Ax-Grothendieck via model theory

August 14, 2022

1 Transporting proofs

It is common practice to observe that certain properties were not used inside some proof and to then conclude that the proof still holds in a more general setting. For instance, we can prove that any ring R has unique additive identity using the following argument: say there were two additive identities $0, 0'$, then we have

$$0 = 0 + 0' = 0' + 0 = 0' \tag{1}$$

and thus $0 = 0'$. Now we observe that we never made use of the multiplicative structure of R in the proof, and so indeed this proof holds in the more general setting where R is any abelian group.

We can do this more precisely 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. $\mathcal{R}$ consists 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.

$$\forall x \forall y \forall z (x + y) + z = x + (y + z) \tag{2}$$
$$\forall x \forall y x + y = y + x \tag{3}$$
$$\forall x x + 0 = x \tag{4}$$
$$\forall x \exists y x + y = 0 \tag{5}$$
$$\forall x \forall y \forall z (x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{6}$$
$$\forall x x \cdot 1 = 1 \cdot x = x \tag{7}$$
$$\forall x \forall y \forall z x \cdot (y + z) = x \cdot y + x \cdot z \tag{8}$$
$$\forall x x + (-x) = 0 \tag{9}$$

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

We observe the following proof π which shows that the additive inverse is unique.

$$\begin{prooftree}
\AxiomC{$\forall x \exists y x + y = 0$}
\RightLabel{$\forall E$}
\UnaryInfC{$\exists y a + y = 0$}
\AxiomC{$[a + b = 0]^1$}
\AxiomC{$\forall z z + 0 = z$}
\RightLabel{$\forall E$}
\UnaryInfC{$c + 0 = c$}
\RightLabel{$= E$}
\BinaryInfC{$a + (b + c) = a$}
\doubleLine
\RightLabel{Associativity}
\UnaryInfC{$(a + b) + c = a$}
\AxiomC{$[a + b = b]^2$}
\AxiomC{$[a + b = 0]^1$}
\RightLabel{$= E$}
\BinaryInfC{$(a + b) + c = 0$}
\RightLabel{$= E$}
\BinaryInfC{$a = 0$}
\RightLabel{$\exists E^1$}
\BinaryInfC{$a = 0$}
\RightLabel{$\Rightarrow I^2$}
\UnaryInfC{$a + b = b \Rightarrow a = 0$}
\RightLabel{$\forall I$}
\UnaryInfC{$\forall x x + b = b \Rightarrow x = 0$}
\RightLabel{$\forall I$}
\UnaryInfC{$\forall y \forall x x + y = y \Rightarrow x = 0$}
\end{prooftree}$$

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. We notice that the proof π only makes use of axioms which appear in the first order theory of abelian groups. That is, π is also a proof pertaining to that first order theory. It then follows from the Soundness Theorem [1] that all abelian groups have a unique additive inverse.

We have demonstrated a proof technique using model theory in a trivial example. The reason why this example is trivial is because there was no need to ever consider rings in the first place. The goal of this note is to use this technique in a non-trivial way. We will prove the Ax-Grothendieck Theorem.

2 Ax-Grothendieck Theorem

The Ax-Grothendieck Theorem is was independently discovered by James Ax and Alexandre Grothendieck, respectively [2], [3]. These notes follow the Swanson's blog post `https://mathmondays.com/ax-grothendieck` [4].

Theorem 2.0.1 (Ax-Grothendieck Theorem)**.** *Let $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a polynomial. If f is injective, then it 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. $\mathcal{F}$ consists 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.

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

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

We then extend this to the first order theory of algebriacally closed fields of characteristic p, where p is either a prime number or 0. We do this by considering the following first order sentences.

Definition 2.0.3. For each $d \geq 1$ define the following formula.

$$P_d := \forall a_0 \ldots \forall a_d \exists x, a_d \neq 0 \wedge a_0 + a_1 x + \ldots + a_{d-1} x^{d-1} + a_d x^d = 0 \qquad (19)$$

For each prime number p define the following formula.

$$S_p := 1 + \ldots + 1 = 0 \qquad (20)$$

where there are p instances of 1 in (20).

Definition 2.0.4. Let $\mathcal{ACF}$ denote the **first order theory of algebrically closed fields** which is over the same language as $\mathcal{F}$ and consists of all the axioms of Definition 2.0.2 along with P_d for each $d \geq 1$.

The **first order theory of algebraically closed fields of characteristic** p is denoted $\mathcal{ACF}_p$ and consists of all the axioms of $\mathcal{ACF}$ along with S_p.

Lastly, the **first order theory of algebraically closed fields of characteristic** 0 is denoted $\mathcal{ACF}_0$ and consists of all the axioms of $\mathcal{ACF}$ along with the formula $\neg S_p$ for each prime number p.

