LECTURE NOTES

The Ax–Grothendieck Theorem

Giulio Fellin

Prerequisites. We use the Fundamental Theorem of Algebra, Hilbert's Nullstellensatz, and Zariski's lemma. More precisely, the forms needed here are: if K is algebraically closed and $J \subseteq K[x_1, \dots, x_n]$ is an ideal, then $I(V(J)) = \sqrt{J}$ (with $V(J) = \varnothing$ exactly when J is the whole ring); and if a field L is finitely generated as a K-algebra, then L is a finite algebraic extension of K. These results are recalled rather than proved. The exercises below are left without solutions.

1 Statement and the one-dimensional case

The main result of these notes is the following:

Theorem 1.1 (Ax–Grothendieck)**.** Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is injective, then f is bijective.

The theorem was proved independently by James Ax using model theory and by Alexander Grothendieck using methods from algebraic geometry. The model-theoretic proof is shorter, while the geometric proof is more closely connected with the philosophy of reduction modulo prime numbers.

The Ax–Grothendieck theorem may be viewed, in some sense, as a vast generalisation of Gauß's Fundamental Theorem of Algebra. Indeed, when $n = 1$, the theorem reduces to the following statement, which follows immediately from the Fundamental Theorem of Algebra.

Proposition 1.1. Let $f : \mathbb{C} \to \mathbb{C}$ be a polynomial. If f is injective, then f is surjective.

Proof. Since f is injective, it cannot be constant. Hence $f(z) - c$ is a nonconstant polynomial for every $c \in \mathbb{C}$. By the Fundamental Theorem of Algebra, every nonconstant complex polynomial has a root. Therefore, for every $c \in \mathbb{C}$, there exists $d \in \mathbb{C}$ such that $f(d) - c = 0$. Equivalently, $f(d) = c$. Thus every element of $\mathbb{C}$ lies in the image of f, and therefore f is surjective. □

2 The proof by reduction to finite fields

The core idea of the proof is surprisingly simple: reduce the problem from characteristic 0 to the finite field setting, where injective maps are automatically surjective because finite sets have the same cardinality as their images. This follows from the pigeonhole principle:

Proposition 2.1 (Pigeonhole principle)**.** Let A, B be finite sets such that $|A| = |B|$. A function $f : A \to B$ is injective if and only if it is surjective.

Proof. We argue by induction on the cardinality of A, B.

- If $A = \emptyset$, then the statement is trivial.

- Suppose A and B have cardinality $n+1$ and the result holds for sets of cardinality n.

  Let $f : A \to B$ be injective. Removing one element $a \in A$ and restricting f to $A \setminus \{a\}$ gives an injective map

  $$f|_{A\setminus\{a\}} : A \setminus \{a\} \to \mathrm{im}(f|_{A\setminus\{a\}})$$

  where domain and codomain have cardinality n, and therefore is surjective by the induction hypothesis. Also, $f(a) \notin \mathrm{im}(f|_{A\setminus\{a\}})$ by injectivity. We get

  $$|\mathrm{im}(f)| = |\mathrm{im}(f|_{A\setminus\{a\}})| + |\{f(a)\}| = n+1.$$

  This implies that $\mathrm{im}(f) = B$, i.e. f is surjective on B as well.

  The other direction is similar. □

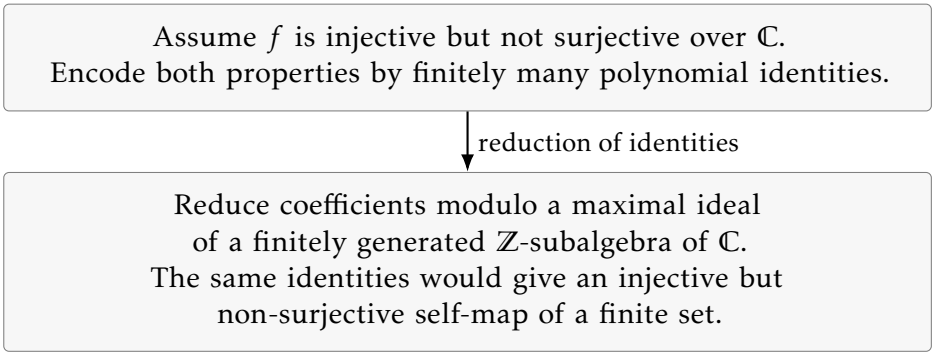
Corollary 2.1 (Ax–Grothendieck for finite fields)**.** Let $\mathbb{K}$ be a finite field, and let $f : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map. If f is injective, then f is bijective.

