AUTOMORPHISM TOWERS AND AUTOMORPHISM GROUPS OF FIELDS WITHOUT CHOICE

ITAY KAPLAN AND SAHARON SHELAH

Dedicated to Professor Rüdiger Göbel on his 70th birthday

ABSTRACT. This paper can be viewed as a continuation of [KS09] that dealt with the automorphism tower problem without Choice. Here we deal with the inequality $\tau_\kappa^{\rm nlg} \leq \tau_\kappa$ without Choice and introduce a new proof to a theorem of Fried and Kollár that any group can be represented as an automorphism group of a field. The proof uses a simple construction: working more in graph theory, and less in algebra.

1. INTRODUCTION AND PRELIMINARIES

Background. Although this paper hardly mentions automorphism towers, it is the main motivation for it. So we shall start by giving the story behind them.

Given any centerless group G, $G \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ so we can embed G into its automorphism group. Also, an easy exercise shows that $\mathrm{Aut}(G)$ is also without center, so we can do this again, and again:

Definition 1.1. For a centerless group G, we define *the automorphism tower* $\langle G^\alpha \mid \alpha \in \mathbf{ord} \rangle$ by

- $G^0 = G$.
- $G^{\alpha+1} = \mathrm{Aut}(G^\alpha)$.
- $G^\delta = \cup \{G^\alpha \mid \alpha < \delta\}$ for δ limit.

Remark 1.2. The union in limit stages can be understood as the direct limit. But we shall think of the tower as an increasing continuous sequence of groups.

The second author would like to thank the United States-Israel Binational Science Foundation for partial support of this research. Publication 913.

The natural question that arises, is whether this process stabilizes, and when. We define

Definition 1.3. For such a group, define $\tau_G = \min\{\alpha \mid G^{\alpha+1} = G^\alpha\}$.

In 1939, Weilandt proved in [Wie39] that for finite G, τ_G is finite. What about infinite G? There exist examples of centerless infinite groups such that this process does not stop in any finite stage. For example — the infinite dihedral group $D_\infty = \langle x, y \mid x^2 = y^2 = 1\rangle$ satisfies $\mathrm{Aut}(D_\infty) \cong D_\infty$ while the automorphism replacing x with y is not in $\mathrm{Inn}(D_\infty)$. The question remained open until the works of Faber [Fab78] and Thomas [Tho85, Tho98] (who was not aware of Faber's work), that showed $\tau_G < \left(2^{|G|}\right)^+$.

Definition 1.4. For a cardinal κ we define τ_κ as the smallest ordinal such that $\tau_\kappa > \tau_G$ for all centerless groups G of cardinality $\leq \kappa$, or in other words

$$\tau_\kappa = \bigcup \{\tau_G + 1 \mid G \text{ is centerless and } |G| \leq \kappa\}.$$

Since $(2^\kappa)^+$ is regular we can immediately conclude $\tau_\kappa < (2^\kappa)^+$.

This paper is concerned with a Choiceless universe, i.e. we do not assume the axiom of Choice. As a consequence, the previous definition is generalized to

Definition 1.5. For a set k, we define $\tau_{|k|}$ to be the smallest ordinal α such that $\alpha > \tau_G$ for all groups G with power $\leq |k|$.

Note that when we write $|X| \leq |Y|$ as in the definition above, we mean that there is an injective function from X to Y. Below we provide a short glossary.

A helpful and close notion is that of *the normalizer tower* $\langle \mathrm{nor}^\alpha_G(H) \mid \alpha \in \mathbf{ord}\rangle$ of a subgroup H of G in G.

Definition 1.6. Let

- $\mathrm{nor}^0_G(H) = H$.
- $\mathrm{nor}^{\alpha+1}_G(H) = \mathrm{nor}_G(\mathrm{nor}^\alpha_G(H))$.
- $\mathrm{nor}^\delta_G(H) = \bigcup\{\mathrm{nor}^\alpha_G(H) \mid \alpha < \delta\}$ for δ limit.

And we let the normalizer length be $\tau^{\mathrm{nlg}}_{G,H} = \min\left\{\alpha \,\middle|\, \mathrm{nor}^{\alpha+1}_G(H) = \mathrm{nor}^{\alpha}_G(H)\right\}$ (sometimes we just write $\tau_{G,H}$).

Analogously to τ_κ, we define

Definition 1.7. For a cardinal κ, let $\tau^{\mathrm{nlg}}_\kappa$ be the smallest ordinal such that $\tau^{\mathrm{nlg}}_\kappa > \tau_{\mathrm{Aut}(\mathfrak{A}),H}$, for every structure $\mathfrak{A}$ of cardinality $\leq \kappa$ and $H \leq \mathrm{Aut}(\mathfrak{A})$ of cardinality $\leq \kappa$.

In general (i.e. without assuming Choice), for a set k, we define $\tau^{\mathrm{nlg}}_{|k|}$ as the smallest ordinal α, such that for every structure $\mathfrak{A}$ of power $||\mathfrak{A}|| \leq |k|$, $\tau_{\mathrm{Aut}(\mathfrak{A}),H} < \alpha$ for every subgroup $H \leq \mathrm{Aut}(\mathfrak{A}) = G$ of power $|H| \leq |k|$. In other words, $\tau^{\mathrm{nlg}}_{|k|} = \sup\{\tau_{G,H} + 1 \,|\, \text{ for such } G, H\}$.

In [JST99, Lemma 1.8], Just, Shelah and Thomas proved the following inequality

$$\tau_\kappa \geq \tau^{\mathrm{nlg}}_\kappa.$$

In fact it was essentially already proved by Thomas in [Tho85].

In [KS09] we dealt with an upper bound of τ_κ without assuming Choice. Here we prove $\tau_\kappa \geq \tau^{\mathrm{nlg}}_\kappa$ without Choice, and also provide a Choiceless variant of $\tau_{|k|} \geq \tau^{\mathrm{nlg}}_{|k|}$.

It is worth mentioning some previous results regarding τ_κ that were proved using this inequality.

In [Tho85], Thomas proved that $\tau_\kappa \geq \kappa^+$. It is a easy to conclude from Main Theorem A below that this result still holds without Choice. We will elaborate in the end of this section (See Corollary 2.5).

In [JST99] the authors found that for uncountable κ one cannot find an explicit upper bound for τ_κ better than $(2^\kappa)^+$ in ZFC (using set theoretic forcing). In [She07], Shelah proved that if κ is strong limit singular of uncountable cofinality then $\tau_\kappa > 2^\kappa$ (using results from PCF theory). In the proofs the authors construct normalizer towers to find lower bound for τ_κ, but we did not check how much Choice was used.

It remains an open question whether or not there exists a countable centerless group G such that $\tau_G \geq \omega_1$.

Description of paper. As mentioned before, we wish to prove $\tau_\kappa \geq \tau_\kappa^{\text{nlg}}$ without Choice. So we started by reading what was done in [JST99] (which is also described in detail in [Tho]).

The proof contains three parts:

(1) Given some structure, code it in a graph (i.e. find a graph with the same cardinality and automorphism group).
(2) Given a graph code it in a field. Now we have a field K with some subgroup $H \leq \text{Aut}(K)$ such that $|K| = |H| = \kappa$.
(3) Use some lemmas from group theory and properties of $PSL(2, K)$ to find a centerless group whose automorphism tower coincides with the normalizer tower of H in $\text{Aut}(K)$.

Our first intention was to mimic this proof, and to prove some version of $\tau_{|k|} \geq \tau_{|k|}^{\text{nlg}}$ (see definitions 1.7 and 1.1 above). To explain what we did prove, we need some notation:

Definition 1.8. Let X be a set.

(1) $X^{<\omega}$ is the set of all finite sequences of members of X.
(2) $[X]^{<\aleph_0} = \{a \subseteq X \mid |a| < \aleph_0\}$.
(3) $X^{\langle<\omega\rangle} = [X^{<\omega}]^{<\aleph_0}$, i.e. the set of all finite subsets of finite sequences of elements of X.

Our methods cannot tackle $\tau_{|k|} \geq \tau_{|k|}^{\text{nlg}}$ without Choice, since one often needs to code finite sequences. The natural way to overcome this is to replace k with $k^{<\omega}$, so that we get $\tau_{|k^{<\omega}|} \geq \tau_{|k^{<\omega}|}^{\text{nlg}}$. However, we managed to proved a slightly different version:

Main Theorem A. *For any set k, $\tau_{\left|k^{\langle<\omega\rangle}\right|} \geq \tau_{\left|k^{\langle<\omega\rangle}\right|}^{\text{nlg}'}$.*

Where $\tau_{|k|}^{\text{nlg}'}$ is a variant of $\tau_{|k|}^{\text{nlg}}$. See Definition 2.2 below.

With Choice there is no difference, and moreover, we get as a corollary the original inequality for a cardinal κ (see Corollary 2.4 below). It is a matter of taste whether replacing $k^{<\omega}$ and nlg by $k^{\langle<\omega\rangle}$ and nlg$'$ matters. Still, one may ask whether $\tau_{|k^{<\omega}|}^{\text{nlg}} \leq \tau_{|k^{<\omega}|}$ or even $\tau_{|k|} \geq \tau_{|k|}^{\text{nlg}}$ holds without Choice.

Part (1) was easy enough. However, it needs a passage to a structure with countable language. This stage uses Choice. In order to fix this, we just bypassed the problem all together and replaced $\tau^{\mathrm{nlg}}_{|k|}$ by $\tau^{\mathrm{nlg}'}_{|k|}$.

Part (3) was easy as well: An algebraic lemma which obviously did not need Choice (Lemma 4.1); And two lemmas regarding $PSL(2,K)$ — Lemma 4.4 and Lemma 4.8. The latter is a theorem of Van der Waerden and Schreier which described $\mathrm{Aut}(PSL(2,K))$. There is a simple model theoretic argument that shows that these lemmas do not require Choice (Lemma 4.5).

However, part (2) seemed to be somewhat harder. In [JST99], the authors referred to the work of Fried and Kollár [FK82]. In [Tho], the author gives a less technical proof that the construction in [FK82] works. The proof, in both cases, was a little bit complicated, and we were suspicious that Choice was used in it. After some time we realized that it is most likely not used, but by then we already came up with a proof of our own, in which the construction of the field is much simpler, and thought that it is worth presenting. So, for part (2) we prove:

Main Theorem B. *Let $\Gamma = \langle X, E\rangle$ be a connected graph. Then for any choice of characteristic there exists a field K_Γ of that characteristic such that $|K_\Gamma| \leq \left|X^{\langle<\omega\rangle}\right|$ and $\mathrm{Aut}(K_\Gamma) \cong \mathrm{Aut}(\Gamma)$.*

The proof of Main Theorem B is given in Section 6. Here we will give a brief outline of the construction.

The plan was this: work a little bit on the graph, so that the algebra would be easier. First code the given graph as a graph with the following properties: its edges are colorable with some finite number N of colors, and the subgraphs induced by any particular color is a union of disjoint stars. This is done in Lemma 6.4.

