6 The Ax–Kochen Eršov Theorem

6.1 Quantifier Elimination in the Pas Language

We will be considering valued fields as three-sorted objects $(K, \Gamma, \boldsymbol{k})$ in the Pas language where we have the language of rings $\{+, -, \cdot, 0, 1\}$ on both the home sort, i.e. the field K, and the residue field sort, the language of ordered groups $\{+, -, <, 0\}$ on the value group sort, the valuation map $v : K^\times \to \Gamma$ and an angular component map $\mathrm{ac} : K^\times \to \boldsymbol{k}^\times$. Not all valued fields have angular component maps, but for any valued field we can pass to an elementary extension where there is an angular component map.

Let Δ_0 be the collection of all formulas of the form

- $\phi(\mathbf{u})$, where ϕ is a quantifier free formula in the language of rings and $\mathbf{u}$ are variables in the field sort;
- $\psi(v(f_1(\mathbf{u})), \ldots, v(f_k)(\mathbf{u})), \mathbf{v}))$ where ψ is a formula in the language of ordered groups, $\mathbf{u}$ are variables in the field sort, f_i is a term in the ring language and $\mathbf{v}$ are variables in the value groups sort;
- $\theta(\mathrm{ac}(g_1(\mathbf{u})), \ldots, \mathrm{ac}(g_k)(\mathbf{u})), \mathbf{w}))$ where ψ is a formula in the language of ordered groups, $\mathbf{u}$ are variables in the field sort, g_i is a term in the ring language, and $\mathbf{w}$ are variables in the residue sort;

Note that we are allowing quantifiers over the value group and the residue field but not over the home sort. Let Δ be the collection of finite boolean combinations of Δ-formulas. Note that each Δ formula is equivalent to a formula of the form

$$\phi(\mathbf{u}) \wedge \psi(v(f_1(\mathbf{u})), \ldots, v(f_k)(\mathbf{u})), \mathbf{v})) \wedge \theta(\mathrm{res}(g_1(\mathbf{u})), \ldots, \mathrm{res}(g_l)(\mathbf{u})), \mathbf{w})),$$

where ϕ, ψ and θ are as above.

Theorem 6.1 (Pas) *Let T be the theory of henselian valued fields with angular components where the residue field has characteristic zero. Then every formula is equivalent to a Δ-formula.*

We will use the following relative quantifier elimination test.

Exercise 6.2 Suppose $\mathcal{L}$ is countable. Let Δ be a collection of formulas closed under finite boolean combinations and let T be an $\mathcal{L}$-theory with the following property.

Whenever $\mathcal{M}$ and $\mathcal{N}$ are models of T, $|\mathcal{M}| = \aleph_0$ $\mathcal{N}$ is $\aleph_1$-saturated, $A \subset \mathcal{M}$ and $f : A \to \mathcal{N}$ is a Δ-embedding (i.e, $\mathcal{M} \models \theta(\mathbf{a}) \Leftrightarrow \mathcal{N} \models \theta(f(\mathbf{a})$ for $\mathbf{a} \in A$ and $\theta \in \Delta$), then there is $\widehat{f} : \mathcal{M} \to \mathcal{N}$ that is Δ preserving.

Show that every $\mathcal{L}$-formula is equivalent to a Δ-formula. [Hint: add predicates for all formulas in Δ.]

Our main step will be proving an embedding result. We look at embeddings that preserved Δ-formulas. A map $f : (A, \Gamma_A, \boldsymbol{k}_A) \to L$ is an Δ-embedding if:

i) $f|A$ is a ring embedding;
ii) $f|\Gamma_A$ is a partial elementary embedding in the language of groups;
iii) $f|\boldsymbol{k}_A$ is a partial elementary embedding in the language of rings;
iii) f preserves v and ac.

Theorem 6.3 *Let $(K, \Gamma, \boldsymbol{k})$ and $(L, \Gamma_L,\ k_L)$ be henselian valued fields with angular component with characteristic zero residue field. Suppose K is countable, L is $\aleph_1$-saturated, $(A, \Gamma_A, \boldsymbol{k}_A)$ is a countable substructure of K, and $f : (A, \Gamma_A, \boldsymbol{k}_A) \to (L, \Gamma_L, \boldsymbol{k}_L)$ is a Δ-embedding. Then there is an extension of f to a Δ-embedding $\widehat{f} : (K, \Gamma_K, \boldsymbol{k}_K) \to (L, \Gamma_L, \boldsymbol{k}_L)$.*

Henceforth, we assume K is countable and L is $\aleph_1$-saturated. We extend our map by iterating the following lemmas.

Note that in a substructure $(A, \Gamma_A, \boldsymbol{k}_A)$, A and $\boldsymbol{k}_A$ are domains, while Γ_A is a subgroup.

