MATH 141A: INTRODUCTION TO THE MODEL THEORY OF FIELDS

SEBASTIEN VASEY

1. Basics of fields

We want to use logical tools to study fields: certain kind of algebraic objects with an addition and multiplication. First, let's introduce a signature in which we will study them:

Definition 1.1. The *signature of fields* σ_f contains two binary function symbols $+$ and $\cdot$, one unary function symbol $-$, and two constant symbols 0 and 1.

Definition 1.2. A *field* is a model of the set AF containing the axioms of fields, defined below:

- Axioms for addition:
  - Associativity: $(\forall x \forall y \forall z)((x + y) + z = x + (y + z))$.
  - Commutativity: $(\forall x \forall y)(x + y = y + x)$.
  - 0 is the identity: $(\forall x)(x + 0 = x)$.
  - Existence of additive inverse: $(\forall x)(x + (-x) = 0)$.
- Axioms for multiplication:
  - Associativity: $(\forall x \forall y \forall z)((x \cdot y) \cdot z = x \cdot (y \cdot z))$.
  - Commutativity: $(\forall x \forall y)(x \cdot y = y \cdot x)$.
  - 1 is the identity: $(\forall x)(x \cdot 1 = x)$.
  - Existence of multiplicative inverse (for nonzero numbers): $(\forall x \exists y)(x = 0 \vee x \cdot y = 1)$.
- Distributivity: $(\forall x \forall y \forall z)(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$.
- Non-triviality: $0 \neq 1$.

As usual when working with numbers, we write xy instead of $x \cdot y$, drop the parentheses when associativity makes it clear they don't matter, and assume that multiplication has priority over addition (so for example $s+xy+z$ really means $s+((x \cdot y)+z)$). The multiplicative inverse of a nonzero element x is unique, and we write x^{-1} for it. We write $x - y$ for $x + (-y)$ and $\frac{x}{y}$ for xy^{-1}. Often, we do not distinguish between the field and its universe, and say for example that "x is an element of the field F" (where we really mean that x is an element of $\text{univ}(F)$). Two other useful bits of notation are:

Definition 1.3. Let F be a field. We write 1_F (or just 1) instead of 1^F, and similarly for 0_F. For an integer n, define n_F as follows:

$$n_F = \begin{cases} 0_F & \text{if } n = 0 \\ \underbrace{1_F + 1_F + \ldots + 1_F}_{n \text{ times}} & \text{if } n > 0 \\ -(\underbrace{1_F + 1_F + \ldots + 1_F}_{|n| \text{ times}}) & \text{if } n < 0 \end{cases}$$

When F is clear from context, we may forget it and just write n. Also define, for an element x of F:

$$x^n = \begin{cases} 1_F & \text{if } n = 0 \\ \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{|n| \text{ times}}) & \text{if } n < 0 \end{cases}$$

Example 1.4.

- $(\mathbb{Q}, +, \cdot, -, 0, 1)$, $(\mathbb{R}, +, \cdot, -, 0, 1)$, $\mathbb{C}, +, \cdot, -, 0, 1)$ are fields. We may abuse notation and just write $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ for the corresponding fields.
- For a natural number $n > 0$, let $\mathbb{F}_n$ denote the structure $(\{0, 1, 2, 3, \ldots, n-1\}, +, \cdot, -, 0, 1)$, where addition, multiplication, and inversion, is done modulo p (i.e. we take the remainder of the result divided by p. For example, if $n = 3$, then $1 + 2 = 0$, $1 + 3 = 1$, $2 \cdot 2 = 1$, etc. It is a (nonobvious) basic fact from algebra that $\mathbb{F}_p$ is a field when p is a prime. On the other hand if we look for example at $\mathbb{F}_6$, then one can check that 2 has no multiplicative inverse. In general, $\mathbb{F}_n$ is a field if and only if n is prime.
- $(\mathbb{Z}, +, \cdot, -, 0, 1)$ is not a field, as multiplicative inverses are lacking.

Many usual properties of numbers that you are used to (such as the fact that $0 \cdot x = 0$ for any x) follow from the axioms of field. For example:

Fact 1.5. Assume F is a field. For all elements x, y, z, w of F and all integers n and m, we have:

- $(xy)^n = x^n y^n$.
- $x^n x^m = x^{n+m}$.
- $(x^n)^m = x^{nm}$.
- $(n + m)_F = n_F + m_F$.
- $(n \cdot m)_F = n_F \cdot m_F$.
- $x \cdot 0 = 0$.
- $-(xy) = (-x)y$.
- $-x = (-1)x$.
- $(-x)(-y) = xy$.
- If $xy = 0$, then $x = 0$ or $y = 0$ (or both).
- $(x + y)(z + w) = xz + xw + yz + yw$,
- $(x + y)^2 = x^2 + 2xy + y^2$.
- $(x - y)^2 = x^2 - 2xy + y^2$.
- $(x + y)(x - y) = x^2 - y^2$.

We omit the proofs (if you prefer, just add these statements to the axioms of fields). We will use these property freely.

An important property of a field is its *characteristic*:

Definition 1.6. The *characteristic* of a field F, denoted $\mathrm{char}(F)$, is the least positive natural number n such that $n_F = 0$, or 0 if there is no such natural number.

For example, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields of characteristic zero, but for p a prime, $\mathbb{F}_p$ is a field of characteristic p. Note that if $n = \mathrm{char}(F) > 0$, and $n = mk$ for natural numbers m and k, then $m_F k_F = 0$, so multiplying both sides by k_F^{-1}, $m_F = 0$. Since n_F was least, $m_F = n_F$. This shows that the characteristic of a field is either zero or a prime number.

A *subfield* of a field F is a field F_0 which is a substructure of F. We also say that F is an *extension* of F_0. Note that if F_0 is a subfield of F, then F_0 contains 1, and so $\mathrm{char}(F_0) = \mathrm{char}(F)$. The *prime subfield* of a field F is its smallest subfield, i.e. the subfield generated by 1_F. It is easily checked that the prime subfield of a field F is isomorphic to $\mathbb{Q}$ if $\mathrm{char}(F) = 0$ and isomorphic to $\mathbb{F}_p$ if $\mathrm{char}(F) = p$ for p a prime.

Going back to logic, is the set AF of axioms of fields complete? The answer is *no*. One trivial reason is that the characteristic has not been specified in the axioms, so for example $\mathbb{F}_p \models p_F = 0$ but $\mathbb{Q} \models p_F \neq 0$. Thus we define:

Definition 1.7. For p a prime, let $\mathrm{AF}_p = \mathrm{AF} \cup \{p = 0\} \cup \{n \neq 0 \mid 1 \leq n < p\}$ (where as before we are using the number p as an abbreviation for $\underbrace{1 + 1 + \ldots + 1}_{p \text{ times}}$).

Also define $\mathrm{AF}_0 = \mathrm{AF} \cup \{n \neq 0 \mid n > 0\}$.

