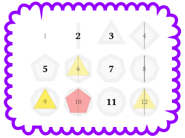
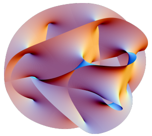
Generalized spaces for constructive algebra

1 Locales

2 Sheaf models



3 Constructive algebra



– an invitation –

Autumn school on Proof and Computation
September 20th to 26th, 2019
Herrsching

Ingo Blechschmidt
Università di Verona

Lecture I: **Locales**

Locales are a kind of space in which **opens** instead of **points** are fundamental.

These "probability clouds", replacing the reassuring material particles of before, remind me strangely of the elusive "open neighborhoods" that populate the topoi, like evanescent phantoms, to surround the imaginary "points".

– Alexander Grothendieck

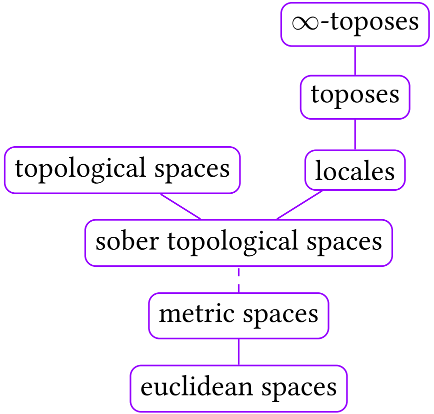
References include:

1. Peter Johnstone. The point of pointless topology, 1983.
2. Peter Johnstone. The art of pointless thinking: a student's guide to the category of locales, 1990.

Our metatheory is a constructive (no law of excluded middle, no choice principles of any kind) but impredicative (free use of the powerset axiom) flavor of English. The contents of this course could be formalized in the internal language of toposes or in IZF. The main ideas of this course are far more robust than this particular presentation, in particular, they can also be made sense of in a predicative setting (such as CZF or the internal language of arithmetic universes).

Locales in context

Definition. A **topological space** X consists of a **set of points** together with a set $\mathcal{O}(X)$ of point sets which are deemed **open** such that unions and finite intersections of open sets are open.



Nontrivial spaces without points

The following locales don't have any points and are nontrivial:

1. the locale of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$
2. $\mathbb{Q} \cap (\mathbb{R} \setminus \mathbb{Q})$
3. the pairwise intersections in the Banach–Tarski paradox
4. Alex Simpson's locale of random binary sequences

Relinquishing points increases flexibility.

The locale of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$ doesn't have any points, but it has lots of interesting opens, such as $U_{n,x}$, the "open of those surjections f such that $f(n) = x$. If x is a fixed real number and n ranges over the naturals, these opens cover the full locale.

The Banach–Tarski paradox is the unintuitive statement that a three-dimensional solid ball of radius r can be partitioned into six disjoint subsets in such a way that rearranging those subsets yields two solid balls of radius r each. These subsets are not measurable and require the axiom of choice for their construction.

The Banach–Tarski paradox can be resolved by adopting the axiom of determinacy instead of the axiom of choice, which entails that all subsets of $\mathbb{R}^3$ are measurable, or by passing from the topological space $\mathbb{R}^3$ to its localic cousin. The localic counterparts of the six pieces will still not have any points in common, but their locale-theoretic pairwise intersection will not be trivial.

Tom Leinster published an accessible exposition of the locale of random sequences at the n-category café.

Issues of constructivity

1. The unit interval $[0, 1]$ is **compact**.

2. **The fundamental theorem of Galois theory:** Let $L|k$ be a Galois extension. Then there is a bijection between

   the intermediate extensions $L|E|k$ and the closed subgroups of $\mathrm{Aut}_k(L)$.

$$\begin{array}{rcl} E & \longmapsto & \{\sigma \in \mathrm{Aut}_k(L) \mid \sigma|_E = \mathrm{id}\} \\ L^H & \longleftarrow & H \end{array}$$

3. **Gelfand duality:** The categories of

$$\text{compact Hausdorff spaces} \quad \text{and} \quad \begin{pmatrix} \text{commutative} \\ C^\star\text{-algebras with unit} \end{pmatrix}^{\mathrm{op}}$$

$$X \longmapsto \{f : X \to \mathbb{C} \mid f \text{ continuous}\}$$

   are equivalent.

By *compact*, we mean any open covering has a (Kuratowski-)finite subcovering. The topological space $[0, 1]$ fails to be compact in some flavors of constructive mathematics, but the localic unit interval is always compact.

