Ax–Grothendieck via model theory

Will Troiani

May 3, 2026

1 Transporting proofs

It is common practice to observe that certain hypotheses were not used inside a proof, and to conclude that the proof still holds in a more general setting. For instance, every ring R has at most one additive identity: if 0 and $0'$ are both additive identities, then

$$0 = 0 + 0' = 0' + 0 = 0',$$

so $0 = 0'$. The proof never refers to the multiplicative structure, so it holds in any abelian group.

We can make this precise using first order logic. Consider the first order theory of rings.

Definition 1.0.1. We define $\mathcal{R}$, the first order theory of rings, beginning with the first order language of rings. Let Σ be a signature consisting of a single sort A. We introduce 5 function symbols.

- $0, 1 : A$,
- $- : A \longrightarrow A$,
- $+, \cdot : A \times A \longrightarrow A$.

The first order language of rings has no relation symbols.

The axioms are given as follows.

$$\forall x \forall y \forall z,\ (x + y) + z = x + (y + z) \tag{1}$$
$$\forall x \forall y,\ x + y = y + x \tag{2}$$
$$\forall x,\ x + 0 = x \tag{3}$$
$$\forall x,\ x + (-x) = 0 \tag{4}$$
$$\forall x \forall y \forall z,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{5}$$
$$\forall x \forall y,\ x \cdot y = y \cdot x \tag{6}$$
$$\forall x,\ x \cdot 1 = x \tag{7}$$
$$\forall x \forall y \forall z,\ x \cdot (y + z) = x \cdot y + x \cdot z \tag{8}$$

This set of formulas forms the axioms of $\mathcal{R}$.

The following proof tree π shows that, given any witness y, the only element x with $x + y = y$ is $x = 0$. That is, additive identities are unique once a witness y is fixed.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x+y=y]^1}{(x+y)+(-y)=y+(-y)}=E \quad \dfrac{\forall a \forall b \forall c,\ (a+b)+c=a+(b+c)}{(x+y)+(-y)=x+(y+(-y))}\forall E}{x+(y+(-y))=y+(-y)}=E \quad \dfrac{\forall a,\ a+(-a)=0}{y+(-y)=0}\forall E}{x+0=0}=E \quad \dfrac{\forall a,\ a+0=a}{x+0=x}\forall E}{x=0}=E}{x+y=y \Rightarrow x=0}\Rightarrow I^1}{\forall x,\ x+y=y \Rightarrow x=0}\forall I}{\forall y \forall x,\ x+y=y \Rightarrow x=0}\forall I$$

The first order theory of abelian groups $\mathcal{A}$ has only one sort, only three function symbols

- $0 : A$
- $- : A \longrightarrow A$
- $+ : A \times A \longrightarrow A$

and consists of the first four axioms listed in Definition 1.0.1. The proof π uses only axioms which appear in $\mathcal{A}$, so π is also a proof in $\mathcal{A}$. By the soundness theorem [1], this property holds in every abelian group.

This is a trivial example: there was no need to consider rings in the first place. The goal of this note is to apply the same technique non-trivially. We will prove the Ax–Grothendieck theorem.

2 Ax–Grothendieck Theorem

The Ax–Grothendieck theorem was independently discovered by James Ax and Alexander Grothendieck [2, 3]. These notes follow Swanson's blog post [5].

Theorem 2.0.1 (Ax–Grothendieck)**.** *Let $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a polynomial map. If f is injective, then f is surjective.*

We will proceed by first defining the first order theory of fields.

Definition 2.0.2. We define $\mathcal{F}$, the first order theory of fields, beginning with the first order language of fields. Let Σ be a signature consisting of a single sort A. We introduce 5 function symbols.

- $0, 1 : A$,
- $- : A \longrightarrow A$,
- $+, \cdot : A \times A \longrightarrow A$.

The first order language of fields has no relation symbols.

The axioms are given as follows.

$$\forall x \forall y \forall z,\ (x+y)+z = x+(y+z) \tag{9}$$
$$\forall x \forall y,\ x+y = y+x \tag{10}$$
$$\forall x,\ x+0 = x \tag{11}$$
$$\forall x,\ x+(-x) = 0 \tag{12}$$
$$\forall x \forall y \forall z,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{13}$$
$$\forall x \forall y,\ x \cdot y = y \cdot x \tag{14}$$
$$\forall x,\ x \cdot 1 = x \tag{15}$$
$$\forall x \forall y \forall z,\ x \cdot (y+z) = x \cdot y + x \cdot z \tag{16}$$
$$0 \neq 1 \tag{17}$$
$$\forall x,\ \big(x \neq 0 \Rightarrow \exists y,\ x \cdot y = 1\big) \tag{18}$$

This set of formulas forms the axioms of $\mathcal{F}$.

We extend this to the first order theory of algebraically closed fields of characteristic p, where p is either prime or 0. Define the following first order sentences.