Lemma 6.4 *Suppose $(A, \Gamma_A, \boldsymbol{k}_A)$ be a subring of K and $f : (A, \Gamma_A, \boldsymbol{k}_A) \to (L, \Gamma, \boldsymbol{k}_L)$ is a Δ-embeddings. Let F be the fraction field of A and let $\boldsymbol{l}$ be the fraction field of $\boldsymbol{k}_A$. We can extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{l})$ into L.*

Proof There is a unique extension of f to $(F, G, \boldsymbol{l})$. Since $v(a/b) = v(a) - v(b)$ and $\mathrm{ac}(x/y) = \mathrm{ac}(x)/\mathrm{ac}(y)$, $v_L(f(a/b)) = f(v(a/b))$ and $\mathrm{ac}_L(f(x/y)) = f(\mathrm{ac}(x/y))$, f is a Δ-embedding. $\square$

Henceforth, we will work only with substructures $(F, \Gamma_F, \boldsymbol{k}_F)$ where F and $\boldsymbol{k}_F$ are fields and Γ_F is a group, $v(F) \subseteq \Gamma_F$ and $\mathrm{ac}(F) \subseteq \boldsymbol{k}_F$.

We next show how to extend the value group.

Lemma 6.5 *Suppose $f : (F, \Gamma_F, \boldsymbol{k}_F) \to (L, \Gamma_L, \boldsymbol{k}_L)$ is a Δ-embedding. We can extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{k}_F)$.*

Proof We will prove this by iterating the following claim.

claim Let $\gamma \in \Gamma \setminus \Gamma_F$ and let G be the group generated by Γ_F and γ, then we can extend f to $(F, G, \boldsymbol{k}_F)$.

Let $p(v)$ be the type $\{\psi(v, f(g_1), \ldots, f(g_m)) : g_1, \ldots, g_m \in \Gamma_F$, ψ a formula in the language of ordered groups where $\Gamma \models \psi(\gamma, g_1, \ldots, g_m)$. If $\psi_1, \ldots, \psi_n \in p(v)$ with parameters $f(g_1), \ldots, f(g_m)$, then, since f is a Δ-embedding

$$\Gamma_L \models \exists v \bigwedge_{i=1}^{n} \psi_i(v, f(g_1), \ldots, f(g_m)).$$

Thus $p(v)$ is consistent and, by $\aleph_1$-saturation, realized in Γ_L. Let γ' be a realization and extend f by $\gamma \mapsto \gamma'$. $\square$

Lemma 6.6 *If we have a Δ-embedding f defined on $(F, \Gamma, \boldsymbol{k}_F)$ we can extend it to $(F, \Gamma, \boldsymbol{k})$.*

Exercise 6.7 Prove Lemma 6.6.

We next make the residue map surjective.

Lemma 6.8 *Suppose f is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$. Then we can find $F \subseteq E \subseteq K$ such that* res : $E \to \boldsymbol{k}$ *is surjective and we can extend f to a Δ-embedding of $(E, \Gamma, \boldsymbol{k})$.*

Proof We iterate the following two claims and Lemma 6.4.

claim 1 Suppose we have a Δ-embedding $f : (F, \Gamma, \boldsymbol{k}) \to (L, \Gamma_L, \boldsymbol{k}_L)$ and $b \in K$ with residue $\overline{b}$ algebraic over $\mathrm{res}(F)$ but not in $\mathrm{res}(F)$. Then we can extend f to $F(b)$.

There is $p(X) \in \mathcal{O}_F[X]$ irreducible with $\overline{p}(X)$ the minimal polynomial of $\overline{b}$ over $\mathrm{res}(F)$. Let $q(X) \in \mathcal{O}_{f(F)}[X]$be the image of p. Since the embedding of residue fields is elementary, $\overline{q}(X)$ is irreducible in $f(\mathrm{res}(F))$ and $\overline{q}(f(\overline{b})) = 0$. Moreover, since $\boldsymbol{k}_L$ has characteristic zero and $\overline{q}$ is irreducible, $\overline{q}'(f(\overline{b})) \neq 0$. Since L is henselian, there is unique $c \in L$ such that $q(c) = 0$ and $\overline{c} = f(\overline{b})$. We extend f to $F(b)$ by $b \mapsto c$.

We need to show that the valuation and angular component are preserved. Let d be the degree of p. Let $x \in F(b) = \alpha(\sum_{i=0}^{d-1} a_i b^i)$ where $\alpha \in F, a_i \in \mathcal{O}_F$ and some $v(a_i) = 0$ for some i. As $\overline{p}$ is the minimal polynomial of $\overline{b}$, $\sum \overline{a}_i \overline{b}^i \neq 0$. Thus $v(x) = v(\alpha)$ and $v(f(x)) = v(f(\alpha))$ and $\mathrm{ac}(x) = \mathrm{ac}(\alpha)(\sum \overline{a}_i \overline{b}^i)$. A similar analysis shows $\mathrm{ac}_L(f(x)) = \mathrm{ac}_L(f(\alpha))(\sum \overline{f(a_i)} \overline{c}^i)$.

claim 2 Suppose we have a Δ-embedding $f : (F, \Gamma, \boldsymbol{k}) \to (L, \Gamma_L, \boldsymbol{k}_L)$ and $b \in B$ with residue $\overline{b}$ transcendental over $\mathrm{res}(F)$. Then we can extend f to $F(b)$.

