

Proof of the Ax-Grothendieck Theorem

Shivansh Gour

CMU-Pitt Directed Reading Program

First-Order Structure

A **structure** $\mathcal{M}$ for a signature σ consists of:

- ▶ A non-empty *domain* (universe) M
- ▶ Interpretations of each symbol in σ :
functions $f^{\mathcal{M}}: M^n \rightarrow M$,
relations $R^{\mathcal{M}} \subseteq M^n$,
constants $c^{\mathcal{M}} \in M$

Examples of Structures

- ▶ $(\mathbb{C}, +, \cdot, 0, 1)$ — a field
- ▶ $(\mathbb{N}, +, \cdot, 0, 1)$ — the natural numbers

Theory & Completeness

A **theory** T is a set of sentences in a fixed language.

- ▶ $\mathcal{M} \models T$: $\mathcal{M}$ is a *model* of T
- ▶ T is **complete** if for every sentence φ ,
$$T \models \varphi \quad \text{or} \quad T \models \neg \varphi$$

Example of a Model

Peano Arithmetic (PA) is a theory in the language of arithmetic. $(\mathbb{N}, +, \cdot, 0, 1)$ is a model of PA: every axiom of PA is true in $\mathbb{N}$.

ACF_p : Algebraically Closed Fields of Characteristic p

ACF_p is the theory of algebraically closed fields of characteristic p . Every polynomial over the field splits completely; $\text{char} = p$ (or 0).

Bijection over a Finite Set

Let A be a **finite** set. For any function $f: A \rightarrow A$:

$$f \text{ injective} \iff f \text{ surjective}$$

Key Blackboxed Facts

- ▶ ACF_p is **complete** for all $p \geq 0$
- ▶ $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

Consistent Theory

A theory T is **consistent** if it has at least one model — i.e. there exists a structure $\mathcal{M}$ such that $\mathcal{M} \models T$.

Compactness Theorem

T is **consistent** if and only if every **finite** subset $T_0 \subset_{\text{fin}} T$ is consistent.

Theorem (Ax, Grothendieck)

Let K be an **algebraically closed field** and $f: K \rightarrow K$ a **polynomial function**.

$$f \text{ injective} \implies f \text{ surjective}$$

Remarks:

- ▶ Grothendieck's original proof used algebraic geometry.
- ▶ Ax gave an elementary **model-theoretic** proof via compactness.
- ▶ The key: completeness of ACF_p — every ACF of char 0 and $\overline{\mathbb{F}_p}$ satisfy the *same* first-order sentences.
- ▶ This generalizes to arbitrary dimensions K^n as well, but in the interest of sanity we will restrict ourselves to the case $n = 1$.

For each $n \in \mathbb{N}$, define the sentence φ_n quantifying over *all* degree- n polynomials:

φ_n : injectivity implies surjectivity for all degree- n polynomials

$$\forall a_0 \cdots \forall a_n \left[\left(\forall x \forall y \, a_n x^n + \cdots + a_0 = a_n y^n + \cdots + a_0 \rightarrow x = y \right) \rightarrow \left(\forall y \, \exists x \, a_n x^n + \cdots + a_0 = y \right) \right]$$

Reduction

Ax-Grothendieck $\iff \text{ACF}_p \models \varphi_n$ for every $n \in \mathbb{N}$ and every $p \geq 0$.

Finite Characteristic: $T_{ACF_p} \models \varphi_n$

Goal: Show every model of T_{ACF_p} satisfies φ_n , for every prime p and every $n \in \mathbb{N}$.

Setup

Let p be prime (field characteristic is always 0 or prime). The algebraic closure $\overline{\mathbb{F}_p} = \bigcup_{m \geq 1} \mathbb{F}_{p^m}$ is a union of **finite** fields, and $\overline{\mathbb{F}_p} \models T_{ACF_p}$ since it is algebraically closed of characteristic p .

Proof that $\overline{\mathbb{F}_p} \models \varphi_n$

Suppose $f: (\overline{\mathbb{F}_p}) \rightarrow (\overline{\mathbb{F}_p})$ is injective.

1. Any input lies in $(\mathbb{F}_{p^m})$ for some m ; f maps $(\mathbb{F}_{p^m}) \rightarrow (\mathbb{F}_{p^m})$.
2. $\mathbb{F}_{p^m}$ is **finite**: $\text{inj} \implies \text{surj}$ on $(\mathbb{F}_{p^m})$.
3. Since every $\mathbf{y} \in (\overline{\mathbb{F}_p})$ lies in some $\mathbb{F}_{p^m}$, f is surjective on $\overline{\mathbb{F}_p}$.
4. ACF_p is **complete** and $\overline{\mathbb{F}_p} \models T_{ACF_p}$, so every model of T_{ACF_p} satisfies φ_n .

Characteristic 0 via Compactness (I)

Goal: Show $\text{ACF}_0 \models \varphi_n$ for every $n \in \mathbb{N}$.

Since ACF_0 is **complete**, for any ACF K of characteristic 0:

$$\text{ACF}_0 \models \varphi_n \iff \text{ACF}_0 \cup \{\neg\varphi_n\} \text{ is inconsistent}$$

By Compactness

$\text{ACF}_0 \cup \{\neg\varphi_n\}$ inconsistent $\iff$ some **finite** $T_0 \subset_{\text{fin}} \text{ACF}_0 \cup \{\neg\varphi_n\}$ is inconsistent.

Any finite $T_0 \subset_{\text{fin}} \text{ACF}_0$ only involves *finitely many* characteristic-0 axioms. Recall ACF_0 contains, for each prime q :

$$\chi_q = \underbrace{1 + 1 + \cdots + 1}_q \neq 0$$

A finite T_0 can only exclude *finitely many* primes.

Key Point

Choose prime $p > n$ large enough that T_0 avoids χ_p . Then T_0 is **consistent with ACF_p** .

Characteristic 0 via Compactness (II): Completing the Proof

The Compactness Argument

1. Fix n . Suppose for contradiction $\text{ACF}_0 \models \neg\varphi_n$.
2. By completeness of ACF_0 : no model of ACF_0 satisfies φ_n .
3. By compactness: some finite $T_0 \subset_{\text{fin}} \text{ACF}_0 \cup \{\neg\varphi_n\}$ is inconsistent.
4. T_0 involves finitely many axioms $\chi_{q_1}, \dots, \chi_{q_k}$ (char-0 axioms). Pick a prime p larger than all of $n, q_1, \dots, q_k$. Then $T_0 \subset_{\text{fin}} T_{\text{ACF}_p} \cup \{\neg\varphi_n\}$.
5. But every model of T_{ACF_p} satisfies φ_n (previous slide), so $T_{\text{ACF}_p} \cup \{\neg\varphi_n\}$ is inconsistent — contradiction. $\Rightarrow \times$

Conclusion

Any **injective** polynomial $f: K \rightarrow K$ over an **alg. closed field** is **surjective**. ■

- Note that this means any injective polynomial from $\mathbb{C}$ to $\mathbb{C}$ is surjective!

Thank You :D