What is the Ax-Grothendieck Theorem?

Ricky Magner
Eastern Connecticut State University

Abstract

The Ax-Grothendieck theorem, proven in the 1960s independently by Ax and Grothendieck, states that any injective polynomial from n-dimensional complex space into itself must also be surjective. We will prove this theorem using algebraic techniques following Tao's exposition, and discuss alternate proofs using tools from complex analysis and model theory.

Introduction

We say that $P : \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial if

$$P(x_1, \ldots, x_n) = (P_1(x_1, \ldots, x_n)), \ldots, P_n(x_1, \ldots, x_n))$$

where each $P_i \in \mathbb{C}[x_1, \ldots, x_n]$. Note that this means the individual maps in one coordinate are polynomials in n variables, so that P is really a collection of n polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. The Ax-Grothendieck theorem states that if P is an injective function, then it must also be surjective. This seems like a lot of information to keep track of and index properly, but the key to the proof of this theorem is that the information required throughout is *finite*.

In the case of $n = 1$, the statement of the theorem is easily verified.

Proposition 1. If $P : \mathbb{C} \to \mathbb{C}$ is an injective polynomial, then P is surjective.

Proof. If P is injective, then it is not constant. Thus for any $z_0 \in \mathbb{C}$, we have $P(z) - z_0$ is a nonconstant polynomial. By the Fundamental Theorem of Algebra, this polynomial has a root, so $P(z) - z_0 = 0$ for some $z \in \mathbb{C}$. Hence $P(z)$ is surjective. □

In light of this proof, we may view the Ax-Grothendieck theorem as an extension of the Fundamental Theorem of Algebra in some sense. Although it may seem that injectivity was a stronger hypothesis than appeared in the proof, it will be used in a crucial way in the general case.

The interesting thing about this theorem is that it involves a "reduction to the finite case," i.e. the proof of the theorem uses the following simple fact that we record for completeness.

Proposition 2. If F is a finite field and $P : F^n \to F^n$ is injective, then it is surjective.

Proof. This is a set-theoretic statement having nothing to do with fields and polynomials! $\square$

Notation. As an abuse of notation, we may sometimes write $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ as $P(\vec{x})$ and $P(x_1, \ldots, x_n, y_1, \ldots, y_n) \in F[x_1, \ldots, x_n, y_1, \ldots, y_n]$ as $P(\vec{x}, \vec{y})$.

The Proof of the $\mathbb{C}^n$ Case

We follow Tao's exposition from [9]. First, we need an important result from algebra.

Theorem 1. (Hilbert's Nullstellensatz.) Let F be an algebraically closed field. Then if $f \in F[x_1, \ldots, x_n]$ vanishes at all points for which $\{g_i\} \in F[x_1, \ldots, x_n]$ vanish then there exist $Q_i \in F[x_1, \ldots, x_n]$ and $r \geq 1$ such that $\sum g_i Q_i = f^r$.

For a proof of this theorem, see any standard reference on algebra. This theorem can be stated in a variety of different forms, but we will only have use for the one stated above. The Nullstellensatz allows us to translate the properties of injectivity and surjectivity of polynomials into algebraic statements with a finite amount of data, which is the main idea in the proof.

Lemma 1. A polynomial $P : F^n \to F^n$ where F is algebraically closed with $P = (P_1, \ldots, P_n)$ is injective if and only if there exist $Q_{i,j} \in F[x_1, \ldots, x_n, y_1, \ldots, y_n]$ and $r_j \geq 1$ such that $\sum_{i=1}^n (P_i(\vec{x}) - P_i(\vec{y}))Q_{i,j}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j}$ for all $1 \leq j \leq n$.

Proof. If an identity as above holds, then clearly $P_i(\vec{x}) - P_i(\vec{y}) = 0$ for all i implies $x_j - y_j = 0$ for all j, i.e. $\vec{x} - \vec{y} = 0$, so the identity implies injectivity.