Thus $F \models \mathrm{AF}_p$ if and only if F has characteristic p. Is AF_p complete? Not yet. For example the field $\mathbb{Q}$ and $\mathbb{R}$ are not elementarily equivalent: $\mathbb{R}$ satisfies the sentence $(\exists x)(x^2 - 2 = 0)$ but $\mathbb{Q}$ does not ($\sqrt{2}$ is not rational). The underlying problem is that polynomials may or may not have roots in a given field.

By the way, what is a polynomial in the language of logic? It is essentially a σ_f-term! More precisely, given a field F, a polynomial (say in one variable) with coefficients from F can be written as $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, where $n < \omega$ and $a_i \in F$. Thus there is a σ_f-term $\tau(x, y_0, y_1, \ldots, y_n)$ such that $F \models (\forall x)(\tau(x, a_0, \ldots, a_n) = a_n x^n + \ldots + a_0)$. Conversely, any term is equal to (after some use of distributivity) a linear combination of products of its variables (and 0 and 1), which is just what a polynomial is.

With this identification, what is an atomic formula in the language of σ_f? It is just an equality $\tau = \rho$ of two polynomials. Keeping in mind that this is equivalent to $\tau + (-\rho) = 0$, an atomic formula exactly says that a certain polynomial has a root (this is why we wanted to add $-$ to the language). When working inside a field F, given a term $\tau(x_1, \ldots, x_n)$, we can plug in elements of F into the free variables to create a new polynomial in fewer variables but with coefficients from F.

It is a nontrivial basic fact of field theory that given a field and a (nontrivial) polynomial in one variable with coefficients from this field, there is an extension of this field with a root for that polynomial:

Fact 1.8. If F is a field, n is a positive natural number, $a_0, a_1, \ldots, a_n$ are elements of F with $a_n \neq 0$, and $\tau(x, a_0, a_1, \ldots, a_n) = a_0 + a_1 x + \ldots + a_n x^n$ is a one variable polynomial with coefficients from F, then there exists a field F' such F is a subfield of F' and $F' \models (\exists x)(\tau(x, a_0, \ldots, a_n) = 0)$.

We give elements that are roots of polynomials a name:

Definition 1.9. If F is a field and X is a subset of F, we say that an element $a \in F$ is *algebraic over* X if there exists $a_0, \ldots, a_n \in X$ and a term $\tau(x, a_0, \ldots, a_n)$ such that $F \models (\exists x)(\tau(x, a_0, \ldots, a_n) \neq 0 \wedge \tau(a, a_0, \ldots, a_n) = 0)$. We write $\operatorname{acl}^F(X)$ (the *algebraic closure of* X *inside* F) for the set of all elements of F that are algebraic over X. If a is *not* algebraic over X, we say that it is *transcendental* over X.

For example, working inside $\mathbb{R}$, $\sqrt{2}$ is algebraic over $\mathbb{Q}$, but e is transcendental over $\mathbb{Q}$. It turns out that, under some conditions, the algebraic closure of a set X is itself a field. However we postpone proving this, as it will be easier to do once we have developed some tools. For now, we will only use the following property, which is an assignment problem:

Exercise 1.10. Let F be a field and X a subset of F. Then $|\operatorname{acl}^F(X)| \leq |X| + \aleph_0$.

It is often useful to consider fields generated by given elements:

Definition 1.11. Given a field F and $X \subseteq F$, we let $\langle X \rangle = \langle X \rangle^F$ be the smallest subfield of F containing X: it is the intersection of all subfields of F containing X – alternatively, it is the substructure obtained when closing X under inverses, addition, and multiplications (also adding 0 and 1). For F_0 a subfield of F and $a \in F$, we let $F_0(a) = (F_0(a))^F$ denote $\langle F_0 \cup \{a\} \rangle^F$.

For example, $\mathbb{Q} = \langle \emptyset \rangle$, and $\mathbb{C} = \mathbb{R}(i)$.

The following facts are fundamental (see any abstract algebra textbook for the proof):

Fact 1.12. If F is a field, F_0 is a finite subfield of F, and $a \in F$ is algebraic over F_0, then $F_0(a)$ is finite.

Fact 1.13. Assume F is a field and F_1, F_2 are extensions of F. Assume $a \in F_1$ and $b \in F_2$. If one of the conditions below hold, then there exists an isomorphism $f : F(a)^{F_1} \cong F(b)^{F_2}$ such that f fixes F and $f(a) = b$.

(1) a and b are transcendental over F.
(2) There exists a nonzero one variable polynomial $\tau(x, a_0, \ldots, a_n)$ with coefficients from F such that (in field-theoretic terms, a and b are algebraic over F and have the same minimal polynomial):
   (a) a is a root of τ and τ is of minimal degree with this property.
   (b) b is a root of τ, and τ is of minimal degree with this property.

2. Algebraically closed fields

Fields where *every* polynomial has a root are given a name:

Definition 2.1. The set of *axioms of algebraically closed fields*, ACF is the set:

$$\mathrm{ACF} = \mathrm{AF} \cup \{(\forall y_0 \dots y_n \exists x)(y_n = 0 \vee y_0 + y_1 x + \dots + y_n x^n = 0) \mid n > 0\}$$

An *algebraically closed field* is a model of ACF. We also define for p a prime or zero, $\mathrm{ACF}_p = \mathrm{ACF} \cup \mathrm{AF}_p$.

For example, neither $\mathbb{Q}$ nor $\mathbb{R}$ are algebraically closed (both are missing a root of $x^2 + 1$). The field $\mathbb{F}_p$ is also not algebraically closed. In fact:

Lemma 2.2. Any algebraically closed field is infinite.

Proof. Let F be a finite field. Say $F = \{a_1, \dots, a_n\}$. Then the polynomial $(x - a_1)(x - a_2) \dots (x - a_n) + 1$ has no roots in F. □

The *fundamental theorem of algebra* says that $\mathbb{C}$ is algebraically closed. This is, however, not needed if we are just interested in building *some* algebraically closed field:

Theorem 2.3. Any field has an algebraically closed extension.

Proof. Iterate Fact 1.8. You will have to give the details in an assignment problem. □

Note that Theorem 2.3 shows in particular that ACF_p is consistent for all p. We will see that it is also complete. This is especially interesting because there is a connection between AF_p and AF_0:

Lemma 2.4. Let A be a set of sentences and let ϕ be a sentence. If $A \cup \mathrm{AF}_0 \models \phi$, then $A \cup \mathrm{AF}_p \models \phi$ for all sufficiently large primes p (that is, there exists a natural number n such that $A \cup \mathrm{AF}_p \models \phi$ for all primes $p \geq n$).