In verifying the fundamental theorem of Galois theory, at some point one has to extend a given k-homomorphism $E \to L$ which is defined on some finite intermediate extension E to L. One-step extensions to larger intermediate extensions are no problem, but extending to all of L requires some form of choice. By passing from the topological Galois group to its localic group, this issue vanishes. References include the papers Galois theory in a topos and Localic groups by Gavin Wraith. Olivia Caramello's paper Topological galois theory is also relevant.

A similar issue arises with Gelfand duality. A fully constructive treatment is possible by passing from compact Hausdorff (topological) spaces to completely regular locales. This treatment unlocks the Bohr topos approach to quantum mechanics.

Localic basics

Definition. A **topological space** X consists of a **set of points** together with a set $\mathcal{O}(X)$ of point sets which are deemed **open** such that unions and finite intersections of open sets are open.

Observation. The partial order $\mathcal{O}(X)$ of open sets has

arbitrary joins $\bigvee$ and finite meets, $\wedge$

and finite meets distribute over arbitrary joins:

$$U \wedge \bigvee_i V_i = \bigvee_i (U \wedge V_i).$$

Localic basics

Definition. A **topological space** X consists of a **set of points** together with a set $\mathcal{O}(X)$ of point sets which are deemed **open** such that unions and finite intersections of open sets are open.

Observation. The partial order $\mathcal{O}(X)$ of open sets has

arbitrary joins and finite meets,
$\bigvee$ $\wedge$

and finite meets distribute over arbitrary joins:

$$U \wedge \bigvee_i V_i = \bigvee_i (U \wedge V_i).$$

Definition. A **frame** is a partial order with arbitrary joins and finite meets such that the distributive law holds.

Definition. A **locale** X is given by a **frame $\mathcal{O}(X)$ of opens**.

Example. Any topological space Y induces a locale $L(Y)$ by setting $\mathcal{O}(L(Y)) := \mathcal{O}(Y)$.

Example. The *one-point locale* pt is the locale induced by the one-point topological space $\{\heartsuit\}$. Its frame of opens is the powerset of $\{\heartsuit\}$, also known as the set Ω of truth values. Its least element is $\bot = \emptyset$ and its largest element is $\top = \{\heartsuit\}$.

Definition. A *frame homomorphism* $L \to L'$ is a monotone map $L \to L'$ which preserves arbitrary joins and finite meets.

Example. A continuous map $f : Y \to Y'$ induces a frame homomorphism $\mathcal{O}(Y') \to \mathcal{O}(Y)$ by mapping $U \mapsto f^{-1}[U]$.

Definition. A *locale morphism* $X \to X'$ is given by a frame homomorphism $\mathcal{O}(X') \to \mathcal{O}(X)$.

Example. A continuous map $Y \to Y'$ induces a locale morphism $L(Y) \to L(Y')$ in the same direction.

Definition. A *point* of a locale X is a locale morphism pt $\to X$, or equivalently a completely prime filter of $\mathcal{O}(X)$. (A frame morphism $\alpha : \mathcal{O}(X) \to \Omega$ gives rise to the completely prime filter $F := \{u \in \mathcal{O}(X) \mid \alpha(u) = \top\}$.)

Localic basics

Definition. A **topological space** X consists of a **set of points** together with a set $\mathcal{O}(X)$ of point sets which are deemed **open** such that unions and finite intersections of open sets are open.

Observation. The partial order $\mathcal{O}(X)$ of open sets has

arbitrary joins $\bigvee$ and finite meets, $\wedge$

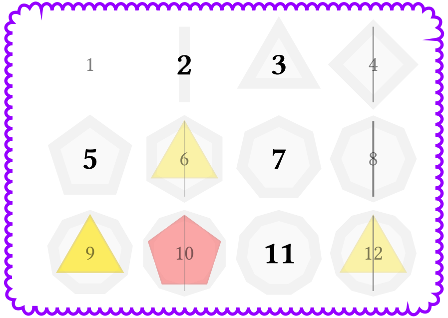
and finite meets distribute over arbitrary joins:

$$U \wedge \bigvee_i V_i = \bigvee_i (U \wedge V_i).$$

Definition. A **frame** is a partial order with arbitrary joins and finite meets such that the distributive law holds.

Definition. A **locale** X is given by a **frame $\mathcal{O}(X)$ of opens**.

The set of points of a locale can be made into a topological space, giving rise to a functor $\mathrm{pt} : \mathrm{Loc} \to \mathrm{Top}$. This functor is right adjoint to L. A locale X is *spatial* iff the canonical morphism $L(\mathrm{pt}(X)) \to X$ is an isomorphism, and a topological space Y is *sober* iff the canonical morphism $Y \to \mathrm{pt}(L(Y))$ is a homeomorphism.



