# Ax-Grothendieck in lean

Joseph Hua

June 15, 2022

Imperial College London

# Motivation

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

**Examples**

- Surjective but not injective: $f : \mathbb{C} \to \mathbb{C} := x \mapsto x^2$

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

**Examples**

- Surjective but not injective: $f : \mathbb{C} \to \mathbb{C} := x \mapsto x^2$
- Neither surjective nor injective: $f : \mathbb{C}^2 \to \mathbb{C}^2 := (x, y) \mapsto (x, xy)$

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

**Examples**

- Surjective but not injective: $f : \mathbb{C} \to \mathbb{C} := x \mapsto x^2$
- Neither surjective nor injective: $f : \mathbb{C}^2 \to \mathbb{C}^2 := (x, y) \mapsto (x, xy)$
- Bijective: $f : \mathbb{C}^3 \to \mathbb{C}^3 := (x, y, z) \mapsto (x, y, z + xy)$

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

**Examples**

- Surjective but not injective: $f : \mathbb{C} \to \mathbb{C} := x \mapsto x^2$
- Neither surjective nor injective: $f : \mathbb{C}^2 \to \mathbb{C}^2 := (x, y) \mapsto (x, xy)$
- Bijective: $f : \mathbb{C}^3 \to \mathbb{C}^3 := (x, y, z) \mapsto (x, y, z + xy)$
- Bijective $f : \overline{\mathbb{F}_2} \to \overline{\mathbb{F}_2} := x \mapsto x^2$

# Polynomial maps

**Definition (Polynomial maps)**

Polynomial maps on a field $K$ are regular endomorphisms on $K^n$, i.e. $n$ polynomials in $K[x_1, \ldots, x_n]$.

**Examples**

- Surjective but not injective: $f : \mathbb{C} \to \mathbb{C} := x \mapsto x^2$
- Neither surjective nor injective: $f : \mathbb{C}^2 \to \mathbb{C}^2 := (x, y) \mapsto (x, xy)$
- Bijective: $f : \mathbb{C}^3 \to \mathbb{C}^3 := (x, y, z) \mapsto (x, y, z + xy)$
- Bijective $f : \overline{\mathbb{F}_2} \to \overline{\mathbb{F}_2} := x \mapsto x^2$
- Surjective but not injective $f : \overline{\mathbb{F}_3} \to \overline{\mathbb{F}_3} := x \mapsto x^2$

**Theorem (Ax-Grothendieck)**

*Any injective polynomial map over an algebraically closed field is surjective. In particular injective polynomial maps over $\mathbb{C}$ are surjective.*

# Ax-Grothendieck

**Theorem (Ax-Grothendieck)**
*Any injective polynomial map over an algebraically closed field is surjective. In particular injective polynomial maps over $\mathbb{C}$ are surjective.*

- Amazing fact (Lefschetz): true for a single algebraically closed field of characteristic $n$ (a model of $\mathsf{ACF}_n$) $\rightarrow$ true for any model of $\mathsf{ACF}_n$ ($n$ is zero or prime).

**Theorem (Ax-Grothendieck)**

*Any injective polynomial map over an algebraically closed field is surjective. In particular injective polynomial maps over $\mathbb{C}$ are surjective.*

- Amazing fact (Lefschetz): true for a single algebraically closed field of characteristic $n$ (a model of $\mathsf{ACF}_n$) $\rightarrow$ true for any model of $\mathsf{ACF}_n$ ($n$ is zero or prime).
- Amazing fact (Lefschetz): true for $\mathsf{ACF}_p$ for all large prime $p \rightarrow$ true for $\mathsf{ACF}_0$.

# Ax-Grothendieck

**Theorem (Ax-Grothendieck)**
*Any injective polynomial map over an algebraically closed field is surjective. In particular injective polynomial maps over $\mathbb{C}$ are surjective.*

- Amazing fact (Lefschetz): true for a single algebraically closed field of characteristic $n$ (a model of $\mathsf{ACF}_n$) $\to$ true for any model of $\mathsf{ACF}_n$ ($n$ is zero or prime).
- Amazing fact (Lefschetz): true for $\mathsf{ACF}_p$ for all large prime $p \to$ true for $\mathsf{ACF}_0$.
- Good news: We can easily show it for algebraic closures of finite fields.

