n \in I ) \}$$

The **Jacobson radical** of  $I$  is

$$\begin{aligned} \text{Jac}(I) &= \{ a \in \mathbf{R} : \forall b \exists c ( 1 - (1 - ab)c \in I ) \} \\ &= \{ a \in \mathbf{R} : \forall b ( 1 \in \langle a, b \rangle \rightarrow 1 \in \langle I, b \rangle ) \} \end{aligned}$$

Note that

$$\sqrt{I} \subseteq \text{Jac}(I)$$

Ideals can be captured by **inductive definitions**:

$$\frac{\emptyset}{0} \quad \frac{\{a, b\}}{a + b} \quad a, b \in \mathbf{R} \quad \frac{\{a\}}{ab} \quad a, b \in \mathbf{R}$$

Prime ideals appear as **non-deterministic** inductive definitions:

$$\frac{\emptyset}{\{0\}} \quad \frac{\{a, b\}}{\{a + b\}} \quad \frac{\{a\}}{\{ab\}} \quad \frac{\{ab\}}{\{a, b\}} \quad \frac{\{1\}}{\emptyset}$$

N.B. Under SGA the class  $\text{Spec}(\mathbf{R})$  of primes is **set-generated**; the class of minimal primes is a set, cf. [Ber13; IN16].

## **Limitations**



## LPO

For every binary sequence  $(a_i)_{i \in \mathbb{N}}$  either

- (a) there exists  $n$  such that  $a_n = 1$ , or
- (b)  $a_n = 0$  for every  $n$ .

## LPO

For every binary sequence  $(a_i)_{i \in \mathbb{N}}$  either

- (a) there exists  $n$  such that  $a_n = 1$ , or
- (b)  $a_n = 0$  for every  $n$ .

Ideals of  $\mathbb{Z}$  need not be principal

## LPO

For every binary sequence  $(a_i)_{i \in \mathbb{N}}$  either

- (a) there exists  $n$  such that  $a_n = 1$ , or
- (b)  $a_n = 0$  for every  $n$ .

Ideals of  $\mathbb{Z}$  need not be principal

Let  $(a_i)_{i \in \mathbb{N}}$  be a binary sequence.

Consider the generated ideal

$$I = \langle \{ a_i : i \in \mathbb{N} \} \rangle \subseteq \mathbb{Z}$$

Suppose that  $I$  has a single generator ...

Free modules need not be projective [MRR88, Ex. II.4.10]

Free modules need not be projective [MRR88, Ex. II.4.10]

Let  $(a_i)_{i \in \mathbb{N}}$  be a binary sequence.

Let  $I = \{0, 1\} / R$ , where  $xRy \equiv (x = y) \vee \exists n (a_n = 1)$ .

Let  $\mathbf{R} = \mathbb{Z}/2\mathbb{Z}$ .

$$\begin{array}{ccc} & & \mathbf{R}^2 \\ & \nearrow f & \downarrow e \\ \mathbf{R}^{(I)} & \xrightarrow{\text{id}} & \mathbf{R}^{(I)} \end{array}$$

Suppose that  $\mathbf{R}^{(I)}$  is projective, and that  $ef = \text{id}$ .

However,  $\mathbf{R}^2$  is discrete ...

## LLPO

For every binary sequence  $(a_i)_{i \in \mathbb{N}}$  that contains at most one 1, either

- (a)  $a_n = 0$  for all odd  $n$ , or
- (b)  $a_n = 0$  for all even  $n$ .

## LLPO

For every binary sequence  $(a_i)_{i \in \mathbb{N}}$  that contains at most one 1, either

- (a)  $a_n = 0$  for all odd  $n$ , or
- (b)  $a_n = 0$  for all even  $n$ .

## Counterexamples

The zero ideal is not prime in  $\mathbb{R}$ .

Splitting fields need not be unique [BR87, Thm. 4.6].

“Summands need not be summands” [MRR88, Ex. II.4.6].

# **The Upside Down**



## Theorem\*

Let  $\mathbf{R}$  be non-trivial. If  $\varphi : \mathbf{R}^m \rightarrow \mathbf{R}^n$  is surjective, then  $m \geq n$ .

## Theorem\*

Let  $\mathbf{R}$  be non-trivial. If  $\varphi : \mathbf{R}^m \rightarrow \mathbf{R}^n$  is surjective, then  $m \geq n$ .

## Proof.

Let  $\mathfrak{m}$  be a maximal ideal of  $\mathbf{R}$ , and consider the field  $k = \mathbf{R}/\mathfrak{m}$ .

Tensoring yields an epimorphism of  $k$ -vector spaces

$$\mathrm{id}_k \otimes \varphi : \underbrace{k \otimes_{\mathbf{R}} \mathbf{R}^m}_{\cong k^m} \rightarrow \underbrace{k \otimes_{\mathbf{R}} \mathbf{R}^n}_{\cong k^n}$$

which implies  $m \geq n$  (Steinitz exchange). □

### Theorem (Richman [Ric88])

If  $\varphi : \mathbf{R}^m \rightarrow \mathbf{R}^n$  is surjective, and  $m < n$ , then  $\mathbf{R}$  is trivial.

# Invariance of rank, constructively

## Theorem (Richman [Ric88])

If  $\varphi : \mathbf{R}^m \rightarrow \mathbf{R}^n$  is surjective, and  $m < n$ , then  $\mathbf{R}$  is trivial.

### Proof.

There is  $\psi : \mathbf{R}^n \rightarrow \mathbf{R}^m$  such that  $\varphi \circ \psi = \text{id}_{\mathbf{R}^n}$ .

Extend  $\varphi$  to  $\mathbf{R}^n = \mathbf{R}^m \oplus \mathbf{R}^{n-m}$  by setting  $\varphi(\mathbf{R}^{n-m}) = 0$ .

View  $\psi$  as a map into  $\mathbf{R}^n$ .

If  $A, B \in \text{Mat}_n(\mathbf{R})$  are the matrices of  $\varphi$  and  $\psi$ , resp., then

$$1 = \det I_n = \det AB = (\det A)(\det B) = (\det A) \cdot 0 = 0 \quad \square$$

# Nakayama's lemma

## Theorem\*

Let  $J \subseteq \bigcap \text{Max}(\mathbf{R})$  be an ideal, and let  $M$  be a finitely generated  $\mathbf{R}$ -module. If  $JM = M$ , then  $M = 0$ .

# Nakayama's lemma

## Theorem\*

Let  $J \subseteq \bigcap \text{Max}(\mathbf{R})$  be an ideal, and let  $M$  be a finitely generated  $\mathbf{R}$ -module. If  $JM = M$ , then  $M = 0$ .

## Proof sketch [Eis04].

- (i) Show first that there is  $a \in J$  for which  $(1 - a)M = 0$ .  
(Corollary to Cayley-Hamilton)
- (ii) Every (proper) maximal ideal avoids  $1 - a$  which thus is a unit. It follows that  $M = 0$ . □

## Nakayama's lemma, constructively

Solution: observe that (classically)

$$\bigcap \text{Max}(\mathbf{R}) = \text{Jac}(\mathbf{R})$$

and substitute the former for the latter.

