QUASI-BOOLEAN GROUPS

AMBRUS PÁL AND GEREON QUICK

Abstract. We give several equivalent characterisations of the maximal pro-2 quotients of real projective groups. In particular, for pro-2 real projective groups we provide a presentation in terms of generators and relations, and a purely cohomological characterisation. As a consequence we explicitly reconstruct such groups from their mod 2 cohomology rings.

1. Introduction

Let G be a profinite group. An *embedding problem for G* is a solid diagram:

$$\begin{array}{ccc} & & G \\ & {\scriptstyle\widetilde{\phi}}\swarrow & \downarrow{\scriptstyle\phi} \\ B & \xrightarrow[\alpha]{} & A \end{array}$$

where A and B are finite groups, the solid arrows are continuous homomorphisms and α is surjective. A *solution* of an embedding problem is a continuous homomorphism $\widetilde{\phi}\colon G \to B$ which makes the diagram commutative. We say that the embedding problem above is *real* if for every involution $t \in G$ with $\phi(t) \neq 1$ there is an involution $b \in B$ with $\alpha(b) = \phi(t)$, i.e., if involutions do not provide an obstruction for the existence of a solution.

Definition 1.1. Following Haran and Jarden [5] we say that a profinite group G is *real projective* if G has an open subgroup without 2-torsion, and if every real embedding problem for G has a solution.

By the work of Haran–Jarden [5], real projective groups play an important role in Galois theory as they are exactly the Galois groups of pseudo real closed fields, which, by the work of Haran [4], can also be characterised as the fields with virtual cohomological dimension at most one (see [8, Section 2]). For a real projective group G, we show in [8, Theorem 1.3] that the differential graded algebra $C^\bullet(G, \mathbb{F}_2)$ of continuous cochains is formal, i.e., $C^\bullet(G, \mathbb{F}_2)$ is quasi-isomorphic as differential graded algebras to its cohomology algebra. Roughly speaking, this means that the cohomology algebra of a real projective group already contains all the information of the differential graded algebra $C^\bullet(G, \mathbb{F}_2)$. The purpose of the present paper is to show that, in fact, the maximal pro-2 quotient of a real projective group can be reconstructed entirely from the mod 2 cohomology ring. In particular, we show that pro-2 real projective groups can be reconstructed entirely from their mod 2 cohomology ring. In order to further describe our results we recall the following terminology from [8].

2020 *Mathematics Subject Classification.* 20E18, 12F10, 20J06.

Definition 1.2. We call an $\mathbb{F}_2$-algebra $B^\bullet = \bigoplus_{i\geqslant 0} B^i$ a *graded Boolean algebra* if $B^0 = \mathbb{F}_2$ and there is a Boolean ring B (see Section 2) such that, for every $i \geqslant 1$, we have $B^i = B$ and multiplication in $B^\bullet$ is induced by B. We call an $\mathbb{F}_2$-algebra $D^\bullet = \bigoplus_{i\geqslant 0} D^i$ a *dual algebra* if $D^0 = \mathbb{F}_2$, and $D^i = 0$ for $i \geqslant 2$. The *connected sum* $D^\bullet \sqcap B^\bullet$ is the graded $\mathbb{F}_2$-algebra with $(D^\bullet \sqcap B^\bullet)^0 = \mathbb{F}_2$, $(D^\bullet \sqcap B^\bullet)^i = D^i \oplus B^i$ for $i \geqslant 1$ and multiplication $D^1 B^i$ and $B^i D^1$ is set to be zero for all $i \geqslant 1$.

In [8], we deduce from Scheiderer's work in [10] that the mod 2 cohomology algebra of a real projective group is a connected sum of a dual and a Boolean graded algebra. Hence, in the terminology of Definition 1.5 below, the maximal pro-2 quotient of a real projective group is a cohomologically quasi-Boolean group. The anonymous referee of [8] suggested that the latter property may even characterise pro-2 real projective groups completely. The purpose of the present paper is to prove this conjecture. In fact, we prove the stronger fact that every pro-2 real projective group has an explicit description as a certain free pro-2 product with explicit generators and relations provided by the cohomology ring (see Theorem 1.8 below). This result significantly strengthens a consequence of the main result of [8]. According to the latter, for a real projective group G, the differential graded $\mathbb{F}_2$-algebra $C^\bullet(G, \mathbb{F}_2)$ and its cohomology $H^\bullet(G, \mathbb{F}_2)$ is Koszul. Hence, by a theorem of Positselski, the $\mathbb{F}_2$-linear co-algebra of the maximal pro-2 quotient H of G can be reconstructed explicitly from the cohomology ring $H^\bullet(H, \mathbb{F}_2) \cong H^\bullet(G, \mathbb{F}_2)$ using the bar construction (see Example 6.3 of [9]). Here we reconstruct the group itself via an even more transparent recipe.

We now describe our main results in more detail. To do so we need the following constructions and terminology:

Definition 1.3. The *free product* $G_1 *_p G_2$ of two pro-p groups G_1, G_2 is the following: let $G_1 * G_2$ be the discrete free product of G_1 and G_2 and let $\mathcal{N}$ be the family of normal subgroups N of G such that $(G_1 * G_2)/N$ is a finite p-group and $N \cap G_1, N \cap G_2$ are open subgroups of G_1, G_2 respectively. Then

$$G_1 *_p G_2 = \varprojlim_{N\in\mathcal{N}} (G_1 * G_2)/N.$$

Definition 1.4. Next we are going to define, following [2], *free pro-2 products of order two groups over topological spaces*. For every topological space X let $\circledast_X \mathbb{Z}/2\mathbb{Z}$ denote the group which is freely generated by the elements of X, subject to the relation that these elements are involutions, and let $\mathcal{N}$ be the family of normal subgroups N of $\circledast_X \mathbb{Z}/2\mathbb{Z}$ such that $\circledast_X \mathbb{Z}/2\mathbb{Z}/N$ is a finite 2-group and the composition of the natural inclusion $\iota\colon X \to \circledast_X \mathbb{Z}/2\mathbb{Z}$ and the quotient homomorphism $\circledast_X \mathbb{Z}/2\mathbb{Z} \to \circledast_X \mathbb{Z}/2\mathbb{Z}/N$ is continuous with respect to the discrete topology on $\circledast_X \mathbb{Z}/2\mathbb{Z}/N$. Then we set

$$\mathbb{B}(X) = \varprojlim_{N\in\mathcal{N}} \circledast_X \mathbb{Z}/2\mathbb{Z}/N.$$

Definition 1.5. We say that a pro-2 group is a *Boolean group* if it is isomorphic to $\mathbb{B}(X)$ for some topological space X. (We will see in Proposition 6.5 below that we may assume without the loss of generality that X is profinite.) We say that a pro-2 group is a *quasi-Boolean group* if it is the free product of a free pro-2 group (in the sense of [12, 1.5 on pages 7–8]) and a Boolean group. We say that a pro-2 group is a *cohomologically Boolean group* if its mod 2 cohomology is a graded Boolean algebra. We say that a pro-2 group is a *cohomologically quasi-Boolean group* if its mod 2 cohomology is the connected sum of a dual algebra and a graded Boolean algebra.

We can now state our main results:

Theorem 1.6. *Let G be a pro-2 group. Then the following are equivalent:*

(*i*) *G is quasi-Boolean.*
(*ii*) *G is real projective.*
(*iii*) *G is the maximal pro-2 quotient of a real projective profinite group.*
(*iv*) *G is cohomologically quasi-Boolean.*

Perhaps the most interesting feature of this theorem is, compared to the results of the paper [6], that it incorporates a purely cohomological characterisation of these pro-2 groups. Our proof is a bit more involved than it might be anticipated; it uses results of Haran–Jarden in the arithmetic of fields, for example a group-theoretical characterisation of real projective groups, a theorem on the existence of sections of profinite principle G-bundles, and profinite versions of two theorems of Quillen on group cohomology. We will also show the following

Corollary 1.7. *Let G be a pro-2 group. Then the following are equivalent:*

(*i*) *G is Boolean.*
(*ii*) *G is cohomologically Boolean.*

Using our results we also demonstrate that quasi-Boolean groups can be reconstructed from their mod 2 cohomology. For every set Y, let $F(Y)$ denote the free pro-2 group as defined in [12, Section 1.5 on pages 7–8]. Let G be a quasi-Boolean group such that $H^\bullet(G, \mathbb{F}_2)$ is the connected sum of a dual algebra $D^\bullet$ and a graded Boolean algebra $B^\bullet$ associated to the Boolean ring B. Let Y be a basis of D^1 and let X be the spectrum of B.

Theorem 1.8. *The pro-2 group G is isomorphic to $F(Y) *_2 \mathbb{B}(X)$.*

Content. In Section 2 we give a modern exposition of the theory of Boolean rings, including Stone duality, using now standard tools from commutative algebra. We cover some background material on profinite spaces, including the profinite completion functor, in the Section 3. In Section 4 we prove that profinite principal G-bundles have sections, a result originally announced by Morel in [7] without proof. We prove that the class of pro-2 real projective groups and the maximal pro-2 quotients of real projective groups are the same in Section 5, the key step being a simple group-theoretical lemma. In Section 6 we show that the class of quasi-Boolean and pro-2 real projective groups are the same, heavily relying on the main results of the previous sections and several theorems of the paper [6]. Then we present profinite versions of some classical results of Quillen on the cohomology of groups, partially following the suggestion at the end of [11], and use these results to derive a local-global principle for the cohomology of cohomologically quasi-Boolean groups analogous to Scheiderer's theorem for real projective groups in Section 7. In section 8 we prove the main results using cohomological obstruction theory for central embedding problems and the local-global principle of the previous section.