# Locally finite fields

**Definition (Locally finite fields)**

Let $K$ be a field of characteristic $p$ a prime. Then the following are equivalent definitions for $K$ being a *locally finite field*:

1. The minimal subfield generated by any finite subset of $K$ is finite.

# Locally finite fields

**Definition (Locally finite fields)**

Let $K$ be a field of characteristic $p$ a prime. Then the following are equivalent definitions for $K$ being a *locally finite field*:

1. The minimal subfield generated by any finite subset of $K$ is finite.
2. $\mathbb{F}_p \to K$ is algebraic.

# Locally finite fields

**Definition (Locally finite fields)**

Let $K$ be a field of characteristic $p$ a prime. Then the following are equivalent definitions for $K$ being a *locally finite field*:

1. The minimal subfield generated by any finite subset of $K$ is finite.
2. $\mathbb{F}_p \to K$ is algebraic.
3. $K$ embeds into an algebraic closure of $\mathbb{F}_p$.

# Locally finite fields

**Definition (Locally finite fields)**

Let $K$ be a field of characteristic $p$ a prime. Then the following are equivalent definitions for $K$ being a *locally finite field*:

1. The minimal subfield generated by any finite subset of $K$ is finite.
2. $\mathbb{F}_p \to K$ is algebraic.
3. $K$ embeds into an algebraic closure of $\mathbb{F}_p$.

**Theorem**

*Locally finite fields satisfy Ax-Grothendieck.*

**Proof.**

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_p(\texttt{coeffs}) \hookrightarrow K$$

$$\downarrow_{\mathbb{F}_p(\texttt{coeffs})} \text{ respects injectivity}$$

$\square$

## The Lefschetz principle

**Theorem (Lefschetz principle)**

*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$*. (If you like* $\mathbb{C} \models \phi$*.)*

**Theorem (Lefschetz principle)**

*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$. *(If you like* $\mathbb{C} \models \phi$.*)*
2. $\mathsf{ACF}_0 \models \phi$

**Theorem (Lefschetz principle)**

*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of $\mathsf{ACF}_0$ satisfies $\phi$. (If you like $\mathbb{C} \models \phi$.)*
2. $\mathsf{ACF}_0 \models \phi$
3. *There exists $n \in \mathbb{N}$ such that for any prime $p$ greater than $n$, $\mathsf{ACF}_p \models \phi$*

**Theorem (Lefschetz principle)**
*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$*. (If you like* $\mathbb{C} \models \phi$*.)*
2. $\mathsf{ACF}_0 \models \phi$
3. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*,* $\mathsf{ACF}_p \models \phi$
4. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*, some model of* $\mathsf{ACF}_p$ *satisfies* $\phi$*.*

# Model Theory

# Languages

```
structure Language : Type (u+1) :=
  (functions : ℕ → Type u)
  (relations : ℕ → Type u)
```

# Languages

```
structure Language : Type (u+1) :=
  (functions : ℕ → Type u)
  (relations : ℕ → Type u)
```

**Definition (Language of rings)**
Let the following be the language of rings:

- The function symbols are the constant symbols $0, 1, +, \times$ for addition and multiplication and $-$ for taking additive inverse.
- There are no relation symbols.

# Languages

```
structure Language : Type (u+1) :=
  (functions : ℕ → Type u)
  (relations : ℕ → Type u)
```

**Definition (Language of rings)**

Let the following be the language of rings:

- The function symbols are the constant symbols $0$, $1$, $+$, $\times$ for addition and multiplication and $-$ for taking additive inverse.
- There are no relation symbols.

**More examples**

- Language of groups
- Language of monoid actions from a monoid $M$ and modules on a ring $A$
- Single binary relations

# Terms and formulas

Terms are “free algebraic expressions” on some number of variables, i.e. sensible combinations of variable and function symbols.

- Terms with $n$ variables in the language of rings can be interpreted as elements of $\mathbb{Z}[x_1, \ldots, x_n]$ (this will identify $x_1 + x_2$ and $x_2 + x_1$, which are *distinct terms*).

# Terms and formulas

Terms are "free algebraic expressions" on some number of variables, i.e. sensible combinations of variable and function symbols.

- Terms with $n$ variables in the language of rings can be interpreted as elements of $\mathbb{Z}[x_1, \dots, x_n]$ (this will identify $x_1 + x_2$ and $x_2 + x_1$, which are *distinct terms*).
- Terms with $n$ variables in the language of groups can be interpreted as elements of the free group on $\{x_1, \dots, x_n\}$.

# Terms and formulas

Terms are "free algebraic expressions" on some number of variables, i.e. sensible combinations of variable and function symbols.

- Terms with $n$ variables in the language of rings can be interpreted as elements of $\mathbb{Z}[x_1, \ldots, x_n]$ (this will identify $x_1 + x_2$ and $x_2 + x_1$, which are *distinct terms*).
- Terms with $n$ variables in the language of groups can be interpreted as elements of the free group on $\{x_1, \ldots, x_n\}$.
- Terms with $n$ variables in the language of modules over a ring $A$ can be interpreted as elements of the free module $A^{\oplus n}$.

