Covers of the multiplicative group of an algebraically closed field of characteristic zero

Boris Zilber
University of Oxford

July 2006

1 Introduction and results

Consider the classical universal cover of the one dimensional complex torus $\mathbb{C}^*$, which gives us the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i_C} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \to 1. \tag{1}$$

Model theoretically one can interpret the sequence as a structure in various ways. The simplest algebraic structure on the sequence which bears interesting algebro-geometric information is the one with the additive group structure in the middle and with the full algebraic geometry on $\mathbb{C}^*$. The latter is equivalent to treating $\mathbb{C}^*$ as $\mathbb{C} \setminus \{0\}$ with the full field structure on $\mathbb{C}$. We call this structure **a group cover** of the multiplicative group of the field.

Is the group cover of $\mathbb{C}^*$ determined uniquely? We can put the question in the following precise form:

Given an exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i_H} H \xrightarrow{\mathrm{ex}} \mathbb{C}^* \to 1 \tag{2}$$

with H a torsion-free divisible abelian group and ex *a group homomorphism, is there an isomorphism σ between the groups covers (1) and (2), that is a group-isomorphism $\sigma_H : \mathbb{C} \to H$ and a field automorphism $\sigma_C : \mathbb{C} \to \mathbb{C}$ such that all squares commute?*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{i_C} & \mathbb{C} & \xrightarrow{\exp} & \mathbb{C}^* & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \sigma_H} & & \downarrow{\scriptstyle \sigma_C} & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{i_H} & H & \xrightarrow{\mathrm{ex}} & \mathbb{C}^* & \longrightarrow & 1
\end{array}$$

This paper gives a positive answer to the question in a more general form.

Theorem 1 *Let $F^\times$ be the multiplicative group of an algebraically closed field of characteristic 0, H an abelian divisible torsion free group such that the sequence*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i} H \xrightarrow{\mathrm{ex}} F^\times \longrightarrow 1 \tag{3}$$

is exact. Then the isomorphism type of the sequence is determined by the isomorphism type of the field F. In other words, if

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i'} H' \xrightarrow{\mathrm{ex}'} F'^\times \longrightarrow 1 \tag{4}$$

is another such sequence, with a field F' isomorphic to F, then there is an isomorphism σ between the sequences, which is induced by a field isomorphism from F to F', is a group isomorphism on H and $\mathbb{Z}$, and all squares commute.

It is worth recalling here that the isomorphism type of an algebraically closed field of a given characteristic is, by Steinitz' theorem, determined by its transcendence degree.

The results of the paper furnish an algebraic background for the study of a more complicated structure, *a field with pseudo-exponentiation* (see [Z1, section 2] and [Z3]) which takes into account that the cover H bears field structure as well.

Theorem 1 is a model-theoretic consequence of Theorem 2 (see the discussion after Theorem 2) which is formulated and proved in a field-theoretic language. The formulation is rather technical but, importantly, it is an arithmetic statement equivalent to the geometric form of Theorem 1. The equivalence is due to the model-theoretical Keisler-Shelah theory of *excellency.* We do not give full details for this equivalence here, leaving it to the forthcoming paper [Z4].

Theorem 1 is not trivial due to the fact that, once for $a \in F^\times$ we fix an $h \in H$ such that $\mathrm{ex}(h) = a$, we fix the whole subgroup $\mathrm{ex}(\mathbb{Q}\cdot h)$. In particular if, for example, $F = F'$ we can not in general take σ to be identity on F.

On the other hand, there is a version of the statement which is quite easy to prove; this is the case when in the definitions $\mathbb{Z}$ is replaced by $\hat{\mathbb{Z}}$, the completion of $\mathbb{Z}$ in the profinite topology. This corresponds to the well-known SGA-construction of "the algebraic π_1". We discuss these issues and provide detailed proofs in the last section of the paper.

The author would like to thank Neil Dummigan for a very substantial contribution to this paper. On the initial step of the research he directed the author to certain Galois calculations, which developed later into the proof of the crucial Lemma 2.19, and also took part in the proof of an important Lemma 2.1, not mentioning helpful general discussions and suggestions.

The author is very thankful to D.Pierce for carefully reading the paper and suggesting many valuable improvements. Also thanks are due to P.Voloch who provided us with a proof of a version of Corollary 1.5 over an algebraically closed field.

In the rest of the section we introduce our main definitions and discuss the main results on a more technical level.

Notation 1.1 For a non-torsion $a \in \mathbb{C}^\times$ let $a^{\mathbb{Q}}$ be a (non unique) multiplicative subgroup of $\mathbb{C}^\times$ containing a and isomorphic to the additive group $\mathbb{Q}$ of the rational numbers. We call such a subgroup **a multiplicatively divisible subgroup associated with** a. (An example of such a subgroup one gets by fixing a value for $\ln a$ and setting

$$a^{\mathbb{Q}} = \{\exp(q \ln a) : q \in \mathbb{Q}\}.)$$

Notice that the definition $a^{\mathbb{Q}}$ makes also sense when a is a root of unity, then this is just the torsion subgroup of the field.

We further denote

$\langle a_1, \ldots, a_n \rangle$ is the multiplicative subgroup generated by $a_1, \ldots, a_n \in \mathbb{C}^\times$.

μ_n is the group of roots of unity of order n in $\mathbb{C}^\times$,

μ is the group of all the roots of unity in $\mathbb{C}^\times$.

Remark 1.2 Notice that, for a fixed $a \in \mathbb{C}^\times$ as above, a choice of $a^{\mathbb{Q}}$ can be made by choosing roots $a^{\frac{1}{m}}$ of a of orders $m \in \mathbb{N}$ in a coherent way, which thus form a projective system, in a natural bijection to the projective system

$$\mu_{ml} \to^{x^m} \mu_l$$

of subgroups of roots of unity. The projective limit of the latter can be identified with the group $\hat{\mathbb{Z}}$, the completion of the cyclic group $\mathbb{Z}$ in the profinite topology. Thus any choice of $a^{\mathbb{Q}}$ corresponds to a point in $\hat{\mathbb{Z}}$.

Usually we consider the multiplicative group $a^{\mathbb{Q}}$ as equipped with a fixed isomorphism to $(\mathbb{Q}, +)$ under which a maps to 1.

Then $a^{\frac{1}{m}}$ will stand for the m-th root of a corresponding to $\frac{1}{m}$ under the assumed isomorphism between $a^{\mathbb{Q}}$ and $\mathbb{Q}$.

For P a subfield of $\mathbb{C}$ and $X_1, \ldots, X_n \subseteq \mathbb{C}$ we let $P(X_1, \ldots, X_n)$ be the subfield generated by $X_1, \ldots, X_n$ over P.

We say that $\{b_1, \ldots, b_l\} \subseteq \mathbb{C}^\times$ are **multiplicatively independent** if, for all integers $n_1, \ldots, n_l$

$$b_1^{n_1} \cdot \cdots \cdot b_l^{n_l} = 1 \text{ if and only if } n_1 = \cdots = n_l = 0.$$

More generally, say that $\{b_1, \ldots, b_l\}$ are **multiplicatively independent** over a field F if, for all integers $n_1, \ldots, n_l$,

$$b_1^{n_1} \cdot \cdots \cdot b_l^{n_l} \in F \text{ if and only if } n_1 = \cdots = n_l = 0.$$