# Nakayama's lemma, constructively

Solution: observe that (classically)

$$\bigcap \text{Max}(\mathbf{R}) = \text{Jac}(\mathbf{R})$$

and substitute the former for the latter.

## Theorem

Let  $J \subseteq \text{Jac}(\mathbf{R})$  be an ideal, and let  $M$  be a finitely generated  $\mathbf{R}$ -module. If  $JM = M$ , then  $M = 0$ .

## Proof.

Step (i) above holds constructively [LQ15].

Now we know that  $1 - a$  is a unit since  $a \in \text{Jac}(\mathbf{R})$ . □



**Computational content from ideal elements:  
Gauß' Lemma and nilpotent coefficients**

## Theorem (Gauß' Lemma)

Let  $f, g \in \mathbf{R}[X]$ .

$$c(f)c(g) \subseteq \sqrt{c(fg)}$$

where  $c(f)$  is the **content** of  $f$ , i.e., the ideal generated by the coefficients of  $f$ .

# Content of polynomials

## Theorem (Gauß' Lemma)

Let  $f, g \in \mathbf{R}[X]$ .

$$c(f)c(g) \subseteq \sqrt{c(fg)}$$

where  $c(f)$  is the **content** of  $f$ , i.e., the ideal generated by the coefficients of  $f$ .

## A classical proof [Eis04].

“It is enough to show that if a prime ideal  $\mathfrak{p}$  contains  $c(fg)$ , then it contains  $c(f)c(g)$ . Factoring out  $\mathfrak{p}$ , we may assume that  $\mathbf{R}$  is a domain and  $\mathfrak{p}$  is 0, and we must show that if  $fg = 0$ , then  $f = 0$  or  $g = 0$ . Since  $R$  is a now domain, this is obvious.”  $\square$

## Example

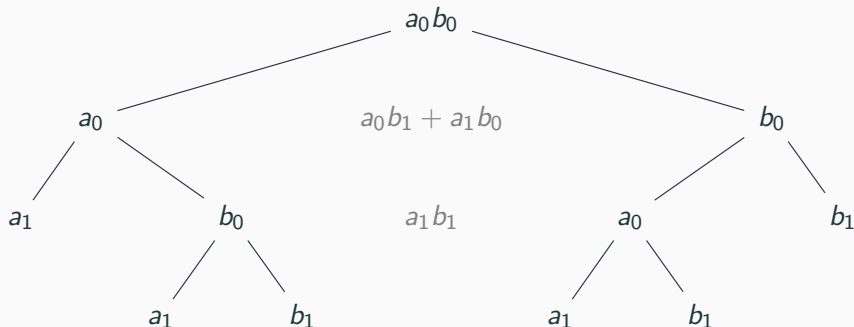
Let  $f = a_0 + a_1X$  and  $g = b_0 + b_1X$ .

Suppose that  $\mathfrak{p}$  contains  $c(fg) = \langle a_0b_0, a_0b_1 + a_1b_0, a_1b_1 \rangle$ .

## Example

Let  $f = a_0 + a_1X$  and  $g = b_0 + b_1X$ .

Suppose that  $\mathfrak{p}$  contains  $c(fg) = \langle a_0b_0, a_0b_1 + a_1b_0, a_1b_1 \rangle$ .



So  $\mathfrak{p}$  contains  $c(f)c(g) = \langle a_0b_0, a_0b_1, a_1b_0, a_1b_1 \rangle$ .

## Example

Now suppose that

$$c \in c(f)c(g)$$

It is immediate that

$$c \in \langle a_0, a_1 \rangle \cap \langle b_0, b_1 \rangle$$

We want to obtain a witness for

$$c \in \sqrt{\langle a_0 b_0, a_0 b_1 + a_1 b_0, a_1 b_1 \rangle}$$

The tree is an instruction!

For  $a \in \mathbf{R}$  and  $U \in \text{Fin}(\mathbf{R})$  write

$$U \triangleright a \equiv a \in \sqrt{\langle U \rangle}$$

# Entailment

For  $a \in \mathbf{R}$  and  $U \in \text{Fin}(\mathbf{R})$  write

$$U \triangleright a \equiv a \in \sqrt{\langle U \rangle}$$

This  $\triangleright$  is a (single-conclusion) **entailment relation**:

$$\frac{U \ni a}{U \triangleright a} \text{ (R)} \qquad \frac{V \supseteq U \triangleright a}{V \triangleright a} \text{ (M)} \qquad \frac{U \triangleright b \quad V, b \triangleright a}{U, V \triangleright a} \text{ (T)}$$



For  $a \in \mathbf{R}$  and  $U \in \text{Fin}(\mathbf{R})$  write

$$U \triangleright a \equiv a \in \sqrt{\langle U \rangle}$$

This  $\triangleright$  is a (single-conclusion) **entailment relation**:

$$\frac{U \ni a}{U \triangleright a} \text{ (R)} \qquad \frac{V \supseteq U \triangleright a}{V \triangleright a} \text{ (M)} \qquad \frac{U \triangleright b \quad V, b \triangleright a}{U, V \triangleright a} \text{ (T)}$$

N.B. (later)

1. This  $\triangleright$  is **inductively generated**.
2. The **models** of  $\triangleright$  precisely are the radical ideals of  $\mathbf{R}$ .

In addition:

$$\frac{U, a \triangleright c \quad V, b \triangleright c}{U, V, ab \triangleright c} (\pi)$$

Because if

$$c^n = u + ra \quad \text{and} \quad c^m = v + sb$$

for certain  $n, m \in \mathbb{N}$ ,  $u \in \langle U \rangle$ ,  $v \in \langle V \rangle$ ,  $r, s \in \mathbf{R}$ , then

$$c^{n+m} = uv + sbu + rav + rsab \in \langle U, V, ab \rangle$$

## Upside down

Following the left branch bottom-up:

$$\frac{a_0, a_0 b_1 + a_1 b_0 \triangleright a_1 b_0 \quad \frac{a_0, a_1 \triangleright c \quad \frac{a_0, a_1 \triangleright c \quad b_0, b_1 \triangleright c}{a_0, b_0, a_1 b_1 \triangleright c} (\pi)}{a_0, a_1 b_0, a_1 b_1 \triangleright c} (\pi)}{a_0, a_0 b_1 + a_1 b_0, a_1 b_1 \triangleright c} (T)$$

## Upside down

Following the left branch bottom-up:

$$\frac{a_0, a_0 b_1 + a_1 b_0 \triangleright a_1 b_0 \quad \frac{a_0, a_1 \triangleright c \quad \frac{a_0, a_1 \triangleright c \quad b_0, b_1 \triangleright c}{a_0, b_0, a_1 b_1 \triangleright c} (\pi)}{a_0, a_1 b_0, a_1 b_1 \triangleright c} (\pi)}{a_0, a_0 b_1 + a_1 b_0, a_1 b_1 \triangleright c} (T)$$

Similarly, we obtain

$$b_0, a_0 b_1 + a_1 b_0, a_1 b_1 \triangleright c$$

Together this yields

$$a_0 b_0, a_0 b_1 + a_1 b_0, a_1 b_1 \triangleright c$$

Cf. [BV96] and the course material.