Acknowledgement. This paper was written as a response to one of the questions asked by the referee to our paper [8]. We are very thankful for the anonymous referee's comments. Both authors gratefully acknowledge the partial support by the RCN Project No. 313472 *Equations in Motivic Homotopy.*

2. A primer on Boolean rings

In this section we recall and prove the results we need on Boolean rings. In particular, we deduce Stone duality in Theorem 2.10.

Definition 2.1. A ring R is called *Boolean* if $x^2 = x$ for every $x \in R$.

Examples 2.2. The field with two elements $\mathbb{F}_2$ is a Boolean ring. In fact, since $x(1-x) = 0$ for all x in a Boolean ring, $\mathbb{F}_2$ is the only Boolean integral domain. The direct product of Boolean rings is Boolean, and so, for every set X, the direct product ring:

$$\mathbb{F}_2^X = \prod_{i \in X} \mathbb{F}_2$$

is a Boolean ring. Now let X be a topological space, and let $\mathbf{B}(X)$ denote the ring of functions $f : X \to \mathbb{F}_2$ which are continuous with respect to the discrete topology on $\mathbb{F}_2$. Since the subrings of Boolean rings are Boolean, and $\mathbf{B}(X)$ is a subring of $\mathbb{F}_2^X$, we get that $\mathbf{B}(X)$ is Boolean, too.

Proposition 2.3. *In a Boolean ring R the following hold:*

- (i) *we have $2x = 0$ for every $x \in R$,*
- (ii) *every prime ideal $\mathfrak{p}$ is maximal, and $R/\mathfrak{p}$ is the field with two elements,*
- (iii) *we have $(x, y) = (x + y - xy)$ for every $x, y \in R$,*
- (iv) *every finitely generated ideal is principal.*

Proof. Since

$$2x = (2x)^2 = 4x^2 = 4x,$$

we get that $2x = 0$ by subtracting $2x$ from both sides. Now let $\mathfrak{p}$ be a prime ideal in R. Then the quotient $R/\mathfrak{p}$ is a Boolean ring. For every $x \in R/\mathfrak{p}$, we have $x(1-x) = 0$ which implies that $x = 0$ or $x = 1$ since $R/\mathfrak{p}$ is an integral domain. Claim (ii) follows. Note that

$$x(x + y - xy) = x^2 + xy - x^2y = x + xy - xy = x.$$

Hence $x, y \in (x + y - xy)$. Since $x + y - xy \in (x, y)$, claim (iii) is clear. Let $I = (x_1, x_2, \ldots, x_n)$ be an finitely generated ideal of R. Since

$$I = ((x_1, x_2, \ldots, x_{n-1}), x_n),$$

we may assume by induction on n that $I = (x, y)$ for some $x, y \in R$. The claim now follows from part (iii). □

Proposition 2.4. *The spectrum* $\mathrm{Spec}(R)$ *of a Boolean ring is compact and totally separated.*

Proof. Since the spectrum of a commutative ring with a unity is compact, the same holds for $\mathrm{Spec}(R)$, too. Recall that a topological space X is totally separated if for any two distinct points $x, y \in X$ there exist disjoint open sets $U \subset X$ containing x and $V \subset X$ containing y such that X is the union of U and V. Now let $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(R)$ be two distinct points. Since they are maximal ideals, there is an $x \in R$ such that $x \in \mathfrak{p}$ and $x \notin \mathfrak{q}$. Since $R/\mathfrak{p} = \mathbb{F}_2$ by part (ii) of Proposition 2.3, the former is equivalent to $1 - x \notin \mathfrak{p}$. As usual for every $f \in R$ let $D(f) \subseteq \mathrm{Spec}(R)$ denote the open subset

$$D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}. \tag{2.4.1}$$

Then $\mathfrak{p} \in D(1-x), \mathfrak{q} \in D(x)$, the intersection $D(x) \cap D(1-x)$ is empty by part (ii) of Proposition 2.3, while the union $D(x) \cup D(1-x)$ is $\mathrm{Spec}(R)$, since if $x, 1-x \in \mathfrak{m}$ for some $\mathfrak{m} \in \mathrm{Spec}(R)$ then $1 \in \mathfrak{m}$ which is a contradiction. □

Notation 2.5. Let R be a Boolean ring. Then for every $a \in R$ the corresponding section of the structure sheaf of $\mathrm{Spec}(R)$ is a continuous function

$$\sigma(a) \colon \mathrm{Spec}(R) \to \mathbb{F}_2$$

by part (ii) of Proposition 2.3, and the furnished map

$$\sigma \colon R \to \mathbf{B}(\mathrm{Spec}(R))$$

is a ring homomorphism.

Theorem 2.6. *For every Boolean ring R, the map $\sigma \colon R \to \mathbf{B}(\mathrm{Spec}(R))$ is an isomorphism.*

Proof. For every $x \in R$ we have $x^n = x$ by induction, so if x is nilpotent, then it is zero. Therefore the nilradical of R is zero, so by Krull's theorem σ is injective. So we only need to show that σ is surjective. Let $f \colon \mathrm{Spec}(R) \to \mathbb{F}_2$ be a continuous function. Then the set

$$D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f(x) = 1\}$$

is a closed subset, so it is compact. But it is also open, so it can be covered by open subsets of the form $D(a)$, where $a \in R$ by the definition of the topology of the spectrum of rings. Since $D(f)$ is compact, it can be covered by finitely many such, so

$$D(f) = D(a_1) \cup D(a_2) \cup \cdots \cup D(a_n)$$

for some $a_1, a_2, \ldots, a_n \in R$. By part (iv) of Proposition 2.3, there is an $a \in R$ such that $(a) = (a_1, \ldots, a_n)$. Then

$$\begin{aligned} D(a) &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid a \notin \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid (a) \nsubseteq \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid (a_1, \ldots, a_n) \nsubseteq \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid a_i \notin \mathfrak{p} \text{ for some } i\} \\ &= D(a_1) \cup D(a_2) \cup \cdots \cup D(a_n), \end{aligned}$$

so $D(f) = D(a)$. Since f and a take values in $\mathbb{F}_2$, we get that $f = a$. □

Notation 2.7. Let X be a topological space. Then for every $p \in X$ the set

$$\beta(p) = \{x \in \mathbf{B}(X) \mid x(p) = 0\}$$

is the kernel of a surjective ring homomorphism $\mathbf{B}(X) \to \mathbb{F}_2$, so it is a maximal ideal in $\mathbf{B}(X)$. Consequently, we have an induced map

$$\beta \colon X \to \mathrm{Spec}(\mathbf{B}(X)).$$

For every $x \in \mathbf{B}(X)$ the pre-image

$$\beta^{-1}(D(x)) = \{p \in X \mid x(p) = 1\}$$

is open. Since the sets $\{D(x) \mid x \in \mathbf{B}(X)\}$ form a sub-basis of $\mathrm{Spec}(\mathbf{B}(X))$, we get that $\beta\colon X \to \mathrm{Spec}(\mathbf{B}(X))$ is continuous.

Theorem 2.8. *When X is compact and totally separated, then β is a homeomorphism.*

Proof. Since X is compact and $\mathrm{Spec}(\mathbf{B}(X))$ is Hausdorff, it will be sufficient to show that β is a bijection. Let $x, y \in X$ be two distinct points. Since X is totally separated, so there exist disjoint open sets $U \subset X$ containing x and $V \subset X$ containing y such that X is the union of U and V. Let $f\colon X \to \mathbb{F}_2$ be the characteristic function of U. It is in $\mathcal{B}(X)$ since the complement of U is open, too. Clearly $f \in \beta(y)$, but $f \notin \beta(x)$, so β is injective.

For every ideal $I \lhd \mathbf{B}(X)$ let $Z(I) \subseteq X$ denote the closed subset

$$Z(I) = \{x \in X \mid f(x) = 0 \quad (\forall f \in I)\}.$$

We claim that for every proper ideal $I \lhd \mathbf{B}(X)$ the set $Z(I)$ is non-empty. First consider the case when $I = (f)$ for some $f \in \mathbf{B}(X)$. Then

$$Z(I) = \{x \in X \mid f(x) = 0\},$$

so if this set is empty, then f is the identically one function, and hence $I = (1) = \mathcal{B}(X)$ is not proper, a contradiction. Next consider the case when I is finitely generated; then it is principal by part (iv) of Proposition 2.3, so $Z(I)$ is non-empty by the above. Finally, consider the general case. Then $Z(I)$ is the intersection of sets of the form $Z(J)$ where J is a finitely generated ideal of I. Since the latter collection of sets is closed under finite intersections, and each member is non-empty by the above, we get $Z(I)$ is also non-empty, since X is compact.

Now let $\mathfrak{m} \lhd \mathbf{B}(X)$ be a maximal ideal. By the above there is an $x \in Z(\mathfrak{m})$. Clearly $\beta(x) \supseteq \mathfrak{m}$, but $\mathfrak{m}$ is maximal, and hence $\beta(x) = \mathfrak{m}$. Therefore β is surjective, too. □

Notation 2.9. Let **BO** denote the category of Boolean rings where morphisms are ring homomorphisms, and let **CTS** denote the category of compact, totally separated topological spaces where morphisms are continuous maps. There are two contravariant functors

$$\mathbf{B}\colon \mathbf{CTS} \to \mathbf{BO}, \quad X \mapsto \mathbf{B}(X),$$

which is well-defined as we saw in Examples 2.2, and

$$\mathbf{S}\colon \mathbf{BO} \to \mathbf{CTS}, \quad R \mapsto \mathrm{Spec}(R),$$

which is well-defined by Proposition 2.4.

Theorem 2.10 (Stone duality)**.** *The functors* **B** *and* **S** *are a pair of dualities of categories.*

Proof. By Theorem 2.6, the map σ is a natural isomorphism between the identity of **BO** and $\mathbf{B} \circ \mathbf{S}$. By Theorem 2.8, the map β is a natural isomorphism between the identity of **CTS** and $\mathbf{S} \circ \mathbf{B}$. □

Corollary 2.11. *Let R be a finite Boolean ring. Then the following are equivalent:*

(i) *R is finite.*
(ii) *R is finitely generated as an $\mathbb{F}_2$-algebra.*
(iii) *R is Noetherian.*
(iv) *R is Artinian.*

(*v*) $\mathrm{Spec}(R)$ *is finite.*
(*vi*) $R \cong \mathbb{F}_2^X$ *for a finite set* X.