Now the construction of the field is as follows: first let $\langle p_0, p_1, \ldots, p_N\rangle$ be a list of distinct odd primes. Start with $\mathbb{Q}$ (or any prime field), and add the set of vertices X as transcendental elements over it. For each one, add p_0^n roots to it for all $n < \omega$. Now, for

each edge, $e = \{s, t\}$, colored with the color $l < N$, adjoin p_{l+1}^n roots for all $n < \omega$ to $(s + t + 1)$. This is it. The reader is invited to compare to [FK82].

This construction can be done without Choice.

In the proof we use a generalized form of a lemma by P. Pröhle that appears in [Prö84]. In their original paper, Fried and Kollár could construct K_Γ with the restriction that $char\,(K_\Gamma) \neq 2$ and Prohle removed this restriction. His "third lemma" from [Prö84] seemed to be perfect for our situation. However, we needed to generalize it in order to suit our purposes (and prove the generalization). This is Lemma 6.8. The proof of Lemma 6.8 is similar to the one in [Prö84] and can be found in Section 7.

Acknowledgment. We would like to thank the referee for many useful remarks and to Haran Pilpel for drawing a graph with certain properties in record time.

A note about reading this paper. If the reader is not interested in Choice, but still wants to see the proof of Main Theorem A and Main Theorem B, he should ignore all the computations of cardinalities, since they become trivial. Also, with Choice, the construction of the field is somewhat easier — in our construction, we took the polynomial ring $\mathbb{Q}[Y]$ (where Y is a set containing the vertices) and then the quotient by an ideal. Then we had to show the ideal is prime in order to take the field of fractions. But with Choice we can construct the field by adding roots from the algebraic closure. See also Remark 6.14.

A small glossary.

- $|X| \leq |Y|$ means: There is an injective function from X to Y.
- $|X| = |Y|$ means: There is a bijection from X onto Y.
- For a structure $\mathfrak{A}$, $|\mathfrak{A}|$ is its universe and $||\mathfrak{A}||$ is its cardinality.
- $\mathbb{V}$ is the universe and $\mathbb{L}$ is Gödel's constructible universe.

2. A variant of $\tau^{\rm nlg}_{|k|}$ and some corollaries of Main Theorem A

Definition 2.1. A structure $\mathfrak{A}$ is called rigid if $\mathrm{Aut}\,(\mathfrak{A}) = 1$, i.e. it has no non-trivial automorphism.

Definition 2.2. For a set k, we define $\tau^{\mathrm{nlg}'}_{|k|}$ as the smallest ordinal α which is greater than $\tau_{\mathrm{Aut}(\mathfrak{A}),H}$ where $\mathfrak{A}, H$ are as in Definition 1.7 and in addition the vocabulary (language) L of $\mathfrak{A}$ satisfies

(1) There is some rigid structure with universe L and a countable vocabulary (for instance, L is well-orderable); and
(2) $|L| \leq \left||\mathfrak{A}|^{\langle<\omega\rangle}\right|$.

Remark 2.3. If κ is a cardinal number (i.e. an $\aleph$), then $\tau^{\mathrm{nlg}}_{\kappa} = \tau^{\mathrm{nlg}'}_{\left|\kappa^{\langle<\omega\rangle}\right|}$ and $\tau_{\kappa} = \tau_{\left|\kappa^{\langle<\omega\rangle}\right|}$. This is true since $\left|\kappa^{\langle<\omega\rangle}\right| = |\kappa|$, and because given any $\mathfrak{A}$ as in the definition, we may assume that $|\mathfrak{A}| \subseteq \kappa$ and that L is $|\mathfrak{A}|^{<\omega} \subseteq \kappa^{<\omega}$ which is well-orderable (see [KS09, Observation 2.3]).

Hence, by Main Theorem A

Corollary 2.4. *(ZF) For a cardinal κ, $\tau^{\mathrm{nlg}}_{\kappa} \leq \tau_{\kappa}$.*

The following is another easy conclusion of Main Theorem A

Corollary 2.5. *(ZF) for any cardinal κ, $\tau_{\kappa} \geq \kappa^{+}$. Moreover, letting $\upsilon_{k^{\langle<\omega\rangle}}$ be the smallest nonzero ordinal α such that there is no injective function $f : \alpha \to k^{\langle<\omega\rangle}$, then $\tau_{\left|k^{\langle<\omega\rangle}\right|} \geq \upsilon_{k^{\langle<\omega\rangle}}$ for any set k.*

Proof. By [Tho85], we know that this result is true with Choice. Moreover, he proves that $\tau^{\mathrm{nlg}}_{\kappa} \geq \kappa^{+}$ (see Lemma in the proof of Theorem 2 there). Let $\alpha < \upsilon_{k^{\langle<\omega\rangle}}$ be some ordinal. We know that $\mathbb{L} \models \tau^{\mathrm{nlg}}_{|\alpha|} \geq |\alpha|^{+} > \alpha$ and that $|\alpha| \leq k^{\langle<\omega\rangle}$.

For a moment we work in $\mathbb{L}$. So there is a group G (the automorphism group of some structure) and a subgroup group $H \leq G$ such that $|H| \leq |\alpha|$ and $\alpha \leq \tau_{G,H}$. We may assume that $|G| \leq |\alpha|$. For one reason, this is the way it is constructed in [Tho85]. However, we give a self-contained explanation:

Let L be the language $\{P, Q, <, R\} \cup L_{\mathrm{Groups}}$ where P, Q are predicates, $<, R$ are binary relation symbols and L_{Groups} is the language of groups. Consider the L-structure $\mathfrak{G}$ with universe the disjoint union of G and α where $P^{\mathfrak{G}} = G$, $Q^{\mathfrak{G}} = \alpha$, with the group

structure on P, the order on Q and $R^{\mathfrak{G}}(x,\beta)$ holds iff $x \in \mathrm{nor}_G^{\beta}(H)$. Let $\mathfrak{G}' \prec \mathfrak{G}$ be an elementary substructure of size $\leq |\alpha|$ such that $H \subseteq P^{\mathfrak{G}'}$, $\alpha \subseteq Q^{\mathfrak{G}'}$ (so $\alpha = Q^{\mathfrak{G}'}$), and let $G' = P^{\mathfrak{G}'}$. As a group G' is a subgroup of G containing H of size $\leq |\alpha|$ and for all $\beta < \alpha$, $\mathrm{nor}_{G'}^{\beta}(H) \neq \mathrm{nor}_{G'}^{\beta+1}(H)$, and in particular $\alpha \leq \tau_{G',H}$.

Now we go back to $\mathbb{V}$, so $|G| \leq |\alpha| \leq \left|k^{\langle<\omega\rangle}\right|$ by assumption. By [KS09, Claim 2.8], $\alpha \leq \tau_{G,H}^{\mathbb{L}} = \tau_{G,H}^{\mathbb{V}}$. Let $\mathfrak{A}$ be the structure with universe G and for each $g \in G$ a unary function f_g taking x to $x \cdot g$. Then $\mathrm{Aut}(\mathfrak{A}) \cong G$. So we conclude that $\tau^{\mathrm{nlg}'}_{k^{\langle<\omega\rangle}} \geq \alpha$ (because G is well-orderable as in Remark 2.3 above). By Main Theorem A, $\tau_{\left|k^{\langle<\omega\rangle}\right|} \geq \alpha$. □

3. Coding structures as graphs

The next lemma allows us to present any automorphism group of an (almost) arbitrary structure as the automorphism group of a graph.

Lemma 3.1. *Let $\mathfrak{A}$ be a structure for the vocabulary (=language) L such that*

(1) There is some rigid structure on L with vocabulary L' such that $|L'| \leq \aleph_0$.
(2) $|L| \leq \left||\mathfrak{A}|^{\langle<\omega\rangle}\right|$.

Then there is a structure $\mathfrak{B}$ with vocabulary $L_{\mathfrak{B}}$ such that

- $||\mathfrak{B}|| \leq ||\mathfrak{A}|| + |L|$ (so $\leq \left||\mathfrak{A}|^{\langle<\omega\rangle}\right|$)
- $\mathrm{Aut}(\mathfrak{B}) \cong \mathrm{Aut}(\mathfrak{A})$
- $|L_{\mathfrak{B}}| = \aleph_0$

Proof. We may assume that both L and L' are relational languages.

Define $\mathfrak{B}$ by:

- $|\mathfrak{B}| = |\mathfrak{A}| \times \{0\} \cup L \times \{1\}$.
- The vocabulary is $L_{\mathfrak{B}} = \{R_n \mid n \in \omega\} \cup L' \cup \{P\}$ where P is a unary predicate and each R_n is an $n+1$ place relation.

Where:

- $Q^{\mathfrak{B}} = Q^L$ on $L \times \{1\}$ for each $Q \in L'$.

- $R_n^{\mathfrak{B}} = \left\{ \left((a_0, 0), \ldots, (a_{n-1}, 0), (R, 1) \right) \middle| \begin{array}{c} R \in L \text{ is an } n \text{ place relation and} \\ (a_0, \ldots, a_{n-1}) \in R^{\mathfrak{A}} \end{array} \right\}$
- $P^{\mathfrak{B}} = L \times \{1\}$.

It is easy to see that $\mathfrak{B}$ is as desired. □

This is well known:

Theorem 3.2. *Let $\mathfrak{A}$ be a structure for the first order language L which is as in the conditions of 3.1. Then there is a connected graph $\Gamma = \langle X_\Gamma, E_\Gamma \rangle$ such that $\mathrm{Aut}(\Gamma) \cong \mathrm{Aut}(\mathfrak{A})$, and $|X_\Gamma| \leq ||\mathfrak{A}||^{<\aleph_0}$.*

Proof. For details see e.g. [Tho, Lemma 4.2.2] or [Hod93, Thereom 5.5.1]. From the construction (which does not use Choice) described there, one can deduce the part regarding the cardinality. The proof uses the fact that we can reduce to structures with countable languages, but this is exactly Lemma 3.1. □

4. Some group theory

Lemma 4.1. *Let S be a simple non-abelian group, and let G be a group such that $\mathrm{Inn}(S) \leq G \leq \mathrm{Aut}(S)$. Then the automorphism tower of G is naturally isomorphic to the normalizer tower of G in $\mathrm{Aut}(S)$.*

The proof of this lemma can be found in [Tho, Theorem 4.1.4] (and, of course, it does not use Choice).

So we need a simple group. Recall

Definition 4.2. Let K be a field, $n < \omega$, then:

- $GL(n, K)$ is the group of invertible $n \times n$ matrices over K.
- $PGL(n, K) = GL(n, K) / Z(GL(n, K))$ (Here, $Z(GL(n, K))$ is the group $K^\times \cdot I$ where I is the identity matrix).
- $SL(n, K) = \{x \in GL(n, K) \mid \det(x) = 1\}$.
- $PSL(n, K) = SL(n, K) / Z(SL(n, K))$ (The denominator is just $Z(GL(n, K)) \cap SL(n, K)$).