## Theorem

If  $f = \sum a_i X^i$  is a unit in  $\mathbf{R}[X]$ , then  $a_i$  is nilpotent for  $i \geq 1$ .

# Nilpotent coefficients

## Theorem

If  $f = \sum a_i X^i$  is a unit in  $\mathbf{R}[X]$ , then  $a_i$  is nilpotent for  $i \geq 1$ .

## A classical proof.

Suppose that  $fg = 1$  in  $\mathbf{R}[X]$ . If  $\mathbf{R}$  is a domain, then since

$$\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$$

we see that  $a_i = 0$  for  $i \geq 1$ . Thus, reducing modulo a generic prime  $\mathfrak{p}$ , we get

$$a_i \in \bigcap \operatorname{Spec}(\mathbf{R}) = \sqrt{0}$$

□

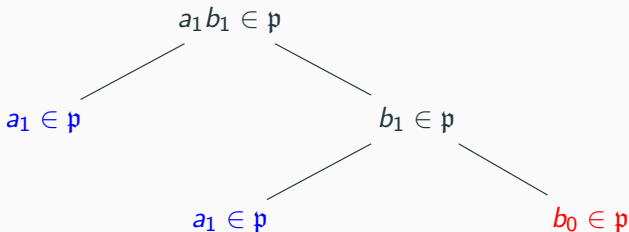
## Example

Let  $f = a_0 + a_1X$  and  $g = b_0 + b_1X$ .

Suppose that

$$a_0b_0 = 1 \quad a_0b_1 + a_1b_0 = 0 \quad a_1b_1 = 0$$

Consider a generic (proper) prime ideal  $\mathfrak{p}$ .



## Upside down

The tree tells us how to infer  $a_1 \in \sqrt{0}$ :

[illegible]

Simple example:

$$2X + 1 \in \mathbb{Z}/4\mathbb{Z}[X]$$

See the course material for a proper discussion.



### Theorem (McAdam, Swan [MS04])

The following are equivalent.

1.  $\mathbf{R}$  is reduced and **connected**, i.e., every idempotent is 0 or 1.
2. For all  $f, g \in \mathbf{R}[X]$ , if  $fg$  is monic, then the (formally) leading coefficients of  $f$  and  $g$  are units.

Again, this can be shown modulo a generic prime ideal.

A constructive argument is hidden in the classical proof!

Cf. [Wes18; Yen03]

# Dedekind's Prague theorem

## Theorem (Kronecker)

Let  $a_0, \dots, a_m, b_0, \dots, b_n$  be indeterminates and let  $\mathbf{R} = \mathbb{Z}[a_i, b_j]$ .

Put

$$c_k = \sum_{i+j=k} a_i b_j.$$

Then each element  $a_i b_j$  is integral over the subring of  $\mathbf{R}$  generated by  $c_0, c_1, \dots, c_{m+n}$ .

- Direct consequence: **Dedekind's Prague theorem** [Edw90]
- Non-constructive proof is based on **valuations** (Bourbaki)
- Coquand and Persson have used (multi-conclusion) entailment relations [CP01; Coq09]

# Conclusion

- Ideal objects like prime ideals and valuation rings can act as **useful fictions**.
- We can systematically keep track of certain identities by means of suitable **entailment relations**.
- The use of maximal ideals can be tackled with a similar **backtracking strategy**:  
Ihsen Yengui. “Making the use of maximal ideals constructive.” In: *Theoret. Comput. Sci.* 392 (2008), pp. 174–178

## Entailment relations

# Entailment relations

Let  $S$  be a set, and let  $\vdash \subseteq \text{Fin}(S) \times \text{Fin}(S)$ .

$\vdash$  is an **entailment relation** if it is reflexive, monotone, and transitive, i.e.,

$$\frac{U \not\sim V}{U \vdash V} \text{ (R)} \quad \frac{U \vdash V}{U, U' \vdash V, V'} \text{ (M)} \quad \frac{U \vdash V, a \quad U', a \vdash V'}{U, U' \vdash V, V'} \text{ (T)}$$

# Entailment relations

Let  $S$  be a set, and let  $\vdash \subseteq \text{Fin}(S) \times \text{Fin}(S)$ .

$\vdash$  is an **entailment relation** if it is reflexive, monotone, and transitive, i.e.,

$$\frac{U \not\sim V}{U \vdash V} \text{ (R)} \quad \frac{U \vdash V}{U, U' \vdash V, V'} \text{ (M)} \quad \frac{U \vdash V, a \quad U', a \vdash V'}{U, U' \vdash V, V'} \text{ (T)}$$

A **model** of  $\vdash$  is a subset  $\alpha$  of  $S$  which “splits entailments”, i.e.,

$$\frac{\alpha \supseteq U \quad U \vdash V}{\alpha \not\sim V}$$

Let  $\text{Spec}(\vdash)$  denote the class of models of  $\vdash$ .

## **Completeness theorem\* (Scott)**

The following are equivalent.

1.  $U \vdash V$
2.  $\forall \alpha \in \text{Spec}(\vdash) (U \subseteq \alpha \rightarrow \alpha \not\subseteq V)$

N.B. Completeness implies excluded middle.

CT is classically equivalent to the prime ideal theorem.

# Completeness necessitates classical logic

Let  $\psi$  be a bounded formula, let  $S = \{*\}$  be a singleton set.

$$\{ (S, S), (S, \emptyset) \} \cup \{ (\emptyset, S) : \psi \} \cup \{ (\emptyset, \emptyset) : \psi \}$$

is an entailment relation. Notice that

$$\vdash * \quad \text{iff} \quad \psi$$

Completeness implies

$$\{ a \in S : \forall \alpha \in \text{Spec}(\vdash)(a \in \alpha) \} = \{ a \in S : \psi \}$$

and therefore

$$\psi \quad \text{iff} \quad \text{Spec}(\vdash) = \emptyset$$



# The fundamental theorem: constructive semantics

## Theorem (Cederquist, Coquand)

Every entailment relation  $(S, \vdash)$  generates a distributive lattice  $L_S$  with a map  $i : S \rightarrow L_S$  such that

$$U \vdash V \quad \text{if and only if} \quad \bigwedge_{a \in U} i(a) \leq \bigvee_{b \in V} i(b)$$

This  $i$  is *universal* among interpretations in distributive lattices:

$$\begin{array}{ccc} (S, \vdash) & \xrightarrow{i} & L_S \\ & \searrow \forall f & \downarrow \exists! g \\ & & L \end{array}$$

## Example: Support of a ring

Consider the entailment relation of (proper) **prime ideal** of  $\mathbf{R}$ .

$$\vdash 0$$

$$a \vdash ab$$

$$a, b \vdash a + b$$

$$ab \vdash a, b$$

$$1 \vdash$$

## Example: Support of a ring

Consider the entailment relation of (proper) **prime ideal** of **R**.

$$\vdash 0$$

$$a \vdash ab$$

$$a, b \vdash a + b$$

$$ab \vdash a, b$$

$$1 \vdash$$

$$D(0) = 1$$

$$D(a) \leq D(ab)$$

$$D(a) \wedge D(b) \leq D(a + b)$$

$$D(ab) \leq D(a) \vee D(b)$$

$$D(1) = 0$$

## Example: Support of a ring

Consider the entailment relation of (proper) **prime ideal** of **R**.