For the converse, we need the Nullstellensatz. Suppose P is injective. Then this means if $P_i(\vec{x}) - P_i(\vec{y}) = 0$ for all i *simultaneously*, then $\vec{x} - \vec{y} = 0$ or $x_j - y_j = 0$ for all j. Fix j, and consider the hypotheses of Theorem 1. By injectivity, the polynomial $x_j - y_j$ vanishes at the points for which the collection $\{P_i(\vec{x}) - P_i(\vec{y})\}$ in $A := F[x_1, \ldots, x_n, y_1, \ldots, y_n]$ vanish. Hence the Nullstellensatz furnishes polynomials $Q_{i,j} \in A$ and $r_j \geq 1$ such that $\sum_{i,j=1}^n (P_i(\vec{x}) - P_i(\vec{y}))Q_{i,j}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j}$. $\square$

Similarly, we express lack of surjectivity using polynomial equations.

Lemma 2. A polynomial $P : F^n \to F^n$ where F is algebraically closed with $P = (P_1, \ldots, P_n)$ is not surjective if and only if there exists a $z_0 \in F^n$ and polynomial $R \in \mathbb{F}$ such that $(P(\vec{x}) - z_0)R(\vec{x}) = 1$.

Proof. If the last equation holds, then $P(\vec{x}) \neq z_0$ for all $\vec{x} \in F^n$, so P is not surjective. Conversely, if P is not surjective, then there exists a $z_0 \in F^n$ for which $P(\vec{x}) - z_0 \neq 0$ for any $\vec{x} \in F^n$. In this case the hypotheses of the Nullstellensatz hold vacuously for the constant polynomial $\mathbf{1}$, so there exists an $R(\vec{x}) \in F[x_1, \ldots, x_n]$ for which $(P(\vec{x}) - z_0)R(\vec{x}) = 1$. □

An important observation to make is that one of the direction for both lemmas was easier to prove, namely existence of a certain type of polynomial relation implies either injectivity or lack of surjectivity. In fact, the Nullstellensatz was not used at all in this case, so these implications hold over any field, not just those which are algebraically closed. This is crucial for the proof of the theorem.

Theorem 2. If $P : \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then P is surjective.

Proof. Suppose P is injective but not surjective. Then we may form the collection of polynomials from the two lemmas: $\{Q_{i,s}, R, z_0\}$ and take the collection $\mathcal{C}$ of their coefficients. This is a *finite* subset of $\mathbb{C}$. Consider $\mathbb{Z}[\mathcal{C}]$, the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and $\mathcal{C}$. Let $\mathfrak{m}$ be a maximal ideal. Then (prove as an exercise) $\mathbb{Z}[\mathcal{C}]/\mathfrak{m}$ is a finite field. The reductions of the polynomial equations created using Lemmas 1 and 2 hold over these finite fields, so by our remark above, this implies that the reduction $\overline{P}$ mapping the finite field $\mathbb{Z}[\mathcal{C}]/\mathfrak{m}$ to itself (Ex: Why does this work?) is injective but not surjective, a contradiction. □

Extensions of the Theorem

Rudin gave a proof of Theorem 2 using complex analysis which yields the stronger result that P^{-1} is itself a polynomial (see [9] for details). Why use such generality when the Nullstellensatz can be substituted with complex analysis? One motivation is that our proof did not use anything special about $\mathbb{C}$ other than the fact that it was algebraically closed. After realizing this, the next result should not seem too surprising.

Theorem 3. Let K be the algebraic closure of a finite field k with characteristic p. Then if $P : K^n \to K^n$ is an injective polynomial, it is surjective.