Let $c \in L$ with $\overline{c} = f(\overline{b})$. Then c is transcendental over F and we can extend f by $b \mapsto c$. We need to show that the valuation and angular component are preserved. If $x \in F[b]$ we can write $x = \alpha(\sum a_i b^i)$ where $\alpha \in F$, $a_i \in O_F$ and $v(a_i) = 0$ for some i. Then as in claim 2, $v(x) = v(\alpha)$ and $v(f(x)) = v(f(\alpha))$, $\mathrm{ac}(x) = \mathrm{ac}(\alpha)(\sum \overline{a}_i \overline{b}^i)$ and v and ac are preserved. As in Lemma 6.4, we can extend to f from $F[b]$ to $F(b)$. $\square$

Next we make the valuation surjective.

Lemma 6.9 *Suppose f is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$. There is $F \subseteq E \subseteq K$ such that $v : E \to \Gamma$ is surjective and we can extend f to $(E, \Gamma, \boldsymbol{k})$.*

Proof The lemma is proved by iterating the following two claims.

claim 1 Suppose we have a Δ-embedding f of $(F, \Gamma, \boldsymbol{k})$ where the residue map from F to $\boldsymbol{k}$ is surjective and $g \in \Gamma$ such $ng \notin v(F)$ for any $n > 0$. Let $b \in K$ with $v(b) = g$. We will extend f to $F(b)$.

Since g is not in the divisible hull of $v(F)$, b is transcendental over F. Let $c \in L$ with $v(c) = f(g)$ and $\mathrm{ac}_L(c) = f(\mathrm{ac}(b))$. We can extent f to $F(b)$ with $b \mapsto c$. Let $x = \sum a_i b^i$ recall that $v(x) = \min(v(a_i) + iv(b))$ and $v_L(f(x)) = \min v_L(f(a_i) + if(g))$. Choose i such that $v(a_i) + iv(b)$ is minimal, then $x = a_i b^i(1 + \epsilon)$ where $v(\epsilon) > 0$ and $\mathrm{ac}(x) = \mathrm{ac}(a_i)\mathrm{ac}(b)^i$. Similarly, $\mathrm{ac}_L(f(x)) = \mathrm{ac}_L(f(a_i)\mathrm{ac}(c)^i$, as desired.

claim 2 Suppose we have a Δ-embedding f of $(F, \Gamma, \boldsymbol{k})$ where the residue map from F to $\boldsymbol{k}$ is surjective and let $n > 0$ be minimal such that there is $g \in \Gamma \setminus v(F)$ such that $g > 0$ and $ng \in v(F)$. Then we can extend F to E with $F \subset E \subseteq K$ and extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$ such that $g \in v(E)$.

Let $a \in F$ and $b_0 \in K$ be such that $v(b_0) = g$ and $v(a) = ng$. Since the residue field does not extend we can choose a such that $\mathrm{ac}(b_0^n) = \overline{a}$, in which case $b_0^n = a(1+\epsilon)$ where $\epsilon \in K$ and $v(\epsilon) > 0$. Since K is henselian, there is $d \in K$ with $v(d) = 0$ such that $d^n = 1 + \epsilon$. Let $b = b_0/d$. Then $b^n = a$. By the minimality of n, $X^n - a$ is the minimal polynomial of b over F.

Similarly, we can find $c \in L$ such that $c^n \in f(F)$ and $v_L(c^n) = v(f(a))$. Then $\mathrm{ac}(c)$ is algebraic over $\boldsymbol{k}_{f(F)}$. But $\boldsymbol{k}_{f(F)} \prec \boldsymbol{k}_L$, thus, $\mathrm{ac}(c_0) \in \boldsymbol{k}_{f(F)}$. Thus there is $d \in \mathcal{O}_{f(F)}$ with $\overline{d} = f(\mathrm{ac}(b))\mathrm{ac}(c_0^{-1})$. Let $c_1 = dc_0$. Then $\mathrm{ac}(c_1) = f(\mathrm{ac}(b))$ and $f(a) = f(b^n) = c_1^n(1+\epsilon)$ where $v(\epsilon) > 0$. By henselianity, there is $e \in L$ such that $e^n = (1+\epsilon)$. Let $c = c_1 e$, then $c^n = f(a)$, $v(c) = f(v(b))$ and $\mathrm{ac}(c) = f(\mathrm{ac}(b))$. We extend f to $F(b)$ by $b \mapsto c$. As in Lemma 6.5, we show that f preserves the valuation and the the angular component map. $\square$

Lemma 6.10 *Suppose the residue and valuation maps of $(F, \Gamma, \boldsymbol{k})$ are surjective and f is a Δ-embedding. Then we can extend F to $(F^h, \Gamma, \boldsymbol{k})$*