Lecture II: **Sheaf models**

Sheaves allow us to explore mathematical objects from custom-tailored mathematical universes.

Frames presented by theories

Definition. A **geometric theory** consists of

1. a set of sorts: $X, Y, Z, \ldots$
2. a set of function symbols: $f : X \times Y \to Z, \ldots$
3. a set of relation symbols: $R \hookrightarrow X \times Y \times Z, \ldots$
4. a set of axioms: $\varphi \vdash_{x:X, y:Y} \psi, \ldots$

Examples. The theory of rings, of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$, of Dedekind cuts, of prime ideals of a given ring, …

Definition. A **set-based model** M of a theory $\mathbb{T}$ consists of

1. a set $[\![X]\!]$ for each sort X,
2. a function $[\![f]\!] : [\![X_1]\!] \times \cdots \times [\![X_n]\!] \to [\![Y]\!]$ for each function symbol $f : X_1 \times \cdots \times X_n \to Y$, and
3. a relation $[\![R]\!] \subseteq [\![X_1]\!] \times \cdots \times [\![X_n]\!]$ for each relation symbol $R \hookrightarrow X_1 \times \cdots \times X_n$

such that M validates the axioms of $\mathbb{T}$.

The formulas appearing to the left and the right of the turnstile in axioms of a geometric theory have to be *geometric formula*. A formula is *geometric* iff it is built using only $= \top \wedge \bot \vee \bigvee \exists$ (but no $\Rightarrow \forall$). Universal quantification and implication can to some extent be emulated by using free variables or the turnstile; but this allows universal quantification and implication only to be used once, on top level, not in nested subformulas.

A geometric theory is called *propositional* iff its set of sorts is empty. Hence the only ingredients of a propositional geometric theory are a set of nullary relation symbols (atomic propositions) and a set of axioms.

Frames presented by theories

Definition. A **geometric theory** consists of

1. a set of sorts: $X, Y, Z, \ldots$
2. a set of function symbols: $f : X \times Y \to Z, \ldots$
3. a set of relation symbols: $R \hookrightarrow X \times Y \times Z, \ldots$
4. a set of axioms: $\varphi \vdash_{x:X, y:Y} \psi, \ldots$

Examples. The theory of rings, of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$, of Dedekind cuts, of prime ideals of a given ring, …

Definition. A **set-based model** M of a theory $\mathbb{T}$ consists of

1. a set $[\![X]\!]$ for each sort X,
2. a function $[\![f]\!] : [\![X_1]\!] \times \cdots \times [\![X_n]\!] \to [\![Y]\!]$ for each function symbol $f : X_1 \times \cdots \times X_n \to Y$, and
3. a relation $[\![R]\!] \subseteq [\![X_1]\!] \times \cdots \times [\![X_n]\!]$ for each relation symbol $R \hookrightarrow X_1 \times \cdots \times X_n$

such that M validates the axioms of $\mathbb{T}$.

Example. The theory of rings has:

1. one sort: R
2. five constant symbols: 0 and 1 (nullary), $-$ (unary), $+$ and $\cdot$ (binary)
3. no relation symbols
4. the usual axioms, such as $\top \vdash_{x:R, y:R} x + y = y + x$

Example. The theory of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$ has:

1. no sorts
2. no function symbols
3. several nullary relation symbols, one for each pair $\langle n, x \rangle \in \mathbb{N} \times \mathbb{R}$, written "$\varphi_{nx}$"
4. axioms: the axiom $\top \vdash \bigvee_{x \in \mathbb{R}} \varphi_{nx}$ for each $n \in \mathbb{N}$; the axiom $\varphi_{nx} \wedge \varphi_{ny} \vdash \bigvee \{\top \mid x = y\}$ for each $n \in \mathbb{N}$, $x, y \in \mathbb{R}$ (the disjunction appearing in that axiom is over a subsingleton of formulas); the axiom $\top \vdash \bigvee_{n \in \mathbb{N}} \varphi_{nx}$ for each $x \in \mathbb{R}$

Frames presented by theories

Definition. A **geometric theory** consists of

1. a set of sorts: X, Y, Z, …
2. a set of function symbols: $f : X \times Y \to Z, \ldots$
3. a set of relation symbols: $R \hookrightarrow X \times Y \times Z, \ldots$
4. a set of axioms: $\varphi \vdash_{x:X, y:Y} \psi, \ldots$