Proof. Suppose P is injective but not surjective. Lemmas 1 and 2 were proven for any algebraically closed field, so they are valid for P in this case. However, the reduction to the finite case is much simpler in this setting. Let $\mathcal{C}$ be the set of coefficients as defined in the previous proof, and consider the subfield of K generated by k and $\mathcal{C}$. Then this is a finitely generated algebraic (!) extension of k, hence this subfield is also finite. Thus the reduction of the polynomial equations from the lemmas descends to polynomial equations over a finite field which imply that P is an injective map of a finite field to itself which is not surjective. $\square$

Other ways to prove the theorem include using model theory, which would require much more time than alloted to discuss. For basic approaches, see for example [3] or [7]. One intuitive reason as to why finite fields and fields of characteristic p can give us information about fields of characteristic 0 is the following: one of the defining properties of a field of characteristic 0 is that the infinite set of axioms $\{n \cdot 1 \neq 0 : n \in \mathbb{N}\}$ hold. If some property of a field with characteristic 0 can be deduced by a proof involving only finitely many statements, then it should not require the usage of all of these infinitely many axioms, i.e. the statements really only need the fact that for *finitely many* $n \in \mathbb{N}$, $n \cdot 1 \neq 0$. This is why certain statements about $\mathbb{C}$ "should" also be true for all fields of sufficiently large characteristic and vice versa. This vague concept can be made precise and rigorous using model theory and mathematical logic.

As a closing remark about the theorem itself, we mention that the theorem can be generalized (and in fact is often stated) to injective morphisms of algebraic varieties over algebraically closed fields. See [5] for more details.

Applications

Although the statement of the Ax-Grothendieck theorem is already impressive in all of its forms, there is an interesting application to the study of cellular automata. A cellular automaton is (roughly) a grid in which every square occupies a specific state, and there are some rules for the configuration to pass from one state to another. A classic example of this is Conway's Game of Life. A state in a cellular automaton is called a "Garden of Eden" state if it is impossible to reach that state from a previous one following the given rules. A pair of twins is a pair of configurations for which interchanging them in any sequence of applications of the rules do not change the sequence for any future states. The Garden of Eden theorem states that a cellular automaton in Euclidean space has a Garden of Eden state if and only if it has twins. This theorem can be generalized to cellular automata over elements of an amenable group, but this proof uses the Ax-Grothendieck theorem. For details on this subject, see [2], [4], and [6].

For other theorems proven similarly to the Ax-Grothendieck theorem (using finite fields/characteristic p to prove the characteristic 0 case), see [8].

References

[1] Ax, James. The elementary theory of finite fields. *Annals of Mathematics (2nd ser.)* (Annals of Mathematics) **88** (1968) (2): 239271.

[2] Ceccherini-Silberstein, Tullio; Coornaert, Michel. On algebraic cellular automata. *J. Lond. Math. Soc. (2)* **84** (2011), no. 3, 541–558.

[3] Clark, Pete. 2010 summer course on model theory, 2010. (Available at http://math.uga.edu/ pete/modeltheory2010FULL.pdf).

[4] Moore, Edward. Machine models of self-reproduction. *Proc. Symp. Applied Mathematics* **14** 17–33, Reprinted in Burks, Arthur W. (1970), *Essays on Cellular Automata*, University of Illinois Press, pp. 187203.

[5] Grothendieck, Alexander. *Elements de geometrie algebrique. IV. Etude locale des schemas et des morphismes de schemas. III.,* Inst. Hautes Etudes Sci. Publ. Math. **28** (1966), pp. 103104, Theorem 10.4.11.

[6] Myhill, John. The converse of Moore's Garden-of-Eden theorem. *Proceedings of the American Mathematical Society* **14** 685–686. Reprinted in Burks, Arthur W. (1970), *Essays on Cellular Automata*, University of Illinois Press, pp. 204205.

[7] Ramsey, Nick. An introduction to model theory by way of the Ax-Grothendieck theorem, 2013. (Available at http://math.berkeley.edu/ jhicks/links/SOTS/nramsey012414.pdf).

[8] Serre, Jean-Pierre. How to use finite fields for problems concerning infinite fields. *Arithmetic, geometry, cryptography, and coding theory.* 183–193, Contemp. Math., 487, *Amer. Math. Soc., Providence, RI,* 2009. (Available at http://arxiv.org/abs/0903.0517).

[9] Tao, Terrence. Infinite Fields, Finite Fields, and the Ax-Grothendieck Theorem, 2009. (Available at http://terrytao.wordpress.com/2009/03/07/infinite-fields-finite-fields-and-the-ax-grothendieck-theorem/).