In this case $R \cong \mathbb{F}_2^{\mathrm{Spec}(R)}$.

Proof. Every Boolean ring is an $\mathbb{F}_2$-algebra, so if R is finite, then it is finitely generated as an $\mathbb{F}_2$-algebra, and hence (i) implies (ii). Every finitely generated $\mathbb{F}_2$-algebra is Noetherian by Hilbert's basis theorem, so (ii) implies (iii). Every Boolean ring is zero dimensional by part (ii) of Proposition 2.3, so if it is Noetherian, it is Artinian by a standard theorem in commutative algebra (see [1, Theorem 8.5 on page 90]). Therefore (iii) implies (iv). Every Artinian ring is a finite direct product of Artinian local rings (see [1, Theorem 8.7 on page 90]), so its spectrum is finite. Therefore (iv) implies (v). Now let R be a Boolean ring whose spectrum is finite. Since $\mathrm{Spec}(R)$ is totally separated by Proposition 2.4, it is discrete, and hence $R \cong \mathbb{F}_2^{\mathrm{Spec}(R)}$ by Theorem 2.6. In particular, (v) implies (vi). If $R \cong \mathbb{F}_2^X$ for a finite set X, then R is clearly finite, so (vi) implies (i). □

Notation 2.12. Let **FBO** denote the category of finite Boolean rings where morphisms are ring homomorphisms, and let **FTS** denote the category of finite, totally separated topological spaces where morphisms are continuous maps. Note that the latter is the same as the category of finite, discrete topological spaces. There are two restrictions of functors

$$\mathbf{B}|_{\mathbf{FTS}} \colon \mathbf{FTS} \to \mathbf{FBO}, \quad X \mapsto \mathbf{B}(X)$$

and

$$\mathbf{S}|_{\mathbf{FBO}} \colon \mathbf{FBO} \to \mathbf{FTS}, \quad R \mapsto \mathrm{Spec}(R),$$

where the latter is well-defined by Corollary 2.4.

Theorem 2.13. *The functors* $\mathbf{B}|_{\mathbf{FTS}}$ *and* $\mathbf{S}|_{\mathbf{FTS}}$ *are a pair of dualities of categories.*

Proof. The restrictions of the natural isomorphisms β and σ onto **FTS** and **FBO** are the respective required natural isomorphisms. □

Definition 2.14. Let R be a Boolean ring. We say that two elements $x, y \in R$ are orthogonal if $xy = 0$. We say that an element $a \in R$ is an *atom* if it is non-zero and cannot be written as the sum of two non-zero orthogonal elements of R. The *support* of an element $x \in R$ is the subset $D(f) \subseteq \mathrm{Spec}(X)$ introduced in (2.4.1).

Lemma 2.15. *Let* R *be a Boolean ring. Then the following holds:*

(*i*) *Two elements* $x, y \in R$ *are orthogonal if and only if the intersection of their support is empty.*
(*ii*) *A non-zero element* $a \in R$ *is an atom if and only if its support cannot be written as the disjoint union of two non-empty open and closed subsets.*
(*iii*) *Every pair of different atoms of* R *are orthogonal to each other.*

Proof. Note that the support of the product xy is the intersection of the supports of x and y. Since the support of an element of R is empty if and only if it is zero by Theorem 2.6, claim (i) follows. If $a = x + y$ such that x, y are orthogonal and both non-zero, then the support of a is the disjoint union of the supports of x and y by part (i). On the other hand if the support of a is the disjoint union of the non-empty open and closed subsets X and Y, there are elements $x, y \in R$ whose support is X, Y, respectively, by Theorem 2.6. By part (i) these are orthogonal, non-zero and their sum has the same support as a. So $a = x + z$, and hence claim (ii) is true.

Let $a, b \in R$ be two atoms whose product is non-zero. Then $a = ab + a(1-b)$ and $aba(1-b) = a^2(b-b^2) = 0$, so $a(1-b) = 0$ by the definition of atoms. We get that $a = ab$. The same reasoning for b show that $b = ab$. Therefore $a = b$, and hence (iii) holds. □

Corollary 2.16. *Let R be a finite Boolean ring. Then the atoms of R form a natural basis of R whose elements are orthogonal to each other. Moreover, every orthogonal basis consists of atoms.*

Proof. By Corollary 2.11, the topological space $\mathrm{Spec}(R)$ is finite, discrete, and $R \cong \mathbb{F}_2^{\mathrm{Spec}(R)}$. Therefore, an element of R is an atom if and only if its support is a point by claim (ii) of Lemma 2.15. These clearly form a basis of R and they are orthogonal by claim (iii) of Lemma 2.15.

Now let $e_1, e_2, \ldots, e_n$ be an orthogonal basis. We need to show that each e_i is an atom. We may assume without the loss of generality that $i = 1$. Let x be characteristic function of an element of the support of e_1. Then x is an atom. The support of e_1 and e_i, $i \neq 1$, is disjoint since they are orthogonal. Hence x and e_i are orthogonal, so $xe_i = 0$. Now write x as a linear combination $\sum_{j \in J} e_j$ of the e_i. Since $0 = xe_i = \sum_{j \in J} e_j e_i$ only if i is not in J, the above argument implies $x = 0$ or $x = e_1$. The former is not possible, since x is not zero. Hence we get $x = e_1$, and e_1 is an atom. □

3. All about profinite spaces

In this section we collect the results we need about profinite topological spaces.

Definition 3.1. We say that a topological space is *profinite* if it is the projective limit of discrete, finite topological spaces. Recall that a topological space X is totally disconnected if for every point $x, y \in X$ the connected component of x in X is x itself.

Every totally separated topological space is totally disconnected, but the converse is not true: there are totally disconnected topological spaces which are not Hausdorff, while every totally separated topological space is Hausdorff. However, the following is true:

Theorem 3.2. *Let X be a topological space. Then the following are equivalent:*

(i) X is profinite.
(ii) X is homeomorphic to a closed subspace of a product of discrete, finite topological spaces.
(iii) X is compact, totally disconnected and Hausdorff.
(iv) X is compact and totally separated.

Proof. First assume that X satisfies (i). Let $\mathcal{C}$ be a small category of discrete, finite topological spaces whose projective limit is X. Let $\mathrm{Ob}(\mathcal{C})$ denote the set of its objects, and let $\mathrm{Hom}_{\mathcal{C}}(A, B)$ denote the set of its morphisms for every $A, B \in \mathrm{Ob}(\mathcal{C})$. By definition, X is homeomorphic to the closed subspace

$$\left\{ \prod_{C \in \mathrm{Ob}(\mathcal{C})} x_C \in \prod_{C \in \mathrm{Ob}(\mathcal{C})} C \mid f(x_A) = x_B \quad (\forall A, B \in \mathrm{Ob}(\mathcal{C}),\ \forall f \in \mathrm{Hom}_{\mathcal{C}}(A, B)) \right\}$$

of $\prod_{C \in \mathrm{Ob}(\mathcal{C})} C$, so X satisfies (ii).

Next assume that X satisfies (ii). Since finite topological spaces are compact, their direct product is also compact by Tychonoff's theorem. Since X is a closed subspace of a compact space, it is compact, too. Moreover, the direct product of totally disconnected and Hausdorff topological spaces is totally disconnected and Hausdorff topological spaces. Since discrete topological spaces are totally disconnected and Hausdorff, and every subspace of a totally disconnected and Hausdorff topological space is also totally disconnected and Hausdorff, we get that the same holds for X, too. Therefore X satisfies (iii).

Now we show that (iii) implies (iv). We will start with the following standard

Lemma 3.3. *Assume that X is a Hausdorff compact topological space. Let $C, D \subset X$ be two disjoint closed subsets. Then there exist disjoint open sets $U \subset X$ containing C and $V \subset X$ containing D.*

Proof. First assume that C consists of a single point $x \in X$. Because X is Hausdorff for every $y \in D$, there are disjoint open sets $U_y \subset X$ containing x and $V_y \subset X$ containing y. Because D is closed, it is compact, so there is a finite subset $y_1, \ldots, y_n \in D$ such that $V_{y_1}, \ldots, V_{y_n}$ cover D. Then $U = U_{y_1} \cap \cdots \cap U_{y_n}$ and $V = V_{y_1} \cup \cdots \cup V_{y_n}$ are disjoint open subsets containing x and D, respectively.

Now consider the general case. By the above for every $x \in C$ there are disjoint open sets $U_x \subset X$ containing x and $V_x \subset X$ containing D. Because C is closed, it is compact, so there is a finite subset $x_1, \ldots, x_n \in C$ such that $U_{x_1}, \ldots, U_{x_n}$ cover C. Then $U = U_{x_1} \cup \cdots \cup U_{x_n}$ and $V = V_{x_1} \cap \cdots \cap V_{y_n}$ are disjoint open subsets containing C and D, respectively. □

For every $x \in X$, let $Z(x)$ denote the set of all open and closed subsets of X containing x, and let Z_x denote the intersection of all elements of $Z(x)$. We need to show that if $y \in X$ is distinct from x then $y \notin Z_x$. Assume that this is not the case for some y. Then Z_x contains at least two points, so it is not connected, since X is totally disconnected. Therefore Z_x is the disjoint union of two non-empty subsets $C, D \subset Z_x$ which are closed in Z_x.