Definition 1.3 Given subgroups $b_1^{\mathbb{Q}}, \ldots, b_l^{\mathbb{Q}}$ of $\mathbb{C}^\times$, a subfield $F \subseteq \mathbb{C}$ and a positive integer m, we will say that the group elements $b_1^{\frac{1}{m}} \in b_1^{\mathbb{Q}}, \ldots, b_l^{\frac{1}{m}} \in b_l^{\mathbb{Q}}$ **determine the isomorphism type of** $b_1^{\mathbb{Q}}, \cdots, b_l^{\mathbb{Q}}$ **over** F if, for any subgroups $c_1^{\mathbb{Q}}, \ldots, c_l^{\mathbb{Q}}$ of $\mathbb{C}^\times$, any field isomorphism

$$\phi_m : F(b_1^{\frac{1}{m}}, \ldots, b_l^{\frac{1}{m}}) \to F(c_1^{\frac{1}{m}}, \ldots, c_l^{\frac{1}{m}}),$$

$$b_i^{\frac{1}{m}} \mapsto c_i^{\frac{1}{m}}$$

over F extends to a field isomorphism

$$\phi_\infty : F(b_1^{\mathbb{Q}}, \ldots, b_l^{\mathbb{Q}}) \to F(c_1^{\mathbb{Q}}, \ldots, c_l^{\mathbb{Q}})$$

$$b_i^{\mathbb{Q}} \mapsto c_i^{\mathbb{Q}}.$$

Theorem 2 *Let $P \subseteq \mathbb{C}$ be a finitely generated extension of $\mathbb{Q}$ and $L_1, \dots, L_n$ be algebraically closed subfields of the algebraic closure of P, $n \geq 0$. Let $a_1, \dots, a_r \in P^\times$, $b_1, \dots, b_l \in \mathbb{C}^\times$ and let $a_1^{\mathbb{Q}}, \dots, a_r^{\mathbb{Q}}, b_1^{\mathbb{Q}}, \dots, b_l^{\mathbb{Q}}$ be multiplicatively divisible subgroups associated with these elements. Suppose that $b_1, \dots b_l$ are multiplicatively independent over $\langle a_1, \dots, a_r \rangle \cdot L_1^\times \cdot \dots \cdot L_n^\times$.*

Then there is an $m \in \mathbb{N}$ such that $b_1^{\frac{1}{m}}, \dots, b_l^{\frac{1}{m}}$ determine the isomorphism type of $b_1^{\mathbb{Q}}, \dots, b_l^{\mathbb{Q}}$ over the field $\hat{P} = P(L_1, \dots, L_n, \mu, a_1^{\mathbb{Q}}, \dots, a_r^{\mathbb{Q}})$.

Remark 1.4 μ is needed in the definition of $\hat{P}$ only in case $n = 0$.

Theorem 2 has the following corollary.

Corollary 1.5 *Let $W^{\frac{1}{n}}$ be the locus of (the minimal algebraic variety containing) $\left\langle b_1^{\frac{1}{n}}, \dots, b_l^{\frac{1}{n}} \right\rangle$ over $\hat{P}$. Then for some m, for each d, the algebraic set*

$$\{(x_1, \dots, x_\ell) : (x_1^d, \dots, x_\ell^d) \in W^{1/m}\}$$

is irreducible over $\hat{P}$ and is precisely $W^{1/dm}$.

The proof of Theorem 1 in case F is countable follows directly from Theorem 2, with $n = 0$, by the standard back-and-forth construction of the isomorphism. For this we only need to notice that if a partial linear isomorphism $\sigma_H : H \to H'$ maps a $\mathbb{Q}$-subspace generated by linearly independent $h_1, \dots, h_r \in H$ to the subspace generated by linearly independent $h_1', \dots, h_r' \in H'$, with $a_1 = \mathrm{ex}(h_1), \dots, a_r = \mathrm{ex}(h_r)$ and $\sigma_F : a_i \to a_i' = \mathrm{ex}(h_i')$ a partial field isomorphism, then we can extend σ to any new h. Indeed, let $\mathrm{ex}(h) = b$, and choose m as in Theorem 2 and $b^{\frac{1}{m}} = \mathrm{ex}(\frac{h}{m})$. Extend the partial field isomorphism σ_F to $b^{\frac{1}{m}}$, then define $b'^{\frac{1}{m}} = \sigma_F(b^{\frac{1}{m}})$ and choose $h' \in H'$ so that $b'^{\frac{1}{m}} = \mathrm{ex}(\frac{h'}{m})$. Finally, put $\sigma_H(h) = h'$.

The case of cardinality $\aleph_1$ can be done applying the case $n = 1$ of Theorem 2 by using one more standard model-theoretic trick. As we want to extend an isomorphism between two countable sequences (3), with successive fields of transcendence degree one over their predecessors, $\aleph_1$ times, we need to be able to extend $\sigma_0 = (\sigma_{H_0}, \sigma_{F_0})$ for countable H_0 and F_0 as in the previous paragraph to (H, F) with $F = \mathrm{ex}(H)$ an algebraically closed field of transcendence degree one over F_0, say

$$F = \mathrm{acl} F_0(b_0) = F_0(b_0, \dots, b_i, \dots).$$

We extend σ_0 by induction to $\sigma_i = (\sigma_{H_i}, \sigma_{F_i})$ with F_i containing $b_0, \ldots, b_{i-1}$ and H_i containing $h_0, \ldots, h_{i-1}$, such that $\mathrm{ex}(h_0) = b_0, \ldots, \mathrm{ex}(h_{i-1}) = b_{i-1}$. Since b_0 is transcendental over F_0 any choice of $b'_0 \in F'$ and $h'_0 \in H'$ with $\mathrm{ex}(h'_0) = b'_0$ will do for $\sigma_{H_1}(h_0)$ and $\sigma_{F_1}(b_0)$.

For step $i > 1$ let L be the algebraically closed subfield of F_0 of finite transcendence degree of the form $F_0 \cap \mathrm{acl}(b_0, \ldots, b_i)$. Then, since F_0 and $\mathrm{acl}(b_0, \ldots, b_i)$ are linearly disjoint over L (see [L], Ch.VIII) any field automorphism of $L(b_0^{\mathbb{Q}}, \ldots, b_i^{\mathbb{Q}})$ over L can be extended to a field automorphism of $F_0(b_0^{\mathbb{Q}}, \ldots, b_i^{\mathbb{Q}})$ over F_0. In particular, if the isomorphism type of $b_0^{\mathbb{Q}}, \ldots, b_i^{\mathbb{Q}}$ over L is determined by $b_0^{\frac{1}{m}}, \ldots, b_i^{\frac{1}{m}}$ then the same is true over F_0. Since such an m is given by the case $n = 1$ of Theorem 2, we can proceed as above extending the isomorphism.

Surprisingly, this does not easily generalise to arbitrary cardinalities. So, the passage from the countable to the general case goes via a direct application of the main result of [Z2], a special case of Shelah's *excellency* theory [Sh], which gives very general conditions for an isomorphism between uncountable structures to exist.

It would be useful to remark that the linear disjointness argument used above corresponds to the general notion of *splitting*, a part of the theory of excellency.

It is highly desirable in view of the discussion of other pseudo-analytic structures in [Z1]:

- to generalise Theorem 2 to fields of arbitrary characteristics;
- to prove a version of Theorem 1 for the sequences of the form

$$0 \longrightarrow \ker \xrightarrow{i} H \xrightarrow{\mathrm{ex}} A(F) \longrightarrow 0, \tag{5}$$

where $A(F)$ is the group of F-points of an abelian variety A of dimension d with the field of definition $F_0 \subseteq F$, F an algebraically closed field, H an abelian torsion free group, $\ker$ an abelian group of rank $2d$, and the isomorphism σ on $A(F)$ being induced by an isomorphism of the field F fixing F_0.

2 Proof of the main theorem

Notice first that Definition 1.3 is equivalent to the following.

$b_1^{\frac{1}{m}} \in b_1^{\mathbb{Q}}, \dots, b_l^{\frac{1}{m}} \in b_l^{\mathbb{Q}}$ *determine the isomorphism type of* $b_1^{\mathbb{Q}} \cdot \cdots \cdot b_l^{\mathbb{Q}}$ *over* F *iff, given subgroups of* $\mathbb{C}^\times$ *the form* $c_1^{\mathbb{Q}} \cdot \cdots \cdot c_l^{\mathbb{Q}}$ *and a field isomorphism* ϕ_m *over* F *such that* $\phi_m(b_i^{\frac{1}{m}}) = c_i^{\frac{1}{m}}$, *we can for any* $d \in \mathbb{N}$ *extend* ϕ_m *to a field isomorphism*

$$\phi_{dm} : F(b_1^{\frac{1}{dm}}, \dots, b_l^{\frac{1}{dm}}) \to F(c_1^{\frac{1}{dm}}, \dots, c_l^{\frac{1}{dm}})$$

taking $b_i^{\frac{1}{dm}}$ *to* $c_i^{\frac{1}{dm}}$.