Proof. Assume that $A \cup \mathrm{AF}_0 \models \phi$. Then (for example by the completeness theorem and finite character of proofs), there exists a finite $A_0 \subseteq A$ such that $A_0 \models \phi$. Thus there exists a natural number n such that A_0 is a subset of $A \cup \mathrm{AF} \cup \{m \neq 0 \mid 1 \leq m < n\}$. Take a prime $p \geq n$. Then $A_0 \subseteq A \cup \mathrm{AF}_p$, so it follows that also $A \cup \mathrm{AF}_p \models \phi$. □

Theorem 2.5 (Transferring statements across characteristics)**.** Let A be a set of sentences such that $A \cup \mathrm{AF}_0$ is complete, and let ϕ be a sentence. The following are equivalent:

(1) $A \cup \mathrm{AF}_0 \models \phi$.
(2) $A \cup \mathrm{AF}_p \models \phi$ for all sufficiently large primes p.
(3) $A \cup \mathrm{AF}_p \models \phi$ for infinitely-many primes p.

Proof. If $A \cup \mathrm{AF}_0 \models \phi$, then $A \cup \mathrm{AF}_p \models \phi$ for all sufficiently-large primes p by Lemma 2.4. If $A \cup \mathrm{AF}_p \models \phi$ for all sufficiently-large primes p, then trivially $A \cup \mathrm{AF}_p \models \phi$ for infinitely-many primes p. Now if $A \cup \mathrm{AF}_p \models \phi$ for infinitely-many primes p, assume for a contradiction that $A \cup \mathrm{AF}_0 \not\models \phi$. Since $A \cup \mathrm{AF}_0$ is complete, $A \cup \mathrm{AF}_0 \models \neg\phi$. By Lemma 2.4, $A \cup \mathrm{AF}_p \models \neg\phi$ for all sufficiently-large primes p. This is a contradiction to the hypothesis that $A \cup \mathrm{AF}_p \models \phi$ for infinitely-many primes p. □

Applying Theorem 2.5 to $A = \text{ACF}$, we will get (once we have proven that ACF_0 is complete) that to prove a statement about ACF_0, it is necessary and sufficient to prove it for infinitely-many non-zero characteristics!

3. Completeness of ACF_p

Earlier in the class, we proved completeness (for example of the theory of non-empty dense chains without endpoints) using back and forth systems. Since we are working in a signature with function symbols, we have to generalize the definitions a little bit and revisit Fraïssé's theorem.

Definition 3.1. Assume σ is a signature, and assume M and N are σ-structures.

(1) A *local isomorphism* from M to N is a function s from a finite subset of the universe of M to a finite subset of the universe of N satisfying the following property: for any *quantifier free* formula $\phi(x_1, \ldots, x_n)$ and any $a_1, \ldots, a_n \in \text{dom}(s)$, $M \models \phi(a_1, \ldots, a_n)$ if and only if $N \models \phi(s(a_1), \ldots, s(a_n))$.
(2) For an ordinal α, define inductively the notion of an *α-isomorphism* from M to N:
   (a) A *0-isomorphism* is just a local isomorphism.
   (b) An *$(\alpha+1)$-isomorphism* is a local isomorphism s such that:
      (i) (Forth) For any a in the universe of M, there exists b in the universe of N such that $s \cup \{(a, b)\}$ is an α-isomorphism.
      (ii) (Back) For any b in the universe of N, there exists a in the universe of M such that $s \cup \{(a, b)\}$ is an α-isomorphism.
   (c) For α limit, an *α-isomorphism* is a map that is a β-isomorphism for all $\beta < \alpha$.

   An *∞-isomorphism* is a function that is an α-isomorphism for all ordinals α.
(3) For tuples $\bar{a} = (a_1, \ldots, a_n)$ and $\bar{b} = (b_1, \ldots, b_n)$ of elements from the universe of M and N respectively, we write $(M, \bar{a}) \sim_\alpha (N, \bar{b})$ if $\{(a_i, b_i) \mid 1 \leq i \leq n\}$ is an α-isomorphism from M to N. We write $M \sim_\alpha N$ if $(M, \langle\rangle) \sim_\alpha (N, \langle\rangle)$ (i.e. the tuples are empty). Equivalently, $M \sim_\alpha N$ if the empty map is an α-isomorphism from M to N. In this case we say that M and N are *α-equivalent*.
(4) A local isomorphism s from M to N is called *p-elementary* if it preserves formulas up to quantifier rank p. That is, for any formula $\phi(x_1, \ldots, x_n)$ of quantifier rank at most p, and any $a_1, \ldots, a_n \in \text{dom}(s)$, $M \models \phi(a_1, \ldots, a_n)$ if and only if $N \models \phi(s(a_1), \ldots, s(a_n))$. We call s *elementary* if it is p-elementary for all $p < \omega$, i.e. it preserves all formulas.

Only one direction of Fraïssé's theorem generalizes (the problem is that with function symbols, or with infinitely-many symbols in the signature, there can be infinitely-many non-equivalent formulas of a given quantifier rank; see the discussion in Poizat). Fortunately, this is the direction that is interesting to prove completeness.

Theorem 3.2 (Fraïssé's theorem)**.** Assume $p < \omega$ and M and N σ-structures. If s is a p-isomorphism, then s is p-elementary. In particular, if $M \sim_\omega N$, then M and N are elementarily equivalent.

Proof. Similar to the proof of Fraïssé's theorem for a single relation. □

For fields, the following quickly follows from the fact that local isomorphisms preserve quantifier-free formulas:

Exercise 3.3. Assume E and F are fields, s is a local isomorphism from E to F, $E_0 = \langle \mathrm{dom}(s) \rangle$ is the subfield of E generated by $\mathrm{dom}(s)$, and $F_0 = \langle \mathrm{im}(s) \rangle$ is the subfield of F generated by $\mathrm{im}(s)$. Then s extends to an isomorphism $f : E_0 \cong F_0$.

Note that this shows in particular that if two fields are 0-equivalent then they have the same characteristic. For algebraically closed fields, we have the following very strong result:

Lemma 3.4. Any local isomorphism between two uncountable algebraically closed fields is an ∞-isomorphism.

Proof. Assume E and F are uncountable algebraically closed fields. We prove by induction on α that any local isomorphism from E to F is a local isomorphism. For $\alpha = 0$, this is the definition of a 0-isomorphism, and for α limit this is also immediate. Assume now that $\alpha = \beta + 1$, and we know that every local isomorphism from F_1 to F_2 is a β-isomorphism.