Since Z_x is the intersection of closed subsets, it is closed in X. Therefore C and D are also closed in X. Hence by Lemma 3.3 there exist disjoint open sets $U \subset X$ containing C and $V \subset X$ containing D. Let E be the complement of the union of U and V in X. It is closed, so it is compact since X is Hausdorff. Since $U \cup V$ contains Z_x, the set E is covered by the union of the complements of elements of $Z(x)$. Since E is compact, it is already covered by the union of finitely many such sets. Therefore there is a finite subset $Z_1, \ldots, Z_n \in Z(x)$ such that $Z = Z_1 \cap \cdots \cap Z_n \subseteq U \cup V$.

Note that since each Z_i is both open and closed, the same also holds for the finite intersection Z. Since each each Z_i contains x, the set Z also contains x. Both $Z \cap U$ and $Z \cap V$ are open in Z, and the latter is open, so $Z \cap U$ and $Z \cap V$ are open in X, too. The complement of Z is open, so both $Z \cap U$ and $Z \cap V$ are the complement of the union of two open sets, so they are closed, too.

One of $Z \cap U$ and $Z \cap V$ contain x, say $Z \cap U$. Then $Z \cap U \in Z(x)$ which means that $Z \cap U$ contains Z_x. But $Z \cap U \cap Z_x = Z \cap (U \cap Z_x) = Z \cap C = C$, which is a contradiction, since the complement of C in Z_x is D, and the latter is non-empty. So condition (iii) implies condition (iv).

Finally we show that (iv) implies (i). We start with the following

Notation 3.4. For every positive integer $n \in \mathbb{N}$, let $\underline{n}$ denote the set $\{1, 2, \ldots, n\}$ equipped with the discrete topology. Now let X be an arbitrary topological space, and let $\mathcal{C}(X)$ denote the small category whose objects are continuous maps $f\colon X \to \underline{n}$ for some $n \in \mathbb{N}$, and the morphisms from an object $f\colon X \to \underline{n}$ to another object $g\colon X \to \underline{m}$ is an automatically continuous map $h\colon \underline{n} \to \underline{m}$ such that $g = h \circ f$.

Definition 3.5. The profinite completion of X is the projective limit $\widehat{X}$ of the small category $\mathcal{C}(X)$. It is equipped with a continuous map $u_X\colon X \to \widehat{X}$ satisfying the following universal property:

(i) $\widehat{X}$ is profinite.
(ii) For every continuous map $f\colon X \to Y$, where Y is a discrete, finite topological space, there is a unique continuous map $\widehat{f}\colon \widehat{X} \to Y$ such that $f = \widehat{f} \circ u_X$.

This is because every discrete, finite topological space is homeomorphic to $\underline{n}$ for some $n \in \mathbb{N}$. Moreover $\widehat{X}$ is determined up to a unique homeomorphism by this universal property by the classical abstract non-sense argument.

It will be sufficient to show that u_X is a homeomorphism when X is compact and totally separated. Since X is compact and $\widehat{X}$ is Hausdorff by the above, it will be sufficient to show that u_X is a bijection. Let $x, y \in X$ be two different points. Since X is totally separated, there is a continuous function $f\colon X \to \underline{2}$ such that $f(x) \neq f(y)$ as we saw in the proof of Theorem 2.8. Then $\widehat{f}(u_X(x)) = f(x) \neq f(y) = \widehat{f}(u_X(y))$, so $u_X(x) \neq u_X(y)$. Therefore u_X is injective. In order to see that u_X is also surjective, we will need the following

Lemma 3.6. *Let X be a compact and totally separated space, and let $C_1, \ldots, C_n \subset X$ be pairwise disjoint closed subsets. Then there exist pairwise disjoint open and closed subsets $U_1, U_2, \ldots, U_n \subset X$ such that U_i contains C_i for each i, and $\cup_i U_i = X$.*

Proof. Note that it is enough to show the claim when $n = 2$ as the general case follows by induction. Indeed let $n > 2$ be such that we already know the claim for every $m < n$. Apply the $m = 2$ case to the closed subsets $D_1 = C_1$ and $D_2 = C_2 \cup \cdots \cup C_n$ to get two disjoint open and closed subsets $W_1, W_2 \subset X$ such that $D_1 \subseteq W_1$, $D_2 \subseteq W_2$, and $W_1 \cup W_2 = X$. Then apply the $m = n - 1$ to $C_2, \ldots, C_n$ inside W_2, which is possible since W_2 is closed in X, so it is compact and totally separated. Therefore there exist pairwise disjoint open and closed subsets $V_2, \ldots, V_n \subset W_2$ such that V_i contains C_i for each $i \geqslant 2$, and $\cup_i V_i = W_2$. Since each V_i is open and closed in an open and closed subset of X, it is also open and closed in W_2. Therefore $U_1 = W_1$ and $U_i = V_i$ for $i \geqslant 2$ have the required properties.

Now consider the $n = 2$ case. By Lemma 3.3 there exist disjoint open sets $V_1 \subset X$ containing C_1 and $V_2 \subset X$ containing C_2. Because X is totally separated, its open and closed sets form a subbasis for its topology, so for every $x \in C_1$ there is a closed and open subset $V_x \subset V_1$ containing x. Because C_1 is closed, it is compact, so there is a finite subset $x_1, \ldots, x_n \in C$ such that $V_{x_1}, \ldots, V_{x_n}$ cover C. Their union $U_1 = V_{x_1} \cup \cdots \cup V_{x_n}$ is the union of open and closed subsets, so it is also open and closed, and it is contained in V_1. Its complement U_2 is also open and closed and contains C_2, so U_1 and U_2 have the required properties. □

Now assume that u_X is not surjective, so there is an $x \in \widehat{X}$ such that $x \notin u_X(X)$. Since X is compact and $\widehat{X}$ is Hausdorff by the above the image $u_X(X)$ is closed in

$\widehat{X}$. So by Lemma 3.6 and since X is compact and totally separated by the above, there are disjoint open and closed subsets $U_1, U_2 \subset \widehat{X}$ such that $u_X(X) \subseteq U_1$ and $x \in U_2$. Let $f : \widehat{X} \to \mathbb{F}_2$ the characteristic function of U_1. It is continuous, since U_1 is open and closed. Let $g : \widehat{X} \to \mathbb{F}_2$ be the identically 1 function; it is also continuous, and $f \circ u_X = g \circ u_X$. However $f \neq g$, as $f(x) \neq g(x)$, which violates the universal property. This is a contradiction, so (iv) implies (i). □

Notation 3.7. Let X be again an arbitrary topological space, and let $\beta\colon X \to \mathrm{Spec}(\mathbf{B}(X))$ be the map introduced in Definition 2.7. By Proposition 2.4 the space $\mathrm{Spec}(\mathbf{B}(X))$ is compact and totally separated, so it is profinite by Theorem 3.2. So it is a projective limit of finite, discrete spaces, and hence by the universal property of the profinite completion there is a unique continuous map $\widehat{\beta}\colon \widehat{X} \to \mathrm{Spec}(\mathbf{B}(X))$ such that $\beta = \widehat{\beta} \circ u_X$.

Theorem 3.8. *The map $\widehat{\beta}\colon \widehat{X} \to \mathrm{Spec}(\mathbf{B}(X))$ is a homeomorphism.*

Proof. According to the universal property of the profinite completion it will be sufficient to show that for every continuous map $f\colon X \to Y$, where Y is a discrete, finite topological space, there is a unique continuous map $\widetilde{f}\colon \mathrm{Spec}(\mathbf{B}(X)) \to Y$ such that $f = \widetilde{f} \circ \beta$. For every continuous map $m\colon T \to Q$ of topological maps let $m^*\colon \mathbf{B}(Q) \to \mathbf{B}(T)$ denote the induced ring homomorphism. Since $\beta^*\colon \mathbf{B}(X) \to \mathbf{B}(\mathrm{Spec}(\mathbf{B}(X))$ is an isomorphism there is a unique ring homomorphism $r\colon \mathbf{B}(Y) \to \mathbf{B}(\mathrm{Spec}(\mathbf{B}(X))$ such that $\beta^* \circ r = f^*$. By Theorem 2.10 there is a unique continuous map $\widetilde{f}\colon \mathrm{Spec}(\mathbf{B}(X)) \to Y$ such that $r = \widetilde{f}^*$. Then $f^* = \beta^* \circ \widetilde{f}^* = (\widetilde{f} \circ \beta)^*$, so it will be sufficient to show that every continuous map $h\colon X \to Y$ is uniquely determined by h^*. Since for every $x \in X$ the point $h(x)$ is uniquely determined by the ideal

$$\{a \in \mathbf{B}(Y) \mid a(h(x)) = 0\} = \{a \in \mathbf{B}(Y) \mid h^*(a)(x) = 0\},$$

this claim is clear. □

4. Profinite principal G-bundles

The purpose of this section is to prove Theorem 4.7 on the existence of sections for profinite principal G-bundles.

Definition 4.1. Let A be a topological space and let $m\colon A \to B$ be a map. The *quotient topology* on B with respect to m is defined the following way: a subset $U \subseteq B$ is open if and only if $m^{-1}(U) \subseteq A$ is open. Now let A be a topological space equipped with a left action of a group H. Let $H\backslash A$ denote the quotient of A with respect to the left action of H equipped with the quotient topology.

Lemma 4.2. *The following hold:*

- (a) *Let A be a topological space and let $m\colon A \to B$ be a map. Let B be equipped with the quotient topology with respect to m. Then a map $h\colon B \to C$ of topological spaces is continuous if and only if the composition $h \circ m$ is continuous.*
- (b) *Let A be a topological space equipped with a left action of a group H. Then the quotient map $A \to H\backslash A$ is open, that is, it maps open sets to open sets.*
- (c) *Let A, B be two topological spaces both equipped with a left action of a group H. Then the product topology on $H\backslash A \times H\backslash B$ is the quotient topology with*

respect to the quotient map

$$A \times B \longrightarrow (H \times H)\backslash(A \times B) = H\backslash A \times H\backslash B.$$

Proof. We first prove (a). Since the composition of continuous functions is continuous, the map $h \circ m$ is continuous if h and m are. However, m is continuous by construction, so $h \circ m$ is continuous if h is. On the other hand, if $h \circ m$ is continuous and $U \subseteq C$ is open, then $(h \circ m)^{-1}(U) \subseteq A$ is open. Therefore $m^{-1}(h^{-1}(U)) = (h \circ m)^{-1}(U)$ is also open, so by definition $h^{-1}(U) \subseteq B$ is open. Hence h is continuous, and now claim (a) is clear.