$\vdash 0$	$D(0) = 1$
$a \vdash ab$	$D(a) \leq D(ab)$
$a, b \vdash a + b$	$D(a) \wedge D(b) \leq D(a + b)$
$ab \vdash a, b$	$D(ab) \leq D(a) \vee D(b)$
$1 \vdash$	$D(1) = 0$

We get Joyal's lattice [Joy75]!

The dual of  $\vdash$  yields the **universal support** on **R**.

# Vast applicability of entailment relations

- **Constructive algebra**  
e.g. dynamical methods (Coste, Lombardi, Roy, ...)
- **Proof theory**  
e.g. Szpilrajn's theorem (Negri, von Plato, Coquand)
- **Point-free topology**  
e.g. localic Hahn-Banach (Mulvey & Pelletier, Coquand)
- **Theoretical computer science**  
e.g. domain theory, resolution (Zhang & Rounds, Coquand)
- **Non-classical logic**  
e.g. many-valued logic (Scott)

## Working with entailment relations

- Aim: capture and replace algebraic structures and their ideal objects syntactically
- Examples include ring spectra and several function spaces.
- We deal with inductively generated entailment relations.
- The task is to obtain a direct, non-inductive description.
- Often, the key is to understand the finite **inconsistent** subsets.

**From inductive to non-inductive description:  
A case study around Hilbert's 17th problem**

**Example** (Motzkin 1967)

$$\begin{aligned} M(x, y) &= x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \\ &= \frac{x^2y^2(x^2 + y^2 + 1)(x^2 + y^2 - 2)^2 + (x^2 - y^2)^2}{(x^2 + y^2)^2} \end{aligned}$$

But  $M(x, y)$  cannot be written as a sum of squares of polynomials.



**Example** (Motzkin 1967)

$$\begin{aligned} M(x, y) &= x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \\ &= \frac{x^2y^2(x^2 + y^2 + 1)(x^2 + y^2 - 2)^2 + (x^2 - y^2)^2}{(x^2 + y^2)^2} \end{aligned}$$

But  $M(x, y)$  cannot be written as a sum of squares of polynomials.

## Hilbert's 17th problem

Suppose that  $f \in \mathbb{R}[x_1, \dots, x_n]$  is nonnegative at all points of  $\mathbb{R}^n$ .  
Is  $f$  a finite sum of squares of rational functions?

Artin gave an affirmative answer.

*"[Artin's] method was as remarkable as the result. It was perhaps the first triumph of what is sometimes called 'abstract' algebra."*

Richard Brauer  
*Emil Artin*

## Key observation

The totally positive elements of a field are precisely the sums of squares.

# Partially ordered rings

A partial order  $\leq$  of a ring  $\mathbf{R}$  is **compatible** if, for all  $a, b, c \in \mathbf{R}$ ,

$$a \leq b \rightarrow a + c \leq b + c$$

$$0 \leq a \wedge 0 \leq b \rightarrow 0 \leq ab$$

## Classical problems

Determine a linear extension

Describe the totally positive elements

## Total orders as ideal elements

Let  $\mathbf{R}$  be an **integral ring**, i.e., such that, for all  $a \in R$ ,

$$a = 0 \vee \forall b \in \mathbf{R} (ab = 0 \rightarrow b = 0)$$

Let  $\vdash$  be generated by all instances of

$$a, -a \vdash$$

$$a, b \vdash ab$$

$$a, b \vdash a + b$$

$$\vdash a, -a \quad \text{for } a \neq 0$$

## Total orders as ideal elements

Given  $\alpha \in \text{Spec}(\vdash)$ , stipulate

$$a <_{\alpha} b \equiv b - a \in \alpha$$

This yields a compatible **strict** order which is total, i.e.,

$$\forall a, b \in \mathbf{R} (a \neq b \rightarrow a <_{\alpha} b \vee b <_{\alpha} a)$$

Conversely, every such  $<$  has a **positive cone**

$$\alpha_{<} = \{ a \in \mathbf{R} : 0 < a \} \in \text{Spec}(\vdash)$$

## Proposition

Let  $U \in \text{Fin}(\mathbf{R})$ . The following are equivalent.

1.  $U \vdash$
2. There are  $a_0, \dots, a_n \in (U)$  and  $x_0, \dots, x_n \in \mathbf{R} \setminus \{0\}$  s.t.

$$\sum_{i=0}^n a_i x_i^2 = 0$$

where  $(U)$  is the multiplicative monoid generated by  $U$ .

# Total orders as ideal elements

## Proof sketch.

Abbreviate the second item by  $\text{Inc}(U)$ .

Show that

- (i)  $\text{Inc}(U)$  implies  $U \vdash$
- (ii)  $\text{Inc}$  is monotone, i.e., if  $\text{Inc}(U)$  and  $U \subseteq V$ , then  $\text{Inc}(V)$
- (iii)

$$\frac{U \vdash V \quad \forall b \in V \text{ Inc}(W, b)}{\text{Inc}(U, W)}$$

□

## Remarks

In (iii) it suffices to consider initial entailments.

This is a general strategy for describing the inconsistent subsets.

## Corollary

Let  $\mathbf{K}$  be a (non-trivial) discrete field.

The following are equivalent.

1.  $\vdash$  **collapses**, i.e.,  $\emptyset \vdash \emptyset$
2.  $-1$  is a sum of squares



## Corollary

Let  $\mathbf{K}$  be a (non-trivial) discrete field.

The following are equivalent.

1.  $\vdash$  **collapses**, i.e.,  $\emptyset \vdash \emptyset$
2.  $-1$  is a sum of squares

## Corollary

Let  $\mathbf{K}$  be a discrete formally real field and let  $0 \neq a \in \mathbf{K}$ .

The following are equivalent.

1.  $a$  is **totally positive**, i.e.,  $\vdash a$
2.  $a$  is a sum of squares.

## Corollary

Let  $\mathbf{K}$  be a **factorial field**, and let  $f \in \mathbf{K}[X]$  be irreducible and of odd degree. Let  $\vdash$  and  $\vdash_f$  be the entailment relations of total order of  $\mathbf{K}$  and  $\mathbf{K}[X]/\langle f \rangle$ , respectively.

Then  $\vdash$  and  $\vdash_f$  **collapse simultaneously**.

Classically, this means that every odd-degree extension of a formally real field is formally real.

## Proof.

By induction on the degree of  $f$ , following the classical proof. □

- Orderability criteria for groups.  
E.g., **Levi's theorem**: “An abelian group is orderable iff it is torsion-free” in terms of collapse.
- Ordered groups and topology.  
E.g., **Sikora's theorem**: “The space of compatible orders of  $\mathbb{Z}^n$ , where  $n > 1$ , is a Cantor space” by Stone duality.
- **Extendability** criteria for partial orders.  
E.g., Serre's theorem on extension of partial orders of fields.
- **Archimedean** property requires geometric sequents!

## **Generalized entailment relations**

# Generalized entailment relations

Let  $S$  be a set, and let  $\vdash \subseteq \text{Fin}(S) \times \text{Pow}(S)$ .