Let s be a local isomorphism from E to F. Let E_0 be the subfield of E generated by $\mathrm{dom}(s)$. By (for example) the downward Löwenheim-Skolem theorem, E_0 is countable. Let F_0 be the subfield generated by $\mathrm{im}(s)$. Exercise 3.3 implies that s extends to an isomorphism $f : E_0 \cong F_0$. We prove the forth condition (as usual, the proof of the back condition will be completely similar). Let $a \in E$. There are three cases:

- If $a \in E_0$, then $t = s \cup \{a, f(a)\}$ is a local isomorphism, and so by the induction hypothesis a β-isomorphism.
- a is transcendental over E_0. Then since F_0 is countable, $\mathrm{acl}(F_0)$ is also countable (Exercise 1.10). By assumption, F is uncountable, so there must exist $b \in F \setminus \mathrm{acl}(F_0)$. Such a b must by definition be transcendental. By Fact 1.13, f extends to an isomorphism $g : F(a) \cong F(b)$. This shows in particular that $t = s \cup \{a, b\}$ preserves quantifier-free formula. By the induction hypothesis, t is a β-isomorphism so we are done.
- a is algebraic over E_0 but not in E_0. Then there exists a polynomial $\tau(x, a_1, \ldots, a_n)$ with coefficients $a_1, \ldots, a_n$ in E_0 such that $\tau(a, a_1, \ldots, a_n) = 0$. If $\tau(x, a_1, \ldots, a_n)$ has a root c in E_0, we can divide τ by $(x - c)$ and get a polynomial of lower degree which still has a as a root. So assume that τ has minimal degree and has no root in E_0. Since F is algebraically closed, the polynomial $\tau(x, s(a_1), \ldots, s(a_n))$ has a root b in F. By Fact 1.13, f extends to an isomorphism $g : F(a) \cong F(b)$. As before, this shows that $s \cup \{(a, b)\}$ is the desired β-isomorphism extending s.

□

Without the hypothesis of uncountability, we can still conclude:

Theorem 3.5. Any local isomorphism between two algebraically closed fields is elementary.

Proof. Assume E_0 and F_0 are algebraically closed fields and assume that s is a local isomorphism from E_0 to F_0. By Lemma 2.2, E_0 and F_0 are infinite. By an assignment problem, this means that E_0 and F_0 have uncountable proper elementary extensions E and F respectively (these will still be algebraically closed fields by elementarity). In particular, s will also be a local isomorphism from E to F. Thus s will be an ∞-isomorphism from E to F by Lemma 3.4. By Fraïssé's theorem, s will be an elementary local isomorphism from E to F. Since E_0 and F_0 are elementary substructures of E and F respectively, s is also an elementary local isomorphism from E_0 to F_0. □

We deduce:

Corollary 3.6. For p a prime or zero, ACF_p is complete.

Proof. Fix p a prime or zero. Let E and F be two models of ACF_p. By assumption, E and F have the same characteristic. Therefore their prime subfields are isomorphic, so the empty map is a local isomorphism from E to F. By Theorem 3.5, the empty map is an elementary local isomorphism from E to F, so they must be elementarily equivalent. □

Corollary 3.7. Assume ϕ is a sentence in the language of σ_f. The following are equivalent:

(1) $\mathbb{C} \models \phi$.
(2) $\text{ACF}_0 \models \phi$.
(3) $\text{ACF}_p \models \phi$ for all sufficiently large primes p.
(4) $\text{ACF}_p \models \phi$ for infinitely-many primes p.

Proof. By the fundamental theorem of algebra, the complex numbers are algebraically closed, hence a model of ACF_0. Thus the equivalence between $\mathbb{C} \models \phi$ and $\text{ACF}_0 \models \phi$ follows from the fact that ACF_0 is complete. The rest follows from Theorem 2.5 applied to $A = \text{ACF}$. □

The equivalence between the first two conditions in Corollary 3.7 is sometimes called the *Lefschetz principle*: if a statement (that can be formulated as a sentence in the language of σ_f) can be proven for the complex numbers, it automatically holds for any other algebraically closed field of characteristic zero. This is quite powerful, as it allows one to use techniques from complex analysis or topology to prove certain results of algebraic geometry over any algebraically closed field of characteristic zero.

4. Quantifier elimination for ACF_p

Recall:

Definition 4.1. A set A of sentences has *quantifier elimination* if for every positive natural number n and every formula $\psi(x_1, \ldots, x_n)$, there exists a *quantifier-free* formula $\phi(x_1, \ldots, x_n)$ such that $A \models (\forall x_1 \ldots \forall x_n)(\psi \leftrightarrow \phi)$.

We have seen for example that the theory of non-empty dense chains without endpoints has quantifier elimination. We could have deduced this directly from the following powerful semantic characterization of quantifier elimination (Theorem 5.3 in Poizat).

Theorem 4.2 (Semantic characterization of quantifier elimination)**.** A set of sentences A has quantifier elimination if and only if any local isomorphism between two models of A is elementary.

Proof. If A has quantifier elimination, then (since local isomorphism preserve quantifier-free formulas by definition), any local isomorphism between two models of A is elementary. Now let us check the converse. Assume that any local isomorphism between two models of A is elementary. Let n be a positive natural number, and let $\psi(x_1, \ldots, x_n)$ be a formula. Let $\bar{x} = (x_1, \ldots, x_n)$, and let us abbreviate $\forall x_1 \ldots \forall x_n$ by $\forall \bar{x}$.

Consider the set Γ of quantifier-free sentences $\phi(\bar{x})$ such that $A \models (\forall \bar{x})(\psi(\bar{x}) \rightarrow \phi(\bar{x}))$. Add new constant symbols $c_1, \ldots, c_n$ and let $\bar{c} = (c_1, \ldots, c_n)$. For a formula $\phi(\bar{x})$, we write $\phi(\bar{c})$ for the formula ϕ where $\bar{x}$ has been substituted by $\bar{c}$ everywhere. Similarly, let $\Gamma(\bar{c})$ denote the set of formulas $\phi(\bar{c})$, where $\phi(\bar{x})$ is in Γ. We will prove:

Claim: $A \cup \Gamma(\bar{c}) \models \psi(\bar{c})$.

Assuming this claim, we have by completeness that there exists a finite $\Gamma_0 \subseteq \Gamma$ such that $A \cup \Gamma_0(\bar{c}) \models \psi(\bar{c})$. Write $\Gamma_0 = \{\phi_1, \ldots, \phi_m\}$. Then by definition $A \models (\forall \bar{x})(\psi \leftrightarrow (\phi_1 \wedge \ldots \wedge \phi_m))$, so $\phi = \phi_1 \wedge \ldots \wedge \phi_m$ is the desired quantifier-free formula.

Proof of Claim: Suppose not. Then there is a model M of $A \cup \Gamma(\bar{c}) \cup \{\neg\psi(\bar{c})\}$. Let:

$$\Gamma' = \{\phi(\bar{x}) \mid \phi \text{ is quantifier-free}, M \models \phi(\bar{c}^M)\}$$

By assumption, $\Gamma \subseteq \Gamma'$ and $M \models \Gamma'(\bar{c})$. We have that $A \cup \Gamma'(\bar{c}) \cup \{\psi(\bar{c})\}$ is consistent. Otherwise, there exists a finite $\Gamma_0' \subseteq \Gamma$ such that $A \cup \Gamma_0'(\bar{c}) \cup \{\psi(\bar{c})\}$ is inconsistent, so writing $\Gamma_0' = \{\phi_1, \ldots, \phi_m\}$, we have that:

$$A \models (\forall \bar{x}) \left(\bigwedge_{1 \leq i \leq m} \phi_i \rightarrow \neg\psi(\bar{x}) \right)$$

The contrapositive is:

$$A \models (\forall \bar{x}) \left(\psi(\bar{x}) \rightarrow \bigvee_{1 \leq i \leq m} \neg\phi_i \right)$$

But then $\bigvee_{1 \leq i \leq m} \neg\phi_i \in \Gamma$ by definition of Γ, and so for some i, $M \models \neg\phi_i(\bar{c})$. This implies that $\neg\phi_i \in \Gamma'$. But we already had that $\phi_i \in \Gamma_0' \subseteq \Gamma'$, so $M \models \phi(\bar{c})$, contradiction.