Indeed we may then define

$$\phi_\infty = \bigcup_{d \in \mathbb{N}} \phi_{dm}.$$

We prove Theorem 2 through the following series of lemmas. Without loss of generality we assume that $L_j \cap P$ contains a transcendence basis of L_j for each $j = 1, \dots, n$, that is L_j is algebraic over its subfield $L_j \cap P$.

Lemma 2.1 *The multiplicative group of the field* P *is isomorphic to a direct product* $A \cdot C$ *of a free abelian group* A *and the group* $C = P^\times \cap \mu$.

The multiplicative group of the field $P(L)$, *for* L *an algebraically closed field, is isomorphic to a direct product* $A \cdot C$ *of a free abelian group* A *and the group* $C = L^\times$.

Proof First let P be a finite (algebraic) extension of $\mathbb{Q}$. We use here Dirichlet's theory of divisors (fractional ideals) and units. Let U be the group of units of the ring of integers of P. The quotient-group $P^\times/U$ is a subgroup of the group of divisors, which is a free abelian group generated by prime ideals (see [He], Ch.7). Hence $P^\times/U$ is free too. By Dirichlet's Unit Theorem ([He], Ch.28), $U = C \cdot U'$ where C is the torsion subgroup of U and U' a finitely generated free abelian group. Hence $P^\times/C$ is free. It follows that $P^\times = A \cdot C$ for some free A.

The multiplicative group of $P(L)$, for P a finitely generated extension of $\mathbb{Q}$, is the multiplicative group of a field which is of finite transcendence degree over the algebraically closed field L. Such a field can be viewed as the field of rational functions of an algebraic variety over L. According to the normalization theorem ([L2], V,4), we can assume the variety normal and projective. On a normal variety the concept of Weil divisor ([H], II.6) makes sense, and the divisors of functions (the principal divisors) form a subgroup of the free abelian group of all Weil divisors on the variety. So $P(L)^\times/U$, where U is the subgroup of functions with trivial divisors, which is the group $L^\times$ of constant functions, is isomorphic to a subgroup A of a free abelian group, and thus is free itself.

In the case that P is a finitely generated extension of $\mathbb{Q}$ we can view P as the function field of an algebraic variety over some finite extension of $\mathbb{Q}$. We can again assume the variety normal over the algebraic closure of $\mathbb{Q}$, by the normalization theorem. The normalization procedure uses only finitely many coefficients, so rather than going to the algebraic closure of $\mathbb{Q}$, some sufficiently large finite extension will do. So let P_1 be the function field of the variety over this sufficiently large finite extension K of $\mathbb{Q}$. As above the group of principal Weil divisors $P_1^\times/K^\times$, is a free abelian group, say A'. But $K^\times$, the multiplicative group of a finite extension of $\mathbb{Q}$, is isomorphic to $A'' \cdot C$, with A'' free, by the above. We thus have $P_1^\times = A' \cdot A'' \cdot C$, with $A = A' \cdot A''$ free and the products direct. Then $P^\times$, being a subgroup of this, also has such a form. $\square$

Recall that a subgroup B of an abelian group is called **pure** if whenever the equation $x^n = b$ for $b \in B$ and $n \geq 1$ has a solution in A, it has a solution in B.

Definition 2.2 A tuple $\{a_1, \ldots, a_k\}$ of elements of $P^\times$ will be called **simple in** P if $\{a_1, \ldots, a_k\}$ is multiplicatively independent and the image of the subgroup $\langle a_1, \ldots, a_k \rangle$ in the quotient-group $P^\times/(P \cap \mu)$ is pure.

Remark 2.3 In case $P = \mathbb{Q}$ any tuple of distinct primes is simple.

Lemma 2.4 *Let $\{a_1, \ldots, a_r\}$ be a multiplicatively independent tuple in P and $C = P \cap \mu$. Then the following conditions are equivalent:*

(i) $\{a_1, \ldots, a_r\}$ can be extended to a basis of a free subgroup A such that $A \cdot C = P^\times$.

(ii) $\langle a_1, \ldots, a_r \rangle$ is a direct summand of $P^\times$.

(iii) the image of $\{a_1, \ldots, a_r\}$ in the quotient-group $P^\times/C$ can be extended to a basis of the free abelian group $P^\times/C$.

(iv) $\{a_1, \ldots, a_r\}$ is simple.

Proof Let $P^\times = A \cdot C$ with A a free abelian subgroup of $P^\times$. This induces the projection $\mathrm{pr} : P^\times \to A$ with kernel C.

(ii) $\Rightarrow$ (i). Suppose $P^\times = \langle a_1, \dots, a_r \rangle \cdot B$ (direct product). Now, pr is a monomorphism on $\langle a_1, \dots, a_r \rangle$ and $\mathrm{pr}(A) = A$ is a direct product of $\langle \mathrm{pr}(a_1), \dots, \mathrm{pr}(a_r) \rangle$ and $\mathrm{pr}(B)$. Choose now a subset $S \subseteq \mathrm{pr}(B)$ freely generating $\mathrm{pr}(B)$ and $T \subseteq \mathrm{pr}^{-1}(S)$ such that $\mathrm{pr}(T) = S$ and $\mathrm{pr}^{-1}(s) \cap T$ consists of one element for any $s \in S$. Then T generates a free subgroup $\langle T \rangle$ such that $\langle T \rangle \cdot C = B$ and so T completes $\{a_1, \dots, a_r\}$ to a set of free generators.

(i) $\Rightarrow$ (iii) by definition, and (iii) $\Rightarrow$ (iv) is obvious.

Also if (iii) holds, let U be a basis of $P^\times / C$ extending the image of $\{a_1, \dots, a_r\}$ and $T \subseteq P^\times$ a set of representatives of elements of U, containing $\{a_1, \dots, a_r\}$. It is easy to see that T generates a free group complementary to C. This proves that (iii) $\Rightarrow$ (i).

Suppose that (iv) holds. Let H be the image of $\langle a_1, \dots, a_r \rangle$ in $P^\times / C$ and let U be as above. Then $H \leq \langle u_1, \dots, u_n \rangle$ for some free generators $u_1, \dots, u_n \in U$. By Corollary 28.3 in [F], under the assumptions that H is a pure subgroup of a finitely generated abelian group, it is a direct summand of the group. I.e.

$$\langle u_1, \dots, u_n \rangle = H \cdot B$$

for some subgroup B of $\langle u_1, \dots, u_n \rangle$. Since the latter is free, B is free as well. So, we may assume that $H = \langle u_1, \dots, u_r \rangle$ and $B = \langle u_{r+1}, \dots, u_n \rangle$. Thus (iv) $\Rightarrow$ (iii).

It is obvious that (i) $\Rightarrow$ (ii). $\Box$

Lemma 2.5 *Let* $\{a_1, \dots, a_r, a_{r+1}\}$ *be simple in* $P_{r+1} = P(a_1, \dots, a_{r+1})$. *Then* $a_1, \dots, a_r$ *is simple in* $P_r = P(a_1, \dots, a_r)$.

Proof Indeed, if, for $b \in \langle a_1, \dots, a_r \rangle$, the equation $x^n = b$ has a solution in $P(a_1, \dots, a_r)$, it has one in $P(a_1, \dots, a_r, a_{r+1})$, and hence it has a solution in the free group $\langle a_1, \dots, a_r, a_{r+1} \rangle$. It follows, on projecting to $\langle a_1, \dots, a_r \rangle$, that the equation has a solution in $\langle a_1, \dots, a_r \rangle$.$\Box$

Definition 2.6 Given a number $k > 1$, a non-zero $a \in P$ is said to be k-simple if $a \notin \mu$ and for any $b \in P$, $\epsilon \in \mu$ and integer d

$$a^d = b^k \cdot \epsilon \text{ implies } k | d.$$

Remark 2.7 Obviously, every simple $a \in P$ is k-simple. On the other hand, e.g. in $\mathbb{Q}$, 5^2 is 3-simple but not 2-simple.