Definition 2.0.3. For each $d \geq 1$, define

$$P_d := \forall a_0 \ldots \forall a_d,\ \big(a_d \neq 0\ \Rightarrow\ \exists x,\ a_0 + a_1 x + \ldots + a_{d-1}x^{d-1} + a_d x^d = 0\big).$$

For each prime number p, define

$$S_p := \underbrace{1 + \ldots + 1}_{p \text{ instances of } 1} = 0. \tag{19}$$

Definition 2.0.4. The first order theory $\mathcal{ACF}$ of **algebraically closed fields** consists of all axioms of $\mathcal{F}$ together with P_d for each $d \geq 1$.

The first order theory $\mathcal{ACF}_p$ of **algebraically closed fields of characteristic** p (for p prime) consists of $\mathcal{ACF}$ together with S_p.

The first order theory $\mathcal{ACF}_0$ of **algebraically closed fields of characteristic** 0 consists of $\mathcal{ACF}$ together with $\neg S_p$ for each prime p.

Theorem 2.0.1 will follow from a corresponding statement in finite characteristic.

Lemma 2.0.5. *Let p be a prime, and let $f : \overline{\mathbb{F}_p}^n \longrightarrow \overline{\mathbb{F}_p}^n$ be a polynomial map. If f is injective, then f is surjective.*

Proof. Let $\underline{y} = (y_1, \ldots, y_n) \in \overline{\mathbb{F}_p}^n$ be arbitrary. Let $K \subseteq \overline{\mathbb{F}_p}$ be the subfield generated over $\mathbb{F}_p$ by $y_1, \ldots, y_n$ and the (finitely many) coefficients of the coordinate polynomials of f. These elements are algebraic over $\mathbb{F}_p$, and there are only finitely many of them, so $K/\mathbb{F}_p$ is a finite extension. Hence K is finite. Since fields are closed under polynomial expressions, $f(K^n) \subseteq K^n$. The restriction $f|_{K^n} : K^n \longrightarrow K^n$ is injective, hence bijective, since K^n is finite. As $\underline{y} \in K^n$, there exists $\underline{z} \in K^n \subseteq \overline{\mathbb{F}_p}^n$ with $f(\underline{z}) = \underline{y}$. $\square$

Corollary 2.0.6. *Let k be an algebraically closed field, and let $f : k^n \longrightarrow k^n$ be a polynomial map. If f is injective, then f is surjective.*

Proof. We need to encode the statement as a first order sentence; this requires fixing both the dimension n and a degree bound d. Let

$$M_{n,d} = \left\{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : |\alpha| \leq d\right\}$$

be the finite set of monomial multi-indices of total degree at most d. For each coordinate $i \in \{1, \ldots, n\}$ and each $\alpha \in M_{n,d}$, introduce a coefficient variable $c_{i,\alpha}$, and write

$$F_i(x_1, \ldots, x_n) = \sum_{\alpha \in M_{n,d}} c_{i,\alpha}\, x^\alpha.$$

Let $\underline{c}$ denote the tuple of all coefficient variables, $\underline{x}, \underline{y}, \underline{z}$ denote n-tuples of variables, and write $F(\underline{x}) = F(\underline{y})$ for the conjunction $F_1(\underline{x}) = F_1(\underline{y}) \wedge \ldots \wedge F_n(\underline{x}) = F_n(\underline{y})$. Define

$$\begin{aligned} B_{n,d} := \forall \underline{c} \Big[\big(\forall \underline{x}\, \forall \underline{y},\ F(\underline{x}) = F(\underline{y}) \Rightarrow \underline{x} = \underline{y}\big) \\ \Rightarrow\ \big(\forall \underline{z}\, \exists \underline{x},\ F(\underline{x}) = \underline{z}\big) \Big]. \end{aligned}$$

This is a first order sentence: n and d are fixed, so there are only finitely many coefficient variables and finitely many monomials. (A polynomial of degree less than d is captured by setting some $c_{i,\alpha} = 0$.)

Fix a prime p. By Lemma 2.0.5, $\overline{\mathbb{F}_p} \models B_{n,d}$. Since $\overline{\mathbb{F}_p}$ is a model of $\mathcal{ACF}_p$, soundness rules out $\mathcal{ACF}_p \vdash \neg B_{n,d}$. By completeness of $\mathcal{ACF}_p$ (Corollary 2.0.12, below), $\mathcal{ACF}_p \vdash B_{n,d}$.

Now $\mathcal{ACF}_0$ is also complete, so either $\mathcal{ACF}_0 \vdash B_{n,d}$ or $\mathcal{ACF}_0 \vdash \neg B_{n,d}$. Suppose for contradiction $\mathcal{ACF}_0 \vdash \neg B_{n,d}$, with proof π. Since π is finite, only finitely many axioms $\neg S_{r_1}, \ldots, \neg S_{r_m}$ from the characteristic-zero scheme appear in π. Choose a prime $q \notin \{r_1, \ldots, r_m\}$. In any field of characteristic q, each $\neg S_{r_i}$ holds, since $r_i \neq q$ implies $r_i \cdot 1 \neq 0$. Hence the same finite argument can be reproduced over $\mathcal{ACF}_q$, giving $\mathcal{ACF}_q \vdash \neg B_{n,d}$. This contradicts the previous paragraph applied at $p = q$. Therefore $\mathcal{ACF}_0 \vdash B_{n,d}$, and by soundness applied to $k \models \mathcal{ACF}_0$, we have $k \models B_{n,d}$.