Fact 4.3. *$PSL(n,K)$ is a normal subgroup of $PGL(n,K)$.*

Lemma 4.4. *$PSL(2,K)$ is simple for any field K such that $|K| \geq 3$.*

The proof of this lemma can be found in many books, e.g. [Rot95]. It is also true in ZF, by the following Lemma and Claim:

Lemma 4.5. *Suppose P is a claim, such that $ZFC \vdash P$, and ψ is a first order sentence (in some language) such that $ZF \vdash$ 'P is true iff ψ does not have a model'. Then $ZF \vdash P$.*

Proof. If we have a model $\mathbb{V}$ of ZF, such that $\mathbb{V} \models \neg P$, then ψ has a model so cannot prove contradiction (there is no use of Choice here). Hence ψ is consistent in $\mathbb{L} = \mathbb{L}^{\mathbb{V}}$ as well. (If ψ was not consistent in $\mathbb{L}$, then a proof of a contradiction from ψ would exist in $\mathbb{V}$ as well). Hence, by Gödel Completeness Theorem in ZFC, $\mathbb{L} \models \neg P$, but $\mathbb{L} \models ZFC$ — a contradiction. □

Claim 4.6. There is a first order sentence ψ such that ψ has a model iff there is a field K, $|K| \geq 3$ such that $PSL(2,K)$ is not simple.

Proof. Let L be the language of fields with an extra 4-ary relation H, i.e. $L = \{+, \cdot, 0, 1, H\}$. Let the sentence ψ say that the universe is a field K of size ≥ 3 and that $H \subseteq K^4$ is a normal subgroup of $SL(2,K)$ (after some choice of coordinates), and that H contains $Z(SL(2,K))$ and also some element outside $Z(SL(2,K))$. □

We close this section by showing one final algebraic fact holds over ZF. Recall:

Definition 4.7. Given any two groups N and H and a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$, we denote by $N \rtimes_\varphi H$ (or simply $N \rtimes H$ if φ is known) the semi-direct product of N and H with respect to φ.

Note that for a field K, there are canonical homomorphisms $\mathrm{Aut}(K) \to \mathrm{Aut}(PSL(2,K))$ and $\mathrm{Aut}(K) \to \mathrm{Aut}(PGL(2,K))$.

Fact 4.8. *(Van der Waerden, Schreier* [vdWS28]*) Let K be a field. Then every automorphism of $PSL(2,K)$ is induced via conjugation by a unique element of $P\Gamma L(2,K) := PGL(2,K) \rtimes \mathrm{Aut}(K)$. Hence $\mathrm{Aut}(PSL(2,K)) \cong P\Gamma L(2,K)$.*

This means that if $\varphi \in \mathrm{Aut}(PSL(2,K))$ then there are unique $\alpha \in \mathrm{Aut}(K)$ and $g \in PGL(2,K)$ such that for every $x \in PSL(2,K)$, $\varphi(x) = g\alpha(x)g^{-1}$.

We again use the model theoretic argument of Lemma 4.5 to give a proof of this fact in ZF:

Claim 4.9.

(1) There is a first order sentence ψ such that ψ has a model iff there is a field K, and an automorphism $\varphi \in \mathrm{Aut}(PSL(2,K))$ such that φ is not in $P\Gamma L(2,K)$. (This implies the existence of (α, g) required by the fact).

(2) There is a first order sentence ψ' such that ψ' has a model iff there is a field K, and some $1 \neq g \in PGL(2,K)$, $\alpha \in \mathrm{Aut}(K)$, such that for every $x \in PSL(2,K)$, $\alpha(x) = gxg^{-1}$. (This implies the uniqueness of (α, g) required by the fact).

Proof. (1): Let K be a field. Recall that $x_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and $z_t = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ generate $SL(2,K)$. Let $g \in PGL(2,K)$, $\sigma \in \mathrm{Aut}(PSL(2,K))$.

Then $\alpha \in \mathrm{Aut}(K)$ satisfies $\sigma(x) = g\alpha(x)g^{-1}$ iff the map $x \mapsto g^{-1}\sigma(x)g$ takes $\bar{x}_t$ to $\bar{x}_{\alpha(t)}$ and $\bar{z}_t$ to $\bar{z}_{\alpha(t)}$. Let L be the language of fields augmented with 4-place function symbols $\{\sigma_i \mid i < 4\}$. ψ says that the universe K is a field, and that σ is an automorphism of $PSL(2,K)$ ($SL(2,K)$ is a definable subset of K^4, as is $Z(SL(2,K))$), such that for all $g \in PGL(2,K)$, the maps $t \mapsto g^{-1}\sigma(\bar{x}_t)g$ and $t \mapsto g^{-1}\sigma(\bar{z}_t)g$ do not induce a well defined automorphism of K.

(2): Let L be the language of fields. ψ' says that the universe K is a field and that there is some nontrivial $g \in PGL(2,K)$ such that the maps $t \mapsto g^{-1}\bar{x}_t g$ and $t \mapsto g^{-1}\bar{z}_t g$ are induced by an automorphism α of K. □

5. Proof of Main Theorem A from Main Theorem B

From Main Theorem B which is proved in the next section, we can now deduce

Main Theorem A. *For any set k, $\tau^{\mathrm{nlg}'}_{\left|k^{\langle<\omega\rangle}\right|} \leq \tau_{\left|k^{\langle<\omega\rangle}\right|}$.*

Proof. (essentially the same proof as in [JST99]). We are given a structure $\mathfrak{A}$, with language L such that on the set L there is a rigid structure with countable vocabulary, and $||\mathfrak{A}|| \leq \left|k^{\langle<\omega\rangle}\right|$. By Theorem 3.2 and Main Theorem B we may assume that $\mathfrak{A}$ is an infinite field, K. We are also given a subgroup $H \leq \mathrm{Aut}(K)$, $|H| \leq \left|k^{\langle<\omega\rangle}\right|$.

Let $G = PGL(2,K) \rtimes H$. Obviously $|G| \leq \left|k^{\langle<\omega\rangle}\right|$.

G is centerless, because by Fact 4.8, the centralizer of $PSL(2,K)$ in $P\Gamma L(2,K)$ is trivial, and $PSL(2,K) \leq G$. So $PSL(2,K) \leq G \leq P\Gamma L(2,K)$. By Lemmas 4.1, 4.4, and 4.8, G^α is isomorphic to $\mathrm{nor}^\alpha_{P\Gamma L(2,K)}(G)$.

Now, by induction on α, one has $\mathrm{nor}^\alpha_{P\Gamma L(2,K)}(G) = PGL(2,K) \rtimes \mathrm{nor}^\alpha_{\mathrm{Aut}(K)}(H)$ and we are done. □

6. coding graphs as fields

In the introduction we mentioned that the following theorem of Fried and Kollár [FK82] was used in [JST99]:

Theorem 6.1. *(Fried and Kollár) (ZFC) For every connected graph Γ there is a field K such that $\mathrm{Aut}(\Gamma) \cong \mathrm{Aut}(K)$, and $|K| = |\Gamma| + \aleph_0$.*

Here we will offer a different proof of the Choiceless version, namely

Main Theorem B. *Let $\Gamma = \langle X, E\rangle$ be a connected graph. Then there exists a field K_Γ of any characteristic such that $|K_\Gamma| \leq \left|X^{\langle<\omega\rangle}\right|$ and $\mathrm{Aut}(K_\Gamma) \cong \mathrm{Aut}(\Gamma)$.*

Corollary 6.2. *If G is a group and there is some rigid structure with countable vocabulary on it, then there is a field K such that $\mathrm{Aut}(K) \cong G$, and $|K| \leq \left|G^{\langle<\omega\rangle}\right|$.*

Proof. (of corollary) Let $\mathfrak{A}$ be the structure with universe G and for each $g \in G$ a unary function f_g taking x to $x \cdot g$ so that $\mathrm{Aut}(\mathfrak{A}) \cong G$. Now apply 3.2 and Main Theorem B. □

6.1. **Coding graphs as colored graphs.** We start by working a bit on the graph, to make the algebra easier.

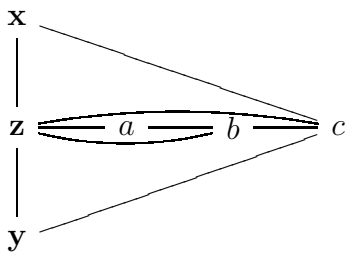
Definition 6.3. A graph $G = \langle X, E\rangle$ is called a star if there is a vertex v (the center) such that $E \subseteq \{\{v, u\} \,|\, u \in V - \{v\}\}$.

Lemma 6.4. *There is some number N such that for every connected graph $\Gamma = \langle X_\Gamma, E_\Gamma\rangle$, there is a connected graph $\Gamma^+ = \langle X_{\Gamma^+}, E_{\Gamma^+}\rangle$ with the following properties:*

(1) $\mathrm{Aut}(\Gamma) \cong \mathrm{Aut}(\Gamma^+)$.
(2) *There is a coloring $C : E_{\Gamma^+} \to N$ of the edges of Γ^+ in N colors such that for all $l < N$ the l-th colored subgraph is a disjoint union of stars.*
(3) *Every $\varphi \in \mathrm{Aut}(\Gamma^+)$ preserves the coloring.*
(4) $|X_{\Gamma^+}| \leq \left|X_\Gamma^{\langle<\omega\rangle}\right|$, *in fact* $|X_\Gamma| \leq |X_{\Gamma^+}| \leq |X_\Gamma| + 4\,|E_\Gamma|$.

Proof. The idea is to replace each edge $\{x, y\}$ by a copy of the graph G described below.

Recall that the valency of a vertex is the number of edges incident to the vertex, and will be denoted by $val(x)$. Let $G = \langle X_G, E_G\rangle$ be the following auxiliary graph:



Note the following properties of G:

- It has only 2 automorphisms: id and σ, where σ switches $\mathbf{x}$ and $\mathbf{y}$, but fixes all other vertices: $\mathbf{z}, b, c$ are characterized by their valency and a is the only vertex with valency 2 which is adjacent to $b, \mathbf{z}$.
- $\mathbf{z}$ is adjacent to all the vertices, its valency is unique and is not divisible by $val(\mathbf{x})$.
- $\mathbf{x}$ and $\mathbf{y}$ are not adjacent.

Description of Γ^+:

The set of vertices is

$$X_{\Gamma^+} = \{(1,x)\,|\,x \in X_\Gamma\} \cup \{(2,u,w)\,|\,u \in E_\Gamma, w \in X_G - \{\mathbf{x},\mathbf{y}\}\}.$$

And the edges are:

- $(2,u,w)$ and $(2,u',w')$ are adjacent iff $u = u'$ and $\{w,w'\} \in E_G$.
- $(1,x)$ and $(2,u,w)$ are adjacent iff $x \in u$ and $\{\mathbf{x},w\} \in E_G$ (iff $\{\mathbf{y},w\} \in E_G$).
- That is all.

So, for each edge $\{x,y\} = u \in E_\Gamma$ there is an induced subgraph Γ^+_u of Γ^+, whose vertices are $\{(1,x),(1,y)\} \cup \{(2,u,w)\,|\,w \neq \mathbf{x},\mathbf{y}\}$, and $\Gamma^+_{\{x,y\}} \cong G$ (by sending $\mathbf{x}$ to $(1,x)$, $\mathbf{y}$ to $(1,y)$ and $w \neq \mathbf{x},\mathbf{y}$ to $(2,u,w)$).