Next we show (b). Let $U \subseteq A$ be open, and let $q\colon A \to H\backslash A$ denote the quotient map. Then $q^{-1}(q(U)) = \bigcup_{\gamma \in H} \gamma U$. Since each $\gamma \in H$ acts as a homeomorphism on A we get that γU is open. Therefore their union $q^{-1}(q(U))$ is also open, and hence $q(U)$ is open by the definition of the quotient topology. Claim (b) is now clear.

Finally, we show that (c) holds. let $q_A\colon A \to H\backslash A$ and $q_B\colon B \to H\backslash B$ be the respective quotient maps. Since the map

$$q_A \times q_B\colon A \times B \longrightarrow H\backslash A \times H\backslash B$$

is continuous with respect to the product topologies, the pre-image of any open subset is open. Therefore we only need to show that if $(q_A \times q_B)^{-1}(U) \subseteq A \times B$ for a subset $U \subseteq H\backslash A \times H\backslash B$ is open, then U is open in the product topology. In this case, $(q_A \times q_B)^{-1}(U)$ is the union of sets of the form $V \times W$, where $V \subseteq A$ and $W \subseteq B$ are open. By part (b) the set $(q_A \times q_B)(V \times W) = q_A(V) \times q_B(W)$ is open in the product topology. Since U is the union of such subsets, it is open, and (c) follows. □

Lemma 4.3. *Let X be a profinite space and let $\mathcal{U}$ be an open covering of X. Then there is a finite open covering $\mathcal{V}$ of X consisting of pairwise disjoint open and closed subsets which is subordinate to $\mathcal{U}$.*

Proof. Because X is profinite, its open and closed subsets form a subbasis of its topology. Therefore there is an open covering $\mathcal{W}$ of X consisting of open and closed subsets which is subordinate to $\mathcal{U}$. Since X is compact, we may assume without the loss of generality that $\mathcal{W}$ is finite. Let R be the subring of $\mathbf{B}(X)$ generated by the characteristic functions of the elements of $\mathcal{U}$. Since R is finitely generated, it is finite by Corollary 2.11.

Let $\mathcal{V}$ be the collection of the characteristic functions of the atoms of R. We claim that $\mathcal{V}$ satisfies the required properties. Because R is finite, the set $\mathcal{V}$ is also finite. Since different atoms of R are orthogonal by part (iii) of Lemma 2.15, their support is pair-wise disjoint by part (i) of Lemma 2.15. Let $e_1, e_2, \ldots, e_n$ be the atoms of R. Then $1 = e_1 + \ldots + e_n$, so the union of their supports is X. Also the elements of $\mathcal{V}$ are open, since they are the supports of elements of $\mathbf{B}(X)$.

Now let e be an atom of R and pick an x in its support V. Since $\mathcal{U}$ is a covering, there is a $U \in \mathcal{U}$ such that $x \in U$. The characteristic function f of U is in R, so it is the sum of different atoms of R. Therefore, ef is either 0 or e by the orthogonality of atoms. In the first case, the intersection of the supports U and V is empty, but both contain x, a contradiction. Hence $ef = e$, so U contains V, and hence $\mathcal{V}$ is subordinate to $\mathcal{U}$. □

Recall that a *section* of a continuous map of topological spaces $f\colon Y \to X$ is a continuous map $s\colon X \to Y$ such that $f \circ g$ is the identity map of X.

Proposition 4.4. *Let $f\colon Y \to X$ be a continuous map such that X is profinite and every $x \in X$ has an open neighbourhood U such that $f|_{f^{-1}(U)}\colon f^{-1}(U) \to U$ has a section. Then $f\colon Y \to X$ has a section.*

Proof. By assumption there is an open cover $\mathcal{U}$ of X such that for every $x \in X$ there is a $U \in \mathcal{U}$ such that $f|_{f^{-1}(U)}\colon f^{-1}(U) \to U$ has a section. By Lemma 4.3 there is a finite open covering $\mathcal{V}$ of X consisting of pairwise disjoint open and closed subsets which is subordinate to $\mathcal{U}$. Let $V \in \mathcal{V}$ and pick a $U \in \mathcal{U}$ which contains V. By assumption there is a section of $f|_{f^{-1}(U)}\colon f^{-1}(U) \to U$; its restriction to V is a section $s_V\colon V \to f^{-1}(V)$ of $f|_{f^{-1}(V)}\colon f^{-1}(V) \to V$. Since the elements of $\mathcal{V}$ of X form an open and pairwise disjoint covering of X, the union $\bigcup_{V\in\mathcal{V}} s_V$ of these sections is a section of $f\colon Y \to X$. □

Proposition 4.5. *Let G be a compact group, and let X be a profinite space equipped with a free continuous group action $g\colon G \times X \to X$. Then both G and $G\backslash X$ are profinite.*

Proof. For the sake of simple notation, in the sequel we will denote any left action of any group on any set by multiplication on the left, if this does not lead to confusion. Since the action g is continuous and free, for every $x \in X$ the map $\gamma \mapsto \gamma x$ from G onto the G-orbit of x is continuous and injective. As G is compact and X is Hausdorff, we get that the image of this map is closed, and the map itself is a homeomorphism from G onto its image. As G is homeomorphic to a closed subspace of a profinite space, it is also profinite by Theorem 3.2.

Let $q\colon X \to G\backslash X$ denote the quotient map. Since q is surjective, continuous, and X is compact, we get that $G\backslash X$ is compact, too. Let $x, y \in G\backslash X$ be two arbitrary different points. The pre-images $C = q^{-1}(x)$ and $D = q^{-1}(y)$ are disjoint G-orbits, and they are also closed by the above. Therefore by Lemma 3.6 there exist disjoint open and closed subsets $U, V \subset X$ such that U contains C and V contains D.

Set $U' = \bigcup_{\gamma\in G} \gamma U$. Since each $\gamma \in G$ acts as a homeomorphism, we get that U' is the union of open subsets, so it is open. It is also the continuous image of $G \times U$. Both G, U are compact since the latter is closed in a profinite space. Hence their product $G \times U$ is also compact. Thus, U' is closed, since Y is Hausdorff. Also $U' \cap D$ is empty; if it were not then $\gamma U \cap D \neq \varnothing$ for some $\gamma \in G$, but then $U \cap D = \gamma^{-1}(\gamma U \cap D) \neq \varnothing$ using that D is G-invariant. This is a contradiction. A similar argument shows that $V' = \bigcup_{\gamma\in N} \gamma U$ is open and closed, and $V' \cap C$ is empty.

Therefore $W = U' \cap V'$ is open and closed, and W is disjoint from $C \cup D$. Therefore its complement $U'' = U' - W$ in U' is also open and closed, and contains C since U' does. Similarly $V'' = V' - W$ is also open and closed, and contains D. Moreover, both U' and V' are G-invariant, so the same holds for W, and hence for U'' and V''. Because these sets are disjoint, their images $q(U'')$ and $q(V'')$ are also disjoint. They are also open by part (b) of Lemma 4.2, and since x, y are in $q(U'')$ and $q(V'')$, respectively, and were arbitrary, we get that $G\backslash X$ is at least Hausdorff.

Going back to the situation above, since U'' and V'' are closed in a profinite space, they are compact. Hence their images $q(U'')$ and $q(V'')$ are closed, since $G\backslash X$ is Hausdorff. Therefore they are a pair of disjoint open and closed neighbourhoods of x and y; since the latter were arbitrary, we get that $G\backslash X$ is even totally separated, so it is profinite by Theorem 3.2. □

Definition 4.6. Let X be a topological space and let G be a compact group. A *profinite principal G-bundle over X* is a continuous map $f\colon Y \to X$ equipped with a free continuous group action $g\colon G \times Y \to Y$ such that Y is profinite, the map f is surjective and the pre-image of each $x \in X$ is a G-orbit.

Theorem 4.7. *Let X be a Hausdorff space and let G be a compact group. Then every profinite principal G-bundle over X has a section.*

Remarks 4.8. (i) In the situation of the theorem above both G and X are profinite. This is immediate for G from Proposition 4.5. Moreover there is a unique bijection $\iota\colon G\backslash Y \to X$ such that $f = \iota \circ q$, where $q\colon Y \to G\backslash Y$ denotes the quotient map. Since f is continuous, we get that ι is a continuous bijection by part (a) of Lemma 4.2. Since $G\backslash Y$ is compact by Proposition 4.5 and X is Hausdorff, we get that ι is a homeomorphism. Moreover $G\backslash Y$ is actually profinite by Proposition 4.5, so the same holds for X, too.

(ii) The reader might wonder if it is true that for every continuous, surjective map $f\colon X \to Y$ of profinite spaces have a section. It turns out that those Y which have this property for every such f have a name: *extremally disconnected spaces*. They can be characterised by the following property: every set of open and closed subsets of Y has a supremum with respect to inclusion (see the Folk Theorem of [3] on page 485). Some spaces, such as the Čech–Stone compactification of discrete spaces have this property, but there are many profinite spaces which do not.

(iii) The theorem above was already stated by Morel, see the remark after Lemma 4 of [7] on page 359. However, no proof was given, just a remark that the strategy of the proof of Proposition 1 of [12] on page 4 works. This is what we will do, but for the sake of the reader we will give a detailed argument.