Lemma 2.8 *Let $a \in P$ and $k > 1$, an integer. Then the following three conditions are equivalent*

(i) a is k-simple;

(ii) given a divisor $m > 1$ of k there is no $\alpha \in P$ and root of unity ϵ such that $a = \alpha^m \epsilon$;

(iii) given a divisor $m > 1$ of k the image of a in the quotient-group $P^\times/C$ ($C = P \cap \mu$) has no roots of order m.

Proof (i) $\Leftrightarrow$ (iii) since the group $P^\times/C$ is torsion-free.

(i) $\Rightarrow$ (ii) is obvious. To prove the converse suppose the negation of (i) holds, i.e. $a^d = b^k\epsilon$ for some $b \in P$, $\epsilon \in C$. Assume that d is minimal for all choices of b, ϵ and k and let $s = (k, d)$ and $m = k/s$. Then by minimality $s = 1$ and $1 = ku + dv$ for some integers u and v. Thus

$$a = a^{dv}a^{ku} = b^{kv}a^{ku}\epsilon' = (a^u b^v)^k\epsilon'$$

for some $\epsilon' \in C$. Hence, letting $\alpha = (a^u b^v)$ we get the negation of (ii). $\Box$

From now on let q be a prime number.

Lemma 2.9 *Let ϵ be a root of unity of order q. Suppose $a \in P$ is q-simple in P. Then a is q-simple in $P(\epsilon)$.*

Proof Suppose

$$a = \alpha^q\zeta$$

for some $\alpha, \zeta \in P(\epsilon)$ and $\zeta^M = 1$ for some integer M. Then

$$a^M = \alpha^{qM}.$$

The orbit of α under the Galois group $(P(\epsilon) : P)$ consists of $d = \deg(\alpha/P) \leq (P(\epsilon) : P) \leq q-1$ elements of the form $\alpha\xi$, for $\xi \in \mu_{qM}$. Hence the norm has the form

$$N_P(\alpha) = \alpha^d\xi' = b \in P$$

for some $\xi' \in \mu_{qM}$. Thus $a^d = b^q\xi''$ for some $\xi'' \in \mu_{qM}$. This contradicts q-simplicity. $\Box$

Lemma 2.10 *If a is q-simple in P and $\imath = \sqrt{-1} \in P$ then a is q-simple in $P(\zeta)$, where ζ is a root of unity of order q^t, $t \geq 1$.*

Proof By Lemma 2.9 the statement holds for $t = 1$. Suppose it holds for $t = t_0$ and fails for $t = t_0 + 1$. We may then assume that ζ_0, a primitive root of unity of order q^{t_0}, is in P.

Let ζ be a primitive root of unity of order q^t, $\zeta^q = \zeta_0$, and we may assume that $\zeta \notin P$. By [L], VI,Thm 6.2, the polynomial $x^q - \zeta_0$ is irreducible over P, thus

$$|P(\zeta) : P| = q$$

By assumptions and Lemma 2.8 there is $\alpha \in P(\zeta) \setminus P$ and $\epsilon \in \mu$ such that

$$a = \alpha^q \epsilon. \tag{6}$$

Of course, $\epsilon \in P(\zeta)$.

If $(m, q) = 1$ then a^m is q-simple in P as well, so by raising the equation (6) to power m we may w.l.o.g. assume that the multiplicative order of ϵ is of the form q^r for some non-negative integer $r \leq t_0 + 1$. Hence $\epsilon^q \in P$ and

$$\alpha^{q^2} = a^q \in P.$$

Then, by [L], VI,Thm 6.2 again, $\deg(\alpha/P)$ divides $|P(\zeta) : P|$, hence $\deg(\alpha/P) = q$.

Let $\sigma \neq 1$ be an element of the Galois group $(P(\zeta) : P)$.

Since $\alpha \in P(\zeta)$, there are unique $c_0, \dots c_{q-1} \in P$ such that

$$\alpha = \sum_{0 \leq i < q-1} c_i \zeta^i.$$

and, since $\zeta^q = \zeta_0 \in P$,

$$\sigma(\zeta) = \zeta \cdot \epsilon,$$

for some ϵ, a primitive root of unity of order q, which is in P.

Thus,

$$\sigma(\zeta^i) = \zeta^i \epsilon^i$$

and

$$\sigma(\alpha) = \sum_{0 \leq i < q} c_i \epsilon^i \zeta^i.$$

On the other hand

$$\sigma(\alpha) = \alpha\xi, \quad \text{for some } \xi, \quad \xi^{q^2} = 1. \tag{7}$$

If $\sigma(\xi) = \xi$ then $\xi \in P$ and

$$\sigma(\alpha) = \sum_{0 \le i < q} c_i \xi \zeta^i.$$

Hence for all i

$$c_i \epsilon^i = c_i \xi,$$

which means $c_i = 0$ for all but one $i = m$,

$$\alpha = c_m \zeta^m$$

and

$$a = b^q \zeta^{mq}, \text{ where } b \in P,$$

which contradicts the assumption of q-simplicity, and we are done in this case.

So we assume that ξ is a root of order q^2, not in P.

By definitions $\sigma(\xi) = \xi^l$ for some $1 < l < q^2$ such that $(l, q) = 1$.

By induction on k the condition (7) extends to

$$\sigma^k(\alpha) = \xi^{1+l+\cdots+l^{k-1}}.$$

Since σ is of order q we have $\sigma^q(\alpha) = \alpha$ and thus

$$1 + l + \cdots + l^{q-1} \equiv 0 (mod\ q^2). \tag{8}$$

But

$$1 + l + \cdots + l^{q-1} = \frac{l^q - 1}{l - 1}$$

and hence

$$l^q \equiv 1 (mod\ q) \quad \text{and so} \quad l \equiv 1 (mod\ q).$$

It follows $l = q + 1$ and $l^k \equiv kq + 1 (mod\ q^2)$, for $k = 0, \ldots, q - 1$, thus

$$1 + l + \cdots + l^{q-1} \equiv q(1 + \frac{q-1}{2})(mod\ q^2).$$

Comparing with (8) we see that only $q = 2$ is possible. But in this case $\xi = \imath \in P$, the contradiction. $\square$

From now on we assume that $\imath \in P$.

Let P_0 be a maximal purely transcendental extension of $\mathbb{Q}$ in P, and let φ denote the Euler function.

Lemma 2.11 *If a is q-simple in P but not q^w-simple in $P(\xi)$ for some root of unity ξ and positive integer w, then $\varphi(q^w)$ divides $|P : P_0|$.*

Proof First consider the case when ξ is a primitive root of unity of order s, some $s \in \mathbb{N}$ with $(s, q) = 1$.

Suppose

$$\alpha^{q^w} = a\epsilon^m, \tag{9}$$

ϵ is a primitive root of unity of order q^w, $\alpha \in P(\xi)$, and $m \in \mathbb{N}$.

By [L], VI,Thm 6.2, polynomial $x^{q^w} - a$ is irreducible over P, thus

$$\deg(\alpha/P) = q^w$$

and for any ϵ, a root of unity of order q^w, there is σ in the Galois group of the normal extension $(P(\xi) : P)$ such that

$$\sigma(\alpha) = \alpha\epsilon.$$

It follows that a primitive root of unity of order q^w, denote it ϵ, belongs to $P(\xi)$.

Now we compare the degrees of some Galois extensions:

$$|P(\epsilon\xi) : P_0| = |P(\epsilon\xi) : P| \cdot |P : P_0|,$$

$$|P(\epsilon\xi) : P_0| = |P(\epsilon\xi) : P_0(\epsilon\xi)| \cdot |P_0(\epsilon\xi) : P_0|.$$

But $|P(\epsilon\xi) : P_0(\epsilon\xi)| = d_1$ is a divisor of $|P : P_0|$ ([L], VI, Thm 1.12) and

$$|P_0(\epsilon\xi) : P_0| = \varphi(q^w) \cdot \varphi(s).$$

Hence

$$|P(\epsilon\xi) : P| = |P : P_0|^{-1} \cdot d_1 \cdot \varphi(q^w) \cdot \varphi(s).$$

Analogously we get

$$|P(\xi) : P| = |P : P_0|^{-1} \cdot d_2 \cdot \varphi(s)$$

for some divisor d_2 of $|P : P_0|$.