Let G' be the subgraph of G induced by removing $\mathbf{y}$, let $N = |E_{G'}|$ (so $N = 7$), and denote $E_{G'} = \{e_0,\ldots,e_{N-1}\}$. Let $f : \Gamma^+ \to G'$ be a homomorphism of graphs defined as follows: $f(1,x) = \mathbf{x}$, $f(2,u,w) = w$. The coloring $C : E_{\Gamma^+} \to N$ is defined by $C(e) = i$ iff $f(e) = e_i$.

Let us now show (2). For each $i < N$, let $\Gamma^+_i = \langle X_i, E_i\rangle$ be the subgraph induced by the color i. If $\mathbf{x} \notin e_i$, then Γ^+_i is a union of disjoint edges by the definitions (and an edge is a star). If $\mathbf{x} \in e_i$, then Γ^+_i is a disjoint union of $|X_\Gamma|$ stars, with centers $\{(1,x)\,|\,x \in X_\Gamma\}$, each having $val_\Gamma(x)$ edges.

For (1), note that $val_{\Gamma^+}(1,x) = val_G(\mathbf{x}) \cdot val_\Gamma(x)$ (or ∞, if $val_\Gamma(x) \geq \aleph_0$), while $val_{\Gamma^+}(2,u,w) = val_G(w)$, hence $val_{\Gamma^+}(2,u,\mathbf{z})$ is not divisible by $val_{\Gamma^+}(1,x)$.

Hence if $\varphi \in \mathrm{Aut}(\Gamma^+)$ then $\varphi(2,u,\mathbf{z}) = (2,u',\mathbf{z})$ for some $u' \in E_\Gamma$. Since $\mathbf{z}$ is adjacent to all the vertices in G, $\Gamma^+_{\{x,y\}}$ consists of all the vertices $(2,u,\mathbf{z})$ is adjacent to and itself. So $\varphi \restriction \Gamma^+_u$ is an isomorphism onto $\Gamma^+_{u'}$. Since $\mathrm{Aut}(G) = \{\mathrm{id},\sigma\}$, for all $w \neq \mathbf{x},\mathbf{y}$, $\varphi(2,u,w) = (2,u',w)$. This allows us to define $\psi_\varphi = \psi \in \mathrm{Aut}(\Gamma)$ by $\psi(x) = x'$ where $\varphi(1,x) = (1,x')$. It is now easy to see that $\varphi \mapsto \psi_\varphi$ is an isomorphism from $\mathrm{Aut}(\Gamma^+)$ onto $\mathrm{Aut}(\Gamma)$.

(3) and (4) should be clear. □

6.2. **Coding colored graphs as fields.** Now we may assume that our graph is as in 6.4, and we start constructing the field.

We use the somewhat nonstandard notation of r as the characteristic of a field, so that $\mathbb{F}_r$ is the prime field with r elements.

Definition 6.5. Let $F \subseteq K$ be a field extension. F is said to be relatively algebraically closed in K if every $x \in K \backslash F$ is transcendental over F.

Definition 6.6. Let p be a prime. An element x in a field F is called *p-high*, if there is a sequence $\langle x_i \,|\, i < \omega \rangle$ of elements in F, such that $x_0 = x$, and $x_{i+1}^p = x_i$. With Choice this means that x has a p^n-th root for all $n < \omega$.

Example 6.7. If $F = \mathbb{Q}$, then for p odd, the only p-high element in F are $1, -1, 0$. If $F = \mathbb{F}_r$ for some prime r, then for every p such that $(p, r-1) = 1$ (i.e. the map $x \mapsto x^p$ is onto), every element in F is p-high.

This next lemma is the technical key. Its proof may use Choice, and this is OK, because we use it for finite Γ (see Remark 6.10 below).

Lemma 6.8. *(taken from* [Prö84, The third lemma] *with some adjustments) Let r be a prime number or 0, p a prime number different from r and let $\{p_0, \ldots, p_{n-1}\}$ be a set of pairwise distinct primes, different from p, r. Let F be a field of characteristic r. For $k < n$, let V_k be some set such that $k \neq l \Rightarrow V_k \cap V_l = \emptyset$, and let $V = \bigcup_{k<n} V_k$.*

For each $v \in V$, let $T_v \in F[X]$ be polynomials such that:

- *none of them is constant.*
- *none of them is divisible by X.*
- *they are separable polynomials.*
- *they are pairwise relatively prime (i.e. no nontrivial common divisor).*

Suppose that K is an extension of F generated by the set $\{z_i \,|\, i < \omega\} \cup \{t_i^v \,|\, v \in V, i < \omega\}$ from the algebraic closure of $F(z_0)$ where:

- *z_0 is transcendental over F.*
- *$(z_{i+1})^p = z_i$ for all $i < \omega$.*
- *For $v \in V$, $t_0^v = T_v(z_0)$*

- *if* $v \in V_k$ *then* $\left(t^v_{i+1}\right)^{p_k} = t^v_i$.

Then we have the following properties:

(1) *F is relatively algebraically closed in K.*

(2) *An equivalent definition of K is the following one: Suppose F is the field of fractions of an integral domain S. Then K is the field of fractions of the integral domain R/I (in particular I is prime) where*
$R = S\left[Y_i, S^v_l \mid i, l < \omega, v \in V\right]$ *(i.e. the ring generated freely by S and these elements) and $I \leq R$ is the ideal generated by the equations:*
   (a) $Y^p_{i+1} = Y_i$ *for* $i < \omega$.
   (b) $S^v_0 = T_v\left(Y_0\right)$ *for* $v \in V$.
   (c) *If* $v \in V_k$, *then* $\left(S^v_{l+1}\right)^{p_k} = S^v_l$ *for* $k < n$, $l < \omega$.

(3) *Each q-high element of K belongs to F whenever q is a prime different from p and* $\langle p_k \mid k < n\rangle$.

(4) *Each p-high element of K is of the form* $c \cdot (z_i)^m$, *where c is a p-high element of F, $i < \omega$ and m is an integer.*

(5) *If p' is a prime different from p then z_0 does not have a p' root.*

(6) *If V is finite then* $|K| \leq \left|F^{\langle<\omega\rangle}\right|$. *Furthermore, the injection witnessing this is definable from the parameters given when constructing K (i.e. the function $v \mapsto T_v$, etc).*

The proof may be found in Section 7.

The rest of the section is devoted to proving

Theorem 6.9. *Let* $\Gamma = \langle X, E, C\rangle$ *be an N-colored graph as in Lemma 6.4. Then there exists a field* K_Γ *such that* $|K_\Gamma| \leq \left|X^{\langle<\omega\rangle}\right|$ *and* $\mathrm{Aut}\left(K_\Gamma\right) \cong \mathrm{Aut}\left(\Gamma\right)$. *Furthermore,* $X \subseteq K_\Gamma$ *and* $\pi \mapsto \pi \restriction X$ *is an isomorphism from* $\mathrm{Aut}\left(K_\Gamma\right)$ *onto* $\mathrm{Aut}\left(\Gamma\right)$. *We can choose* K_Γ *to be of any characteristic.*

So Main Theorem B immediately follows from this and Lemma 6.4.

The construction of K_Γ: Let L be the field $\mathbb{Q}$ or $\mathbb{F}_r$ for some prime r. Let $\langle p_i \,|\, i \leq N \rangle$ list odd prime numbers which are different then r, and do not divide $r-1$ (so that in L there are no p_i-roots of unity). Let R be the ring $L[Y_\Gamma]$ where $Y_\Gamma = \{x_s^i \,|\, i < \omega, s \in X\} \cup \{x_e^i \,|\, i < \omega, e \in E\}$[1] is an algebraically independent set. Let $I_\Gamma \subseteq R$ be the ideal generated by the equations:

- $(x_s^{i+1})^{p_0} = x_s^i$ for all $s \in X$ and $i < \omega$.
- If $e = \{s, t\}$ then $x_e^0 = x_s^0 + x_t^0 + 1$ for all $s, t \in X$ and $e \in E$.
- If $C(e) = l$ then $(x_e^{i+1})^{p_{l+1}} = x_e^i$ for all $e \in E$.

Now let R_Γ be the ring R/I_Γ.

Remark 6.10.

(1) If Γ, Γ' are N-colored graphs, and $\Gamma \cong \Gamma'$ (and the isomorphism respects the coloring) then $R_\Gamma \cong R_{\Gamma'}$.

(2) Hence we may use Choice when proving properties regarding R_Γ (and later K_Γ) when Γ is finite because we may assume $\Gamma \in \mathbb{L}$ (hence also $R_\Gamma \in \mathbb{L}$ etc). In that case we may use Lemma 6.8 even if there is Choice in the proof.

Proposition 6.11. *I_Γ is prime, so we let K_Γ be be the field of fractions of R_Γ.*

The proof uses the following remark (when it makes sense)

Remark 6.12. If $\Gamma_0 \subseteq \Gamma_1$ are finite where $\Gamma_i = \langle X_i, E_i, C_i \rangle$ for $i < 2$ and $X_1 = X_0 \cup \{t\}$, $t \notin X_0$, then the field extension $K_{\Gamma_0} \subseteq K_{\Gamma_1}$ is as in Lemma 6.8, where

- F is the field K_{Γ_0}; r is its characteristic; p is p_0; $\{p_0, \ldots, p_{n-1}\}$ is $\{p_{l+1} \,|\, l < N\}$; V_k is the set of edges $\{t, s\} \in E$ of color k; for $s \in X_0$ such that $v = \{t, s\} \in E$, T_v is the polynomial $X + x_s^0 + 1$; z_i is x_t^i and for $v = e = \{t, s\}$, t_i^v is x_e^i.

Proof. (of proposition) We may assume Γ is finite, so the proof is by induction on $|X|$. Suppose that $\Gamma_0 \subseteq \Gamma_1$ where $\Gamma_i = \langle X_i, E_i, C_i \rangle$ for $i < 2$ and that $X_1 = X_0 \cup \{t\}$, $t \notin X_0$. By induction, I_{Γ_0} is prime, so $R = R_{\Gamma_0}$ is an integral domain.

[1] The i s are indices not exponents! Later we will use parentheses in order not to confuse a superscript with an exponent.

Let $Y_t = \{x_t^i \mid i < \omega\} \cup \{x_e^i \mid i < \omega, t \in e \in E_1\}$; $I_t \subseteq R[Y_t]$ be the ideal generated by the equations related to t and $\{e \in E_1 \mid t \in e\}$.

By Lemma 6.8, clause (2), I_t is prime.

Consider the canonical projection $\pi : L[Y_{\Gamma_1}] \to R[Y_t]$ so that $\pi(I_{\Gamma_1}) = I_t$ and $\langle I_{\Gamma_0} \rangle = \ker(\pi)$. Hence, π induces an isomorphism $L[Y_{\Gamma_1}]/I_{\Gamma_1} \to R[Y_t]/I_t$ and we are done since the right hand side is an integral domain. □

Definition 6.13. (ZFC) Let F be a field and let p be a natural number. Let S be a set of elements from F. Then $F(S,p)$ denotes the field which is obtained by adjoining the elements $\{s(l) \mid s \in S, l < \omega\}$ from the algebraic closure of F where:

- $s(0) = s$.
- $s(l+1)^p = s(l)$, $l < \omega$.