Proof of Theorem 4.7. We start with the proof of the following significant special case:

Proposition 4.9. *The theorem holds when G is finite.*

Proof. By Proposition 4.4 it will be sufficient to show that every $x \in X$ has an open neighbourhood U such that $f|_{f^{-1}(U)}\colon f^{-1}(U) \to U$ has a section. Since $f^{-1}(x)$ is homeomorphic to G, it is non-empty, so there is a $y \in Y$ such that $f(y) = x$. Because G is finite, and every point of Y is closed, as Y is Hausdorff by Theorem 3.2, there exist pairwise disjoint open and closed subsets $U_\gamma \subset X$ for all $\gamma \in G$ such that U_γ contains γy for each γ by Lemma 3.6.

Set $V = \bigcap_{\gamma \in G} \gamma^{-1} U_\gamma$. It is the intersection of finitely many open and closed subsets, so it is also open and closed. For every $\gamma \in G$ we have $\gamma V \subseteq \gamma(\gamma^{-1}U_\gamma) = U_\gamma$, so $V \cap \gamma V = \varnothing$ for every $\gamma \neq 1$ in G. Therefore the restriction of f to V is injective. Since V is closed, it is compact, while its image $f(V)$ is Hausdorff, so $f|_V$ has a continuous inverse $f(V) \to V$. Since $y = \gamma^{-1}(\gamma y) \in \gamma^{-1}U_\gamma$, we get that $y \in \gamma^{-1}U_\gamma$ for every $\gamma \in G$, so $y \in V$, and hence $x \in f(V)$.

Therefore it will be sufficient to show that $f(V)$ is open in X. Set $Z = \bigcup_{\gamma \in G} \gamma V$; it is clearly G-invariant, and since it is the union of open subsets, it is also open. Therefore its complement $W = Y - Z$ in Y is G-invariant and closed. Moreover $f(V) = f(Z)$, as f is G-equivariant, and f is surjective, so the complement of $f(V)$ in X is $f(W)$. Since W is closed, it is compact, and X is Hausdorff, so $f(W)$ is closed. Therefore its complement $f(V)$ is open. □

Definition 4.10. Let N be a closed, normal subgroup of G and let $G_N = N\backslash G$ denote the quotient: it is a profinite group. Let $r_N : G \to G_N$ be the quotient map, which is a continuous group homomorphism. There is a unique map $f_N : N\backslash Y \to X$ such that $f : Y \to X$ is the composition of the quotient map $q_N : Y \to N\backslash Y$ and f_N. There is a unique group action $G \times N\backslash Y \to N\backslash Y$ which makes f_N a G-equivariant map. The restriction of this action onto N is trivial, so it induces a group action $g_N : G_N \times N\backslash Y \to N\backslash Y$.

Proposition 4.11. *The map $f_N : N\backslash Y \to X$ equipped with the group action $g_N : G_N \times N\backslash Y \to N\backslash Y$ is a profinite principal G_N-bundle over X.*

Proof. Since the composition $f = f_N \circ q_N$ is continuous, we get that the map f_N is continuous by part (a) of Lemma 4.2. By part (c) of Lemma 4.2 the topology on $G_N \times N\backslash Y$ is the quotient topology with respect to $r_N \times q_N$, so g_N is continuous if $g_N \circ (r_N \times q_N)$ is by part (a) of Lemma 4.2. However, the composition $q_N \circ g$ is continuous, so by the commutativity of the following diagram:

$$\begin{array}{ccc} G \times Y & \xrightarrow{\ g\ } & Y \\ {\scriptstyle r_N \times q_N}\downarrow & & \downarrow{\scriptstyle q_N} \\ G_N \times N\backslash Y & \xrightarrow{\ g_N\ } & N\backslash Y \end{array}$$

the group action g_N is continuous. Clearly the action g_N is free, the map f_N is surjective, and the pre-image of each $x \in X$ is a G_N-orbit. Finally, $N\backslash Y$ is profinite by Proposition 4.5 since the action of N on Y is free and N is compact. □

Definition 4.12. Let M, N be a pair of closed, normal subgroups of G such that $M \subseteq N$. There is a unique map $f_{M,N} : M\backslash Y \to N\backslash Y$ such that $q_N : Y \to N\backslash Y$ is the composition of the quotient map $q_M : Y \to M\backslash Y$ and $f_{M,N}$. Let $\mathcal{S}$ denote the set whose elements are ordered pairs (N, s), where N is a closed, normal subgroup of G and s is a section of $f_N : N\backslash Y \to X$. Let $\geqslant$ denote the binary relation on $\mathcal{S}$ such that $(M, r) \geqslant (N, s)$ if and only if $M \subseteq N$, and $f_{M,N} \circ r = s$. Since for every triple $L \subseteq M \subseteq N$ of closed, normal subgroups of G we have $f_{M,N} \circ f_{L,M} = f_{L,N}$, we get that $\geqslant$ is a partial ordering on $\mathcal{S}$.

Proposition 4.13. *The poset $\mathcal{S}$ has a maximal element.*

Proof. For $N = G$ the map f_N is a bijection from a compact space onto a Hausdorff topological space, so it is a homeomorphism. Therefore its inverse is a section, and hence $\mathcal{S}$ is not empty. So by Zorn's lemma we only need to show that every chain $\mathcal{C} \subseteq \mathcal{S}$ has a maximal element. Set $C = \bigcap_{(N,s)\in\mathcal{C}} N$; since it is the intersection of closed, normal subgroups, it is also a closed, normal subgroup of G.

For every $(N, s) \in \mathcal{C}$, let $\Gamma(N, s) \subseteq C\backslash Y$ denote $f^{-1}_{C,N}(s(X))$, the pre-image of the section $s : X \to N\backslash Y$ with respect to $f_{C,N} : C\backslash Y \to N\backslash Y$. Since X is compact and $N\backslash Y$ is Hausdorff the image $s(X)$ is closed; as $f_{C,N}$ is continuous the pre-image $\Gamma(N, s)$ is also closed. Therefore their intersection $\Gamma \subseteq C\backslash Y$ is closed, and hence compact. So it will be sufficient to show that the restriction $f_C|_\Gamma : \Gamma \to X$, which is continuous, is also bijective, as X is Hausdorff.

Fix an $x \in X$; then for every $(N, s) \in \mathcal{C}$ the intersection $\Gamma(N, s) \cap f^{-1}_C(x)$ is a non-empty closed subset, and these form a descending chain with respect to inclusion. Hence by the compactness of $C\backslash Y$ their intersection $\Gamma \cap f^{-1}_C(x)$ is non-empty. Therefore $f_C|_\Gamma : \Gamma \to X$ is surjective. Now assume that we have two different

$y, z \in \Gamma \cap f_C^{-1}(x)$; then there is a unique $1 \neq \gamma \in C\backslash G$ such that $z = \gamma y$. Since C is the intersection $\bigcap_{(N,s)\in\mathcal{C}} N$, there is an $(N, s) \in \mathcal{C}$ such that the image of γ under the quotient homomorphism $C\backslash G \to N\backslash G$ is not 1. Then the images $f_{C,N}(y)$ and $f_{C,N}(\gamma y)$ are still different, since $f_{C,N}$ is G-equivariant. However, both $f_{C,N}(y)$ and $f_{C,N}(\gamma y)$ lie in the intersection of $s(X)$ and $f_N^{-1}(x)$, which consists of the single point $s(x)$: a contradiction. Therefore $f_C|_\Gamma \colon \Gamma \to X$ is injective, too. □

Now let (N, s) be a maximal element of $\mathcal{S}$. If we have $N = \{1\}$, then the theorem holds. So let us assume that this is not the case, and pick a non-zero $\gamma \in N$. Then there is an open normal subgroup $P \subset G$ such that $\gamma \notin P$. Let $M = N \cap P$. Since M is the intersection of closed normal subgroups, as every open subgroup is closed in a profinite group, it is such a group, and $\Gamma = M\backslash N$ is finite. Let $\Delta \subseteq M\backslash Y$ denote $f_{M,N}^{-1}(s(X))$, the pre-image of the section $s\colon X \to N\backslash Y$ with respect to $f_{M,N}\colon M\backslash Y \to N\backslash Y$. The action g_M restricted to Γ leaves Δ invariant.

Lemma 4.14. *The restriction $f_M|_\Delta\colon \Delta \to X$ equipped with the group action $g_M|_{\Gamma\times\Delta} : \Gamma \times \Delta \to \Delta$ is a profinite principal Γ-bundle over X.*

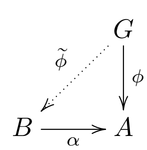
Proof. Since $f_M|_\Delta$ is the restriction of a continuous map, it is continuous, and for similar reasons $g_M|_{\Gamma\times\Delta}$ is continuous and Γ-equivariant, too. Since X is compact and $N\backslash Y$ is Hausdorff the image $s(X)$ is closed; as $f_{M,N}$ is continuous the pre-image Δ is also closed. Therefore it is a profinite space, as $M\backslash Y$ is profinite. Finally, for every $x \in X$ the fibre $f_M|_\Delta^{-1}(x)$ is bijective Γ-equivariantly to Γ. □

By Lemma 4.14 and Proposition 4.9 there is a section $r\colon X \to \Delta$. Let r also denote the composition of this map with the inclusion map $\Delta \to M\backslash Y$ by slight abuse of notation. Then $(M, r) \in \mathcal{S}$ such that $(M, r) \geqslant (N, s)$, but $(M, r) \neq (N, s)$. This contradicts the maximality of (N, s), so $N = \{1\}$. This completes the proof of Theorem 4.7. □

5. Maximal pro-2 quotients of real projective groups

The goal of this section is to prove Theorem 5.4. We first introduce the following type of embedding problems:

Definition 5.1. Let G be a profinite group. An embedding problem for G:



is a 2-*embedding problem* if both A and B are 2-groups.