So, under the condition $\epsilon \in P(\xi)$, we obtain

$$d_1 \cdot \varphi(q^w) = d_2,$$

which implies that $\varphi(q^w)$ divides $|P : P_0|$.

In the general case assume $\alpha \in P(\epsilon\xi)$ and (9) holds. Let $\beta \in P(\xi)$ satisfy the equation

$$\beta^{q^u} = a\epsilon^n$$

for the maximal possible integer u and some integer n. Then $\varphi(q^u)$ divides $|P : P_0|$ by what was proved above, and β is q-simple in $P(\xi)$. By Lemma 2.10 β is q-simple in $P(\xi, \epsilon)$, which implies $u \geq w$ and $\varphi(q^w)$ divides $|P : P_0|$. $\square$

Corollary 2.12 *If a is simple in P then there is a positive integer N such that $a^{\frac{1}{N}} \in P(\xi)$, for some root of unity ξ, and $a^{\frac{1}{N}}$ is simple in $P(\xi')$ for any root of unity ξ' such that $P(\xi) \subseteq P(\xi')$.*

Proof Let N be the maximal positive integer with the property that $\varphi(N)$ divides $|P : P_0|$ and $a^{\frac{1}{N}} \in P(\xi)$ for some ξ.

Such an integer exists because the first part of the condition is satisfied by at most finitely many integers.

If there is M and ξ' such that

$$(a^{\frac{1}{N}})^{\frac{1}{M}} \in P(\xi'),$$

then, by Lemma 2.11, $\varphi(N \cdot M)$ divides $|P : P_0|$. By the choice of N, $N \cdot M \leq N$, hence $M = 1$.$\square$

Lemma 2.13 *Let A be a free abelian subgroup of rank r of a torsion free group A'. Suppose there is a natural number N such that $a^N \in A$ for any $a \in A'$. Then A' is a free abelian group of rank r.*

Proof By assumptions the group A'/A is periodic, of a bounded exponent. Proposition 18.3 of [F] states under these conditions that A' is a direct product of cyclic groups, in our case all the cyclic groups are infinite, i.e. the group is free. The rank of A' must be r too, because any $b_1, \dots, b_s \in A'$ with $s > r$ must be multiplicatively dependent, since $b_1^N, \dots b_s^N$ are dependent elements in A. $\Box$

Lemma 2.14 *Let $a_1, \dots, a_r \in P$ be multiplicatively independent and let A be the subgroup of $P^\times$ generated by $a_1, \dots, a_r$. Let $\bar{P} = P(\mu)$, the extension of P by all the roots of unity, and let $A^\#$ be the pure hull of A in $\bar{P}^\times$, i.e. the group of those elements $b \in \bar{P}^\times$ such that $b^n \in A$ for some n.*

Then $A' = A^\# / A^\# \cap \mu$ is a free abelian group of rank r.

Proof By assumptions A can be naturally identified with $A/A \cap \mu$ and is a free abelian group of rank r. By Corollary 2.12, given $b \in A^\#$, the least positive integer N such that $b^N \in A \cdot \mu$ is bounded by $|P : P_0|$. Thus A'/A is periodic of bounded exponent. It follows that A and A' satisfy the assumptions of Lemma 2.13. Thus A' is free abelian of rank r.$\Box$

From now on let $\bar{P} = P(\mu)$, the extension of P by all the roots of unity.

The next result follows from Lemma 2.14.

Corollary 2.15 *For any multiplicatively independent tuple $\{a_1, \dots, a_r\} \subseteq P^\times$ there is a tuple*

$$\{a_1', \dots, a_r'\} \subseteq \bar{P}^\times \cap a_1^{\mathbb{Q}} \cdot \dots \cdot a_r^{\mathbb{Q}}$$

such that $\{a_1', \dots, a_r'\}$ is simple in the field $\bar{P}$.

The above Corollary is sufficient for the proof of the main theorem (Theorem 2) in case $n = 0$. The following statements 2.16 - 2.19 investigate the case $n \neq 0$.

Lemma 2.16 *Given a field K containing all roots of unity, suppose $\{a_1, \dots, a_r\} \subseteq K^\times$ is simple in K and $b_1, \dots, b_r$ in an extension of K generate a subgroup $\langle b_1, \dots, b_r \rangle$ containing $\langle a_1, \dots, a_r \rangle$.*

Then $\{b_1, \dots, b_r\}$ is simple in $K(b_1, \dots, b_r)$.

Proof It follows from the assumptions that $(\langle b_1,\dots,b_r\rangle : \langle a_1,\dots,a_r\rangle)$ is finite, hence there is an m such that $b_1^m,\dots,b_r^m \in \langle a_1,\dots,a_r\rangle$. Also $K\cap \langle b_1,\dots,b_r\rangle = \langle a_1,\dots,a_r\rangle$ and, for every integer M, $K^M \cap \langle b_1,\dots,b_r\rangle = \left\langle a_1^M,\dots,a_r^M\right\rangle$, where K^M is the M-powers subgroup of $K^\times$.

Claim. Suppose $b\in\langle b_1,\dots,b_r\rangle$ has a root $\beta\in K(b_1,\dots,b_r)$ of order l. Then b has a root of order l in $\langle b_1,\dots,b_r\rangle$.

Indeed, there is a positive integer $M\le ml$ such that $\beta^M\in K$ and $b_i^M\in K$, for all i. By [L], VI, Theorem 8.1 (Kummer's Theory)

$$(K(\beta,b_1,\dots,b_r):K) = (\left\langle \beta^M, b_1^M,\dots,b_r^M\right\rangle \cdot K^M : K^M),$$

and the right-hand-side by the above is equal to $(\left\langle \beta^M, b_1^M,\dots,b_r^M\right\rangle : \left\langle a_1^M,\dots,a_r^M\right\rangle)$.

On the other hand $K(\beta,b_1,\dots,b_r) = K(b_1,\dots,b_r)$ and

$$(K(b_1,\dots,b_r):K) = (\left\langle b_1^M,\dots,b_r^M\right\rangle\cdot K^M : K^M) = (\left\langle b_1^M,\dots,b_r^M\right\rangle : \left\langle a_1^M,\dots,a_r^M\right\rangle).$$

It follows that

$$(\left\langle \beta^M, b_1^M,\dots,b_r^M\right\rangle : \left\langle a_1^M,\dots,a_r^M\right\rangle) = (\left\langle b_1^M,\dots,b_r^M\right\rangle : \left\langle a_1^M,\dots,a_r^M\right\rangle).$$

Hence $\beta\cdot\epsilon\in\langle b_1,\dots,b_r\rangle$, for $\epsilon^M=1$. Since $\beta^l\cdot\epsilon^l = b\cdot\epsilon^l$, we have $\epsilon^l\in\langle b_1,\dots,b_r\rangle$, so $\epsilon^l=1$ and $\beta\cdot\epsilon$ is the requred root of b of order l. This proves the claim.

The Lemma follows directly from the claim. □

Lemma 2.17 *Suppose $\{a_1,\dots,a_r\}\subseteq P^\times$ is multiplicatively independent over $L_1^\times\cdot\dots\cdot L_n^\times$. Then there are $a_1',\dots,a_r'\in P(L_1,\dots,L_n)$ which are free generators of the group $a_1^{\mathbb{Q}}\cdot\dots\cdot a_r^{\mathbb{Q}}\cap P(a_1',\dots,a_r',L_i)$ for every $i\in\{1,\dots,n\}$.*

Proof Suppose, for $0\le k<n$, we found $a_1',\dots,a_r'\subseteq P(L_1,\dots,L_n)$ which are free generators of the group $a_1^{\mathbb{Q}}\cdot\dots\cdot a_r^{\mathbb{Q}}\cap P(a_1',\dots,a_r',L_j)$ for every $j\in\{1,\dots,k\}$. Since $a_1^{\mathbb{Q}}\cdot\dots\cdot a_r^{\mathbb{Q}} = a_1'^{\mathbb{Q}}\cdot\dots\cdot a_r'^{\mathbb{Q}}$, we may assume $a_i'=a_i\in P$, $i=1,\dots,r$. By Lemma 2.1, $a_1^{\mathbb{Q}}\cdot\dots\cdot a_r^{\mathbb{Q}}\cap P(a_1,\dots,a_r,L_{k+1})$ is free, so let $a_1',\dots,a_r'$ be free generators of it.