Remark 6.14. Choice is a priori needed in this definition because the construction implicitly assumes the existence of an algebraic closure, and some ordering of S and of the p-roots of the $s(l)$s.

Definition 6.15. Let $K_{-1} = L(Y)(Y, p_0)$, where $Y = \{x_t^0 \mid t \in X\}$, and $L(Y)$ denotes the purely transcendental extension of L, and for $l < N$, $K_l = K_{l-1}(E_l, p_{l+1})$, where $E_l = \{x_s^0 + x_t^0 + 1 \mid \{s,t\} = e \in E, C(e) = l\}$.

Lemma 6.16.

(1) *For* Γ *finite*[2]*,* K_Γ *is canonically isomorphic to* K_{N-1}.

(2) *If* $\Gamma_0 \subseteq \Gamma_1$ *then* $K_{\Gamma_0} \subseteq K_{\Gamma_1}$.

Proof. (1) follows from Lemma 6.8, (2) by induction on the size of Γ, similarly to the proof of Proposition 6.11. (2) follows from (1) for finite Γ, which is enough. □

From now on, fix some Γ.

[2]The assumption that Γ is finite is only to insure that K_{N-1} is well defined, with Choice this assumption is not needed.

Definition 6.17. For each $Y \subseteq X$, let Γ_Y be the induced subgraph generated by Y (i.e. $\Gamma_Y = \langle Y, E \restriction Y \rangle$) and let $R_Y = R_{\Gamma_Y}$, $K_Y = K_{\Gamma_Y}$.

Some properties of K_Γ:

Lemma 6.18. *For Γ as in Lemma 6.4,*

(1) *For any prime p, if $a \in K_Y$ for some $Y \subseteq X$ and is p-high in K_Γ then a is already p-high in K_Y.*
(2) *For each $i < \omega$, the set $\{x_s^i \mid s \in X\}$ is algebraically independent over L.*
(3) *If $X_1 \subseteq X_2$ then K_{X_1} is relatively algebraically closed in K_{X_2} (in particular L is r.a.c in K_Γ).*

Proof. (1) and (2) follows from (3). For (3), we may assume X_1, X_2 are finite, and then it is enough to prove it for the case $X_2 = X_1 \cup \{t\}, t \notin X_1$. Now use Remark 6.12, and clause (1) of Lemma 6.8. □

Now we shall define the isomorphism from $\mathrm{Aut}(\Gamma)$ to $\mathrm{Aut}(K_\Gamma)$:

Proposition 6.19. *For Γ as in 6.4, there is a canonical injective homomorphism $\sigma : \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(K_\Gamma)$ defined by $\sigma(\varphi)(x_t^i) = x_{\varphi(t)}^i$, and $\sigma(\varphi)(x_e^i) = x_{\varphi(e)}^i$, for $\varphi \in \mathrm{Aut}(\Gamma)$ and all $t \in X, e \in E$.*

Proof. σ is well defined because of clause (3) of Lemma 6.4. σ is obviously a homomorphism. It is injective: If $\sigma(\varphi) = \mathrm{id}$, while $\varphi(s) = t \neq s$, then $x_s^0 = \sigma(\varphi)(x_s^0) = x_t^0$ — a contradiction to clause (2) of Lemma 6.18. □

Our aim is to prove that σ is onto. We start with:

Claim 6.20. Suppose that $a \in K_\Gamma$ is p-high, then:

(1) If $p = p_0$ then a can be written in the form $\varepsilon \cdot \prod \{(x_s^{n_s})^{m_s} \mid s \in X_0\}$ for some finite $X_0 \subseteq X$, some choice of $m_s \in \mathbb{Z}, n_s < \omega$ for $s \in X_0$ and a p_0-high element $\varepsilon \in L$.
(2) If $p = p_{l+1}$ for some $l < N$ then a can be written in the form $\varepsilon \cdot \prod \{(x_e^{n_e})^{m_e} \mid e \in E_0\}$ for some finite $E_0 \subseteq E$ such that $C \restriction E_0 = l$, some choice of $n_e < \omega, m_e \in \mathbb{Z}$ for $e \in E_0$ and a p_{l+1}-high element $\varepsilon \in L$.

Proof. By Lemma 6.18, clause (1), there is some $X_0 \subseteq X$ such that a is p-high in K_{X_0}. The proof is by induction on $|X_0|$. The base of the induction — $X_0 = \emptyset$ — is clear. For the induction step, we prove that if $X_0 \subseteq X_1$ are finite and $X_1 = X_0 \cup \{t\}$, $t \notin X_0$, and the claim is true for X_0, then every $a \in K_{X_1}$ which is p-high has the desired form.

For clause (1), Remark 6.12 implies that we can use Lemma 6.8, clause (4).

For (2), we shall use the assumption on the coloring.

Case 1. There is no edge $e_0 \ni t$ in Γ_{X_1} such that $C(e_0) = l$. In that case, we use clause (3) of Lemma 6.8, and conclude that $a \in K_{X_0}$.

Case 2. There is an edge $e_0 \ni t$ in Γ_{X_1} with $C(e_0) = l$, but only one such edge. If $e_0 = \{s, t\}, s \in X_0$ then $x^0_{e_0} = x^0_s + x^0_t + 1 \in K_{X_1}$ is transcendental over K_{X_0} (because x^0_t is). In addition $x^0_t = x^0_{e_0} - x^0_s - 1$ and for all vertices $r \in X_0$ such that $e_r = \{t, r\}$ is an edge (of some other color), $x^0_{e_r} = x^0_{e_0} - x^0_s + x^0_r$. The polynomials $X - x^0_s - 1$, $X - x^0_s + x^0_r$ satisfy the conditions of Lemma 6.8, and so, by clause (4), a is of the form $\left(x^i_{e_0}\right)^m \cdot c$ for c which is p_{l+1}-high in K_{Γ_0} and we are done (we do not use the lemma in the same way as in Remark 6.12 — here z_0 is played by $x^0_{e_0}$, but it is the same idea).

Case 3. There is more than one edge $e_0 \ni t$ in Γ_{X_1} with color l. Then t is the center of a star in the subgraph of Γ_1 induced by that color. Assume that $s_1, \ldots, s_k \in X_0$ list the vertices such that $C(s_i, t) = l$, $(k \geq 2)$. Let $X^- = X_0 \setminus \{s_1, \ldots, s_k\}$, and $X' = X^- \cup \{t\}$. Note that $|X'| < |X_1|$, so by the induction hypothesis, the claim is true for $K_{X'}$. Γ_{X_1} is built from $\Gamma_{X'}$ by adding $s_1, \ldots, s_k$ and in each step we are in the previous case (because t was the center of a star), so we are done.

□

Lemma 6.21. *For all $s \in X$, x^0_s does not have a p' root for p' a prime different from p_0.*

Proof. Again, it is enough to prove this finite $X_0 \subseteq X$, and the proof is by induction on $|X_0|$, and follows from clause (5) of Lemma 6.8. □

This is the main proposition:

Proposition 6.22. *Assume $\varphi \in \mathrm{Aut}(K_\Gamma)$ and that $\{s_0, t_0\} \in E$ of color l. Then there is an edge $\{s_1, t_1\} \in E$ of the same color such that $\varphi\left(x^0_{s_0}\right) = x^0_{s_1}$ and $\varphi\left(x^0_{t_0}\right) = x^0_{t_1}$.*

Proof. Let $f_1 = \varphi\left(x^0_{s_0}\right)$, $f_2 = \varphi\left(x^0_{t_0}\right)$, $f = \varphi\left(x^0_{s_0} + x^0_{t_0} + 1\right) = f_1 + f_2 + 1$. From Claim 6.20 it follows that

- $f_1 = \varepsilon_1 \cdot \prod\left\{\left(x^{i_s}_s\right)^{m_s} \mid s \in X_0\right\}$, $f_2 = \varepsilon_2 \cdot \prod\left\{\left(x^{i_s}_t\right)^{m_t} \mid t \in Y_0\right\}$ and $f = \varepsilon_3 \cdot \prod\left\{\left(x^{i_e}_e\right)^{m_e} \mid e \in E_0\right\}$,

where $X_0, Y_0 \subseteq X$ and $E_0 \subseteq E$ are finite nonempty; $i_s < \omega$, $m_s \in \mathbb{Z}$ for $s \in X_0$; $i_t < \omega$, $m_t \in \mathbb{Z}$ for $t \in Y_0$; and E_0 is homogeneous of color l and $i_e < \omega$, $m_e \in \mathbb{Z}$ for $e \in E_0$. Let $p = p_{l+1}$, so f is p-high.

We can assume that unless $i_s = 0$, $p_0 \nmid m_s$ for $s \in X_0 \cup Y_0$, and that unless $i_e = 0$, $p \nmid m_e$ for $e \in E_0$.

Raising the equation $f_1 + f_2 + 1 = f$ by p^k where $k = \max\{i_e \mid e \in E_0\}$, we have an equation of the form

$$\left(\varepsilon_1 \prod \left(x^{i_s}_s\right)^{m_s} + \varepsilon_2 \prod \left(x^{i_t}_t\right)^{m_t} + 1\right)^{p^k} = \varepsilon_3^{p^k} \prod \left(x^0_r + x^0_w + 1\right)^{p^{k - i_{\{r,w\}}} m_{\{r,w\}}}.$$

Let $i = \max\{i_t \mid t \in X_0 \cup Y_0\}$. We can replace $x^{i_t}_t$ by $\left(x^i_t\right)^{p_0^{i - i_t}}$ and the same for $x^{i_s}_s$. Also replace x^0_r by $\left(x^i_r\right)^{p_0^i}$ and the same for x^0_w. For $t \in T := X_0 \cup Y_0 \cup \bigcup E_0$, let $y_t = x^i_t$, then we get

$$\left(\varepsilon_1 \prod (y_s)^{p_0^{i - i_s} m_s} + \varepsilon_2 \prod (y_t)^{p_0^{i - i_t} m_t} + 1\right)^{p^k} = \varepsilon_3^{p^k} \prod \left((y_r)^{p_0^i} + (y_w)^{p_0^i} + 1\right)^{p^{k - i_{\{r,w\}}} m_{\{r,w\}}}.$$

By Lemma 6.18, these elements are algebraically independent so this is an equation in the field of rational functions $L(y_t \mid t \in T)$.

The next step is to see that the exponents (m_t and $m_{\{r,w\}}$) are non-negative. For that we use valuations.

Recall that for any field, F and any irreducible $g \in F[X]$ there is a unique discrete (i.e. with value group $\mathbb{Z}$) valuation on the field of rational functions $F(t)$ defined by $v(g(t)) = 1$, $v \restriction F^\times = 0$. In this case, $v \restriction F[t] \geq 0$ and $v(m(t)) > 0$ iff $g | m$ for $m \in F[X]$. This is the g-adic valuation.

Suppose m_{t_0} is negative for some $t \in X_0 \cup Y_0$. Consider the discrete valuation v on the field $L(y_t \mid t \in T)$ defined by $v(y_{t_0}) = 1$, $v \restriction L(y_t \mid t \neq t_0)^\times = 0$. Then on the left hand side we get $v(LHS) < 0$ while on the right hand side, $v(RHS) = 0$ — contradiction.