Examples. The theory of rings, of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$, of Dedekind cuts, of prime ideals of a given ring, …

Definition. A **set-based model** M of a theory $\mathbb{T}$ consists of

1. a set $[\![X]\!]$ for each sort X,
2. a function $[\![f]\!] : [\![X_1]\!] \times \cdots \times [\![X_n]\!] \to [\![Y]\!]$ for each function symbol $f : X_1 \times \cdots \times X_n \to Y$, and
3. a relation $[\![R]\!] \subseteq [\![X_1]\!] \times \cdots \times [\![X_n]\!]$ for each relation symbol $R \hookrightarrow X_1 \times \cdots \times X_n$

such that M validates the axioms of $\mathbb{T}$.

Associated to any propositional geometric theory $\mathbb{T}$ is its *Lindenbaum algebra*. This is the set of formulas over the signature of the theory modulo provable equivalence. Endowed with the partial order given by

$$[\varphi] \leq [\psi] \quad :\Longleftrightarrow \quad \mathbb{T} \text{ proves } \varphi \vdash \psi,$$

the Lindenbaum algebra becomes a frame.

The Lindenbaum algebra of $\mathbb{T}$ is the free frame generated by the atomic propositions of $\mathbb{T}$ modulo the axioms of $\mathbb{T}$. The associated locale $L(\mathbb{T})$ is the *classifying locale of* $\mathbb{T}$. Its points are in canonical bijection with the set-based models of $\mathbb{T}$.

Definition. The *localic real line* is the classifying locale of the theory of Dedekind cuts. The *locale of surjections* $\mathbb{N} \twoheadrightarrow \mathbb{R}$ is the classifying locale of the theory of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$. The *empty locale* is the classifying locale of the *inconsistent theory* (which has no sorts, no function symbols, no relations symbols, and one axiom, namely $\top \vdash \bot$).

The points of the localic real line are in canonical bijection with the Dedekind cuts, hence with the elements of the set of (Dedekind) real numbers. The points of the locale of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$ are in canonical bijection with the surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$. Assuming a classical metatheory, there are no such points, but the locale is still nontrivial.

Frames presented by theories

Definition. A **geometric theory** consists of

1. a set of sorts: $X, Y, Z, \ldots$
2. a set of function symbols: $f : X \times Y \to Z, \ldots$
3. a set of relation symbols: $R \hookrightarrow X \times Y \times Z, \ldots$
4. a set of axioms: $\varphi \vdash_{x:X,y:Y} \psi, \ldots$

Examples. The theory of rings, of surjections $\mathbb{N} \twoheadrightarrow \mathbb{R}$, of Dedekind cuts, of prime ideals of a given ring, …

Definition. A **set-based model** M of a theory $\mathbb{T}$ consists of

1. a set $[\![X]\!]$ for each sort X,
2. a function $[\![f]\!] : [\![X_1]\!] \times \cdots \times [\![X_n]\!] \to [\![Y]\!]$ for each function symbol $f : X_1 \times \cdots \times X_n \to Y$, and
3. a relation $[\![R]\!] \subseteq [\![X_1]\!] \times \cdots \times [\![X_n]\!]$ for each relation symbol $R \hookrightarrow X_1 \times \cdots \times X_n$

such that M validates the axioms of $\mathbb{T}$.

Any locale is (isomorphic to) the classifying locale of some propositional geometric theory, namely the "theory of its points". The same locale can often be presented by widely different-looking theories, and the topos-theoretic version of this observation is the basis for Olivia Caramello's research program.

Exercise. Which explicit theory is the two-point locale (the locale induced from the discrete topological space $\{0, 1\}$) the classifying locale of?

Sheaves

Definition. A **presheaf** F on a locale X is given by

1. a set $F(U)$ for each open U of X and
2. a map $(\cdot)|^U_V : F(U) \to F(V)$ for each opens $V \leq U$

such that $(\cdot)|^U_U = \mathrm{id}_{F(U)}$ for all U and $(\cdot)|^V_W \circ (\cdot)|^U_V = (\cdot)|^U_W$ for all $W \leq V \leq U$. A **compatible family** with respect to a covering $U = \bigvee_i U_i$ is a family $(s_i)_i$ of sections $s_i \in F(U_i)$ such that $s_i|^{U_i}_{U_i \wedge U_j} = s_j|^{U_j}_{U_i \wedge U_j}$. F is a **sheaf** iff for any such family there is a unique section $s \in F(U)$ such that $s|^U_{U_i} = s_i$ for all i.