Proof There is a unique valuation preserving extension of f from F to $g : F^h \to L$. We know that F^h is an immediate extension of f. If $a \in F^h \setminus F$, there is $b \in F$, with $v(a) = v(b)$, but then $v(g(a)) = v(g(b))$. There is c a unit in $\mathcal{O}_F$ such that $\mathrm{res}(c) = \mathrm{res}(a/b)$. Thus $\mathrm{ac}(a) = \mathrm{ac}(b)\mathrm{ac}(c)$ and $\mathrm{ac}_L(g(a)) = \mathrm{ac}_L(g(b))\mathrm{ac}_L(g(c))$. $\square$

We can now finish the proof of Theorem 6.3

Thus we may assume that we have a $(F, \Gamma, \boldsymbol{k})$ such that F is henselian, $v : F \to \Gamma$ and $\mathrm{res} : F \to \boldsymbol{k}$ are surjective and f is a Δ-embedding. Then K is an immediate extension of F. By Zorn's Lemma, we may assume that $F \subseteq K$ is maximal henselian such that there is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$ into L extending f. We claim that $F = K$. If not, let $b \in K \setminus F$. We will show that we can extend f to $F(b)$. Since F is henselian and $\boldsymbol{k}_B$ has characteristic zero, by Theorem 5.14, b is transcendental over F.

We can find a pseudocauchy sequence (a_α) in F of transcendental type with no pseudolimit in F such that $(a_\alpha) \rightsquigarrow b$, (a_α) has no pseudolimit in F and $(v(p(a_\alpha))$ is eventually constant for $p \in F[T]$.

By $\aleph_1$-saturation, we can find $c \in L$ such that $(f(a_\alpha)) \rightsquigarrow c$. Extend f to $F(b)$ by $x \mapsto c$. For $p \in F[T]$,

$$v_L(f(p(b))) = v_L(f(p)(b)) = v_L(f(p)(f(a_\alpha))) = v_L(f(p(a_\alpha)) = f(v(p(a_\alpha)) = f(v(p(b)))$$

for large enough α. Similarly, $\mathrm{ac}(p(b)) = \mathrm{ac}(p(a_\alpha))$ for large enough α and it follows that $f(\mathrm{ac}(p(b))) = \mathrm{ac}_L(f(p(b)))$. But this contradicts the maximality of F.

This completes the proof.

6.2 Consequence of Quantifier Elimination

Let T_0 be the theory in the language of three sorted valued fields asserting that we have $(K, \Gamma, \boldsymbol{k})$ where K is a henselian valued field where Γ is the value group and $\boldsymbol{k}$ is a the residue field.

Corollary 6.11 (Ax-Kochen, Eršov) *Let $(K, \Gamma, \boldsymbol{k})$ be a henselain valued field with characteristic zero residue field. Let T_Γ be the theory of the value group in the language of ordered groups and $T_{\boldsymbol{k}}$ be the theory of the residue field in the language of rings. Then $T = T_0 \cup T_\Gamma \cup T_{\boldsymbol{k}}$ is complete.*

Proof Let K and L be models of T and let $K \prec K^*$ and $L \prec L^*$ be $\aleph_1$-saturated elementary extensions. We can define angular component maps on K^* and L^*. Consider the substructure $(\mathbb{Q}, \{0\}, \mathbb{Q})$. Since T_Γ and $T_{\boldsymbol{k}}$ are complete, the identification of this structure in K^* and L^* is a Δ-embedding. Let K' be a countable elementary submodel of K^* in the Pas-language. By Theorem 6.3, we can extend this to a Δ-embedding of K into L^*. Let ϕ be any sentence in the language of valued fields. There is ψ a disjunction of Δ-sentences equivalent to ϕ. Then

$$K \models \phi \Leftrightarrow K^* \models \phi \Leftrightarrow K' \models \psi \Leftrightarrow L^* \models \psi \Leftrightarrow L^* \models \phi \Leftrightarrow L \models \phi.$$

$\square$

Corollary 6.12 *Let $\mathcal{U}$ be an nonprinciple ultrafilter on the set of primes. Then*

$$\prod \mathbb{Q}_p/\mathcal{U} \equiv \prod \mathbb{F}_p((T))/\mathcal{U}.$$

In particular, for any sentence in the language of valued fields $\mathbb{Q}_p \models \phi$ for all but finitely many primes p if and only if $\mathbb{F}_p((T)) \models \phi$ for all but finitely many primes p.

Proof $\prod \mathbb{Q}_p/\mathcal{U}$ and $\prod \mathbb{F}_p((T))/\mathcal{U}$ are henselian valued fields with value group $\prod \mathbb{Z}/\mathcal{U}$ and characteristic zero residue field. Hence they are elementarily equivalent.