Suppose $m_{\{r,w\}} < 0$ for some $\{r, w\} \in E_0$. Consider the valuation v on the field $L(y_t \mid t \in T)$ defined by $v(g(y_r)) = 1$, $v \restriction L(y_t \mid t \neq r)^\times = 0$ where g is any irreducible polynomial dividing $X^{p_0^i} + (y_w)^{p_0^i} + 1$. So $v\left((y_r)^{p_0^i} + (y_w)^{p_0^i} + 1\right) > 0$, while g does not divide $\left(X^{p_0^i} + (y_{w'})^{p_0^i} + 1\right)$ for $w \neq w$' (they relatively prime) so $v(RHS) < 0$. On the other hand, since $v(y_r) = 0$, $v(RHS) \geq 0$ — contradiction.

Hence we can consider this equation as one in the polynomial ring $L[y_t \mid t \in T]$. Moreover, since these elements are algebraically independent, each one appearing in the left hand side must appear in the right hand side and vice versa, i.e. $T = X_0 \cup Y_0 = \bigcup E_0$.

By examining the free factor, $\varepsilon_3^{p^k} = 1$.

By substituting y_r and y_w with 0 for some r, w , we can show that $E_0 = \{\{r, w\}\}$ (so $k = i_{\{r,w\}}$) and that there are no mixed monomials in the left hand side, i.e. we get an equation of the form

$$\left(\varepsilon_1 (y_r)^{p_0^{i-i_r} m_r} + \varepsilon_2 (y_w)^{p_0^{i-i_w} m_w} + 1\right)^{p^k} = \left((y_r)^{p_0^i} + (y_w)^{p_0^i} + 1\right)^{m_{\{r,w\}}}.$$

Suppose $i = i_r$ and $i \neq 0$, then $p_0 \nmid m_r$, by examining the degree of y_r, we get a contradiction, so $i = 0$ and by choice of i, $i_w = 0$ as well. In the same way we can deduce that $k = 0$. From this it follows that $\varepsilon_1 = \varepsilon_2 = 1$ and $m_r = m_w$. So we have

$$f_1 + f_2 + 1 = \left(x_r^0\right)^{m_r} + \left(x_w^0\right)^{m_w} + 1 = \left(x_r^0 + x_w^0 + 1\right)^{m_{\{r,w\}}} = f.$$

So $\{r, w\}$ is an edge of color l, $m := m_{\{r,w\}} = m_w = m_r$, and $m = 1$ or a power of r (the characteristic).

So finally we have that $\varphi\left(x_{t_0}^0\right)$ is a power of m which is a power of r. This implies that $x_{t_0}^0$ itself has an m-root. But if $m > 1$, this is a contradiction, because $x_{t_0}^0$ has no r-roots by Lemma 6.21.

This concludes the proof of the proposition. □

Corollary 6.23. *The map $\sigma : \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(K_\Gamma)$ is a bijection.*

Proof. Recall that all that is left is to show that σ is onto (by Proposition 6.19).

Let $\varphi \in \mathrm{Aut}(K_\Gamma)$. Let $t \in X$ and suppose $\{t, t_0\} \in E$. By Proposition 6.22, $\varphi(x^0_t) = x^0_{t'}$ for the some $t' \in X$. Since the graph Γ is connected, we can define $\varepsilon \in \mathrm{Aut}(\Gamma)$ by $\varepsilon(t) = t'$ (note that t' does not depend on the choice of t_0). Proposition 6.22 implies that ε is indeed an automorphism.

Since there are no p_i-roots of unity in L for all the primes we chose, it follows then that $\varphi(x^i_t) = x^i_{\varepsilon(t)}$ and that $\varphi(x^i_e) = x^i_{\varepsilon(e)}$, and hence $\varphi = \sigma(\varepsilon)$. □

We still have to prove that $|K_\Gamma| \leq \left|X^{\langle<\omega\rangle}\right|$.

Lemma 6.24. *If $X_i \subseteq X$ $(i = 1, 2)$ are two subsets of the vertices set then $K_{X_1} \cap K_{X_2} = K_{X_1 \cap X_2}$.*

Proof. We may assume that X_1, X_2 are finite. Assume $x \in K_{X_1} \cap K_{X_2}$ and that $|X_1|$ is minimal with respect to $x \in K_{X_1}$. If $X_1 \subseteq X_2$ then we are done. If not, let $t \in X_1 \setminus X_2$ be some vertex, and let $X' = X_1 \setminus \{t\}$. So $x \notin K_{X'}$, and x is transcendental over $K_{X'}$ while x^0_t is algebraic over $K_{X'}(x)$. Let $X'_2 = X' \cup X_2$, $X_3 = X'_2 \cup \{t\}$. We have $x \in K_{X_2} \subseteq K_{X'_2}$, and $x^0_t \in K_{X_3}$ is transcendental over $K_{X'_2}$. This is a contradiction, because x^0_t is algebraic over $K_{X'}(x) \subseteq K_{X'_2}$. Hence there is no such t i.e. $X_1 \subseteq X_2$. □

And now it is easy to define an injective map $\Psi : K_\Gamma \to X^{\langle<\omega\rangle}$. Define by induction on n injective function $\Psi_Y : K_Y \to X^{\langle<\omega\rangle}$ for $|Y| \leq n$ such that $Y_1 \subseteq Y_2$ implies $\Psi_{Y_1} \subseteq \Psi_{Y_2}$. This is enough, since by the lemma above, $\bigcup \{\Psi_Y \mid Y \subseteq X, |Y| < \omega\}$ is an injection from K_Γ to $X^{\langle<\omega\rangle}$.

For the construction of $\Psi_Y : K_Y \to X^{\langle<\omega\rangle}$, the idea is that given $x \in K_Y$ such that $x \notin K_{Y'}$ for any $Y' \subsetneq Y$ we can code x using the set Y and the set of codes that Lemma 6.8, clause (6) gives us for any choice of $Y' \subsetneq Y$ of size $|Y| - 1$.

This (and Lemma 6.8, clause (6)) was the reason we chose $X^{\langle<\omega\rangle}$ and not $X^{<\omega}$: in order to code $x \in K_\Gamma$, we need first to code the minimal set Y such that $x \in K_Y$, and then x can be coded in $|Y|$ different ways, depending on the choice of $|Y'|$ as above. However, there is

no well ordering of Y, so we have no way of ordering these codes. For instance, the code of $x_t^0 + x_s^0$ for $s, t \in X$, should be $\{\langle s \rangle, \langle t \rangle, \ldots\}$.

7. SOME TECHNICAL LEMMAS ON FIELDS

This section is devoted to technical lemmas concerning fields. We may use Choice here — see Remark 6.10.

First, some simple and known facts:

Fact 7.1. *(Abel's Theorem) Suppose that p is prime and K is a field. Then the polynomial $X^p - a$ is irreducible iff a does not have a p-th root in K.*

Lemma 7.2. *Let n be a positive integer and let K be a field of characteristic r, where $r = 0$ or $r \nmid n$, which contains a primitive n-th root of unity. Let $0 \neq a \in K$ and suppose z is a root of the equation $X^n = a$. If $b \in K(z)$ satisfies $b^n \in K$, then $b = c \cdot z^k$ for some $0 \leq k < n$ and $c \in K$.*

Proof. This is an easy consequence of Kummer Theory. See [Lan02, VI.8, Theorem 8.2]. □

Lemma 7.3. *Let K be a field containing all roots of unity. Assume that t solves the equation $X^p = a$ for some $a \in K$ and prime p, and $L = K(t)$. Then if $b \in L$ satisfies $b^{q^m} \in K$ for some prime $q \neq p, m < \omega$, then $b \in K$.*

Proof. By Abel's theorem, and since K contains all p and q roots of unity, $[L : K] = p$ or $[L : K] = 1$, while $[K(b) : K]$ is a power of q, so it must be 1. □

Lemma 7.4. *Assume K and L are fields such that:*

1. *$K \supseteq L$ and is a L is relatively algebraically closed in K.*
2. *K is a finite algebraic extension of the simple transcendental extension $L(y)$.*

Then if p is a prime and $x \in K$ is p-high, then $x \in L$.

Proof. (This proof is taken from [Prö84]). Assume $x \in K \backslash L$. Then y is algebraic over $L(x)$ (by (1)). Denote by x_m for $m < \omega$ the p^m-th root of x given in Definition 6.6. Then

we have $L(x) \subseteq L(x_1) \subseteq L(x_2) \subseteq \ldots \subseteq K$. As $K/L(x)$ is algebraic of finite degree, $L(x_l) = L(x_{l+1})$ for some l, so $x_{l+1} \in L(x_l)$ — the transcendental element x_l has a p root in $L(x_l)$ — this is a contradiction. □

Another easy fact:

Fact 7.5. *Let R be an integral domain, F its field of fractions. $\alpha_1, \ldots, \alpha_n$ elements algebraic over F such that:*

- *The minimal* monic *polynomial of α_1 over F, $m_1(X_1)$, belongs to $R[X_1]$.*
- *The minimal* monic *polynomial of α_2 over $F(\alpha_1)$, $m_2(\alpha_1, X_2)$, belongs to $R[\alpha_1, X_2]$.*
- *And so on.*

Then $R[\alpha_1, \ldots, \alpha_n] = R[X_1, \ldots, X_n]/(m_1, m_2, \ldots, m_n)$. In particular, $(m_1, \ldots, m_n)$ is prime.

And here is the main technical lemma:

Lemma 7.6. *(an expanded version of* [Prö84, The third lemma]*) Let r be a prime number or 0, p a prime number different from r and let $\{p_0, \ldots, p_{n-1}\}$ be a set of pairwise distinct primes, different from p, r. Let F be a field of characteristic r which contains all roots of unity. For $k < n$, let V_k be some set such that $k \neq l \Rightarrow V_k \cap V_l = \emptyset$, and let $V = \bigcup_{k<n} V_k$.*

For each $v \in V$, let $T_v \in F[X]$ be polynomials such that:

- *none of them is constant.*
- *none of them is divisible by X.*
- *they are separable polynomials.*
- *they are pairwise relatively prime (i.e. no nontrivial common divisor).*

Suppose that $K = K_{\langle T_v \mid v \in V \rangle}$ is an extension of F generated by the set $\{z_i \mid i < \omega\} \cup \{t_i^v \mid v \in V, i < \omega\}$ from the algebraic closure of $F(z_0)$ where:

- *z_0 is transcendental over F.*
- *$(z_{i+1})^p = z_i$ for all $i < \omega$.*
- *$t_0^v = T_v(z_0)$.*

- *if* $v \in V_k$ *then* $\left(t^v_{i+1}\right)^{p_k} = t^v_i$.

Let $1 \leq j \leq \omega$, *and* $\rho : V \to (\omega + 1 \setminus \{0\})$. *Denote the subfield* $F\left(z_i, t^v_{l_v} \mid i < j, l_v < \rho(v), v \in V\right)$ *of* K *by* $F(j,\rho) = F(j,\rho)_{\langle T_v \mid v \in V\rangle}$.

Then we have the following properties:

(1) *The polynomial* $X^p - z_{j-1}$ *is irreducible over* $F(j,\rho)$ *for every* ρ *and* $1 \leq j$.