Proof. Immediate from the previous proposition, since $\mathbb{K}^n$ is finite. □

We now present a proof of the Ax–Grothendieck theorem using methods from algebraic geometry. The guiding philosophy is that algebraic statements over fields of characteristic 0 can often be understood by reducing modulo prime numbers and studying the corresponding statements over finite fields.

The key observation is that over a finite set, injective maps are automatically surjective. The main difficulty is therefore to express injectivity and non-surjectivity by polynomial identities that survive reduction modulo maximal ideals.

This approach is often attributed to Alexander Grothendieck and reflects one of the central ideas of modern algebraic geometry: arithmetic information over finite fields can be used to deduce geometric statements over fields of characteristic 0.



Proposition 2.2. Let $\mathbb{K}$ be algebraically closed and let $f = (f_1, \dots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map. Write $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$. Then:

(1) f is injective if and only if there are polynomials $g_{i,j} \in \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$ and integers $r_j \geq 1$ such that, for every $j = 1, \dots, n$,

$$\sum_{i=1}^{n} \Big(f_i(\mathbf{x}) - f_i(\mathbf{y})\Big) g_{i,j}(\mathbf{x}, \mathbf{y}) = (x_j - y_j)^{r_j}.$$

(2) f is surjective if and only if, for every $Q = (Q_1, \dots, Q_n) \in \mathbb{K}^n$ and every choice of $h_1, \dots, h_n \in \mathbb{K}[x_1, \dots, x_n]$,

$$\sum_{i=1}^{n} (f_i(\mathbf{x}) - Q_i) h_i(\mathbf{x}) \neq 1.$$

Proof. (1) Suppose first that such identities exist. If $f(P) = f(Q)$, i.e. $f_i(P) - f_i(Q) = 0$ for all $1 \leq i \leq n$, then the left-hand side vanishes, and therefore $(P_j - Q_j)^{r_j} = 0$ for all j. Since $\mathbb{K}$ is a field, this implies $P_j - Q_j = 0$ for all j, hence $P = Q$. Therefore f is injective.

Conversely, suppose that f is injective. Let $R := \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$. Then the system of equations

$$f_i(\mathbf{x}) - f_i(\mathbf{y}) = 0, \qquad 1 \leq i \leq n,$$

has exactly the same solutions as

$$x_j - y_j = 0, \qquad 1 \leq j \leq n.$$

Fix j. Since f is injective, the polynomial $x_j - y_j$ vanishes at every common zero of the polynomials $f_i(\mathbf{x}) - f_i(\mathbf{y})$. By Hilbert's Nullstellensatz,

$$x_j - y_j \in \sqrt{(f_1(\mathbf{x}) - f_1(\mathbf{y}), \dots, f_n(\mathbf{x}) - f_n(\mathbf{y}))},$$

therefore there exists an integer $r_j \geq 1$ such that

$$(x_j - y_j)^{r_j} \in \langle f_1(\mathbf{x}) - f_1(\mathbf{y}), \dots, f_n(\mathbf{x}) - f_n(\mathbf{y}) \rangle.$$

Equivalently, there exist polynomials $g_{i,j} \in R$ such that

$$\sum_{i=1}^{n} (f_i(\mathbf{x}) - f_i(\mathbf{y})) g_{i,j}(\mathbf{x}, \mathbf{y}) = (x_j - y_j)^{r_j}.$$

(2) We prove the contrapositive, i.e. that f is *not* surjective if and only if there exist a point $Q \in \mathbb{K}^n$ and polynomials $h_1, \dots, h_n \in \mathbb{K}[x_1, \dots, x_n]$,

$$\sum_{i=1}^{n} (f_i(\mathbf{x}) - Q_i)\, h_i(\mathbf{x}) = 1.$$

Suppose first that such an identity exists. If there were some $P \in \mathbb{K}^n$ such that $f(P) = Q$, then every term on the left-hand side would vanish, leading to $1 = 0$. Hence Q is not in the image of f, so f is not surjective.