Proposition 5.2. *Let G be a pro-2 group such that every real 2-embedding problem over G has a solution. Then every real embedding problem over G has a solution, too.*

Proof. We need the following group-theoretical

Lemma 5.3. *Let $f\colon C \to D$ be a surjective homomorphism of finite groups such that D is a 2-group. Let $P \subseteq C$ be a 2-Sylow subgroup and let $x \in C$ be a 2-torsion element. Then*

(*i*) *The restriction $f|_P\colon P \to D$ is surjective.*

(*ii*) *There is an* $h \in C$ *such that* $h^{-1}xh \in P$ *and* $f(x) = f(h^{-1}xh)$.

Proof. Let 2^b denote the order of D. Let N be the kernel of f and write the order of N as $2^a r$ where r is not divisible by 2. Then the order of C is $2^{a+b}r$, so the order of P is 2^{a+b}, while the order of $P \cap N$ is at most 2^a. Since the kernel of the restriction $f|_P : P \to H$ is $P \cap N$, we get that the image of $f|_P$ is at least 2^b. Therefore $f|_P$ is surjective.

Since the order of the subgroup generated by g divides 2 there is a $t \in C$ such that $t^{-1}gt \in P$ by the second Sylow theorem. By the above there is a $v \in P$ such that $f(v) = f(t)$. Set $h = tv^{-1}$. Then

$$h^{-1}gh = v(t^{-1}gt)v^{-1} \in vPv^{-1} = P,$$

since $v^{-1} \in P$. Moreover

$$f(h^{-1}gh) = f(v)f(t)^{-1}f(g)f(t)f(v)^{-1} = f(g)$$

using that f is a homomorphism and $f(v) = f(t)$. □

Let

$$\begin{array}{ccc} & & G \\ & \swarrow^{\tilde{\phi}} & \downarrow \phi \\ B & \xrightarrow{\alpha} & A \end{array}$$

be a real embedding problem **E** for G. Let $H \subseteq A$ be the image of ϕ. Since G is a pro-2 group, H is a 2-group. Let $C \subseteq B$ be the pre-image of H with respect to α and let $P \subseteq C$ be a 2-Sylow subgroup. By part (*i*) of Lemma 5.3 the restriction $\alpha|_P$ is surjective. Clearly,

$$\begin{array}{ccc} & & G \\ & \swarrow^{\tilde{\phi}} & \downarrow \phi \\ P & \xrightarrow[\alpha|_P]{} & H \end{array}$$

is a 2-embedding problem **F** for G such that if it has a solution then **E** also has a solution. Therefore it will be enough show that **F** is real because of our assumptions on G. Let $x \in G$ be an involution; by assumption there is a 2-torsion element $g \in C$ such that $\alpha(g) = \phi(x)$. Then there is a $y \in P$ which is conjugate to g in C such that $\alpha(y) = \phi(x)$ by part (*ii*) of Lemma 5.3. Since y is conjugate to a 2-torsion element, it is also 2-torsion. So **F** is real. □

Theorem 5.4. *Let G be a pro-2 group. Then the following are equivalent:*

(*i*) *G is real projective.*

(*ii*) *G is isomorphic to the maximal pro-2 quotient of a real projective group.*

Proof. Since the maximal pro-2 quotient of a pro-2 group is the group itself, clearly (*i*) implies (*ii*). Now let G be a pro-2 group which satisfies (*ii*). We start the proof of the other implication by showing that every real embedding problem for G has a solution. By Proposition 5.2 we need to show that any real 2-embedding problem **E**:

$$\begin{array}{ccc} & & G \\ & \swarrow^{\tilde{\phi}} & \downarrow \phi \\ B & \xrightarrow{\alpha} & A \end{array}$$

has a solution. Now let K be a pseudo real closed field such that G is isomorphic to the maximal pro-2 quotient of the absolute Galois group Γ of K. Such a field exists by the work of Haran–Jarden in [5, 6]. Let $q\colon \Gamma \to G$ be the corresponding quotient homomorphism. We claim that

$$\begin{array}{ccc} & & \Gamma \\ & \overset{\tilde{\phi}}{\swarrow} & \downarrow{\scriptstyle \phi\circ q} \\ B & \xrightarrow{\alpha} & A \end{array}$$

is a real embedding problem $\mathbf{F}$. Indeed, let $x \in \Gamma$ be an involution such that $\phi \circ q(x)$ is also an involution. Then $q(x) \in G$ is also an involution, so there is an involution $g \in B$ such that $\alpha(g) = \phi(q(x)) = \phi \circ q(x)$. So $\mathbf{F}$ is real. Since Γ is real projective, the embedding problem $\mathbf{F}$ has a solution $\widetilde{\phi}\colon \Gamma \to B$. But B is a 2-group, so $\widetilde{\phi}$ is the composition of q and a continuous homomorphism $G \to B$. The latter is a solution to $\mathbf{E}$. To finish the proof of Theorem 5.4 we need the following notation and lemma.

Notation 5.5. For every profinite group G, let G_2 denote its maximal pro-2 quotient and let $t_G\colon G \to G_2$ denote the quotient map. This assignment is functorial, that is, for every homomorphism $h\colon G \to H$ of profinite groups there is a unique homomorphism $h_2\colon G_2 \to H_2$ such that the diagram:

$$\begin{array}{ccc} G & \xrightarrow{h} & H \\ {\scriptstyle t_G}\downarrow & & \downarrow{\scriptstyle t_H} \\ G_2 & \xrightarrow[h_2]{} & H_2 \end{array}$$

is commutative.

Lemma 5.6. *Let G be a profinite group, let $H \subseteq G_2$ be an open subgroup, let I be the pre-image $t_G^{-1}(H) \subseteq G$, and let $h\colon I \to H$ denote the restriction of t_G onto I. Then $h_2\colon I_2 \to H_2 = H$ is an isomorphism.*

Proof. Because h is surjective, the map h_2 is also surjective, so we only need to show that it is injective, too. Let $1 \neq \gamma \in I_2$ be arbitrary. Then there is an open, normal subgroup $U \subseteq I_2$ such that $\gamma \notin U$. Since t_I is continuous, the pre-image $t_I^{-1}(U)$ is an open subgroup of 2-power index in I. Since I is an open subgroup of 2-power index in G, we get that $t_I^{-1}(U)$ is an open subgroup of 2-power index in G, too. Set $N = \bigcap_{\delta\in G} \delta^{-1}t_I^{-1}(U)\delta$; clearly it is a normal subgroup. Since $\delta^{-1}t_I^{-1}(U)\delta$ only depends on the coset $t_I^{-1}(U)\delta$, of which there are only finitely many, we get that N is a finite intersection of open subgroups of 2-power index in G, so it is also an open subgroup of 2-power index in G. Therefore the subgroup $t_I(N) \subseteq I_2$ is the pre-image of $t_G(N) \subseteq G_2$, but clearly $\gamma \notin t_I(N)$, and hence $h_2(\gamma) \neq 1$. □

Now we return to the proof of Theorem 5.4. By Definition 1.1, it remains to show that $G = \Gamma_2$ contains an open subgroup without 2-torsion. Let K be the field introduced above, and let $\Delta \subseteq \Gamma$ be the open subgroup corresponding to the finite extension $K(\sqrt{-1})/K$. As Δ is isomorphic to the absolute Galois group of $K(\sqrt{-1})$, it has cohomological dimension at most 1. By the Rost–Voevodsky norm residue theorem [14] (formerly known as the Milnor conjecture), the pull-back map $H^\bullet(\Delta_2, \mathbb{Z}/2) \to H^\bullet(\Delta, \mathbb{Z}/2)$ induced by the quotient map $t_\Delta\colon \Delta \to \Delta_2$ is an isomorphism. Therefore, Δ_2 also has cohomological dimension at most 1. Hence, by [12, Proposition 14 on page 19], any closed subgroup of Δ_2 has cohomological dimension at most 1. Since a finite subgroup would have infinite cohomological dimension, Δ_2 is torsion-free. Moreover, Δ has index dividing two in Γ, so Δ_2 is isomorphic to the kernel of the homomorphism $\Gamma_2 \to \mathbb{Z}/2\mathbb{Z}$ corresponding to the homomorphism $\Gamma \to \mathrm{Gal}(K(\sqrt{-1})/K) \subseteq \mathbb{Z}/2\mathbb{Z}$ by Lemma 5.6. Therefore, Δ_2 is an open, torsion-free subgroup of Γ_2. This finishes the proof of Theorem 5.4. □

6. Pro-2 real projective groups versus quasi-Boolean groups

The goal of this section is to prove Theorems 6.6 and 6.17. We begin with the following recollection and notation.

Remark 6.1. The free product of pro-p groups G_1 and G_2 is the coproduct of G_1 and G_2 in the category of pro-p groups, that is, it has the following universal property. For $j = 1, 2$, let $\iota_j : G_j \to G_1 *_p G_2$ be the composition of the natural inclusion $G_j \to G_1 * G_2$ and the quotient homomorphism $G_1 * G_2 \to G_1 *_p G_2$. Then for every pro-2 group G and for every pair of homomorphisms $f_j : G_j \to G$ of pro-2 groups, there is a unique homomorphism $f_1 *_p f_2 : G_1 *_p G_2 \to G$ of pro-2 groups such that $(f_1 *_p f_2) \circ \iota_j = f_j$ for $j = 1, 2$. This follows obviously from the definition when G is finite, and the general case follows by taking the projective limit.

Definition 6.2. Let G be a profinite group. Let $\mathcal{Y}_p(G)$ denote the subset of elements of order dividing p in G. We equip $\mathcal{Y}_p(G)$ with the subset topology. Let $\mathcal{X}_p(G)$ denote the quotient of $\mathcal{Y}_p(G)$ by the conjugation action of G. We equip $\mathcal{X}_p(G)$ with the quotient topology. Let $\mathcal{Y}^*_p(G)$ denote the complement of 1 in $\mathcal{Y}_p(G)$, and let $\mathcal{X}^*_p(G)$ denote the complement of the conjugacy class of 1 in $\mathcal{X}_p(G)$. When $p = 2$ we let $\mathcal{Y}(G), \mathcal{X}(G), \mathcal{Y}^*(G), \mathcal{X}^*(G)$ denote $\mathcal{Y}_p(G), \mathcal{X}_p(G), \mathcal{Y}^*_p(G), \mathcal{X}^*_p(G)$, respectively.