Thus we have established that $A \cup \Gamma'(\bar{c}) \cup \{\psi(\bar{c})\}$ is consistent. Let N be a model of this set of sentences. Then M and N are both models of $A \cup \Gamma'(\bar{c})$, and Γ' is a complete set of quantifier-free sentences, so the function sending the elements

of $\bar{c}^M$ to the corresponding elements of $\bar{c}^N$ is a local isomorphism from M to N. However it is not elementary because $M \models \psi(\bar{c})$ but $N \models \neg\psi(\bar{c})$. This contradiction concludes the proof of the claim. $\dagger_{\text{Claim}}$

□

Corollary 4.3. ACF has quantifier elimination.

Proof. By Theorem 3.5, we can apply Theorem 4.2 with $A = \text{ACF}$. □

Geometrically, quantifier elimination for ACF means that if F is an algebraically closed field and $V \subseteq F^n$ is a set defined by a polynomial equation (a variety), then its projection to F^m (whose definition will have a "$\exists$") will actually also be given by a polynomial equation (i.e. will also be a variety). Another consequence is:

Corollary 4.4. If E and F are algebraically closed and E is a subfield of F, then E is an elementary substructure of F.

Proof. Immediate from quantifier elimination and the definition of an elementary substructure (note that subfields are substructures, and quantifier-free formulas are preserved across substructures). □

5. Some applications

One quick application of quantifier elimination is:

Theorem 5.1. Assume F_0 is a field, $\bar{a}$ is a tuple from F_0, and $\phi(\bar{x}, \bar{y})$ is a quantifier-free formula. If there exists a field F_1 such that $F_0 \subseteq F_1$ and $F_1 \models (\exists \bar{x})(\phi(\bar{x}, \bar{a})$, then for *all* algebraically closed extensions F of F_0, $F \models (\exists \bar{x})(\phi(\bar{x}, \bar{a})$.

Proof. Let F be an algebraically closed extension of F_0. Pick a quantifier-free formula $\phi'(\bar{y})$ equivalent to $(\exists \bar{x})(\phi(\bar{x}, \bar{y})$ over ACF. Take an algebraically closed extension F_2 of F_1. Then $F_2 \models (\exists \bar{x})(\phi(\bar{x}, \bar{a})$, so $F_2 \models \phi'(\bar{a})$, hence since ϕ' is quantifier-free, $F_0 \models \phi'(\bar{a})$ and $F \models \phi'(\bar{a})$, so $F \models (\exists \bar{x})(\phi(\bar{x}, \bar{a}))$. □

This can be used to prove Hilbert's weak Nullstellensatz theorem. Indeed, a quantifier-free formula ϕ as above can be thought as a system of finitely-many equations and inequations, and Hilbert's basis theorem says that any ideal in a ring of polynomials with coefficients in a field is finitely-generated.

We can also deduce more properties of the algebraic closure:

Definition 5.2. For any structure M, any formula $\phi(x, y_1, \ldots, y_n)$, and any $a_1, \ldots, a_n$ in the universe of M, let $\phi(M, a_1, \ldots, a_n)$ denote the set $\{a \in M \mid M \models \phi(a, a_1, \ldots, a_n)\}$.

Lemma 5.3. Assume F is an algebraically closed field, $\phi(x, y_1, \ldots, y_n)$ is a formula and $a_1, \ldots, a_n \in F$. Then $\phi(F, a_1, \ldots, a_n)$ is either finite or cofinite (i.e. its complement is finite).

Proof. By quantifier elimination, we can assume without loss of generality that ϕ is quantifier-free. Writing ϕ in disjunctive normal form, we see that ϕ is equivalent to $\bigvee_{i \leq n} \bigwedge_{j \leq m} \psi_{i,j}$, where $\psi_{i,j}$ is either an inequality or an equality. If we can prove the result for each $\psi_{i,j}$ we would be done (because finite and cofinite sets

are closed under finite intersections and unions). Now if $\psi_{i,j}$ is an equality, then it says that two polynomials are equal, i.e. that their difference has a root. Since a polynomial has only finitely-many roots, this has only finitely-many solutions (or if the polynomials are trivial cofinitely-many). An inequality is the complement of such a set, so the result follows. □

Lemma 5.4. Assume F is an algebraically closed field, X is a subset of F, and $a \in F$. Then $a \in \mathrm{acl}^F(X)$ if and only if there exists a formula $\psi(x, y_1, \ldots, y_n)$ and $a_1, \ldots, a_n \in X$ such that $\psi(x, a_1, \ldots, a_n)$ has only finitely-many solutions in F, and $F \models \psi(a, a_1, \ldots, a_n)$.

Proof. If $a \in \mathrm{acl}^F(X)$, then there is a polynomial $\tau(x, a_1, \ldots, a_n)$ witnessing it, and the formula $\tau(x, a_1, \ldots, a_n) = 0$ has only finitely-many solutions in F. Conversely, assume that there exists a formula $\phi(x, y_1, \ldots, y_n)$ and $a_1, \ldots, a_n \in X$ such that $\phi(F, a_1, \ldots, a_n)$ is finite and $F \models \phi(a, a_1, \ldots, a_n)$.

By quantifier elimination, we can assume without loss of generality that ϕ is quantifier-free. Writing ϕ in disjunctive normal form, we see that ϕ is equivalent to $\bigvee_i \bigwedge_j \phi_{i,j}$, where $\phi_{i,j}$ is either an inequality or an equality. We know that for some i, for all j, $F \models \phi_{i,j}(a, a_1, \ldots, a_n)$. Since the set of solutions of an inequality must be cofinite (or empty), there exists at least one j such that $\psi_{i,j}$ is an equality. Thus $\psi_{i,j}$ is $\tau(x, y_1, \ldots, y_n) = \rho(x, y_1, \ldots, y_n)$, so $(\tau - \rho)(x, a_1, \ldots, a_n)$ gives the desired polynomial that a is a root of. □

Before proving the next theorem, it will be convenient to introduce the following abbreviations:

Definition 5.5. Let $\rho(z, x_1, \ldots, x_n)$ be a formula. For k a positive natural number, we write $(\exists^{\geq k} z)(\rho)$ for the formula:

$$(\exists z_1 \ldots \exists z_k) \left(\bigwedge_{1 \leq i < j \leq k} z_i \neq z_j \wedge \bigwedge_{1 \leq i \leq k} \rho(z_i, x_1, \ldots, x_n) \right)$$

Also let $(\exists^{\geq 0} z)(\rho)$ stand for $(\forall z)(z = z)$. For k a natural number, write $(\exists^{> k} z)(\rho)$ for $(\exists^{\geq k+1} z)(\rho)$, $(\exists^{\leq k} z)(\rho)$ for $\neg(\exists^{> k} z)(\rho)$, and $(\exists^{< k} z)(\rho)$ for $\neg(\exists^{\geq k} z)(\rho)$. Finally, write $(\exists^{= k} z)(\rho)$ for $(\exists^{\geq k} z)(\rho) \wedge (\exists^{\leq k} z)(\rho)$.