Theorem 2.0.1 will follow the corresponding statement in the finite characteristic case.

Lemma 2.0.5. *Let $f : \overline{\mathbb{F}_p}^n \longrightarrow \overline{\mathbb{F}_p}^n$ be a polynomial (p a prime number). If f is injective then it is surjective.*

Proof. Let $\underline{y} = (y_1, \ldots, y_n) \in \overline{\mathbb{F}_p}^n$ be arbitrary. Consider the field extension $K \supseteq \mathbb{F}_p$ generated by $y_1, \ldots, y_n$ as well as the coefficients of f. Since every element of $\overline{\mathbb{F}_p}$ is algebraic over $\mathbb{F}_p$ (by the definition of an algebraic closure) we have K is an algebraic extension and thus a finite extension of $\mathbb{F}_p$. Since $\mathbb{F}_p$ is finite, this implies K is finite. Lastly, we notice that fields are closed under polynomial expressions, and so $f(K^n) \subseteq K^n$, which by injectivity and finiteness implies $f(K^n) = K^n$. Hence there exists $\underline{z} \in K^n \subseteq \overline{\mathbb{F}_p}^n$ such that $f(\underline{y}) = \underline{z}$. □

Corollary 2.0.6. *Let k be an algebraically closed field and $f : k^n \longrightarrow k^n$ a polynomial. If $\mathcal{ALG}_p$ is complete for all $p = 0$ or p prime, and if f is injective, then f is surjective.*

Proof. We need to turn the statement of the corollary into a first order formula, but we cannot do that if we try to work with a polynomial of arbitrary degree. So instead we will consider the statement "If f is an injective, degree d polynomial then it is surjective". The idea is to take the following statement

$$\begin{aligned} &\forall a_0 \dots \forall a_d (\forall x \forall y, f(x) = f(y) \Rightarrow x = y) && (21)\\ &\qquad \Longrightarrow \forall y \exists x, y = f(x) && (22)\end{aligned}$$

and write out f explicitly. This is where we use the fact that f is a polynomial (of degree d). Our first order statement is:

$$\begin{aligned} \forall a_0 \dots \forall a_d (\forall x \forall y, & a_0 + a_1 x + \ldots + a_{d-1} x^{d-1} + a_d x^d \\ &= a_0 + a_1 y + \ldots + a_{d-1} y^{d-1} + a_d y^d \Rightarrow x = y) \\ &\Rightarrow \forall y \exists x, y = a_0 + a_1 x + \ldots + a_{d-1} x^{d-1} + a_d x^d \end{aligned}$$

Denote this formula B_d.

Fix a prime p. Since $\mathcal{ACF}_p$ is complete, we either have

$$\mathcal{ACF}_p \vdash B_d \quad \text{or} \quad \mathcal{ACF}_p \vdash \neg B_d \tag{23}$$

Say $\mathcal{ACF}_p \vdash \neg B_d$. Then in any model $\mathcal{I}$ of $\mathcal{ACF}_p$ and any valuation ν we would have $\mathcal{I}_\nu(\neg B_d) = 1$. This means $\mathcal{I}_\nu(B_d) = 0$, and unwinding B_d we eventually obtain a polynomial f which is injective but *not* surjective, contradicting Lemma 2.0.5. Thus, $\mathcal{ACF}_p \not\vdash \neg B_d$, that is, there is no proof in $\mathcal{ACF}_p$ of $\neg B_d$.

Now, $\mathcal{ACF}_0$ is also complete, so either

$$\mathcal{ACF}_0 \vdash B_d \quad \text{or} \quad \mathcal{ACF}_0 \vdash \neg B_d \tag{24}$$

Again, assume $\mathcal{ACF}_0 \vdash \neg B_d$. Let π be such a proof of $\mathcal{ACF}_0 \vdash \neg B_d$. Since π is finite, only finitely many axioms of $\mathcal{ACF}_0$ appear amongst its premises. Thus, there exists some prime q such that $\neg S_q$ does *not* appear amongst the premises of π. That is, π is a valid proof in $\mathcal{ACF}_q$! This contradicts the first half of this proof, and so $\mathcal{ACF}_0 \not\vdash \neg B_d$. That is, $\mathcal{ACF}_0 \vdash B_d$. The result then follows by soundness. □

It now remains to show that $\mathcal{ALG}_p$ is complete for all $p = 0$ and p prime. In [1] we prove the Lowenhiem-Skolem Theorem and the Łoś-Vaught test.