Conversely, suppose that f is not surjective. Then there exists $Q \in \mathbb{K}^n$ such that the system

$$f_i(\mathbf{x}) - Q_i = 0, \qquad 1 \leq i \leq n,$$

has no solution in $\mathbb{K}^n$. By Hilbert's Nullstellensatz,

$$\langle f_1(\mathbf{x}) - Q_1, \dots, f_n(\mathbf{x}) - Q_n \rangle = \mathbb{K}[x_1, \dots, x_n],$$

and in particular, $1 \in \langle f_1(\mathbf{x}) - Q_1, \dots, f_n(\mathbf{x}) - Q_n \rangle$. So there exist polynomials $h_1, \dots, h_n \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\sum_{i=1}^{n} (f_i(\mathbf{x}) - Q_i)\, h_i(\mathbf{x}) = 1. \qquad \square$$

Exercise 2.1. Let R be a finitely generated $\mathbb{Z}$-algebra, and let $\mathfrak{m} \subseteq R$ be a maximal ideal. Show that the quotient $R/\mathfrak{m}$ is a finite field.

Lemma 2.1 (Finite-type fields over $\mathbb{Z}$)**.** If a field L is a finitely generated $\mathbb{Z}$-algebra, then L is a finite field.

Proof. Suppose first that L has characteristic zero. It then contains $\mathbb{Q}$, and is finitely generated as a $\mathbb{Q}$-algebra. By Zariski's lemma, $L/\mathbb{Q}$ is a finite extension. Each algebra generator is algebraic over $\mathbb{Q}$, so all generators are integral over $\mathbb{Z}[1/N]$ for a sufficiently large positive integer N, obtained by clearing the denominators of their monic rational equations. Consequently L is integral over $\mathbb{Z}[1/N]$. But an integral extension of domains cannot be a field unless the smaller ring is a field, and $\mathbb{Z}[1/N]$ is not a field. This is a contradiction. Hence L has positive characteristic p and is a finitely generated $\mathbb{F}_p$-algebra. Zariski's lemma now implies that L is a finite extension of the finite field $\mathbb{F}_p$, so L is finite. $\square$

Proof of Ax–Grothendieck. Write $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$, as in Proposition 2.2. Suppose, for contradiction, that f is injective but not surjective.

By Proposition 2.2(1), for each $1 \le j \le n$, there exist $g_{i,j} \in \mathbb{C}[x_1, \dots, x_n, y_1, \dots, y_n]$ and $r_j \ge 1$, where $1 \le i, j \le n$, such that for all $j \le n$,

$$\sum_{i=1}^{n} \Big(f_i(\mathbf{x}) - f_i(\mathbf{y})\Big) g_{i,j}(\mathbf{x}, \mathbf{y}) = (x_j - y_j)^{r_j}.$$

By Proposition 2.2(2), since f is not surjective, there exist a point $Q \in \mathbb{C}^n$ and polynomials $h_1, \dots, h_n \in \mathbb{C}[x_1, \dots, x_n]$ such that

$$\sum_{i=1}^{n} (f_i(\mathbf{x}) - Q_i)\, h_i(\mathbf{x}) = 1.$$

Let S be the finite set consisting of all coefficients appearing in: $f_i, g_{i,j}, h_i, Q_i$. Let $R := \mathbb{Z}[S] \subseteq \mathbb{C}$ be the subring generated by $\mathbb{Z}$ and the elements of S.

Choose a maximal ideal $\mathfrak{m} \subseteq R$. Then $\mathbb{K} := R/\mathfrak{m}$ is a finite field by Lemma 2.1. Reducing all coefficients modulo $\mathfrak{m}$, we obtain a polynomial map $\overline{f} : \mathbb{K}^n \to \mathbb{K}^n$.