If $\mathbb{Q}_p \models \phi$ for all but finitely many primes and D is an infinite set of primes where $\mathbb{F}_p((T)) \models \neg\phi$, let $\mathcal{U}$ be an ultrafilter on the primes such that $D \in \mathcal{U}$. Then, by the Fundamental Theorem of Ultraproducts $\prod \mathbb{Q}_p/\mathcal{U} \models \phi$ and $\prod \mathbb{F}_p((T))/\mathcal{U} \models \neg\phi$, a contradiction. The converse is similar. $\square$

Exercise 6.13 Show that if the Continuum Hypothesis is true then $\prod \mathbb{Q}_p/\mathcal{U} \cong \prod \mathbb{F}_p((T))/\mathcal{U}$.

We will discuss applications of this in the next section.

Corollary 6.14 *Suppose $(K, \Gamma, \boldsymbol{k})$ is a valued field with angular component and T_Γ and $T_{\boldsymbol{k}}$ have quantifier elimination, then every formula is equivalent to a quantifier free formula.*

Proof Every Δ-formula is equivalent to a quantifier free formula. $\square$

Exercise 6.15 Let $K \subset L$ be henselian valued fields of characteristic zero. Suppose $\Gamma_K \prec \Gamma_L$ and $\boldsymbol{k}_K \prec \boldsymbol{k}_L$. Show that $K \prec L$.

We can generalize Corollary 5.17 to drop the assumption that our field is ordered and the valuation ring is convex.

Corollary 6.16 *Let K be a henselian valued field with real closed residue field and divisible value group. Then K is real closed.*

As in ACVF in equicharacteristic zero henselian valued fields the resiude field and value group are stably embedded and orthogonal.

Exercise 6.17 Let $(K, \Gamma, \boldsymbol{k})$ be a henselian valued field with characteristic zero residue field. Any definable subset of $\Gamma^m \times \boldsymbol{k}^n$ is a finite union of rectangles $A \times B$ where $A \subseteq \Gamma^m$ is definable in the group language and $B \subset \boldsymbol{k}^n$ is definable in the ring language.

NIP

Not all theories of henselian valued fields have NIP. For example the theory of $\prod \mathbb{Q}_p/\mathcal{U}$ has the independence property since the pseudofinite field $\prod \mathbb{F}_p/\mathcal{U}$ has the independence property.

Exercise 6.18 **[Duret]** **[14]** Show that the theory of any infinite pseudofinite field has the independence property. In particular, show that for any distinct $a_1, \ldots, a_m$ there are b_I for $I \subseteq \{1, \ldots, m\}$ such that $a_i + b_J$ is a square if and only if $i \in J$. [Recall that in an infinite pseduofinite field every absolutely irreducible variety has a point.]

Indeed the theory of $\prod \mathbb{Q}_p/\mathcal{U}$ is NTP$_2$. In fact, failure of NIP in the residue field is the only obstruction to NIP. Delon [6] proved that a Henselian valued field with characteristic zero residue field has NIP if and only if the theories of the residue field and the value group have NIP. But Gurevich and Schmitt [18] showed that all theories of ordered abelian groups have NIP.

Theorem 6.19 (Delon) *Henselian valued field with characteristic zero residue fields have NIP if and only if the theory of the residue field has NIP and the theory of value group has NIP.*

Corollary 6.20 *Henselian valued field with characteristic zero residue fields have NIP if and only if the theory of the residue field has NIP.*

We will give a proof of Delon's theorem from Simon [31]. We will use an alternative characterization of the independence property (see [31] 2.7).

Lemma 6.21 *A formula $\phi(x, \mathbf{y})$ has the independence property if and only if, in a suitably saturated model, there is an indiscernible sequence $(x_0, x_1, \ldots)$ and $\mathbf{b}$ such that $\phi(x_i, \mathbf{b})$ holds if and only if i is even.*

Lemma 6.22 *Let $(K, \Gamma, \boldsymbol{k})$ be a valued field with angular component, $f(X) = a_0 + a_1 X + \cdots + a_d X^d \in K[X]$ and let $x_0, x_1, \ldots$ be a sequence of elements of K such that $v(x_0), v(x_1), \ldots$ is strictly increasing or strictly decreasing. There is $r \leq d$ and $t \in \mathbb{N}$ such that*

$$v(f(x_i)) = v(a_r x_i^r) < v(a_j x_i^j) \text{ and } \mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$$

for all $i \geq t$ and $j \neq r$.

Proof Consider the cut $v(x_i)$ makes with respect to the finite set $X = \{\frac{v(a_j)-v(a_k)}{k-j} : 0 \leq i < j \leq d\}$. Since $v(x_i)$ is strictly increasing or strictly decreasing, there is an t such that for all $v(x_i)$ are not in X and realize the same cut over X for $i \geq t$.