Example. The **sheaf of continuous functions** on a locale X is given by $\mathcal{C}(U) = \mathrm{Hom}(U, \mathbb{R})$.

Non-example. The **presheaf of constant functions**, $\mathcal{C}_c(U) =$ "the set of constant functions $U \to \mathbb{R}$", is usually not a sheaf.

All definitions on this slide literally also make sense for topological spaces instead of locales, since only the notion of opens and their inclusion relation is used.

The maps $(\cdot)|^U_V$ are called *restriction maps*. For the sheaf $\mathcal{C}$ of continuous real-valued functions, they are given by actual restriction of functions to smaller domains, that is by

$$\mathcal{C}(U) \longrightarrow \mathcal{C}(V),\ s \longmapsto s|_V.$$

Exercise. Find, in the case $X = [0, 1]$, a compatible family of sections of the presheaf $\mathcal{C}_c$ which shows that this presheaf is not a sheaf.

Sheaf semantics

Let X be a locale. We recursively define what it means for a **first-order formula over an open U of X** to be forced:

$U \models \top$	iff true
$U \models \bot$	iff ~~false~~ $U = \bot$
$U \models s = t$	iff $s = t$ when evaluated as elements of $F(U)$
$U \models \varphi \wedge \psi$	iff $U \models \varphi$ and $U \models \psi$
$U \models \varphi \vee \psi$	iff ~~$U \models \varphi$ or $U \models \psi$~~ there exists a covering $U = \bigvee_i U_i$ such that for all i: $U_i \models \varphi$ or $U_i \models \psi$
$U \models \varphi \Rightarrow \psi$	iff for all $V \leq U$: $V \models \varphi$ implies $V \models \psi$
$U \models \forall s : F.\, \varphi(s)$	iff for all $V \leq U$ and sections $s_0 \in F(V)$: $V \models \varphi(s_0)$
$U \models \exists s : F.\, \varphi(s)$	iff ~~there exists $s_0 \in F(U)$ such that $U \models \varphi(s_0)$~~ there exists a covering $U = \bigvee_i U_i$ such that for all i: there exists $s_0 \in F(U_i)$ such that $U_i \models \varphi(s_0)$

Theorem. If $U \models \varphi$ and if φ entails ψ intuitionistically, then $U \models \psi$.

A *formula over an open U of X* is a first-order formula (made up using $= \top \wedge \bot \vee \Rightarrow \forall \exists$) over the signature which has one sort for each sheaf F, one constant symbol of sort F for each section $s \in F(U)$, one function symbol $f : F \to G$ for each morphism of sheaves, and so on.

Proposition. The sheaf semantics is monotone and local in the following sense: If $V \leq U$, then $U \models \varphi$ implies $V \models \varphi$. If $U = \bigvee_i U_i$ and if $U_i \models \varphi$ for all i, then $U \models \varphi$.

Exercise. For any formula φ over any open U of any locale X, there is a largest open $V \leq U$ such that $V \models \varphi$. (Hint: Set $V := \bigvee\{W \leq U \mid W \models \varphi\}$ and exploit the monotonicity and locality of the sheaf semantics.)

Exercise. For any formula φ over any open U of any locale X, $U \models \neg\neg\varphi$ iff there exists an open $V \leq U$ which is dense in U such that $V \models \varphi$.

Internalizing parameter-dependence

Let X be a topological space. Let $(f_x)_{x \in X}$ be a continuous family of continuous functions $\mathbb{R} \to \mathbb{R}$ (that is, let a continuous function $X \times \mathbb{R} \to \mathbb{R}$, $(x, a) \mapsto f_x(a)$ be given). This family defines a sheaf morphism $f : \mathcal{C} \to \mathcal{C}$ by $f_U : \mathcal{C}(U) \to \mathcal{C}(U)$, $s \mapsto (x \mapsto f_x(s(x)))$.

- $X \models$ "$\mathcal{C}$ is the set of Dedekind real numbers".
- $X \models$ "the function $f : \mathcal{C} \to \mathcal{C}$ is continuous".
- Iff $f_x(-1) < 0$ for all $x \in X$, then $X \models f(-1) < 0$.
- Iff $f_x(+1) > 0$ for all $x \in X$, then $X \models f(+1) > 0$.
- Iff all f_x are increasing, then $X \models$ "f is increasing".
- Iff there is an open cover $X = \bigcup_i U_i$ such that for each i, there is a continuous function $s : U_i \to \mathbb{R}$ with $f_x(s(x)) = 0$ for all $x \in U_i$, then $X \models \exists s : \mathcal{C}.\, f(s) = 0$.