Theorem 5.6. Assume F is an algebraically closed field, X, Y are subsets of F, and $a, b \in F$. Then:

(1) (Monotonicity) $X \subseteq \mathrm{acl}(X)$.
(2) (Finite character) If $a \in \mathrm{acl}(X)$, then there exists a finite $X_0 \subseteq X$ such that $a \in \mathrm{acl}(X_0)$.
(3) (Transitivity) If $X \subseteq \mathrm{acl}(Y)$, then $\mathrm{acl}(X) \subseteq \mathrm{acl}(Y)$.
(4) (Exchange) If $a \in \mathrm{acl}(X \cup \{b\}) \setminus \mathrm{acl}(X)$, then $b \in \mathrm{acl}(X \cup \{a\})$.

Proof. For monotonicity, observe that if $c \in X$ then c is a root of $x - c$, so $c \in \mathrm{acl}(X)$. Finite character is trivial. For transitivity, assume $X \subseteq \mathrm{acl}(Y)$, and let $c \in \mathrm{acl}(X)$. By finite character, $c \in \mathrm{acl}(X_0)$ for some finite $X_0 \subseteq X$. Set $X_0 = \{a_1, \ldots, a_n\}$. By Lemma 5.4, there is a formula $\psi(x, a_1, \ldots, a_n)$ with finitely-many solutions (say

k many) which is satisfied by c. Since $X_0 \subseteq \text{acl}(Y)$, by finite character there also is a finite subset $Y_0 \subseteq Y$ such that $X_0 \subseteq \text{acl}(Y_0)$. Set $Y_0 = \{b_1, \dots, b_m\}$. For each $i \leq n$, there exists (Lemma 5.4) a formula $\phi_i(x, b_1, \dots, b_m)$ with only finitely-many solutions which is satisfied by a_i.

Now consider the formula $\phi(x, b_1, \dots, b_m)$ given by:

$$(\exists y_1 \dots \exists y_n) \left(\bigwedge_{1 \leq i \leq n} \phi_i(y_i, b_1, \dots, b_m) \wedge (\exists^{=k} z)(\psi(z, y_1, \dots, y_n)) \wedge \psi(x, y_1, \dots, y_n) \right)$$

It is easy to see that $\phi(x, b_1, \dots, b_m)$ has only finitely-many solutions (the quantifier-free part has finitely-many solutions for each possible choice of $y_1, \dots, y_n$, and there are only finitely-many such choices by definition of the ϕ_i's), and is satisfied by c. Thus by Lemma 5.4, $b \in \text{acl}(Y_0) \subseteq \text{acl}(Y)$, as desired.

Finally, for exchange, assume $a \in \text{acl}(X \cup \{b\}) \setminus \text{acl}(X)$. Assume for simplicity that $X = \emptyset$ (in the general case, carry the parameters through the proof). There exists a formula $\phi(x, y)$ such that $F \models \phi(a, b)$ and $\phi(x, b)$ has n solutions, for $n < \omega$. Replacing $\phi(x, y)$ by $\phi(x, y) \wedge (\exists^{=n} z)(\phi(z, y)$ if necessary, we can assume without loss of generality that:

$$(\forall x \forall y)(\phi(x, y) \to \exists^{=n} z \phi(z, y))$$

We claim that $\phi(a, y)$ has finitely-many solutions, which will imply the result. Suppose not. Then $\phi(a, y)$ has cofinitely-many solutions, so $\neg\phi(a, y)$ has only finitely-many solutions, say k-many. Now the set $(\exists^{\leq k} y)(\neg\phi(F, y))$ cannot be finite, as it contains a, and $a \notin \text{acl}(\emptyset)$. Thus we can pick distinct $a_1, \dots, a_{n+1}$ that are solutions of $(\exists^{\leq k} y)(\neg\phi(x, y))$. We then have by assumption that for each $i \leq n+1$, $\phi(a_i, F)$ is cofinite, hence $\bigcap_{1 \leq i \leq n+1} \phi(a_i, F)$ is not empty. For any b' inside this set, we have that $(\exists^{>n} x)(\phi(x, b'))$, contradicting the choice of ϕ. □

Corollary 5.7. If F is an algebraically closed field and $X \subseteq F$, then $\text{acl}^F(X)$ is the smallest algebraically closed subfield of F containing X.

Proof. Immediate from the transitivity property of acl. For example, to see that if $a \in \text{acl}(X)$ then $a^{-1} \in \text{acl}(X)$, use that a^{-1} is a root of the polynomial $xa - 1$. This is a polynomial with coefficient from $\text{acl}(X)$, so $a \in \text{acl}(\text{acl}(X))$. However by transitivity $\text{acl}(\text{acl}(X)) \subseteq \text{acl}(X)$, as desired. □

Corollary 5.8. If E and F are algebraically closed fields, E_0 is a subfield of E, F_0 is a subfield of F, and $f : E_0 \cong F_0$ is an isomorphism, there exists an isomorphism $g : \text{acl}^E(E_0) \cong \text{acl}^F(F_0)$ extending f.

Proof. Exercise – use Fact 1.13 repeatedly. □

Corollary 3.7 sometimes allows us to treat fields of characteristic zero as if they were finite:

Definition 5.9. Let F be a field and n be a positive natural number. A *polynomial mapping* f from $F^n \to F^n$ is a function $f : F^n \to F^n$ for which there exists polynomials $\tau_1, \tau_2, \ldots, \tau_n$ in n variables such that $f(a_1, \ldots, a_n) = (\tau_1(a_1, \ldots, a_n), \ldots, \tau_n(a_1, \ldots, a_n))$.

Theorem 5.10 (Ax-Grothendieck theorem)**.** Assume F is an algebraically closed field, n is a positive natural number, and $f : F^n \to F^n$ is a polynomial map. If f is injective, then f is surjective.