(2) *If* $w \in V_k$ *then the polynomial* $X^{p_k} - t^w_{\rho(w)-1}$ *is irreducible over* $F(j,\rho)$ *for all* ρ, j *such that* $\rho(w) < \omega$.

(3) *If* $k < n$ *and the* $(p_k)^m$*-th power* $(1 \leq m)$ *of an element of* $F(j,\rho)$ *belongs to the subfield* $F(z_l)$ *where* $l < j \leq \omega$ *then this element can be written in the form*

$$c \cdot \frac{f(z_i)}{g(z_i)} \prod_{v \in W_k} \left(t^v_{r_v}\right)^{l_v}$$

for some $c \in F$, f *and* g *are relatively prime monic polynomials over* F, $i \leq l$, W_k *is a finite subset of* V_k *where* $v \in W_k \Rightarrow 1 \leq r_v < \rho(v)$, $r_v \leq m$, *and* $0 < l_v < (p_k)^{r_v}$.

(4) F *is relatively algebraically closed in* K.

(5) *An equivalent definition of* K $(F(j,\rho))$ *is the following one: Suppose* F *is the field of fractions of an integral domain* S. *Then* K $(F(j,\rho))$ *is the field of fractions of the integral domain* R/I *where* $R = S\left[Y_i, S^v_l \mid i, l < \omega, v \in V\right]$ $\left(R = S\left[Y_i, S^v_{l_v} \mid i < j, l_v < \rho(v), v \in V\right]\right)$ *(i.e. this is a polynomial ring) and* $I \leq R$ *is the ideal generated by the equations:*

   (a) $Y^p_{i+1} = Y_i$ *for* $i < \omega$ $(i < j)$

   (b) $Y^v_0 = T_v(Y_0)$ *for* $v \in V$.

   (c) *If* $v \in V_k$ *for* $k < n$, $\left(S^v_{l+1}\right)^{p_k} = S^v_l$ *for* $l < \omega$ $(l < \rho(v))$.

(6) *Each* q*-high element of* K *belongs to* F *whenever* q *is a prime different from* p *and* $\langle p_k \mid k < n\rangle$.

(7) *Each* p*-high element of* K *is of the form* $c \cdot (z_i)^m$, *where* c *is a* p*-high element of* F, $i < \omega$ *and* m *is an integer.*

(8) *If* p' *is a prime different from* p *then* z_0 *does not have a* p' *root.*

(9) *If V is finite then $|K| \leq \left|F^{\langle<\omega\rangle}\right|$. Furthermore, the injection witnessing this is definable from the parameters given when constructing K (i.e. the function $v \mapsto T_v$, etc).*

(10) *Clauses (1)–(9) except clause (3) are true for* any *field F of characteristic r.*

Proof. This proof is an adaptation of [Prö84, Third Lemma]. There it is dealt with just adding one q root to T_v, while we deal with infinite such roots. The difference between the proofs is not large.

Let us assume that $n = 1$. i.e. there is only one prime different from p, r and denote it by q. The proof is the essentially the same if $n > 1$, but involves more indices, and after reading the proof for this case, the general case should be easy. Throughout the proof, let $\rho : V \to (\omega + 1 \setminus \{0\})$, $\mathrm{supp}(\rho) = \{v \mid \rho(v) \neq 1\}$ and $|\rho| = \sum \{\rho(v) - 1 \mid v \in \mathrm{supp}(\rho), \rho(v) < \omega\}$. When we say that $\mathrm{supp}(\rho)$ is finite, we also mean that $|\rho|$ is finite, and $\rho[V] \subseteq \omega$.

First let us note that it is enough to prove (1), (2) and (3) for finite $\mathrm{supp}(\rho)$ and j. In addition we may assume for these clauses that $j = 1$:

Suppose $i < \omega$, and let $S^i_v \in F[X]$ be $S^i_v(X) = T_v\left(X^{p^i}\right)$ for $v \in V$. Then $\{S^i_v \mid v \in V\}$ satisfy the conditions of the lemma.

Note that for finite j and ρ with finite $\mathrm{supp}(\rho)$, $F(j,\rho)_{\langle T_v \mid v\in V\rangle} \cong F(1,\rho)_{\left\langle S_v^{j-1} \mid v\in V\right\rangle}$ (taking z_{j-1} to z_0 and T_v to S_v^{j-1}). Hence if we know (1) and (2) for the case $j = 1$, then they are true for any j. Regarding (3), we note that by Lemma 7.3, if an element $x \in F(i+1,\rho)$ satisfies $x^{q^m} \in F(i,\rho)$ then x belongs to $F(i,\rho)$. Hence we may assume $j = l + 1$, and after applying the isomorphism above — $j = 1$.

So let us begin:

First we prove (2) and (3). We prove this by induction on $|\rho|$. For $|\rho| = 0$, $F(1,\rho) = F(z_0)$ is just the quotient field of the polynomial ring $F[z_0]$, therefore (3) is true in that case. Now we prove that if (3) is true for ρ then (2) is true as well. So, in order to prove (2), it is enough, by Abel's Theorem (Lemma 7.1), to prove that $t^w_{\rho(w)} \notin F(1,\rho)$. If this is

not the case, then, by (3), we get an equation of the form:

$$g(z_0)\cdot t^w_{\rho(w)} = cf(z_0)\prod_{v\in W}\left(t^v_{r_v}\right)^{l_v}$$

For some finite $W\subseteq V$, $1\leq r_v\leq \rho(w)$, $0<l_v<q^{r_v}$, $r_v<\rho(v)$ for $v\in W$. After raising both sides of the equation to the power of q, $\rho(w)$ times, we get an equation of the form

$$g^{q^{\rho(w)}}\cdot T_w = c^{q^{\rho(w)}} f^{q^{\rho(w)}}\prod_{v\in W}\left(T_v^{q^{\rho(w)-r_v}}\right)^{l_v}$$

By the conditions on the polynomials T_v, $g=f=1$, and we get a contradiction (because we get $W=\{w\}$ and $r_w=\rho(w)$).

Now the induction step for (3). Suppose $b\in F(1,\rho)$ and $b^{q^m}\in F(z_0)$ (assume $m>0$), and let $v\in V$ be such that $\rho(v)>1$.

Define ρ' by:

- $\rho'(v)=\rho(v)-m$ (unless $\rho(v)-m<1$ and then $\rho'(v)=1$).
- $\rho'(w)=\rho(w)$ for $w\neq v$.

So $F(1,\rho')\left(t^v_{\rho(v)-1}\right)=F(1,\rho)$. Now, $b\in F(1,\rho')\left(t^v_{\rho(v)-1}\right)$, $b^{q^m}\in F(z_0)\subseteq L:=F(1,\rho')$ and $\left(t^v_{\rho(v)-1}\right)^{q^m}\in L$. By Kummer Theory (Lemma 7.2), we have $b=c\cdot\left(t^v_{\rho(v)-1}\right)^l$ for some $c\in L$, $0\leq l<q^m$. Note that if $q\mid l$ then we are done by induction, so assume $q\nmid l$.

If $\rho(v)-1\leq m$ the we are done: it follows that $c^{q^m}\in F(z_0)$ and by the induction hypothesis we know c can be represented in the right form (and t_v does not appear there, as $\rho'(v)=1$). So assume $\rho(v)-1>m$.

Surely, $c^{q^{\rho(v)-1}}\in F(z_0)$, so by the induction hypothesis (recall $c\in L$), c can be written in the form

$$d\cdot\frac{f(z_0)}{g(z_0)}\prod_{u\in W}\left(t^u_{r_u}\right)^{l_u}$$

where $d\in F$, $W\subseteq V$ and finite, and $1\leq r_u<\rho'(u), r_u\leq\rho(v)-1$ for $u\in W$ (hence, of course, $W\subseteq\operatorname{supp}(\rho')$). By this representation of c, $c^{q^m}\in F(1,\rho'')$ where $\rho''(w)=\rho'(w)-m$ for all $w\in V$ (and again, if $\rho'(w)-m<1$, $\rho''(w)=1$). Since $b^{q^m}\in F(z_0)$, $\left(t^v_{\rho(v)-1}\right)^{l\cdot q^m}=\left(t^v_{\rho(v)-m-1}\right)^l\in F(1,\rho'')$. Since $q\nmid l$, $\left(l,q^{\rho(v)-m-1}\right)=1$ so $t^v_{\rho(v)-m-1}\in$

$F(1,\rho'')$. But $\rho''(v) \leq \rho'(v) - 1 = \rho(v) - m - 1$, and we get a contradiction to (2) (because it follows that $t^v_{\rho''(v)} \in F(1,\rho'')$).

So (2) and (3) are proven.

Now we prove (1) for $j = 1$ and finite $|\rho|$ by induction on $|\rho|$. By Abel's Theorem it is enough to prove that $z_1 \notin F(1,\rho)$. For $|\rho| = 0$, it is clear. The induction step follows from 7.3.

Next we prove (4). Again we assume that $|\rho|$ is finite. Let x be an algebraic element of K over F. Let $L = F(x)$. The element z_0 is transcendental over L, since x is algebraic. All the other conditions of the lemma are also satisfied with respect to L instead of F. Let $v \in V$, and $\rho^+ : V \to \omega + 1$ defined by $\rho^+(v) = \rho(v) + 1$ and for $w \neq v$, $\rho^+(w) = \rho(w)$. Suppose $x \in F(\omega,\rho^+) \setminus F(\omega,\rho)$. Then $F(\omega,\rho)(x) = F(\omega,\rho^+)$ (because $[F(\omega,\rho^+) : F(\omega,\rho)] = q$ — a prime — by (2)) and in particular $t^v_{\rho(v)} \in F(\omega,\rho)(x) \subseteq L(\omega,\rho)$ — a contradiction. So inductively we get $x \in F(\omega,1)$ (where 1 is the constant sequence). Hence, $x \in F(z_i)$, so $x \in F$.

Next we prove (5). Denote by $S(j,\rho)$ and $I(j,\rho)$ the ring R and ideal I mentioned in (5). We shall show that $S(j,\rho)/I(j,\rho)$ is naturally embedded in K. It is enough as the field of fractions contains all of $F(j,\rho)$'s generators.

It is enough to show this for finite $j, |\rho|$. Let $R' = S[z_0] \cong S[Y_0]$. By (1) and (2) we can use 7.5 and we have

$$\begin{aligned} K \supseteq\ & R'\left[z_i, t^v_{l_v} \mid i < j, l_v < \rho(v)\right] \cong \\ & S[Y_0]\left[Y_i, S^v_{l_v} \mid 1 < i < j, l_v < \rho(v)\right]/I(j,\rho) = S(j,\rho)/I(j,\rho) \end{aligned}$$

As desired.

Next we prove (6). Suppose x is q-high in K. So $x \in F(i,\rho)$ for some $i < \omega$ and finite $|\rho|$. By Lemma 7.3, x is q-high already in $F(i,\rho)$. Now apply (4) and Lemma 7.4.

Next we prove (7). If $x \in F(\omega,\rho)$ is p-high, then by Lemma 7.3, x is already p-high in $F(\omega,\rho_0)$ where $|\rho_0|$ is finite. So it is enough to prove by induction on $|\rho|$ that the p-high elements of $F(\omega,\rho)$ are of the form $c \cdot z_i^m$.