# Terms and formulas

Terms are "free algebraic expressions" on some number of variables, i.e. sensible combinations of variable and function symbols.

- Terms with $n$ variables in the language of rings can be interpreted as elements of $\mathbb{Z}[x_1, \ldots, x_n]$ (this will identify $x_1 + x_2$ and $x_2 + x_1$, which are *distinct terms*).
- Terms with $n$ variables in the language of groups can be interpreted as elements of the free group on $\{x_1, \ldots, x_n\}$.
- Terms with $n$ variables in the language of modules over a ring $A$ can be interpreted as elements of the free module $A^{\oplus n}$.
- Terms with $n$ variables in the language of binary relations is just the set $\{x_1, \ldots, x_n\}$.

# Terms and formulas

Formulas are logical combinations of terms, equality, (and other relation symbols from the language if there are any).

$$x_0^2 + 2x_1 + 1 = x_2$$

We only need $\perp$, $=$, $\rightarrow$, $\forall$, and the relation symbols from the language.

# Terms and formulas

Formulas are logical combinations of terms, equality, (and other relation symbols from the language if there are any).

$$x_0^2 + 2x_1 + 1 = x_2$$

$$x_0^2 + 2x_1 + 1 = x_2 \ \rightarrow\ x_2 \neq x_0$$

We only need $\perp$, $=$, $\rightarrow$, $\forall$, and the relation symbols from the language.

# Terms and formulas

Formulas are logical combinations of terms, equality, (and other relation symbols from the language if there are any).

$$x_0^2 + 2x_1 + 1 = x_2$$

$$x_0^2 + 2x_1 + 1 = x_2 \;\to\; x_2 \neq x_0$$

$$\forall x_2\, x_1, \exists x_0, x_0^2 + 2x_1 + 1 = x_2 \;\to\; x_2 \neq x_0$$

We only need $\perp, =, \to, \forall$, and the relation symbols from the language.

# Structures in a language

If $L$ is a language and $M$ is a set then an $L$-*structure* on $M$ consists of the following

- Each function symbol $f$ of arity $n$ is interpreted as a function $M^n \to M$.

# Structures in a language

If $L$ is a language and $M$ is a set then an $L$-*structure* on $M$ consists of the following

- Each function symbol $f$ of arity $n$ is interpreted as a function $M^n \to M$.
- Each relation symbol $r$ of arity $n$ is interpreted as a proposition on $M^n \to \texttt{Prop}$, or equivalently as a subset $S \hookrightarrow M^n$.

# Structures in a language

If $L$ is a language and $M$ is a set then an $L$-*structure* on $M$ consists of the following

- Each function symbol $f$ of arity $n$ is interpreted as a function $M^n \to M$.
- Each relation symbol $r$ of arity $n$ is interpreted as a proposition on $M^n \to \mathtt{Prop}$, or equivalently as a subset $S \hookrightarrow M^n$.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{F}_p, \{0\}$ can be made into structures in the language of rings.

# Structures in a language

If $L$ is a language and $M$ is a set then an *$L$-structure* on $M$ consists of the following

- Each function symbol $f$ of arity $n$ is interpreted as a function $M^n \to M$.
- Each relation symbol $r$ of arity $n$ is interpreted as a proposition on $M^n \to \texttt{Prop}$, or equivalently as a subset $S \hookrightarrow M^n$.

  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{F}_p, \{0\}$ can be made into structures in the language of rings.

  $\varnothing$ cannot be.

# Structures

Fix a structure $M$ in a language $L$. Terms with $n$ variables are interpreted as functions from the structure to itself.

# Structures

Fix a structure $M$ in a language $L$. Terms with $n$ variables are interpreted as functions from the structure to itself.

- Variables are interpreted as projection to an affine line.

# Structures

Fix a structure $M$ in a language $L$. Terms with $n$ variables are interpreted as functions from the structure to itself.

- Variables are interpreted as projection to an affine line.

Formulas with $n$ free variables are interpreted as predicates on the structure in the obvious way.

# Structures

Fix a structure $M$ in a language $L$. Terms with $n$ variables are interpreted as functions from the structure to itself.

- Variables are interpreted as projection to an affine line.

Formulas with $n$ free variables are interpreted as predicates on the structure in the obvious way. Example: $b$, $c$ are elements of $M$ then

$$\forall x_0, x_0^2 + 2x_1 + 1 = x_2$$

applied to $b$, $c$ is interpreted as the proposition

“for all $a$ in $M$, $a^2 + 2b + 1 = c$”

# Models

A theory is a set of sentences (formulas with no free variables), a model is a structure that satisfies all those sentences.