$\vdash$  is a **generalized entailment relation** if it is reflexive, monotone

$$\frac{U \not\leq V}{U \vdash V} \text{ (R)} \qquad \frac{U \vdash V}{U, U' \vdash V} \text{ (M)}$$

and transitive

$$\frac{U \vdash V \quad \forall b \in V (U', b \vdash W)}{U, U' \vdash W} \text{ (T)}$$

# Inductively generated entailment relations

An **axiom set** for  $\vdash$  is given by a set-indexed family  $(U_i, V_i)_{i \in I}$  of initial entailments.

## Proposition (Cut elimination)

The relation  $\vdash$  defined inductively by

$$\frac{U \wp V}{U \vdash V} \text{ (R)} \qquad \frac{\forall b \in V_i (U, b \vdash W)}{U, U_i \vdash W} \text{ (T}_i\text{)}$$

is the least entailment relation to contain  $(U_i, V_i)_{i \in I}$ .

## Example: discrete fields

Let  $\mathbf{R}$  be a commutative ring with 1.

Consider on  $\mathbf{R}$  the entailment relation generated by

$$\begin{aligned} &\vdash 0 \\ &a \vdash ab \\ &a, b \vdash a + b \\ &\vdash a, \{ 1 - ab : b \in \mathbf{R} \} \end{aligned} \tag{f}$$

Axiom (f) captures the geometric sequent of **discrete field**:

$$\top \vdash x = 0 \text{ **op** } \exists y (xy = 1)$$

Geometric axioms can be used within **dynamical proofs** [CLR01].

## Example: discrete fields

A discrete field is **without zerodivisors**, i.e.,

$$ab \vdash a, b$$

Indeed, for every  $x \in \mathbf{R}$  notice that

$$ab, 1 - ax \vdash b$$

is witnessed by  $xab + b(1 - ax) = b$ . Now apply (T) with (f).

Notice the special case of **reducedness**, i.e.,

$$a^2 \vdash a$$



## Semantics, again

$\vdash$  is **complete** if, for all  $(U, V) \in \text{Fin}(S) \times \text{Pow}(S)$ ,

$$\forall \alpha \in \text{Spec}(\vdash) (U \subseteq \alpha \rightarrow \alpha \not\subseteq V) \text{ implies } U \vdash V.$$

## Semantics, again

$\vdash$  is **complete** if, for all  $(U, V) \in \text{Fin}(S) \times \text{Pow}(S)$ ,

$$\forall \alpha \in \text{Spec}(\vdash) (U \subseteq \alpha \rightarrow \alpha \not\subseteq V) \text{ implies } U \vdash V.$$

### Proposition\*

1. Countably generated entailment relations are complete.
2. An entailment relation  $\vdash$  is complete if

$$\frac{U \vdash V \quad \forall b \in V \text{ Fin}(W, b) \not\subseteq \text{Inc}}{\text{Fin}(U, W) \not\subseteq \text{Inc}} \quad (\text{P})$$

where  $W \in \text{Pow}(S)$  and  $\text{Inc} = \{ U \in \text{Fin}(S) : U \vdash \}$ .

3. Every conventional entailment relation is complete.

# Interpretation

An **interpretation**

$$i : (S, \vdash) \rightarrow (S', \vdash')$$

of entailment relations is given by a function  $i : S \rightarrow S'$  such that

$$U \vdash V \quad \text{implies} \quad i(U) \vdash' i(V)$$

An interpretation is **conservative** if

$$i(U) \vdash' i(V) \quad \text{implies} \quad U \vdash V$$

and **weakly conservative** if

$$i(U) \vdash' \quad \text{implies} \quad U \vdash$$

Every interpretation  $i : (S, \vdash) \rightarrow (S', \vdash')$  induces a mapping of model classes:

$$i^{-1} : \text{Spec}(\vdash') \rightarrow \text{Spec}(\vdash), \quad \beta \mapsto i^{-1}(\beta)$$

Every interpretation  $i : (S, \vdash) \rightarrow (S', \vdash')$  induces a mapping of model classes:

$$i^{-1} : \text{Spec}(\vdash') \rightarrow \text{Spec}(\vdash), \quad \beta \mapsto i^{-1}(\beta)$$

## **Proposition\*** (“Lying over”)

Suppose that  $\vdash$  is complete and  $\vdash'$  satisfies (P).

The following are equivalent.

1.  $i$  is weakly conservative.
2.  $\forall \alpha \in \text{Spec}(\vdash) \exists \beta \in \text{Spec}(\vdash') (\alpha \subseteq i^{-1}(\beta)).$

**Digression: formal spaces**

## Formal spaces from entailment relations

Let  $\vdash$  be inductively generated by  $(U_i, V_i)_{i \in I}$ .

Consider

$$C : \text{Fin}(S) \rightarrow \text{Pow}(\text{Pow}(\text{Fin}(S)))$$

$$U \mapsto \bigcup_{i \in I} \{ \{ U \cup \{ b \} : b \in V_i \} : U_i \subseteq U \}$$

## Formal spaces from entailment relations

Let  $\vdash$  be inductively generated by  $(U_i, V_i)_{i \in I}$ .

Consider

$$C : \text{Fin}(S) \rightarrow \text{Pow}(\text{Pow}(\text{Fin}(S)))$$
$$U \mapsto \bigcup_{i \in I} \{ \{ U \cup \{ b \} : b \in V_i \} : U_i \subseteq U \}$$

$(\text{Fin}(S), \supseteq, C)$  is a **covering system**, i.e.,

for every  $U \in \text{Fin}(S)$  and  $X \in C(U)$ ,

1.  $X \subseteq \downarrow \{ U \}$
2. if  $U' \supseteq U$ , then there is  $Y \in C(U')$  such that  $Y \subseteq \downarrow X$ .



## Formal spaces from entailment relations

$C$  gives way to an inductive definition:

$$\Phi = \{ (X, U) : U \in \text{Fin}(S) \text{ and } X \in C(U) \},$$

and, for  $\mathcal{U} \in \text{Pow}(\text{Fin}(S))$ , we put

$$\mathcal{AU} = I(\Phi, \downarrow \mathcal{U}).$$

## Formal spaces from entailment relations

$C$  gives way to an inductive definition:

$$\Phi = \{ (X, U) : U \in \text{Fin}(S) \text{ and } X \in C(U) \},$$

and, for  $\mathcal{U} \in \text{Pow}(\text{Fin}(S))$ , we put

$$\mathcal{AU} = I(\Phi, \downarrow \mathcal{U}).$$

The operator  $\mathcal{A}$  has the following properties:

1.  $\downarrow(\mathcal{AU}) \subseteq \mathcal{AU}$
2.  $\mathcal{U} \subseteq \mathcal{AV}$  implies  $\mathcal{AU} \subseteq \mathcal{AV}$
3.  $\mathcal{AU} \cap \mathcal{AV} \subseteq \mathcal{A}(\mathcal{U} \downarrow \mathcal{V})$

## Formal spaces from entailment relations

A subset  $\mathcal{U} \subseteq \text{Fin}(S)$  is  $\mathcal{A}$ -**saturated** if  $\mathcal{U} = \mathcal{A}\mathcal{U}$ .