Proof. Let $\tau_1, \ldots, \tau_n$ be the polynomials defining f. Let $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ be the sentence

$$\bigwedge_{1 \leq i \leq n} y_i = \tau_i(x_1, \ldots, x_n)$$

Let ϕ_{inj} be the sentence:

$$(\forall x_1 \ldots \forall x_n \forall x_1' \ldots \forall x_n' \forall y_1 \ldots \forall y_n)((\phi(x_1, \ldots, x_n, y_1, \ldots, y_n) \wedge \phi(x_1', \ldots, x_n', y_1, \ldots, y_n)) \to \bigwedge_{1 \leq i \leq n} x_i = x_i')$$

and let ϕ_{surj} be the sentence:

$$(\forall y_1 \ldots \forall y_n \exists x_1 \ldots \exists x_n)(\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

Then a field F' will satisfy ϕ_{inj} if and only if the function defined by $\tau_1, \ldots, \tau_n$ is injective, and similarly for ϕ_{surj}. Let ψ be the sentence $\phi_{\text{inj}} \to \phi_{\text{surj}}$. We will prove that ACF $\models \psi$. By Corollary 3.7, it suffices to prove that $\text{ACF}_p \models \psi$ for every prime p. Fix a prime p. Let K' be an algebraically closed field of characteristic p, and let $K = \text{acl}^{K'}(\emptyset)$. By Corollary 5.7, K is an algebraically closed field. Since ACF_p is complete, it suffices to see that $K \models \psi$. So assume that $K \models \phi_{\text{inj}}$. We have to see that the polynomial map defined by ϕ is surjective. So fix $\bar{b} = (b_1, \ldots, b_n) \in K^n$. We have to find $\bar{a} = (a_1, \ldots, a_n)$ such that $K \models \phi(\bar{a}, \bar{b})$. We know that each b_i is algebraic over the empty set. Of course, the field generated by $\emptyset$ is just an isomorphic copy of $\mathbb{F}_p$ which is finite so iterating Fact 1.12, there exists K_0 a subfield of K that is finite and contains $\bar{b}$. Now the restriction g of the map defined by ϕ to K_0^n has codomain K_0^n (because ϕ is a polynomial map and K_0 is a subfield of K), and g is injective. Since K_0^n is finite, g is also surjective. Therefore we can find $\bar{a} \in K_0^n$ such that $g(\bar{a}) = \bar{b}$, as desired. □

6. Categoricity in fields and beyond

It is helpful to restate Theorem 5.6 in more general terms:

Definition 6.1. A *pregeometry* (often also called a *matroid*) on a set W is a function $\text{cl} : \mathcal{P}(W) \to \mathcal{P}(W)$ satisfying the following properties. For any set $X, Y \subseteq W$ and any $a, b \in W$:

(1) (Monotonicity) $X \subseteq \text{cl}(X)$.
(2) (Finite character) If $a \in \text{cl}(X)$, then there exists a finite $X_0 \subseteq X$ such that $a \in \text{cl}(X_0)$.
(3) (Transitivity) If $X \subseteq \text{cl}(Y)$, then $\text{cl}(X) \subseteq \text{cl}(Y)$.

(4) (Exchange) If $a \in \text{cl}(X \cup \{b\}) \setminus \text{cl}(X)$, then $b \in \text{cl}(X \cup \{a\})$.

In these terms, Theorem 5.6 established that for any algebraically closed field F, acl was a pregeometry on F. Even more, we showed that anytime we have a σ-structure M, where any definable set with parameters (that is a set of the form $\phi(M, a_1, \ldots, a_n)$ for ϕ a formula and $a_1, \ldots, a_n$) is either finite or cofinite, then we can define a closure operator $\text{cl}^M(A)$ by looking at the set of elements of M that are the solutions of a formula with only finitely-many solutions. Such a structure M is called *minimal*. Lemma 5.3 established that algebraically closed fields are minimal, but there are other such structures. For example, sets with no structure are minimal. Vector spaces (say over $\mathbb{Q}$, with a unary function symbol for multiplication by each rational) are also minimal (in this case, $\text{cl}^M(A)$ is the linear span of the set A – it is a good exercise to check the axioms of pregeometries directly).

Pregeometries are a setup where an abstract theory of independence (generalizing linear independence in vector spaces and algebraic independence in fields) is possible.

Lemma 6.2 (Basic properties of pregeometries)**.** Let (W, cl) be a pregeometry, let $X, Y \subseteq W$.

(1) If $X \subseteq Y$, then $\text{cl}(X) \subseteq \text{cl}(Y)$.
(2) (Idempotence) $\text{cl}(\text{cl}(X)) = \text{cl}(X)$.
(3) $|\text{cl}(X)| = |X| + \sup_{X_0 \subseteq X, |X_0| < \aleph_0} |\text{cl}(X_0)|$.

Proof.

(1) Combine monotonicity and transitivity.
(2) Let $Y = \text{cl}(X)$. By monotonicity, $Y \subseteq \text{cl}(Y)$. Now $Y = \text{cl}(X) \subseteq \text{cl}(X)$, so by transitivity, $\text{cl}(Y) \subseteq \text{cl}(X) = Y$. Thus $Y = \text{cl}(Y)$.
(3) Exercise.

□

In any pregeometry, one can define a notion of basis:

Definition 6.3. Let (W, cl) be a pregeometry. A set $I \subseteq W$ is called *independent* if for all $i \in I$, $i \notin \text{cl}(I \setminus \{i\})$. A *basis* is a maximal independent set (i.e. an independent set with no proper independent extension).

Using transfinite induction, it is easy to see that any independent set extends to a basis. In particular (starting with the empty independent set), any pregeometry has a basis. Moreover:

Lemma 6.4. Assume that (W, cl) is a pregeometry. If I is an independent set and $a \in W$, then $I \cup \{a\}$ is independent if and only if $a \notin \text{cl}(I)$. In particular, if I is a basis then $\text{cl}(I) = W$.

Proof. If $a \in \text{cl}(I)$, then $a \in \text{cl}((I \cup \{a\}) - \{a\})$, so $I \cup \{a\}$ is not independent. Conversely, assume that $a \notin \text{cl}(I)$. Let $J = I \cup \{a\}$. Pick $j \in J$. If $j = a$, then by definition $a \notin \text{cl}(J \setminus \{j\}) = \text{cl}(I)$. Suppose now that $j \neq a$, i.e. $j \in I$, and suppose that $j \in \text{cl}(J - \{j\})$. By the assumption that I is independent, $j \notin \text{cl}(I - \{j\}) =$

$\mathrm{cl}((J - \{j\}) - \{a\})$. Setting $X = I - \{j\}$, we have that $j \in \mathrm{cl}(X \cup \{a\}) \setminus \mathrm{cl}(X)$, so by exchange $a \in \mathrm{cl}(X \cup \{j\}) = \mathrm{cl}(I)$, a contradiction. □

More interesting, just like in vector spaces, any two bases have the same cardinality:

Theorem 6.5. In a pregeometry, any two bases have the same cardinality.