Theorem 2.0.7 (Lowenhiem-Skolem Theorem). *Let $\mathbb{T}$ be a first order theory with one sort A which admits a model $\mathcal{I}$ so that $\mathcal{I}(A)$ is infinite in cardinality. Then for any cardinal κ there exists a model $\mathcal{J}$ of $\mathbb{T}$ so that $|\mathcal{J}(A)| = \kappa$.*

Lemma 2.0.8 (Łoś-Vaught test)**.** *Let $\mathbb{T}$ be a first order theory over Σ. Assume $\mathbb{T}$ satisfies the following.*

- *Σ has only 1 sort, A say.*
- *$\mathcal{T}$ has no finite models (that is, for every model $\mathcal{I}$ we have $\mathcal{I}(A)$ is an infinite set.*
- *There exists some infinite cardinal κ for which there is exactly one model of $\mathcal{T}$ of size κ up to isomorphism.*

Then $\mathcal{T}$ is complete.

All $\mathcal{ALG}_p$ for p a prime number or 0 are first order theories with only one sort. That $\mathcal{ALG}_p$ satisfies the second dotpoint is the following Lemma.

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

Proof. Say k was finite. Consider the polynomial

$$f(x) = 1 - \prod_{\alpha \in k}(x - \alpha) \in k[x] \tag{25}$$

Then for all $\alpha \in k$ we have $f(\alpha) = 1 \neq 0$, and so k is not algebraically closed. □

Now we establish the third dotpoint. We begin by recalling the algebraic closure of a field.

Lemma 2.0.10. *Every field F can be embedded into an algebraically closed field $\overline{F}$.*

Proof. Let Λ be the collection of monic, irreducible polynomials with coefficients in F. For each $f \in F$, let $u_{f,0}, ..., u_{f,d}$ be formal indeterminants, where d is the degree of f. Let $F[\{U\}]$ be the polynomial ring over F where U is the collection of all $u_{f,i}$. Write

$$f - \prod_{i=0}^{d}(x - u_{f,i}) = \sum_{i=0}^{d-1} \alpha_{f,i} x^i \in F[\{U\}][x]$$

Let I be the ideal generated by $\alpha_{f,i}$. I is not all of $F[\{U\}]$ so there exists a maximal ideal M containing I. Let $F_1 = F[\{U\}]/M$. Repeat this process to define f_i for all $i > 0$. Then $\cup_{i=1}^{\infty} F_i$ is algebraically closed which F embeds into, and moreover is an algebraic extension of F. □

Corollary 2.0.11. *If F is infinite, then the cardinality of F is equal to the cardinality of $\overline{F}$.*

If F is finite, then the cardinality of $\overline{F}$ is countably infinite.

Proof. Using the notation of the proof of Lemma 2.0.10, we first observe that the $|\{U\}| = |F|$ □

Lemma 2.0.12. *Let p be either a prime number or 0 and let $\kappa \geq \aleph_1$ be an uncountable cardinal. There exists an algebraically closed field of characteristic p whose cardinality is κ. Moreover, this field is unique up to isomorphism.*

Proof. Define F to be

$$p = \begin{cases} \mathbb{Q}, & p = 0 \\ \mathbb{F}_p, & p \neq 0 \end{cases} \tag{26}$$

Let X be any set of cardinality κ (eg, $X = \mathbb{R}$) and consider the polynomial ring $F[\{X\}]$. The ideal $I \subseteq F[\{X\}]$ generated by X is not all of $F[\{X\}]$ and so is contained in some maximal ideal $\mathfrak{m}$ (using Zorn's Lemma). The field $F[\{X\}]/\mathfrak{m}$ has cardinality $\aleph_1$, as there are countably many polynomials over a single indeterminant, and we claim that the algebraic closure $\overline{F[\{X\}]/\mathfrak{m}}$ of $F[\{X\}]/\mathfrak{m}$ also has cardinality κ.

Thus, in the notation of Lemma 2.0.10, F_i has cardinality κ for all $i \geq 0$. Since $\overline{F[\{X\}]/\mathfrak{m}}$ is the countable union of all of these fields, it follows that the cardinality of $\overline{F[\{X\}]/\mathfrak{m}}$ is κ.

The uniqueness claim follows easily by considering a transcendental basis of $\overline{F[\{X\}]/\mathfrak{m}}$ and observing that this basis has cardinality κ. The rest follows from the universal property of the algebraic closure. □

Corollary 2.0.13. *There is only one model (up to isomorphism) of $\mathcal{ALG}_0$ and of $\mathcal{ALG}_p$ for each cardinal $\kappa \geq \aleph_1$.*

References

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

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

[3] *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III.*, Inst. Hautes Études Sci. Publ. Math., vol. 28, pp. 103–104, Theorem 10.4.11.

[4] H. Swanson *Math Mondays* `https://mathmondays.com/ax-grothendieck`