The induction base: Suppose $x \in F(\omega,1)$.

If x is already p-high in $F(z_i)$ for some i, then by 7.4 $x \in F$.

Suppose now that x is not p-high in any finite stage. Let $i < \omega$ be such that $x \in F(z_i)$, so there are relatively prime polynomials $f_0, g_0 \in F[z_i]$, none of them divisible by z_i, such that $x = (z_i)^{l_0} \frac{f_0(z_i)}{g_0(z_i)}$ for some $l_0 \in \mathbb{Z}$. So it is enough to show that $u = x/(z_i)^{l_0}$ is p-high already in $F(z_i)$. So suppose not. Let $X_m = \left\{ y \in F(\omega, 1) \,\middle|\, y^{p^m} = u \right\}$. Let $j < \omega$ be the first such that $X_j \subseteq F(z_i), X_{j+1} \nsubseteq F(z_i)$. Let s be the least natural number for which $X_{j+1} \subseteq F(z_s)$ $(s > i)$. Suppose $v \in X_{j+1}$, and let $v' = v^p \in X_j \subseteq F(z_i)$. So $v' = (z_i)^{l_1} \frac{f_1(z_i)}{g_1(z_i)}$ where f_1, g_1 are relatively prime, neither of them divisible by z_i, $l_1 \in \mathbb{Z}$. Since $(v')^{p^j} = u$, $l_1 = 0$. As $v^p \in F(z_i)$, by 7.2, we can write $v = (z_s)^m \cdot d$ for some $d \in F(z_i)$, $m < \omega$, $p \nmid m$ (as $v \notin F(z_{s'})$ for $s' < s$). Denote $d = (z_i)^{l_2} \frac{f_2(z_i)}{g_2(z_i)}$ where $f_2, g_2 \in F[z_i]$ are relatively prime, none of them divisible by z_i, $l_2 \in \mathbb{Z}$. Since $v^p = v'$, we have

$$(z_{s-1})^m \cdot (z_i)^{l_2 p} \left(\frac{f_2(z_i)}{g_2(z_i)} \right)^p = \left(\frac{f_1(z_i)}{g_1(z_i)} \right)$$

and after raising to the power of p, $s-1-i$ times, we get $p^{s-i} l_2 + m = 0$, so $p \mid m$ — a contradiction.

The induction step: Suppose we have ρ^+ and ρ as before (i.e. $\rho^+(v) = \rho(v) + 1$ for some $v \in V$ and $\rho^+(w) = \rho(w)$ for $w \neq v$) and $x \in F(\omega, \rho^+)$ is p-high there. Let $K' = F(\omega, \rho^+)$ and $L = F(\omega, \rho)$. By (2), the degree of the extension K'/L is q.

Denote by $N : K' \to L$ the norm of the extension. We use the following properties of the norm:

- Its multiplicative, and $N(a) = a^q$ for $a \in L$.
- If $K_i = F(i, \rho^+)$ and $L_i = F(i, \rho)$ then $N \restriction K_i = N_{K_i} : K_i \to L_i$.

$N(x)$ is p-high in L. So $y = x^q / N(x)$ is p-high in K'. Choose $i < \omega$ such that $x, y \in F(i+1, \rho^+)$. We shall show that y is p-high in $F(i+1, \rho^+)$. Suppose that $u \in F(\omega, \rho^+) \setminus F(i+1, \rho^+)$ satisfies $u^p \in F(i+1, \rho^+)$ and y is a p^m power of u for some $m < \omega$. Let $k = \max\{n \mid u \notin F(n+1, \rho^+)\} \geq i$. By Lemma 7.2, as $u \in F(k+2, \rho^+)$ and $u^p \in F(k+1, \rho^+)$, we have $u = h \cdot (z_{k+1})^b$ where $h \in F(k+1, \rho^+)$ and $0 < b < p$. Hence $N(u) = N(h) \cdot N(z_{k+1})^b = N(h) \cdot (z_{k+1})^{bq}$. Now, $N(h) \in F(k+1, \rho)$, so $N(u) \notin F(k+1, \rho)$ because by (1) $z_{k+1} \notin F(k+1, \rho)$ and $(p, bq) = 1$. On the other

hand, $N(y) = N(u)^{p^m}$ and $N(y) = N(x^q/N(x)) = N(x)^q/N(x)^q = 1$, so $N(u)$ is algebraic over F, which is a contradiction to (4).

By Lemma 7.4, $y \in F$ and is p-high there, therefore $y \cdot N(x) = x^q$ is p-high in L. By the induction hypothesis, x^q has the form $c \cdot (z_i)^m$, hence $x^q \in F(z_i)$. By (3), we get the equation:

$$c \cdot (z_i)^m = x^q = d^q \left(\frac{f^q(z_i)}{g^q(z_i)} \right) \prod_{w \in W} (T_w(z_0))^{l_w}$$

for some finite $W \subseteq V$, $0 < l_w < q$. This implies $g = 1$, $q \mid m$, $f(z_i) = (z_i)^{m/q}$, and $W = \emptyset$. Hence $x = \varepsilon \cdot \left(d \cdot (z_i)^{m/q} \right)$ where $\varepsilon^q = 1$ (so $\varepsilon \in F$) as promised.

Clause (8) follows from the previous clauses: if $x^{p'} = z_0$, then: if $p' = q$ then by (3) $x = c \cdot \frac{f(z_0)}{g(z_0)} \prod_{v \in W'} (t_1^v)^{l_v}$ $(0 < l_v < q)$, so $z_0 = x^q = c \cdot \left(\frac{f(z_0)}{g(z_0)} \right)^q \prod_{v \in W} (T_v)^{l_v}$, so $W = \emptyset$, $g = 1$, and we easily derive a contradiction. If $p' \neq q$, use Lemma 7.3.

Clause (9): one defines by induction on $|\rho|, n$ an injective function $\varphi_{n,\rho} : F(n,\rho) \to F^{\langle <\omega \rangle}$ such that $\varphi_{n,\rho} \subseteq \varphi_{n',\rho'}$ whenever $n \leq n'$ and $\rho \leq \rho'$ (i.e. $\rho(v) \leq \rho'(v)$ for all $v \in V$). Why is this enough? we shall need:

Proposition. *for all* $1 \leq m, n < \omega$, $\rho, \rho' \in^V \omega$,
$F(n,\rho) \cap F(m,\rho') = F(\min(n,m), \min(\rho,\rho'))$ *where* $\min(\rho,\rho')(v) = \min(\rho(v), \rho'(v))$.

Proof. The proof is an argument similar to the one used to prove (4) and Lemma 6.24.

Assume $x \in F(n,\rho) \cap F(m,\rho')$. Assume that $n, |\rho|$ is minimal with respect to $x \in F(n,\rho)$. If $(n,\rho) \leq (m,\rho')$ then we are done. If not, suppose $m < n$ (the case where $\rho \not\leq \rho'$ is similar). So $x \notin F(m,\rho)$. Since $x \in F(m,\rho')$, we can find $\rho \leq \rho_1, \rho_2$ such that $\rho_1(v) = \rho_2(v)$ for all $v \neq v_0$ but $\rho_2(v_0) = \rho_1(v_0) + 1$ and $x \in F(m,\rho_2) \setminus F(m,\rho_1)$ and then $F(m,\rho_2) = F(m,\rho_1)(x)$, so also $F(n,\rho_2) = F(n,\rho_1)(x)$ but since $x \in F(n,\rho_1)$, we get that $F(n,\rho_1) = F(n,\rho_2)$ and this contradicts (2). □

By this proposition, $\bigcup \{ \varphi_{n,\rho} \mid n \in \omega, \rho \in^V \omega \}$ will be an injective function from K to $F^{\langle <\omega \rangle}$.

For the construction, one should use the fact that we can represent the sequence ρ as a function from polynomials to ω, hence it has a code in $F^{\langle <\omega \rangle}$. So the idea is that given x with

minimal (n,ρ) such that $x \in F(n,\rho)$, code x as (n,ρ) and then for each choice of (n',ρ') such that $(n',\rho') < (n,\rho)$ with difference exactly one (either $n' = n-1$ or $\rho'(v) = \rho(v) - 1$ for some v), use the code we already have for $F(n',\rho')$ and the representation of x as linear combination of $(z_{n-1})^i$, $i < p$ or $\left(t^v_{\rho(v)-1}\right)^i$, $i < q$.

Now for clause (10):

Assume then, that F is some field, not necessary containing any roots of unity. Let $\bar{F}$ be its algebraic closure. The lemma works for $\bar{F}$ because z_0 is transcendental over F hence over $\bar{F}$ and the conditions on the polynomials T_v still hold. Denote by K' the field corresponding to it. So $K \subseteq K'$, and for every n, ρ, $F(n,\rho) \subseteq \bar{F}(n,\rho)$. (1) and (2) are clearly true (for F) as they are true for $\bar{F}$.

Hence, (4) is true as well: the proof uses only (2). (4) implies that $K \cap \bar{F} = F$, and this allows us to prove all the other clauses, for example — (7) — If x is p-high in K then it is p-high in K' hence it has the form $c \cdot (z_i)^m$ for $c \in \bar{F}$, but then $c \in \bar{F} \cap K = F$.

This completes the proof of this lemma. □

References

[Fab78] V. Faber. Large abelian subgroups of some infinite groups. II. *Rocky Mountain J. Math.*, 8(3):481–490, 1978.

[FK82] E. Fried and J. Kollár. Automorphism groups of fields. In *Universal algebra (Esztergom, 1977)*, volume 29 of *Colloq. Math. Soc. János Bolyai*, pages 293–303. North-Holland, Amsterdam, 1982.

[Hod93] Wilfrid Hodges. *Model Theory*, volume 42 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, Great Britain, 1993.

[JST99] Winfried Just, Saharon Shelah, and Simon Thomas. The automorphism tower problem revisited. *Adv. Math.*, 148(2):243–265, 1999.

[KS09] Itay Kaplan and Saharon Shelah. The automorphism tower of a centerless group without choice. *Arch. Math. Logic*, 48(8):799–815, 2009.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Prö84] Péter Pröhle. Does the Frobenius endomorphism always generate a direct summand in the endomorphism monoids of fields of prime characteristic? *Bull. Austral. Math. Soc.*, 30(3):335–356, 1984.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[She07] Saharon Shelah. The height of the automorphism tower of a group. *preprint*, 2007. `arXiv:math/0405116[math.LO]`.

[Tho] Simon Thomas. The automorphism tower problem. Book in preperation. See `www.math.rutgers.edu/~sthomas/book.ps`.

[Tho85] Simon Thomas. The automorphism tower problem. *Proc. Amer. Math. Soc.*, 95(2):166–168, 1985.

[Tho98] Simon Thomas. The automorphism tower problem. II. *Israel J. Math.*, 103:93–109, 1998.

[vdWS28] Bartel Leendert van der Waerden and Otto Schreier. Die automorphismen der projectiven gruppen. *Abh. Math. Sem. Univ. Hamburg.*, 6:303–332, 1928.

[Wie39] Helmut Wielandt. Eine Verallgemeinerung der invarianten Untergruppen. *Math. Z.*, 45(1):209–244, 1939.