The class  $\text{Sat}(\mathcal{A})$  of all  $\mathcal{A}$ -saturated subsets of  $\text{Fin}(S)$  is a **set-generated frame**, where

1.  $\mathcal{A}\mathcal{U} \wedge \mathcal{A}\mathcal{V} = \mathcal{A}(\mathcal{U} \downarrow \mathcal{V})$
2.  $\bigvee_{i \in I} \mathcal{A}\mathcal{U}_i = \mathcal{A}(\bigcup_{i \in I} \mathcal{U}_i)$

A set of generators is given by

$$\{ \mathcal{A}\{U\} : U \in \text{Fin}(S) \}$$

# Formal spaces from entailment relations

## Theorem (CZF<sup>+</sup>)

Let  $\vdash$  be an inductively generated generalized entailment relation. There is a set-generated frame  $F$  together with a map  $i : S \rightarrow F$  such that

$$U \vdash V \quad \text{if and only if} \quad \bigwedge_{a \in U} i(a) \leq \bigvee_{b \in V} i(b)$$

This  $i$  is universal among interpretations in frames:

$$\begin{array}{ccc} (S, \vdash) & \xrightarrow{i} & F \\ & \searrow \forall f & \downarrow \exists ! f' \\ & & F' \end{array}$$

# Completely prime filters

Let  $i : (S, \vdash) \rightarrow F$  be the universal interpretation.

1. If  $\mathfrak{p}$  is a completely prime filter of  $F$ , then

$$i^{-1}(\mathfrak{p}) \in \text{Spec}(\vdash).$$

2. If  $\alpha \in \text{Spec}(\vdash)$ , then

$$\mathfrak{p}_\alpha = \left\{ x \in F : \exists U \in \text{Fin}(\alpha) \bigwedge i(U) \leq x \right\}$$

is a completely prime filter such that  $\alpha = i^{-1}(\mathfrak{p}_\alpha)$ .

Cf. Thierry Coquand and Guo-Qiang Zhang. “Sequents, Frames, and Completeness”. In: *Computer Science Logic. 14th International Workshop, CSL 2000 Annual Conference of the EACSL*. ed. by Helmut Schwichtenberg and Peter G. Clote.

**Proper, prime, and maximal ideals**

Let  $\mathbf{R}$  be a commutative ring with 1.

The entailment relation  $\vdash$  of **proper ideal** of  $\mathbf{R}$  is generated by:

$$\vdash 0$$

$$a \vdash ab$$

$$a, b \vdash a + b$$

$$1 \vdash$$

On top of  $\vdash$  we can put axioms for **primality**

$$ab \vdash_p a, b$$

and **maximality**

$$\vdash_m a, \{ 1 - ab : b \in \mathbf{R} \}$$

## Proposition

The following are equivalent.

1.  $U \vdash_{\mathfrak{m}} a_1, \dots, a_k$
2.  $a_1 \cdots a_k \in \text{Jac}(\langle U \rangle)$



## Proposition

The following are equivalent.

1.  $U \vdash_{\mathfrak{m}} a_1, \dots, a_k$
2.  $a_1 \cdots a_k \in \text{Jac}(\langle U \rangle)$

## Proposition (Constructive PIT and Krull)

The inclusions

$$(\mathbf{R}, \vdash) \hookrightarrow (\mathbf{R}, \vdash_{\mathfrak{p}}) \hookrightarrow (\mathbf{R}, \vdash_{\mathfrak{m}})$$

are weakly conservative.

## Proposition

If  $\mathbf{R}$  is discrete and non-trivial, then the following are equivalent.

1.  $(\mathbf{R}, \vdash) \hookrightarrow (\mathbf{R}, \vdash_p)$  is conservative.
2.  $\mathbf{R}$  is a field.

## Proposition

If  $\mathbf{R}$  is discrete and non-trivial, then the following are equivalent.

1.  $(\mathbf{R}, \vdash) \hookrightarrow (\mathbf{R}, \vdash_p)$  is conservative.
2.  $\mathbf{R}$  is a field.

## Proposition

The following are equivalent.

1.  $(\mathbf{R}, \vdash_p) \hookrightarrow (\mathbf{R}, \vdash_m)$  is conservative.
2.  $\text{Kdim } \mathbf{R} \leq 0$ , i.e.,  $\forall x \in \mathbf{R} \exists n \in \mathbb{N} \exists a \in \mathbf{R} (x^n = ax^{n+1})$ .

## Primary ideals

The entailment relation  $\vdash_{\mathfrak{p}'}$  of **primary ideal** of  $\mathbf{R}$  is generated by the axioms of proper ideal together with

$$ab \vdash_{\mathfrak{p}'} a, \{ b^n : n > 0 \}$$

# Primary ideals

The entailment relation  $\vdash_{\mathfrak{p}'}$  of **primary ideal** of  $\mathbf{R}$  is generated by the axioms of proper ideal together with

$$ab \vdash_{\mathfrak{p}'} a, \{ b^n : n > 0 \}$$

## Proposition

The following are equivalent.

1.  $\mathbf{R}$  is reduced and  $(\mathbf{R}, \vdash_{\mathfrak{p}'}) \hookrightarrow (\mathbf{R}, \vdash_{\mathfrak{m}})$  is conservative.
2.  $\mathbf{R}$  is **von Neumann regular**, i.e.,  $\forall a \exists x (a = xa^2)$ .

(“If  $\mathbf{R}$  is absolutely flat, every primary ideal is maximal” [AM69, Ex. 4.3])

## Minimal prime ideals

The entailment relation  $\vdash$  of **proper prime filter** of  $\mathbf{R}$  is dual to the entailment relation of proper prime ideal:

$$\vdash 1$$

$$ab \vdash a$$

$$a, b \vdash ab$$

$$a + b \vdash a, b$$

$$0 \vdash$$

## Minimal prime ideals

The entailment relation  $\vdash$  of **proper prime filter** of  $\mathbf{R}$  is dual to the entailment relation of proper prime ideal:

$$\vdash 1$$

$$ab \vdash a$$

$$a, b \vdash ab$$

$$a + b \vdash a, b$$

$$0 \vdash$$

On top of  $\vdash$  we can put the axiom for **maximal** filter:

$$\vdash_{\mathbf{m}} a, \text{Ann}(a)$$

where  $\text{Ann}(a) = \{ x \in \mathbf{R} : xa = 0 \}$ .

## Proposition (Coquand, Lombardi [CL06])

Suppose that  $\mathbf{R}$  is reduced. The following are equivalent.

1.  $a_1, \dots, a_k \vdash_{\mathbf{m}} b_1, \dots, b_\ell$
2.  $\text{Ann}(b_1, \dots, b_\ell) \subseteq \text{Ann}(a_1 \cdots a_k)$ .



## Proposition (Coquand, Lombardi [CL06])

Suppose that  $\mathbf{R}$  is reduced. The following are equivalent.

1.  $a_1, \dots, a_k \vdash_{\mathbf{m}} b_1, \dots, b_\ell$
2.  $\text{Ann}(b_1, \dots, b_\ell) \subseteq \text{Ann}(a_1 \cdots a_k)$ .

## Proposition

The following are equivalent.