Note that if $\frac{v(a_j)-v(a_k)}{k-j} < v(x_i)$, then $v(a_j x_i^j) < v(a_k x_i^k)$. Choose r such that $v(a_r x_i^r)$ is minimal, then r is unique and works for all $i \geq t$. In this case, $v(f(x_i)) = v(a_r x_i^r)$ and $\mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$ for $i \geq t$, as desired. $\square$

Lemma 6.23 *Let $(K, \Gamma, \boldsymbol{k})$ be an $\aleph_1$-saturated valued field with angular component and let $x_0, x_1, \ldots$ be a sequence of indiscernibles in K. Then there are indiscernible sequences $g_0, g_1, \ldots$ of indiscernibles in Γ and $b_0, b_1, \ldots$ of indiscernibles in $\boldsymbol{k}$ such that for any $f \in K[X]$ there is r and $\gamma \in \Gamma$ such that $v(f(x_i)) = \gamma + r g_i$ and there is $q \in \boldsymbol{k}[x]$ such that $\mathrm{ac}(f(x_i)) = q(b_i)$ for all large enough i.*

Proof

case 1 The sequence $v(x_0), v(x_1), \ldots$ is nonconstant.

We take $g_i = v(x_i)$ and $b_i = \mathrm{ac}(x_i)$. Then by indiscernibility it is either strictly increasing or strictly decreasing and we can apply the previous lemma to conclude that $v(f(x_i)) = v(a_r x_i^r)$ and $\mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$ for large enough i. Thus the lemma is true if we take $\gamma = v(a_r)$ and $q(X) = a_r X^r$.

From now on we assume that $v(x_0), v(x_1), \ldots$ is a constant sequence. Let $y_i = x_i - x_0$. The sequence $v(y_0), v(y_1), \ldots$ is not strictly increasing. If it were, then

$$v(x_i - x_1) = v((x_i - x_0) - (x_1 - x_0)) = v(y_i - y_1) = v(y_1).$$

But then the sequence $(v(x_i - x_1))$ is constant, while the sequence $v(x_i - x_0)$ is increasing, contradicting indiscernibility.

case 2 The sequence $v(y_1), v(y_2), \ldots$ is decreasing.

In this case we will take $g_i = v(y_{i+1})$, $a_i = \mathrm{ac}(y_{i+1}$. Let $f(X) \in K[X]$. There is $h(X) \in K[X]$ such that $f(x_i) = f(x_0 + y_i) = f(x_0) + h(y_i)$ for all $i > 0$. As in case 1, we can apply the previous lemma applied to the sequence $y_1, y_2, \ldots$.

case 3 The sequences $(v(y_i))$ and $(\mathrm{ac}(y_i))$ are constant.

Then

$$v(x_2 - x_1) = v(y_2 - y_1) > v(y_1) = v(y_2) = v(x_2 - x_0)$$

Find $x_\omega \in K$ such that $x_0, x_1, \ldots, x_\omega$ is an indiscernible sequence of order type $\omega + 1$. Let $z_i = x_\omega - x_i$. By indiscernibility, $v(z_1), v(z_2), \ldots$ is an increasing sequence. Let $g_i = v(z_{i+1})$ and $a_i = \mathrm{ac}(z_i)$. For $f(X) \in K[X]$ as in case 2 there is $h(X) \in K[X]$ such that for $i > 0$ $f(x_i) = h(z_i)$ using the lemmas we proceed as in the previous cases.

case 4 The sequence $v(y_i)$ is constant but the sequence $(\mathrm{ac}(y_i))$ is not.

In this case let $g_i = v(y_0)$, a constant sequence, and let $b_i = \mathrm{ac}(y_i)$.

For any $f(X) \in K[X]$ we can find $h(X) \in K[X]$ such that

$$f(x_0 + Y) = h(y_i) = \sum_{n=0}^{d} a_n Y^n.$$

Let $A \subset \{0, \ldots, d\}$ be the set of n such that $v(a_n) + ng_0$ is minimal. Let $q(X) = \sum_{n \in A} \mathrm{ac}(a_n) X^n$. For sufficiently large i, $q(\mathrm{ac}(y_i)) \neq 0$. But then

$$v(f(x_i)) = v\left(\sum_{n=0}^{d} a_n y_i^n\right) = v\left(\sum_{n \in A} a_n y_i^n\right) = v(a_n) + ng_0 = v(a_n) + ng_i$$

and

$$\mathrm{ac}(f(x_i)) = q(\mathrm{ac}(y_i))$$

where n is any fixed element of A and i is sufficiently large. $\square$

We are now ready to prove Delon's Theorem. By the Pas quantifier elimination and the basic facts about NIP from Lemma 4.21. it suffices to show that formulas of the following form have NIP.