To prove this, we need a variation on the exchange property:

Lemma 6.6. Assume (W, cl) is a pregeometry and A and B are bases. For any $a \in A$, there exists $b \in B$ such that $(A - \{a\}) \cup \{b\}$ is a basis.

Proof. We know that $W = \mathrm{cl}(A) = \mathrm{cl}(B)$. Also, $a \notin \mathrm{cl}(A - \{a\})$, so $\mathrm{cl}(A - \{a\}) \neq W$. By transitivity, $B \not\subseteq \mathrm{cl}(A - \{a\})$, so there exists $b \in B$ such that $b \notin \mathrm{cl}(A - \{a\})$. Let $I = (A - \{a\}) \cup \{b\}$. By Lemma 6.4, I is independent. It remains to see that $W = \mathrm{cl}(I)$. Write $A_0 = A - \{a\}$.

We know that $b \in \mathrm{cl}(A) = \mathrm{cl}(A_0 \cup \{a\}) = W$, but $b \notin \mathrm{cl}(A_0)$. By exchange, $a \in \mathrm{cl}(A_0 \cup \{b\}) = \mathrm{cl}(I)$. By transitivity, this means that $W = \mathrm{cl}(A_0 \cup \{a\}) \subseteq \mathrm{cl}(I)$, so $\mathrm{cl}(I) = W$. □

We now start out by proving Theorem 6.5 for finite bases.

Lemma 6.7. Assume (W, cl) is a pregeometry and A and B are bases. If A is finite and $|A| \leq |B|$, then $|A| = |B|$.

Proof. Set $n = |A|$. Write $A = \{a_i : i < n\}$. We build $(b_i)_{i<n}$ elements of B such that for all $i \leq n$, the set:

$$C_i = \{a_j : i \leq j < n\} \cup \{b_j : j < i\}$$

is a basis.

The construction is by induction on i. Fix $i < n$ and assume we are given $(b_j)_{j<i}$ and we know that C_i is a basis (when $i = 0$, $C_0 = A$ so it is a basis by assumption). Apply Lemma 6.6 to C_i, B, and a_i to obtain $b_i \in B$ such that $C_{i+1} = (C_i - \{a_i\}) \cup \{b_i\}$ is a basis.

When we are done, the set $C_n = \{b_i : i < n\}$ is a basis that is a subset of B. Since B is itself a basis, we must have that $C_n = B$, so $|B| \leq n = |A|$, as desired. □

Proof of Theorem 6.5. Assume (W, cl) is a pregeometry and fix bases A and B. Without loss of generality, $|A| \leq |B|$. If A is finite, we are done so assume that A, and hence B, are infinite. Assume also for a contradiction that $|A| < |B|$. Since $\mathrm{cl}(A) = W = \mathrm{cl}(B)$, we have in particular that (finite character) for each $b \in B$, there exists a finite $A_b \subseteq A$ such that $b \in \mathrm{cl}(A_b)$. There are only $|A|$-many finite subsets of A (since A is infinite), so by the (infinite) pigeonhole principle, there exists an infinite $B' \subseteq B$ and a finite $A_0 \subseteq A$ such that $A_b = A_0$ for all $b \in B'$. In particular, $B' \subseteq \mathrm{cl}(A_0)$. Now let $W_0 = \mathrm{cl}(A_0)$, and consider the pregeometry induced by cl on W_0. In this pregeometry, A_0 is a finite basis, but B' is an infinite independent set, which can be extended to an infinite basis. This contradicts Lemma 6.7. □

Theorem 6.5 allows us to make the following definition:

Definition 6.8. The *dimension* of a pregeometry is the cardinality of its bases.

The relationship between dimension and cardinality is given by:

Lemma 6.9. If (W, cl) is a pregeometry where W is uncountable and the closure of any finite set is countable, then (W, cl) has dimension $|W|$.

Proof. Exercise. □

For algebraically closed fields, the dimension of the pregeometry induced by algebraic closure is called the *transcendence degree*. It uniquely determines the field:

Theorem 6.10. Any two algebraically closed fields with the same characteristic and the same transcendence degree are isomorphic.

Proof. Let F and K be algebraically closed fields of transcendence degree λ. Let B and C be bases for F and K respectively. They both have dimension λ, so there is a bijection $f : B \to C$. We know that F and K have the same characteristic, so there exists an isomorphism $g : F_0 \cong K_0$ between their prime subfields. By Corollary 5.8, g extends to an isomorphism $g_0 : \text{acl}(F_0) \cong \text{acl}(K_0)$. Now take $b \in B$ (note that $\text{acl}(F_0) = \text{acl}(\emptyset)$, so does not contain B). By Fact 1.13, g_0 extends to $g_1 : \text{acl}(F_0)(b) \cong \text{acl}(K_0)(f(b))$. We can then extend g_1 again to the algebraic closure of each field. Continuing in this way (into the transfinite, taking unions at limits), we can build an isomorphism $g_\lambda : \text{acl}(B) \cong \text{acl}(C)$. But $\text{acl}(B) = F$ and $\text{acl}(C) = K$, so we are done. □

Corollary 6.11. Let λ be an uncountable cardinal and let F and K be two algebraically closed fields of cardinality λ with the same characteristic. Then $F \cong K$. In other words, for any p prime or zero ACF_p is categorical in every uncountable cardinal.

Proof. We know that (F, acl) and (K, acl) are pregeometries. Moreover, the algebraic closure of a countable set is countable by Exercise 1.10. By Lemma 6.9 it follows that F and K have transcendence degree λ. By the previous theorem, $F \cong K$. □

Corollary 6.12. Any algebraically closed field of characteristic zero and cardinality $2^{\aleph_0}$ is isomorphic to $\mathbb{C}$.

We emphasize that many of those results could have been derived just using field theory. Here, we tried to minimize the reliance on field theory and instead use general logical methods. Such methods can be applied to other objects. For example, there is a well-developed theory of *differential fields*, where we also add an operator ∂ to the field, assumed to have some of the properties of the derivative (we think of the objects of the field as differentiable functions). The properties of differentially *closed* fields (roughly, differential fields where any differential equation that can possibly have a solution has a solution) are then key. See Poizat's book for more on differential fields.

Pushing the logical methods further, one can also prove the following deep "converse" to categoricity of ACF_0 in uncountable cardinals:

Theorem 6.13 (Morley's categoricity theorem)**.** If a countable theory is categorical in *some* uncountable cardinal, then it is categorical in *all* uncountable cardinals.

Part of one proof of Morley's theorem uses minimal formulas to prove categoricity in a way similar to what has been done in these notes. Still, a lot of the model-theoretic ideas of the proof have not been touched on here. The philosophical content of the theorem is that if a theory is categorical in some uncountable cardinal, then it must be for a "reason", namely the existence of a notion of independence, and hence of a notion of dimension, and this reason is strong-enough to imply categoricity everywhere as well. Exploring the ideas, ramifications, and generalizations of the proof of Morley's categoricity theorem is an important goal of modern model theory.