By Lemma 2.16 $\{a_1',\dots,a_r'\}$ is simple in $P(a_1',\dots,a_r',L_j)$ for $j\le k$ and the same holds, by the choice, for $j=k+1$. The lemma follows now by induction on k. □

The following 'amalgamation property' is crucial for the proof of the main theorem.

Proposition 2.18 *Given $\{a_1, \ldots, a_r\} \subseteq \bar{P}$ multiplicatively independent over $\bar{P} \cap L_1^\times \cdot \cdots \cdot L_n^\times$, there is $\{a'_1, \ldots, a'_r\} \subseteq \bar{P}(L_1, \ldots, L_n)$ simple in $\bar{P}(L_1, \ldots, L_n)$, such that $a_1, \ldots, a_r \in \langle a'_1, \ldots, a'_r \rangle$.*

Proof By Lemma 2.17 we can find $\{a'_1, \ldots, a'_r\}$ simple in $\bar{P}(a'_1, \ldots, a'_r, L_j)$ for each $j \in \{1, \ldots, n\}$. We may assume $a'_i = a_i \in \bar{P}$, for all i, and that $\{a_1, \ldots, a_r\}$ is simple in $P(L_i)$ for each $i \in \{1, \ldots, n\}$.

Since $L_1, \ldots, L_n$ are countable fields, we can represent

$$P(L_1, \ldots, L_n) = \bar{P}(L_1, \ldots, L_n) = \bigcup_{i \in \mathbb{N}} P^{(i)},$$

where $P^{(0)} = \bar{P}$ and $P^{(i+1)} = P^{(i)}(\lambda_i)$ for some $\lambda_i \in L_1 \cup \cdots \cup L_n$. Moreover, letting $L_j^{(i)} = L_j \cap P^{(i)}$, we may assume that either $L_j^{(i+1)} = L_j^{(i)}$, or $L_j^{(i+1)} = L_j^{(i)}(\lambda_i)$ and $(L_j^{(i+1)} : L_j^{(i)})$ is a normal extension with simple Galois group, that is with no intermediate normal extensions. In the second case, since $\lambda_i \in \mathrm{acl}(L_j^{(i)})$ and $L_j^{(i)}$ is algebraically closed in $P^{(i)}$, by Lemma 4.10 of [L], VIII, we have linear disjointness and an isomorphism of Galois groups $(L_j^{(i+1)} : L_j^{(i)})$ and $(P^{(i+1)} : P^{(i)})$.

To prove the proposition it is enough to check that if an element $a \in \bar{P}$ is simple in $P^{(i)}(L_j)$, for all j, it is simple in $P^{(i+1)}(L_j)$ for all j.

Suppose towards a contradiction that a is not simple in $P^{(i+1)}(L_j)$. That is there is a root α of a of some order $m > 1$ in $P^{(i+1)}(L_j)$. Choosing m minimal, we have that α generates a cyclic (hence normal) extension of $P^{(i)}$ of order m. Since $(P^{(i+1)} : P^{(i)})$ has no intermediate normal extensions, it must be cyclic generated by α, so, for some $l \leq n$, $\lambda_i \in L_l$ and $(L_l^{(i+1)} : L_l^{(i)})$ is cyclic of order m as well. Hence, we may assume $\lambda_i = \lambda$ is a root of order m of an element $b \in L_l^{(i)}$. Consider the unique representation

$$\lambda = p_0 + p_1\alpha + \cdots + p_{m-1}\alpha^{m-1},$$

with $p_0, \ldots, p_{m-1} \in P^{(i)}$.

Let σ be an automorphism of $(P^{(i+1)} : P^{(i)})$ which sends α to $\alpha\xi$, for ξ a primitive root of 1 of order m. Then

$$\sigma(\lambda) = p_0 + p_1\alpha\xi + \cdots + p_{m-1}\alpha^{m-1}\xi^{m-1}$$

and at the same time

$$\sigma(\lambda) = \lambda\xi^k = p_0\xi^k + p_1\alpha\xi^k + \cdots + p_{m-1}\alpha^{m-1}\xi^k$$

for some k.

Comparing the two expressions we get that all but one p_i is zero and $\lambda = p_k\alpha^k$, in fact k coprime with m. Thus $\alpha = p_k^{-1}\lambda^{m'}$ for some m' and so $\alpha \in P^{(i)} \cdot L_l$, proving that a is not simple in $P^{(i)}(L_l)$. The contradiction.$\square$

Lemma 2.19 *Let $R \subseteq \mathbb{C}$ be a field containing a primitive root of unity of order n, let $\{a_1, \ldots, a_r\} \subseteq R$ be simple in R and let $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$, be such that $\alpha_i^n = a_i$ for $1 \le i \le r$. Then the Galois group $(R(\alpha_1, \ldots, \alpha_r) : R)$ is isomorphic to $\mathbb{Z}_n^r$, the rth Cartesian power of the cyclic group of order n. That is, any other collection $(\alpha_1', \ldots, \alpha_r')$ of roots of $(a_1, \ldots, a_r)$ of order n is conjugated to $(\alpha_1, \ldots, \alpha_r)$ by an automorphism over R.*

Proof Let $R^{\times n}$ be the n-powers subgroup of $R^\times$. Since $\{a_1, \ldots, a_r\}$ is simple, we have the group isomomorphism

$$\langle a_1, \ldots, a_r\rangle \,/\, \langle a_1, \ldots, a_r\rangle \cap R^{\times n} \cong \mathbb{Z}_n^r.$$

On the other hand, by Kummer's theory (Theorem 8.1 of [L], Ch.VI)

$$(R(\alpha_1, \ldots, \alpha_r) : R) \cong \langle a_1, \ldots, a_r\rangle \,/\, \langle a_1, \ldots, a_r\rangle \cap R^{\times n}.$$

$\square$

Proof of the Theorem 2.

Let $C = \mu \cdot L_1^\times \cdot \cdots \cdot L_n$. We may assume that $\{a_1, \ldots, a_r\}$ is multiplicatively independent over C. Let

$$A = \mu \cdot \langle a_1, \ldots, a_r, b_1, \ldots, b_l\rangle \cap P(b_1, \ldots, b_l).$$

Since $A/A \cap C$ is a free group of rank $r+l$, by Proposition 2.18 there is $\{a'_1, \ldots, a'_r, b'_1, \ldots, b'_l\} \subseteq a_1^{\mathbb{Q}} \cdot \cdots \cdot a_r^{\mathbb{Q}} \cdot b_1^{\mathbb{Q}} \cdot \cdots \cdot b_l^{\mathbb{Q}}$ simple in $\bar{P}(a'_1, \ldots, a'_r, b'_1, \ldots, b'_l)$. We preserve this property with any choice of free generators of the group $\langle a'_1, \ldots, a'_r, b'_1, \ldots, b'_l \rangle$, in particular we may assume

$$\{a'_1, \ldots, a'_r\} \subseteq a_1^{\mathbb{Q}} \cdot \cdots \cdot a_r^{\mathbb{Q}}.$$

By Lemma 2.19 $(b'_1, \ldots, b'_l)$ determines the isomorphism type of $({b'_1}^{\mathbb{Q}}, \ldots, {b'_l}^{\mathbb{Q}})$ over
$\bar{P}({a'_1}^{\mathbb{Q}}, \ldots, {a'_r}^{\mathbb{Q}}, L_1, \ldots, L_n)$.