1.  $\mathbf{R}$  is von Neumann regular.
2.  $\mathbf{R}$  is reduced and  $(\mathbf{R}, \vdash) \hookrightarrow (\mathbf{R}, \vdash_{\mathbf{m}})$  is conservative.
3.  $\mathbf{R}$  is reduced and every prime ideal of  $\mathbf{R}$  is minimal.\* [Mat83]

Let  $L$  be a distributive lattice.

Let  $\vdash$  be the entailment relation of (proper) prime ideal of  $L$ ,  
let  $\vdash_m$  extend  $\vdash$  with the axiom of maximality.

## Proposition

The following are equivalent.

1.  $(L, \vdash) \hookrightarrow (L, \vdash_m)$  is conservative.
2.  $L$  is Boolean.

This yields **Nachbin's theorem**:

A distributive lattice is Boolean if and only if  
all of its prime ideals are maximal.\*Cf. [Bel99]

**Towards formal Baer criteria**

# Injective modules

Let  $M$  be an  $\mathbf{R}$ -module.

The following are classically equivalent:

1. Given any exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

of  $\mathbf{R}$ -modules, the sequence

$$0 \rightarrow \operatorname{Hom}_{\mathbf{R}}(C, M) \rightarrow \operatorname{Hom}_{\mathbf{R}}(B, M) \rightarrow \operatorname{Hom}_{\mathbf{R}}(A, M) \rightarrow 0$$

is exact.

2.  $M$  is a direct summand of every extension of itself.

# Detecting injective modules

## Baer's criterion\*

A module is injective iff it is injective w.r.t. inclusions of ideals

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & R \\ & & \downarrow & \nwarrow & \\ & & M & & \end{array}$$

# Detecting injective modules

## Baer's criterion\*

A module is injective iff it is injective w.r.t. inclusions of ideals

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & R \\ & & \downarrow & \nwarrow & \\ & & M & & \end{array}$$

## Consequences\*

Abelian groups are injective (as  $\mathbb{Z}$ -modules).

The category of **R**-modules has **enough injectives**.

## Stepwise extension

Suppose that  $M$  is “ideal-injective” and let  $A \subseteq B$ .

Given  $\varphi : A \rightarrow M$  and  $b \in B$ , consider the conductor ideal

$$I = \{ r \in \mathbf{R} : rb \in A \}$$

and put

$$\mu : I \rightarrow M \quad r \mapsto \varphi(rb)$$

By assumption, there is

$$\nu : \mathbf{R} \rightarrow M \quad \text{s.t.} \quad \nu|_I = \mu$$

Now define

$$\varphi' : A + \mathbf{R}b \rightarrow M, \quad a + rb \mapsto \varphi(a) + \nu(r)$$

## Stepwise extension

To “exhaust”  $B$  we need transfinite methods, e.g., Zorn’s lemma.

$$\begin{array}{ccccc} A & \longrightarrow & A + \mathbf{R}b & \dashrightarrow & B \\ & \searrow \varphi & \downarrow \varphi' & \nearrow & \\ & & M & & \end{array}$$

A finite and de-Zornified version lives in the Upside Down!



*“Regarding the theorem instead from a logical viewpoint, it is clear that the import of the assertion is that the extension of the theory of functionals on the subspace  $A$  to that on the seminormed space  $B$  is actually conservative [...]. In other words, no more may be proved about the subspace  $A$  in terms of functionals on the seminormed space  $B$  than may already be proved by considering only functionals on the subspace  $A$ .”*

C.J. Mulvey and J. Wick Pelletier

*A globalization of the Hahn-Banach theorem*

## Hom-sets as spectra

Let  $\vdash$  on  $A \times M$  be generated by all instances of

$$\begin{aligned}(a, m), (a, m') &\vdash & (m \neq m') \\ (a, m), (b, n) &\vdash (ra + sb, rm + sn) \\ &\vdash (0_A, 0_M) \\ &\vdash \{ (a, m) : m \in M \}\end{aligned}$$

## Hom-sets as spectra

Let  $\vdash$  on  $A \times M$  be generated by all instances of

$$\begin{aligned}(a, m), (a, m') &\vdash & (m \neq m') \\(a, m), (b, n) &\vdash (ra + sb, rm + sn) \\&\vdash (0_A, 0_M) \\&\vdash \{ (a, m) : m \in M \}\end{aligned}$$

Notice that

$$\text{Spec}(\vdash) = \text{Hom}_{\mathbf{R}}(A, M)$$

Every  $\mu \in \text{Hom}_{\mathbf{R}}(A, B)$  induces an interpretation

$$i_\mu : (A \times M, \vdash) \rightarrow (B \times M, \vdash'), \quad (a, m) \rightarrow (\mu(a), m)$$

### Proposition

Suppose that  $\mathbf{K}$  is a non-trivial discrete field.

Let  $A, B$  be  $\mathbf{K}$ -vector spaces, and  $\mu \in \text{Hom}_{\mathbf{K}}(A, B)$  be injective.

Then  $i_\mu$  is weakly conservative.

### Proposition

Suppose that  $\mathbf{K}$  is a non-trivial discrete field.

Let  $A, B$  be  $\mathbf{K}$ -vector spaces, and  $\mu \in \text{Hom}_{\mathbf{K}}(A, B)$  be injective.

Then  $i_\mu$  is weakly conservative.

### Proof sketch.

Show that the following are equivalent:

1.  $(a_1, m_1), \dots, (a_k, m_k) \vdash$
2. There are  $\lambda_1, \dots, \lambda_k \in \mathbf{K}$  such that

$$\sum_{i=1}^k \lambda_i(a_i, m_i) = (0, 1).$$

□

### Proposition\*

Let  $A, B, M \in \mathbb{Z}\text{-Mod}$ , and  $\mu \in \text{Hom}_{\mathbb{Z}}(A, B)$  be injective.

If  $M$  is divisible, then  $i_{\mu}$  is weakly conservative.

### Proposition\*

Let  $A, B, M \in \mathbb{Z}\text{-Mod}$ , and  $\mu \in \text{Hom}_{\mathbb{Z}}(A, B)$  be injective.  
If  $M$  is divisible, then  $i_{\mu}$  is weakly conservative.

### Proof sketch.

Show that the following are equivalent:

1.  $(a_1, m_1), \dots, (a_k, m_k) \vdash$
2. There are  $n_1, \dots, n_k \in \mathbb{Z}$  and  $0 \neq c \in M$  such that

$$\sum_{i=1}^k n_i(a_i, m_i) = (0, c).$$

□

### Proposition\*

Suppose that  $\mathbf{R}$  is an integral ring.

Let  $A, B, M \in \mathbf{R}\text{-Mod}$  and  $\mu \in \text{Hom}_{\mathbf{R}}(A, B)$  be injective.

1. If  $M$  is torsion-free and divisible, then  $i_{\mu}$  is weakly conservative.
2. If  $\mathbf{R}$  is a Dedekind ring, and  $M$  is divisible, then  $i_{\mu}$  is weakly conservative.

In both cases, the classical arguments reapply.