# Models

A theory is a set of sentences (formulas with no free variables), a model is a structure that satisfies all those sentences. The theory of rings contains the sentences corresponding to the axioms of a ring.

# Models

A theory is a set of sentences (formulas with no free variables), a model is a structure that satisfies all those sentences. The theory of rings contains the sentences corresponding to the axioms of a ring. Example: commutativity of multiplication

```
def mul_comm : sentence ring_signature :=
  ∀' ∀' ( x_ 0 * x_ 1 ≃ x_ 1 * x_ 0 )
```

# Models

A theory is a set of sentences (formulas with no free variables), a model is a structure that satisfies all those sentences. The theory of rings contains the sentences corresponding to the axioms of a ring. Example: commutativity of multiplication

```
def mul_comm : sentence ring_signature :=
  ∀' ∀' ( x_ 0 * x_ 1 ≃ x_ 1 * x_ 0 )
```

- Ring axioms
- Field axioms $=$ ring axioms $\cup$ inverse $\cup\ 0 \neq 1$
- ACF
- Characteristic

# Models

A theory is a set of sentences (formulas with no free variables), a model is a structure that satisfies all those sentences. The theory of rings contains the sentences corresponding to the axioms of a ring. Example: commutativity of multiplication

```
def mul_comm : sentence ring_signature :=
  ∀' ∀' ( x_ 0 * x_ 1 ≃ x_ 1 * x_ 0 )
```

- Ring axioms
- Field axioms = ring axioms $\cup$ inverse $\cup$ $0 \neq 1$
- ACF
- Characteristic

# The Lefschetz principle

**Theorem (Lefschetz principle)**

*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$*. (If you like* $\mathbb{C} \vDash \phi$*.)*
2. $\mathsf{ACF}_0 \vDash \phi$
3. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*,* $\mathsf{ACF}_p \vDash \phi$
4. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*, some model of* $\mathsf{ACF}_p$ *satisfies* $\phi$*.*

# The Lefschetz principle

**Theorem (Lefschetz principle)**

*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$. *(If you like* $\mathbb{C} \vDash \phi$.*)*
2. $\mathsf{ACF}_0 \vDash \phi$
3. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$, $\mathsf{ACF}_p \vDash \phi$
4. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$, *some model of* $\mathsf{ACF}_p$ *satisfies* $\phi$.

**Proof.**

(1. $\leftrightarrow$ 2.) *and* (3. $\leftrightarrow$ 4.) *"*$\mathsf{ACF}_n$ *is complete" by Vaught's test.*

**Theorem (Lefschetz principle)**
*Let $\phi$ be a sentence in the language of rings. Then the following are equivalent:*

1. *Some model of* $\mathsf{ACF}_0$ *satisfies* $\phi$*. (If you like* $\mathbb{C} \vDash \phi$*.)*
2. $\mathsf{ACF}_0 \vDash \phi$
3. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*,* $\mathsf{ACF}_p \vDash \phi$
4. *There exists* $n \in \mathbb{N}$ *such that for any prime* $p$ *greater than* $n$*, some model of* $\mathsf{ACF}_p$ *satisfies* $\phi$*.*

**Proof.**
(1. $\leftrightarrow$ 2.) *and* (3. $\leftrightarrow$ 4.) *"*$\mathsf{ACF}_n$ *is complete" by Vaught's test.*

(2. $\leftrightarrow$ 3.) *"*$\chi$*-change" by compactness theorem.* $\square$

# Ax-Grothendieck proof

$$
\begin{tikzcd}
\text{(algebraic) Ax-G for } \overline{\mathbb{F}_p} \arrow[d, "\text{i-soundness}"] & & \\
\text{(model th.) Ax-G for } \overline{\mathbb{F}_p} \arrow[d, "\mathsf{ACF}_p \text{ is complete}"] & & \\
\text{(model th.) } \chi_p \text{ Ax-G} \arrow[r, "\text{i-completeness}"'] \arrow[d, "\text{Lefschetz } \chi\text{-change}"] & \text{(algebraic) } \chi_p \text{ Ax-G} \arrow[dr] & \\
\text{(model th.) } \chi_0 \text{ Ax-G} \arrow[r, "\text{i-completeness}"'] & \text{(algebraic) } \chi_0 \text{ Ax-G} \arrow[r, "\text{case on } \chi"] & \text{(algebraic) Ax-G}
\end{tikzcd}
$$