1. $f(x, \mathbf{y}) = 0$, $f \in K[X, \mathbf{Y}]$ and $x, \mathbf{y}$ are variables in the home sort;

2. $\phi(x, t_1(\mathbf{y}), \ldots, t_m(\mathbf{y}))$ where ϕ is a formula in the language of ordered groups, $\mathbf{y}$ are variables from the home and value group sort and $t_1, \ldots, t_m$ are terms with values in the value group sort;

3. $\psi(x, t_1(\mathbf{y}), \ldots, t_m(\mathbf{y}))$ where ψ is a formula in the language of rings , $\mathbf{y}$ are variables from the home and residue field sort and $t_1, \ldots, t_m$ are terms with values in the residue sort;

4. $\theta(v(f_1(x, \mathbf{y})), \ldots, v(f_m(x, \mathbf{y})), \mathbf{z})$ where θ is a formula in the language ordered groups x and $\mathbf{y}$ are variables in the home sort, $f_1, \ldots, f_m \in \mathbb{Z}[X, \mathbf{Y}]$ and $\mathbf{z}$ are variables in the ordered group;

5. $\chi(\mathrm{ac}(f_1(x, \mathbf{y})), \ldots, \mathrm{ac}(f_m(x, \mathbf{y})), \mathbf{z})$ where χ is a formula in the language rings x and $\mathbf{y}$ are variables in the home sort, $f_1, \ldots, f_m \in \mathbb{Z}[X, \mathbf{Y}]$ and $\mathbf{z}$ are variables in the ring sort;

Formulas of types 1, 2 and 3 are easily seen to by NIP. If the x variable is of degree d in $f(x, \mathbf{y})$, then $f(x, \mathbf{y}) = 0$ fails to shatter a set of size $d + 2$. Thus formulas of the first type are NIP. Formulas of the second and third type are NIP by our assumptions on the theories of the residue field and the value group.

Consider $\Theta(x, \mathbf{y}, \mathbf{z}) = \theta(v(f_1(x, \mathbf{y})), \dots, v(f_m(x, \mathbf{y})), \mathbf{z})$ of type 4. If Θ has the independence property, then we can find a sequence of indiscernibles in K $(x_1, x_2, \dots)$ and $\mathbf{b}_1, \mathbf{b}_2$ such that $\Theta(x_i, \mathbf{b}_1, \mathbf{b}_2)$ holds if and only if i is even. By Lemma 6.23 there is are $g_0, g_1, \dots$ an indiscernible sequence of elements in the value group such that for $j = 1, \dots, n$ there are $h_j \in \Gamma$ and $r_j \in \mathbb{N}$ such that $v(f_j(x_i, \mathbf{b}_1) = h_j + r_j g_j$ for sufficiently large i. Consider the formula $\Theta^*(v, \mathbf{h}, \mathbf{b}_2)$ which is $\theta(h_1 + r_1 v, \dots, h_m + r_m v, \mathbf{b}_2)$ where v is a variable over the value group. Since the theory of the value group has NIP, $\Theta^*(g_i, \mathbf{h}, \mathbf{b}_2)$ is either eventually true, or eventually false for large i, but $\Theta^*(g_i, \mathbf{h}, \mathbf{b}_2)$ is equivalent to $\Theta(x_i, \mathbf{b}_1, \mathbf{b}_2)$ for large i. Thus Θ does not have the independence property.

The argument for formulas of type 5 is similar.

6.3 Artin's Conjecture

We say that a field K is a C_m*-field* if whenever $f(X_1, \dots, X_n)$ is a homogeneous polynomial of degree d where $n > d^m$, then f has a nontrivial zero in K.

Exercise 6.24 Show that K is a C_m-field if and only if every homogeneous polynomial of degree $d^m + 1$ has a nontrivial zero in K

Tsen and Lang [23] proved that if F is a finite field then $F(\!(T)\!)$ is a C_2 field and Artin conjecture that each $\mathbb{Q}_p$ is a C_2-field. This is false.

Exercise 6.25 [Terjanian] Let

$$p(X, Y, Z) = X^2YZ + XY^2Z + XYZ^2 + X^2Y^2 + X^2Z^2 - X^4 - Y^4 - Z^4$$

let

$$q(X_1, \dots, X_9) = p(X_1, X_2, X_3) + p(X_4, X_5, X_6) + p(X_7, X_8, X_9)$$

and

$$r(X_1, \dots, X_{18}) = q(X_1, \dots, X_9) + 4q(X_{10}, \dots, X_{18}).$$

a) Show that if $(x, y, z) \in \mathbb{Z}^3$ are not all even, then $p(x, y, z) = 3(\text{mod } 4)$.

b) Show that if $(x_1, \dots, x_9) \in \mathbb{Z}^9$ are not all even , then $q(x_1, \dots, x_9) \neq 0(\text{mod } 4)$.

c) If $\mathbf{x} = (x_1, \dots, x_{18}) \in \mathbb{Z}_2^{18}$ and some x_i is a unit, then $v_2(\mathbf{x}) = 0$ or 2.

d) Conclude that Artin's conjecture fails for $\mathbb{Q}_2$ with $n = 18$ and $d = 4$.

Nevertheless, the Ax, Kochen, Eršov transfer principle tell us is true for sufficiently large p.

Corollary 6.26 *Fix d. There is a prime p_0 such that for all primes $p \geq p_0$ every homogenous polynomials of degree d in $n > d^2$ variables has a nontrivial zero in $\mathbb{Q}_p$.*

Proof The statement that every homogeneous polynomial of degree d in d^2+1 variables has a nontrivial zero is a first order sentence that is true in every $\mathbb{F}_p(\!(T)\!)$ and hence true in $\mathbb{Q}_p$ for p sufficiently large. $\square$

The Tsen–Lang Theorem

We will prove that $F((T))$ is C_2 if F is finite.