Obviously, $b'_1, \ldots, b'_l$ are in the subgroup generated by $b_1^{\frac{1}{m}}, \ldots, b_l^{\frac{1}{m}}$, μ and $a_1^{\mathbb{Q}} \cdot \cdots \cdot a_r^{\mathbb{Q}}$, for some integer m, and thus $(b_1^{\frac{1}{m}}, \ldots, b_l^{\frac{1}{m}})$ determines the isomorphism type of $({b_1}^{\mathbb{Q}}, \ldots, {b_l}^{\mathbb{Q}})$ over $\bar{P}({a'_1}^{\mathbb{Q}}, \ldots, {a'_r}^{\mathbb{Q}}, L_1, \ldots, L_n)$. $\square$

3 Theorem 1

As has been mentioned in the first section of the paper, the proof of Theorem 1 from Theorem 2 is based on a rather general model theoretic construction.

First, let us represent a sequence of the form (3) as a one sorted structure $\mathbf{H}$. The domain of $\mathbf{H}$ will be H, the only basic operation is $+$, the group operation, and the basic relations on H are: a binary equivalence relation E, with interpretation

$$E(h_1, h_2) \text{ iff } \mathrm{ex}(h_1) = \mathrm{ex}(h_2),$$

and a ternary relation S with the interpretation

$$S(h_1, h_2, h_3) \text{ iff } \mathrm{ex}(h_1) + \mathrm{ex}(h_2) = \mathrm{ex}(h_3).$$

So, each equivalence class hE with a representative $h \in H$ corresponds to a non-zero element $\mathrm{ex}(h)$ of F. The multiplication in F corresponds to the group operation $+$ on H, and we also have S to speak about addition in F. In particular, the equivalence class corresponding to the unit 1 of F, which is just the kernel of ex, is definable in $\mathbf{H}$.

The appropriate formal logical language to consider the structures is $L_{\omega_1,\omega}$, the language with countable conjunctions and finite number of variables studied in [K].

Lemma 3.1 *There is an $L_{\omega_1,\omega}$-sentence Σ such that any model $\mathbf{H}$ of Σ represents a sequence (3) with some algebraically closed field F and conversely, any $\mathbf{H}$ corresponding to a sequence of the form (3) is a model of Σ.*

Proof The sentence Σ should say that:

(i) $(H, +)$ is a divisible torsion free abelian group;

(ii) H/E, with regards to the operations coming from $+$ and S, can be identified as $F \setminus \{0\}$ for some algebraically closed field F of characteristic zero;

and

(iii) $$\exists x_0 \in \ker\ , \forall x \in \ker \quad (\bigvee_{z \in \mathbb{Z}} x = z x_0),$$

where $\ker$ stands for the kernel of the homomorphism ex. □

We also can define a closure operator cl on the domain H of a model $\mathbf{H}$ of Σ by setting for $X \subseteq H$

$$\mathrm{cl}(X) = \mathrm{ex}^{-1}(\mathrm{acl}(\mathrm{ex}(X))),$$

where acl is the algebraic closure operator in the sense of the field structure on $F = \mathrm{ex}(H) \cup \{0\}$.

Lemma 3.2 *For any model $\mathbf{H}$ of Σ and $X \subseteq H$:*

(i) $\mathrm{cl}(X)$ *is countable if X is finite;*

(ii)
$$\mathrm{cl}(Y) = \bigcup_{X \subseteq Y,\ \ X \textit{ finite}} \mathrm{cl}(X);$$

(iii) $X \to \mathrm{cl}(X)$ is a monotone idempotent operator;

(iv) cl *satisfies the exchange principle:*

$$z \in \mathrm{cl}(X \cup \{y\}) \setminus \mathrm{cl}(X) \Rightarrow y \in \mathrm{cl}(X \cup \{z\});$$

(v) $\mathrm{cl}(X)$ *with the induced relations is a model of Σ.*

Proof Follows immediately from the properties of acl.$\Box$

Definition 3.3 Let $\mathbf{H}, \mathbf{H}'$ be models of Σ and let G be a common subset. A (partial) mapping $\varphi : \mathbf{H} \to \mathbf{H}'$ is called a G-**monomorphism**, if it preserves quantifier-free formulas with parameters from G, that is for any such formula $\Phi(v_1, \ldots, v_n)$ and elements $h_1, \ldots, h_n \in H$

$$\mathbf{H} \models \Phi(h_1, \ldots, h_n) \text{ iff } \mathbf{H}' \models \Phi(\varphi(h_1), \ldots, \varphi(h_n)).$$

Remark 3.4 The G-monomorphism type of a linearly independent tuple $(x_1, \ldots, x_l)$ in H is determined by the algebraic type of $(\mathrm{ex}(q_1 x_1), \ldots, \mathrm{ex}(q_l x_l))$ for all rational numbers $q_1, \ldots, q_l$. In other words, setting $y_i^q = \mathrm{ex}(q x_i)$, we want to know the field theoretic isomorphism type of $(y_1^{\mathbb{Q}}, \ldots, y_l^{\mathbb{Q}})$.

Lemma 3.5 *Models of* Σ *are* ω-**homogeneous over a model**. *That is, given* $\mathbf{H}$ *and* $\mathbf{H}'$ *models of* Σ *and a common submodel* $G \subseteq \mathbf{H}$, $G \subseteq \mathbf{H}'$ *the following holds:*

(i) Suppose $X_0 \subseteq H$, $X_0' \subseteq H'$ *are finite subsets of models* $\mathbf{H}$ *and* $\mathbf{H}'$ *correspondingly, and there is a* G*-monomorphism* $\varphi_0 : X_0 \to X_0'$. *Suppose also* $X \subseteq H$ *and* $X' \subseteq H'$ *are* cl*-independent over* $X_0 \cup G$ *and* $X_0' \cup G$, *correspondingly. Then any bijection* $\varphi : X_0 X \to X_0' X'$ *extending* φ_0 *is a* G*-monomorphism.*

(ii) If a partial mapping $\varphi : \mathbf{H} \to \mathbf{H}'$ *is a* G*-monomorphism,* Dom $\varphi = X$, *with* X *finite, then for any* $y \in \mathbf{H}$ *there is a* G*-monomorphism* φ' *extending* φ *with* Dom $\varphi' = X \cup \{y\}$.

(iii) if $\varphi : X \cup \{y\} \to X' \cup \{y'\}$ *is a* G*-monomorphism, then*

$$y \in \mathrm{cl}(X) \text{ iff } y' \in \mathrm{cl}(X').$$

Proof (i) is obvious if one remembers that the cl-independence of X over X_0 means that $\mathrm{ex}(X)$ is algebraically independent over $\mathrm{ex}(X_0)$ in the field F.

(ii) follows directly from Theorem 2 (see also Corollary 1.5), when one takes $\mathrm{ex}(G) = L = L_1 = \cdots = L_n$, algebraically closed subfield of F, X to be $\{a_1, \ldots, a_r\}$ and $y = b_1$, $l = 1$.

(iii) is obvious.$\Box$

Lemma 3.6 *Given countable submodels $G_1, \dots, G_n \subseteq \mathbf{H}$ and $h_1, \dots, h_l \in$ $\mathrm{cl}(G_1 \cup \dots \cup G_n)$, the locus of $(h_1, \dots, h_l)$ over $G_1 \cup \dots \cup G_n$ is finitely determined, i.e. there is a finite subset $A \subseteq G_1 \cup \dots \cup G_n$, such that any $\varphi : \{h_1, \dots, h_l\} \to \mathbf{H}$ which is an A-monomorphism is also a $(G_1 \cup \dots \cup G_n)$-monomorphism.*

Proof Let $L_i = \mathrm{ex}(G_i)$, $i = 1, \dots, n$, $b_j^q = \mathrm{ex}(qh_j)$, for $j = 1, \dots, l$, $q \in \mathbb{Q}$. We may assume that $h_1, \dots, h_l$ are $\mathbb{Q}$-linearly independent over the vector subspace $G_1 + \dots + G_n$, which implies the multiplicative independence of $b_1, \dots, b_l$ over $L_1^\times \cdot \dots \cdot L_n^\times$.