# Summary

# Summary

- We have made combined use of ideas and principles from proof theory and formal topology.
- Hilbert's programme, i.e., the constructive explanation of ideal objects, works for large parts of abstract algebra.
- Statements involving ideal objects are cases of make-believe—however, often we can do “as if”, and gather computationally relevant information.

## References

- [Acz06] Peter Aczel. “Aspects of general topology in constructive set theory”. In: *Annals of Pure and Applied Logic* 137.1–3 (2006), pp. 3–29.
- [AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Reading, MA: Addison-Wesley Publishing Company, Inc., 1969.
- [Bel99] John L. Bell. “Boolean algebras and distributive lattices treated constructively”. In: *Mathematical Logic Quarterly* 45.1 (1999), pp. 135–143.

## References II

- [Ber13] Benno van den Berg. “Non-deterministic inductive definitions”. In: *Arch. Math. Logic* 52.1-2 (2013), pp. 113–135. ISSN: 0933-5846.
- [BR87] Douglas Bridges and Fred Richman. *Varieties of Constructive Mathematics*. Vol. 97. London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 1987.
- [BV96] B. Banaschewski and J.J.C Vermeulen. “Polynomials and radical ideals”. In: *Journal of Pure and Applied Algebra* 113.3 (1996), pp. 219–227.

- [CC00] Jan Cederquist and Thierry Coquand. “Entailment relations and distributive lattices”. In: *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*. Ed. by Samuel R. Buss, Petr Hájek, and Pavel Pudlák. Vol. 13. Lect. Notes Logic. Natick, MA: A. K. Peters, 2000, pp. 127–139.

## References IV

- [CCN98] Jan Cederquist, Thierry Coquand, and Sara Negri. “The Hahn-Banach theorem in type theory”. In: *Twenty-Five Years of Constructive Type Theory (Venice, 1995)*. Ed. by G. Sambin and J.M. Smith. Vol. 36. Oxford Logic Guides. Oxford University Press, New York, 1998, pp. 57–72.
- [CL06] Thierry Coquand and Henri Lombardi. “A logical approach to abstract algebra”. In: *Mathematical Structures in Computer Science* 16.5 (2006), pp. 885–900.

- [CLR01] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. “Dynamical method in algebra: Effective Nullstellensätze.” In: *Ann. Pure Appl. Logic* 111.3 (2001), pp. 203–256.
- [Coq+03] Thierry Coquand et al. “Inductively generated formal topologies”. In: *Ann. Pure Appl. Logic* 124 (2003), pp. 71–106.
- [Coq06] Thierry Coquand. “Geometric Hahn-Banach theorem”. In: *Math. Proc. Cambridge Philos. Soc.* 140 (2006), pp. 313–315.
- [Coq09] Thierry Coquand. “Space of valuations”. In: *Annals of Pure and Applied Logic* 157.2–3 (2009), pp. 97–109.



## References VI

- [CP01] Thierry Coquand and Henrik Persson. “Valuations and Dedekind’s Prague theorem”. In: *Journal of Pure and Applied Algebra* 155 (2001), pp. 121–129.
- [CZ] Thierry Coquand and Guo-Qiang Zhang. “Sequents, Frames, and Completeness”. In: *Computer Science Logic. 14th International Workshop, CSL 2000 Annual Conference of the EACSL*. Ed. by Helmut Schwichtenberg and Peter G. Clote.
- [CZ00] Thierry Coquand and Guo-Qiang Zhang. “Sequents, frames, and completeness”. In: *Computer Science Logic (Fischbachau, 2000)*. Ed. by Peter G. Clote and Helmut Schwichtenberg. Vol. 1862. Lecture Notes in Comput. Sci. Springer, Berlin, 2000, pp. 277–291.

- [Edw90] Harold M. Edwards. *Divisor Theory*. Birkhäuser Boston, 1990.
- [Eis04] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. Springer, 2004.
- [FG82] Michael Fourman and Robin Grayson. “Formal spaces”. In: *The L.E.J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*. Vol. 110. Stud. Logic Found. Math. Amsterdam: North-Holland, 1982, pp. 107–122.

## References VIII

- [IN16] Hajime Ishihara and Takako Nemoto. “Non-Deterministic Inductive Definitions and Fullness”. In: *Concepts of Proof in Mathematics, Philosophy, and Computer Science*. Ed. by D. Probst and P. Schuster. Vol. 6. Ontos Mathematical Logic. Berlin: Walter de Gruyter, 2016, pp. 163–170.
- [Joy75] André Joyal. “Les théorèmes de Chevalley-Tarski”. In: *Cahiers de topologie et géométrie différentielle catégoriques* 16.3 (1975), pp. 256–258.
- [LQ15] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*. Dordrecht: Springer Netherlands, 2015.

## References IX

- [M E05] Harold M. Edwards. *Essays in Constructive Mathematics*. New York: Springer, 2005.
- [Mat83] Eben Matlis. “The minimal prime spectrum of a reduced ring”. In: *Illinois Journal of Mathematics* 27.3 (1983), pp. 353–391.
- [MRR88] Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra*. Universitext. New York: Springer-Verlag, 1988.

## References X

- [MS04] Stephen McAdam and Richard G. Swan.  
“Factorizations of Monic Polynomials”. In: *Rings, Modules, Algebras, and Abelian Groups*. Ed. by Alberto Facchini, Evan Houston, and Luigi Salce. Vol. 236. Lecture Notes in Pure and Applied Mathematics. Marcel Dekker, 2004.
- [MW91] Christopher J. Mulvey and Joan Wick-Pelletier. “A globalization of the Hahn-Banach theorem”. In: *Advances in Mathematics* 89 (1991), pp. 1–59.
- [NPC04] Sara Negri, Jan von Plato, and Thierry Coquand.  
“Proof-theoretical analysis of order relations”. In: *Arch. Math. Logic* 43 (2004), pp. 297–309.

## References XI

- [Ric88] Fred Richman. “Nontrivial uses of trivial rings”. In: *Proceedings of the American Mathematical Society* 103.4 (1988), pp. 1012–1014.
- [Sam03] Giovanni Sambin. “Some points in formal topology”. In: *Theoretical Computer Science* 305.1-3 (2003), pp. 347–408.
- [Sco74] Dana Scott. “Completeness and axiomatizability in many-valued logic”. In: *Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. California, Berkeley, Calif., 1971)*. Ed. by Leon Henkin et al. Providence, RI: Amer. Math. Soc., 1974, pp. 411–435.

## References XII

- [VS72] P. Vámos and D. W. Sharpe. *Injective modules*. Cambridge Tracts in Mathematics and Mathematical Physics, 62. Cambridge University Press, 1972.
- [Wes18] Daniel Wessel. *A note on connected reduced rings*. 2018.
- [Yen03] Ihsen Yengui. “An algorithm for the divisors of monic polynomials over a commutative ring”. In: *Mathematische Nachrichten* 260.1 (2003), pp. 93–99.
- [Yen08] Ihsen Yengui. “Making the use of maximal ideals constructive.” In: *Theoret. Comput. Sci.* 392 (2008), pp. 174–178.

- [Yen15]    Ihsen Yengui. *Constructive commutative algebra. Projective modules over polynomial rings and dynamical Gröbner bases*. Vol. 2138. Lecture Notes in Mathematics. Cham: Springer, 2015.