Any particular polynomial map $f : k^n \longrightarrow k^n$ has degree at most some d, so injectivity implies surjectivity. □

Theorem 2.0.1 follows from Corollary 2.0.6 applied to $k = \mathbb{C}$.

It remains to establish completeness of $\mathcal{ACF}_p$ for each $p \in \{0\} \cup \{\text{primes}\}$. We use the Łoś–Vaught test.

Theorem 2.0.7 (Löwenheim–Skolem, upward)**.** *Let $\mathcal{T}$ be a first order theory in a countable language. If $\mathcal{T}$ has an infinite model, then for every infinite cardinal κ, $\mathcal{T}$ has a model of cardinality κ.*

Lemma 2.0.8 (Łoś–Vaught test)**.** *Let $\mathcal{T}$ be a first order theory in a countable signature with no finite models. If there exists an uncountable cardinal κ such that all models of $\mathcal{T}$ of cardinality κ are isomorphic, then $\mathcal{T}$ is complete.*

We verify the hypotheses for $\mathcal{ACF}_p$.

Lemma 2.0.9. *If k is an algebraically closed field, then k is infinite.*

Proof. Suppose k is finite. Then

$$f(x) = 1 + \prod_{\alpha \in k} (x - \alpha) \in k[x]$$

satisfies $f(\alpha) = 1 \neq 0$ for every $\alpha \in k$, contradicting algebraic closedness. □

We need one fact about cardinalities of algebraically closed fields. We will not reprove existence of algebraic closures here; see [4] for a standard treatment.

Lemma 2.0.10. *Let F be a field with algebraic closure $\overline{F}$.*

- *If F is infinite, then $|\overline{F}| = |F|$.*
- *If F is finite, then $|\overline{F}| = \aleph_0$.*

Proof. Every element of $\overline{F}$ is a root of some nonzero polynomial in $F[x]$, and each polynomial has finitely many roots, so $|\overline{F}| \leq |F[x]| \cdot \aleph_0 = \max(|F|, \aleph_0)$. Conversely $F \subseteq \overline{F}$ gives $|F| \leq |\overline{F}|$, and $\overline{F}$ is infinite by Lemma 2.0.9. □

Lemma 2.0.11 (κ-categoricity)**.** *Let p be either a prime or 0, and let κ be an uncountable cardinal. Up to isomorphism, there is exactly one algebraically closed field of characteristic p and cardinality κ.*

Proof. Let $k_p = \mathbb{F}_p$ if p is prime, and $k_p = \mathbb{Q}$ if $p = 0$, so k_p is the prime field. Let T be a set of cardinality κ. Form the rational function field $k_p(T)$, and let K be its algebraic closure. Since κ is uncountable, $|k_p(T)| = \kappa$, and Lemma 2.0.10 gives $|K| = \kappa$. Hence at least one such field exists.

For uniqueness, let K, K' be algebraically closed of characteristic p and cardinality κ. Choose a transcendence basis $T \subseteq K$ for K over k_p, and a transcendence basis $T' \subseteq K'$ for K' over k_p. Then K is algebraic over $k_p(T)$ and K' is algebraic over $k_p(T')$. Lemma 2.0.10 applied to $k_p(T)$ and $k_p(T')$ together with $|K| = |K'| = \kappa > \aleph_0$ forces $|T| = |T'| = \kappa$. Any bijection $T \to T'$ extends uniquely to a k_p-isomorphism $k_p(T) \to k_p(T')$, which extends (by the universal property of algebraic closures) to an isomorphism $K \to K'$. □

Corollary 2.0.12. *Each of $\mathcal{ACF}_0$ and $\mathcal{ACF}_p$ for p prime is complete.*

Proof. By Lemma 2.0.9, neither theory has any finite models. By Lemma 2.0.11, each is κ-categorical for every uncountable κ. The language of fields is finite, so countable. The Łoś–Vaught test (Lemma 2.0.8) gives completeness. □

This completes the proof of Theorem 2.0.1.

References

[1] W. Troiani. *Elementary first order logic.*

[2] J. Ax. "The elementary theory of finite fields," *Annals of Mathematics, Second Series*, 88(2):239–271, 1968.

[3] A. Grothendieck and J. Dieudonné. *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, III.* Inst. Hautes Études Sci. Publ. Math. 28 (1966), Theorem 10.4.11.

[4] S. Lang. *Algebra*, revised third edition, Springer, 2002.

[5] H. Swanson. "Ax–Grothendieck," *Math Mondays*. https://mathmondays.com/ax-grothendieck.