Apply Theorem 2 with the above notation assuming $r = 0$. Since the type of $(h_1, \dots, h_l)$ over $G_1 \cup \dots \cup G_n$ is determined by the field-theoretic type of $(b_1^{\frac{1}{m}}, \dots, b_l^{\frac{1}{m}})$, for some m, only finitely many parameters from $G_1 \cup \dots \cup G_n$ are needed to fix the type. □

In [Z2] we call an $L_{\omega_1,\omega}$-definable class **quasi-minimal excellent** if it satisfies the statements of Lemmas 3.2-3.6.

Proof of Theorem 1. The main Theorem 2 of [Z2] immediately implies that, if the class of models of a Σ is quasi-minimal excellent, then, given an uncountable cardinality, a model of Σ of this cardinality is unique, up to isomorphism. This completes the proof of Theorem 1. □

Remark 3.7 The unique model of Σ of cardinality ω_1 is not homogeneous. So we can not apply Keisler's theory of categoricity and stability (see [K]) to this sentence. In fact, Σ provides a natural example for negative answers to Open Questions in [K], pp. 100-101. Earlier an artificial counterexample to the questions was published in [M].

Indeed, consider a transcendental $a \in F^\times$ and $h \in H$ such that $\mathrm{ex}(h) = a$. Let for every $n \in \mathbb{N}$

$$a_n = \mathrm{ex}(\frac{1}{n}h) + 1 \text{ and } \mathrm{ex}(h_n) = a_n.$$

Let $X = \{h_n : n \in \mathbb{N}\}$, $X_i = \{h_n : n \leq i\}$ and

$$p = \mathrm{tp}(h/X).$$

Notice that $a, a_1, \ldots, a_n$ are multiplicatively independent over $\mathbb{Q}^\times$, since a is transcendental. Then any subtype $p_i = \mathrm{tp}(h/X_i)$ is, by Theorem 2, atomic and actually defined by the minimal polynomial for $a^{\frac{1}{m}} = \mathrm{ex}(\frac{h}{m})$, for some m, over $\mathbb{Q}(\mathrm{ex}(span_{\mathbb{Q}} X_i))$ which is also an $L_{\omega_1,\omega}$-complete formula. This also implies that any two roots of $a^{\frac{1}{m}}$ of any order $k > 0$ are indiscernible over X_i. But they are discernible over X_{mk}, being elements of $\mathbb{Q}(\mathrm{ex}(span_{\mathbb{Q}} X_{mk}))$. Hence p_i is not complete over X, hence p is not atomic. It follows that, given any countable fragment L' of $L_{\omega_1,\omega}$, there is a countable model $\mathbf{H}_0$ of Σ containing an L'-equivalent copy X' of X and omitting the type, p', which corresponds to p. By ω_1-categoricity $\mathbf{H}_0$ is embeddable in $\mathbf{H}$, and p' is omitted in $\mathbf{H}$ as well, since any realisation h' of p' satisfies $\mathrm{ex}(h') \in \mathrm{acl}(\mathrm{ex}(X)) \subseteq \mathbf{H}_0$ and hence $h' \in \mathbf{H}_0$.

The last observation contrasts with the case of a cover with *compact kernel*, that is the case when the kernel of ex is assumed to be $\widehat{\mathbb{Z}}$, the closure of $\mathbb{Z}$ in the profinite topology, corresponding to a sequence of the form

$$0 \to \widehat{\mathbb{Z}} \to^{i_H} H \to^{\mathrm{ex}_H} F^\times \to 1. \tag{10}$$

Proposition 3.8 *If in an exact sequence of groups*

$$0 \to \widehat{\mathbb{Z}} \to^{i_G} G \to^{\mathrm{ex}_G} F^\times \to 1 \tag{11}$$

G is a divisible torsion-free abelian group, then there is a group isomorphism

$$\sigma : H \to G$$

such that $\mathrm{ex}_H = \mathrm{ex}_G \circ \sigma$.

Proof Let $h \in H$ and $g \in G$ satisfy $\mathrm{ex}_H(h) = \mathrm{ex}_G(g) = a$ for some $a \in F^\times$.

Claim. There is a unique $\nu \in \ker \mathrm{ex}_G$ such that

$$\mathrm{ex}_H(\frac{h}{n}) = \mathrm{ex}_G(\frac{g+\nu}{n}) \text{ for all } n \geq 1.$$

Indeed, let

$b_n = \mathrm{ex}_H(\dfrac{h}{n})\mathrm{ex}_G(\dfrac{g}{n})^{-1}$ and let $\beta_n \in G$ such that $\mathrm{ex}_G(\dfrac{\beta_n}{n}) = b_n,$ for each $n \geq 1$.

Obviously,

$$\beta_n \in \ker \mathrm{ex}_G \text{ and } \frac{\beta_{nm} - \beta_n}{n} \in \ker \mathrm{ex}_G.$$

We may identify the additive group $\ker \mathrm{ex}_G$ with the group $\widehat{\mathbb{Z}}$ and look for ν as a solution of the system of equations mod n for $z \in \widehat{\mathbb{Z}}$

$$z \equiv \beta_n \mod n\widehat{\mathbb{Z}}, \quad n \in \mathbb{N}. \tag{12}$$

The system is finitely satisfiable, for to find a solution for $n_1, \ldots, n_k$, it is enough to solve one equation

$$z \equiv \beta_m \mod m\widehat{\mathbb{Z}}$$

for $m = n_1 \cdot \cdots \cdot n_k$.

The defining property of $\widehat{\mathbb{Z}}$ is that any finitely satisfiable system of the form (12) has a unique solution (see [F], Ch.VII). This proves the claim.

By the Claim, to every $h \in H$ we can assign a unique g with the property

$$\mathrm{ex}_H(\frac{h}{n}) = \mathrm{ex}_G(\frac{g}{n}) \text{ for all } n \geq 1.$$

Denoting this g by $\sigma(h)$ we have $\mathrm{ex}_H = \mathrm{ex}_G \circ \sigma$ and also, by uniqueness, $\sigma(h_1 + h_2) = \sigma(h_1) + \sigma(h_2)$. $\square$

References

[F] L.Fuchs, **Infinite Abelian Groups**, vol.1, Academic Press, New York and London, 1970

[H] R.Hartshorne, **Algebraic Geometry**, Springer-Verlag, Berlin, Heidelberg, New York, 1977

[He] H.Hasse, **Number Theory**,Grundlehren der mathematischen Wissenschafte; 229, Springer-Verlag, Berlin, 1980

[L] S.Lang, **Algebra**, Addison-Wesley Publishing Co., Reading, Mass., 1965

[L2] S.Lang, **Introduction to Algebraic Geometry**, Interscience, 1958

[M] L.Marcus, *A prime minimal model with an infinite set of indiscernibles*, Isr.J.Math., 1972, 180-183

[K] H.J. Keisler, **Model theory for infinitary logic. Logic with countable conjunctions and finite quantifiers**. Studies in Logic and the Foundations of Mathematics, Vol. 62. North-Holland Publishing Co., Amsterdam-London, 1971

[Sh] S.Shelah, *Classification theory for non-elementary classes.I: the number of uncountable models of* $\psi \in L_{\omega,\omega}(Q)$., Parts A,B, Isr.J.Math., v.46, (1983), 212-240, 241-273.

[Z1] B.Zilber, *Analytic and pseudo-analytic structures*, to appear in **Proceedings of European Logic Colloquium. Paris 2000**

[Z2] ——, *A categoricity theorem for quasi-minimal excellent classes,* to appear in **Proceedings of the workshop on nonelementary theories,** Ann-Arbor, 2002.

[Z3] ——, *Pseudo-exponentiation on algebraically closed fields of characteristic zero,* to appear in Annals of Pure and Applied Logic

[Z4] ——, *Model theory, geometry and arithmetic of semi-Abelian varieties,* to appear in **Proceeding of Model Theory conference**, Ravello, 2001.