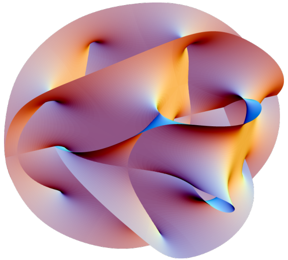
Hence:

1. The standard formulation of the intermediate value theorem fails in $\mathrm{Sh}(X)$, because its external interpretation is that in continuous families of continuous functions, zeros can locally be picked continuously. That claim is false, as this counterexample demonstrates.

   As a corollary, we deduce that the standard formulation of the intermediate value theorem is not constructively provable.

2. The *approximate* intermediate value theorem (stating that for any $\varepsilon > 0$, there is a number x such that $|f(x)| < \varepsilon$) has a constructive proof and therefore holds in $\mathrm{Sh}(X)$. The external interpretation is that in continuous families of continuous functions, approximate zeros can locally be picked continuously.

3. The *monotone* intermediate value theorem, stating that a strictly increasing continuous function with opposite signs has a unique zero, admits a constructive proof and therefore holds in $\mathrm{Sh}(X)$. The external interpretation is that in continuous families of strictly increasing continuous functions, zeros can globally be picked continuously. You are invited to prove this fact directly, without reference to the internal language. This exercise isn't particularly hard, but it's not trivial either.



Lecture III: **Applications in constructive algebra**

Without loss of generality, any reduced ring is a field.

A remarkable sheaf

Let A be a reduced ring ($x^n = 0 \Rightarrow x = 0$). Then there is a certain sheaf $A^\sim$ of rings on a certain locale X such that …

$A^\sim$ is close to A:

There is a **canonical bijection** $A \to A^\sim(X)$.
$A^\sim$ inherits any property of A which is **localization-stable**.
A geometric sequent holds for $A^\sim$ iff* it holds for **all stalks** $A_\mathfrak{f}$.

$A^\sim$ has better properties than A:

$A^\sim$ is a **field**: $\forall x : A^\sim.\, (\neg(\exists y : A^\sim.\, xy = 1) \Rightarrow x = 0)$.
$A^\sim$ has **¬¬-stable equality**: $\forall x, y : A^\sim.\, \neg\neg(x = y) \Rightarrow x = y$.
$A^\sim$ is **anonymously Noetherian**.

This observation can be exploited to give short, conceptual and constructive proofs.

Examples

Injective matrices

Let M be an injective matrix with more columns than rows over a ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal prime filter $\mathfrak{f} \subseteq A$. The matrix is injective over the field $A_{\mathfrak{f}}$; contradiction to basic linear algebra.

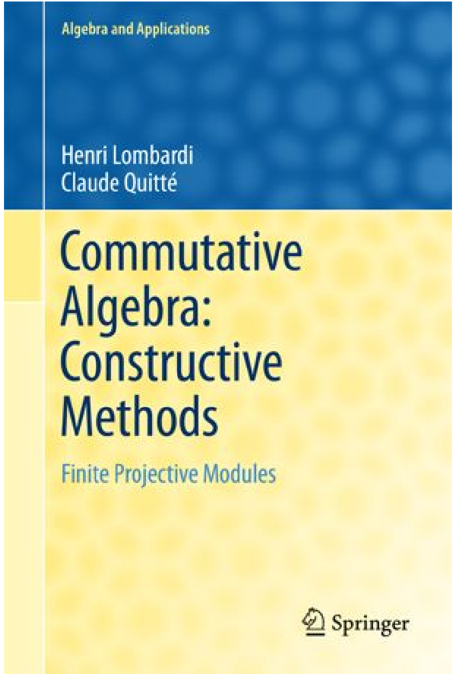
Proof. M is also injective as a matrix over $A^\sim$. This is a contradiction by basic linear algebra. Thus $X \models \bot$. This amounts to $1 = 0$ in A.

Generic freeness

Let M be a finitely generated A-module. If $f = 0$ is the only element of A such that $M[f^{-1}]$ is a free $A[f^{-1}]$-module, then $1 = 0$ in A.

Proof. See [Stacks Project].

Proof. The claim amounts to $X \models$ "$M^\sim$ is **not not** free". This statement follows from basic linear algebra over the field $A^\sim$.



The book is available on the arXiv and warmly recommended, as are all slides by Thierry Coquand on constructive algebra.«