The polynomial identities above remain valid after reducing their coefficients modulo $\mathfrak{m}$. Here we use the *easy directions* of Proposition 2.2, which hold over *any* field: if $\overline{f}(a) = \overline{f}(b)$, the reduced identities give $(a_j - b_j)^{r_j} = 0$ for every j, hence $a = b$; thus $\overline{f}$ is injective. On the other hand, evaluating the reduced identity

$$\sum_{i=1}^{n} (\overline{f}_i(x) - \overline{Q}_i)\, \overline{h}_i(x) = 1$$

at a hypothetical preimage x of $\overline{Q}$ would give $0 = 1$. Hence $\overline{Q}$ is not in the image and $\overline{f}$ is not surjective. We do *not* apply the Nullstellensatz over the finite residue field.

But $\mathbb{K}^n$ is a finite set, and an injective self-map of a finite set must be surjective. This is the desired contradiction. Therefore f must be surjective. □

Remark 2.1. Walter Rudin gave a proof of the Ax–Grothendieck theorem using methods from complex analysis. His argument yields the stronger conclusion that if $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then the inverse map $f^{-1} : \mathbb{C}^n \to \mathbb{C}^n$ is itself polynomial.

3 Fields of characteristic p

Example 3.1. Let $\mathbb{K}$ be a field of characteristic $p > 0$. The *Frobenius endomorphism* is the function

$$\begin{aligned} F : \mathbb{K} &\to \mathbb{K}, \\ x &\mapsto x^p. \end{aligned}$$

More generally, one can define the coordinate-wise Frobenius endomorphism on affine space:

$$\begin{aligned} F : \quad \mathbb{K}^n &\to \mathbb{K}^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1^p, \ldots, x_n^p). \end{aligned}$$

Basic property. The Frobenius endomorphism is always a ring homomorphism:

$$F(x+y) = (x+y)^p = x^p + y^p = F(x) + F(y),$$

$$F(xy) = (xy)^p = x^p y^p = F(x)F(y),$$

where the binomial expansion simplifies because in characteristic p all intermediate binomial coefficients $\binom{p}{k}$ are divisible by p.
Injectivity and surjectivity.

- The Frobenius endomorphism is injective: if $F(x) = F(y)$, then $(x-y)^p = 0$, hence $x = y$ because $\mathbb{K}$ is a field.
- If $\mathbb{K} = \mathbb{F}_q$ with $q = p^r$, then

  $$F^r(x) = x^q = x \quad \text{for all } x \in \mathbb{F}_q.$$

  Hence its r-fold composition is the identity on $\mathbb{F}_q$.

  In particular, the Frobenius map is bijective over finite fields.
- For any field $\mathbb{K}$ of characteristic p, Frobenius is surjective if and only if $\mathbb{K}$ is *perfect*.

Exercise 3.1. Let $\mathbb{F}_p$ be the finite field with p elements, and let $\mathbb{K} := \mathbb{F}_p(x)$. Show that the Frobenius endomorphism on $\mathbb{K}$ is not surjective.

4 The model-theoretic viewpoint

There is also a famous proof of the Ax–Grothendieck theorem due to James Ax using methods from model theory. The argument uses Łoś's theorem and ultraproducts of finite fields to transfer the statement "injective implies surjective" from finite fields to algebraically closed fields of characteristic 0, using the following:

Exercise 4.1 (Ax–Grothendieck for algebraically closed fields of positive characteristic)**.** Let $\mathbb{K}$ be a finite field, and let $f : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^n$ be a polynomial map. If f is injective, then f is bijective.

Remark 4.1 (Model-theoretic proof: outline)**.** The additional idea is that for a fixed finite tuple of coefficients, injectivity and surjectivity of a polynomial map can be encoded by first-order formulas in the language of fields. A suitable ultraproduct of algebraic closures of finite fields, taken over characteristics tending to infinity, is an algebraically closed field of characteristic zero. By Łoś's theorem and the positive-characteristic case, the relevant first-order statement holds in this ultraproduct. To obtain the conclusion over $\mathbb{C}$ one also uses the transfer principle for algebraically closed fields of characteristic zero (or an appropriate identification of the coefficient field). This is a sketch, not a self-contained proof: it requires model-theoretic tools not developed in these notes.