Lemma 6.27 *If F is a finite field with $|F| = q$ and $n < q-1$, then*

$$\sum_{x \in F} x^n = 0$$

Proof Let $a \in F^\times$ with $a^n \neq 1$. Since $x \mapsto ax$ is a bijection,

$$\sum x^n = \sum (ax)^n = a^n \sum x^n.$$

Since $a^n \neq 1$, $\sum x^n = 0$. $\square$

Theorem 6.28 (Chevalley–Warning) *Let F be a finite field of characteristic p and let $f_1, \ldots, f_m \in F[X_1, \ldots, X_n]$ be polynomials of degrees $d_1, \ldots, d_m$ with $n > \sum d_i$. Then the number of zeros of $f_1 = \cdots = f_m$ in F is divisible by p.*

In particular, if the polynomials $f_1, \ldots, f_m$ are homogeneous, there is a nontrivial zero in F.

Proof Let F have characteristic p and cardinality q. Let N be the number of zeros of $f_1 = \cdots = f_m = 0$ in F^n. Note that for all $\mathbf{x} \in F^n$

$$\prod_{i=1}^{k} (1 - f_i(\mathbf{x})^{q-1}) = \begin{cases} 1 & \text{if } f_1(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Thus the number of zeros of f is

$$N = \sum_{\mathbf{x} \in F^n} \prod_{i=1}^{k} (1 - f_i(\mathbf{x})^{q-1}) = \sum_{\mathbf{x} \in F^n} \sum_{\mathbf{j} \in J} c_j \mathbf{x}^{\mathbf{j}} = \sum_{\mathbf{j} \in J} c_j \left(\sum_{\mathbf{x} \in F^n} \mathbf{x}^{\mathbf{j}} \right) (\text{mod } p)$$

where $J = \{\mathbf{j} = (j_1, \ldots, j_n) : \sum j_i \leq (q-1) \sum d_i\}$.

Fix $\mathbf{j} = (j_1, \ldots, j_n) \in J$. Note that, since $n > \sum d_i$, we must have some $j_{\hat{i}} < q-1$. Then

$$\sum_{\mathbf{x} \in F^n} \mathbf{x}^{\mathbf{j}} = \prod_{i=1}^{n} \sum_{x \in F} x^{j_i}$$

Thus, by the lemma, $\sum_{x \in F} x^{j_{\hat{i}}} = 0$ and $N = 0 (\text{mod } p)$. $\square$

We can combine this with Greenleaf's Theorem 2.27.

Corollary 6.29 *If $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$ where f_i has degree d_i and $n > \sum d_i$, then for all but finitely many primes p, $f_1 = \cdots = f_m = 0$ has a solution in $\mathbb{Z}_p$.*

Lemma 6.30 *Let $F(T)$ be the field of rational functions over a finite field F. Let $f \in F(T)[X_1, \ldots, X_n]$ be homogeneous of degree $d^2 < n$. Then f has a nontrivial zero in $F(T)^n$.*

Proof Clearing denominators, we may assume $f \in F[T][X_1, \ldots, X_n]$. We will look for a solution of the form $(x_1, \ldots, x_n)$ where for some suitably large s

$$x_i = y_{i,0} + y_{i,1}T + \cdots + y_{i,s}T^s.$$

Let r be the maximum of the degrees of the coefficients of f. Choose $s > (d(r+1) - n)/n - d^2$. Then $n(s+1) > d(ds + r + 1)$ Then

$$f(x_1, \ldots, x_n) = f_0(\mathbf{y}) + f_1(\mathbf{y})T + \cdots + f_{ds+r}(\mathbf{y})T^{ds+r}.$$

Since $n(s+1) > d(ds + r + 1)$, by Chevalley-Warning, there is a nontrivial zero $\mathbf{y} = (y_{1,0}, \ldots, y_{n,s}) \in F$. $\square$

Corollary 6.31 *Let $f \in F(\!(T)\!)[X_1, \ldots, X_n]$ be homogeneous of degree d with $d^2 < n$ and F is a finite field. Then f has a nontrivial zero in $F(\!(T)\!)$.*

Proof We may assume $f \in F[[T]](X_1, \ldots, X_n)$. For k sufficiently large let $f|k(X_1, \ldots, X_n)$ be the polynomial over $F[T]$ obtained by truncating all the coefficients of f to polynomials of degree at most k. By the lemma $f_k(X_1, \ldots, X_n)$ has a nontrivial zero $\mathbf{a}_k \in F(T)^n$. We may assume that $v(a_{k,i}) \geq 0$ for all i and some $v(a_{k,i}) = 0$. Since the residue field is finite we see that $F[[T]]$ is compact so we can choose a Cauchy subsequence of the $\mathbf{a}_k$ that converges to a nonzero element of $F[[T]]^n$. $\square$