Remark 6.3. Let X be a topological space. Recall from Definition 1.4 the free pro-2 power $\mathbb{B}(X)$. We note that $\mathbb{B}(X)$ has the following universal property: Let $\iota_X : X \to \mathbb{B}(X)$ be the composition of the natural inclusion $X \to \circledast_X \mathbb{Z}/2\mathbb{Z}$ and the quotient homomorphism $\circledast_X \mathbb{Z}/2\mathbb{Z} \to \mathbb{B}(X)$. Then, for every pro-2 group G and for every continuous map $f : X \to \mathcal{Y}(G)$, there is a unique homomorphism $b_f : \mathbb{B}(X) \to G$ of pro-2 groups such that $b_f \circ \iota_X = f$. This follows obviously from the definition when G is finite, and the general case follows by taking the projective limit.

Notation 6.4. Let $f : X \to Y$ be a continuous map of topological spaces. Since $i_Y : Y \to \mathbb{B}(Y)$ is continuous and its image lies in $\mathcal{Y}(\mathbb{B}(Y))$, by the universal property in the remark above there is a unique homomorphism $\mathbb{B}(f) : \mathbb{B}(X) \to \mathbb{B}(Y)$ of pro-2 groups such that $\mathbb{B}(f) \circ \iota_X = \iota_Y \circ f$. This makes the assignment $X \mapsto \mathbb{B}(X)$ into a functor.

Proposition 6.5. *For every topological space X, the map $\mathbb{B}(u_X) : \mathbb{B}(X) \to \mathbb{B}(\widehat{X})$ induced by the profinite completion $u_X : X \to \widehat{X}$ is an isomorphism of pro-2 groups.*

Proof. First we are going to show that $\mathbb{B}(u_X)$ is surjective. Since the image is compact, it is closed, so it will be sufficient to show that the image is dense. In order to do so it will be enough to prove that, for every 2-group G and continuous surjective homomorphism $f : \mathbb{B}(\widehat{X}) \to G$, the composition $f \circ \mathbb{B}(u_X)$ is surjective. Note that $\widehat{X}$ generates $\circledast_{\widehat{X}} \mathbb{Z}/2\mathbb{Z}$, so $f(\widehat{X})$ generates G. Since $u_X(X)$ is dense in

$\widehat{X}$, the image $f \circ u_X(X)$ is dense in $f(\widehat{X})$. But G is finite, so it is discrete, and hence $f \circ u_X(X)$ is equal to $f(\widehat{X})$. So $f \circ u_X(X)$ generates G, therefore $f \circ \mathbb{B}(u_X)$ is surjective.

Next we are going to show that $\mathbb{B}(u_X)$ is injective. In order to do so it will be sufficient to show that $u_X \circ \iota_X : X \to \mathbb{B}(\widehat{X})$ has the universal property in Remark 6.3. Indeed then there is a continuous homomorphism $f : \mathbb{B}(\widehat{X}) \to \mathbb{B}(X)$ such that $f \circ \mathbb{B}(u_X) \circ \iota_X$ is ι_X, and hence $f \circ \mathbb{B}(u_X)$ is the identity of $\mathbb{B}(X)$. Now let G be a pro-2 group and $f : X \to \mathcal{Y}(G)$ be a continuous map. Since $\mathcal{Y}(G)$ is profinite, there is a unique continuous map $g : \widehat{X} \to \mathcal{Y}(G)$ such that $f = g \circ u_X$ because of the universal property of u_X. Using the universal property of $\mathbb{B}(\widehat{X})$ we get that there is a continuous homomorphism $b_g : \mathbb{B}(\widehat{X}) \to G$ of pro-2 groups such that $b_f \circ \iota_{\widehat{X}} = g$. □

We recall from Definition 1.5 that we call a pro-2 group *Boolean* if it is isomorphic to $\mathbb{B}(X)$ for some topological space X. By Proposition 6.5 we can always assume that X is profinite. We call a pro-2 group *quasi-Boolean* if it is the free product of a free pro-2 group and a Boolean group.

Theorem 6.6. *Every quasi-Boolean pro-2 group is real projective.*

Proof. Let G be a quasi-Boolean pro-2 group. It will be sufficient to show that G is the maximal pro-2 quotient of a real projective group by Theorem 5.4. In order to do so, we will use a group-theoretical characterisation of real projective groups by Haran and Jarden. Following [6, Definition 1.1 on page 156] we define:

Definition 6.7. A profinite group D is said to be *real free* if it contains disjoint closed subsets X and Y such that $X \subseteq \mathcal{Y}^*(D)$, $1 \in Y$, and every continuous map ϕ from $X \cup Y$ into a profinite group H such that $\phi(x)^2 = 1$ for every $x \in X$ and $\phi(1) = 1$ extends to a unique homomorphism of D into H.

Theorem 6.8 (Haran–Jarden)**.** *A profinite group G is real projective if and only if G is isomorphic to a closed subgroup of a real free group.*

Proof. This claim is [6, Theorem 3.6 on page 160]. □

Now we return to the proof of Theorem 6.6. For every set Y, let $F(Y)$ denote the free pro-2 group on Y as defined in [12, Section 1.5 on pages 7–8]. By assumption, G is the free product of a free pro-2 group $F(Y)$ and a Boolean group $\mathbb{B}(X)$ for a set Y and a profinite space X. By Theorem 6.8 it will be sufficient to show that G is the maximal pro-2 quotient of a real free profinite group. Let $\widehat{G}$ be the free product $\ast_X \mathbb{Z} * \ast_X \mathbb{Z}/2\mathbb{Z}$, i.e., the group which is freely generated by the elements of the disjoint union of Y and X, subject to the relation that these elements are involutions. Let $\mathcal{N}$ be the family of normal subgroups N of $\widehat{G}$ such that

- (i) the quotient $\widehat{G}/N$ is finite,
- (ii) the composition of the natural inclusion $Y \to \widehat{G}$ and the quotient homomorphism $\widehat{G} \to \widehat{G}/N$ maps all but finitely many elements of Y to 1,
- (iii) the composition of the natural inclusion $X \to \widehat{G}$ and the quotient homomorphism $\widehat{G} \to \widehat{G}/N$ is continuous with respect to the discrete topology on $\widehat{G}/N$.

Set
$$\overline{G} = \varprojlim_{N \in \mathcal{N}} \widehat{G}/N.$$
Clearly G is the maximal pro-2 quotient of $\overline{G}$. On the other hand, $\overline{G}$ is a real free profinite group. In fact, $\overline{G}$ is the group $\widehat{D}(X, Y_+, e)$ in [6, Lemma 1.3 on pages 156–157], where Y_+ is the one-point compactification of Y equipped with the discrete topology, and $e \in Y_+ - Y$ is the point at infinity. This finishes the proof of Theorem 6.6. □

Next, we set out to prove the converse, i.e., every real projective pro-2 group is quasi-Boolean. We begin with the following

Definition 6.9. Let A be an abelian profinite group. A *complement* of a closed subgroup $B \subset A$ is a closed subgroup $C \subseteq A$ such that $B \cap C$ is trivial, and $B + C = A$.

The following lemma is probably very well-known, but we could not find a convenient reference:

Lemma 6.10. *Let G be a p-torsion abelian profinite group. Then the following holds:*

- (i) *there is an isomorphism $G \cong \mathbb{F}_p^X$ for some set X,*
- (ii) *every closed subgroup of G has a complement.*

Proof. The Pontryagin dual of G is a discrete $\mathbb{F}_p$-linear vector space V, since G is compact. Note that every isomorphism between discrete $\mathbb{F}_p$-linear vector spaces is automatically a homeomorphism, so V is isomorphic to the direct sum $\mathbb{F}_p^{\oplus X}$, equipped with the discrete topology, as a topological group for some set X. The Pontryagin dual of $\mathbb{F}_p^{\oplus X}$ is $\mathbb{F}_p^X$, which is isomorphic to G by Pontryagin duality. So claim (i) holds.

Assertion (ii) is equivalent to the following claim: let $i\colon B \to A$ be a monomorphism of p-torsion abelian profinite groups. Then there is a morphism $j\colon A \to B$ such that $j \circ i = \mathrm{id}_B$. By Pontryagin duality, it is equivalent to the following claim: let $p\colon V \to U$ be an epimorphism of $\mathbb{F}_p$-linear vector spaces. Then there is a morphism $r\colon U \to V$ such that $p \circ r = \mathrm{id}_V$. The latter is well-known. □

Again let G be a quasi-Boolean pro-2 group which is the free product of a free pro-2 group F and a Boolean group $\mathbb{B}(X)$ for a profinite space X. Let $j_X\colon X \to \mathcal{X}(\mathbb{B}(X))$ denote the composition of the map $i_X\colon X \to \mathcal{Y}(\mathbb{B}(X))$, the inclusion $\mathcal{Y}(\mathbb{B}(X)) \subseteq \mathcal{Y}(G)$, and the quotient map $\mathcal{Y}(G) \to \mathcal{X}(G)$. It is useful to record the following fact:

Theorem 6.11. *The map j_X is a homeomorphism onto $\mathcal{X}^*(G)$.*

Proof. Since X is compact and $\mathcal{X}^*(G)$ is Hausdorff, it will be sufficient to show that j_X maps X onto $\mathcal{X}^*(G)$ bijectively. Let $x, y \in X$ be two different elements. Then there is a continuous map $s\colon X \to \mathbb{Z}/2$ such that $s(x) \neq s(y)$. Let $\overline{s}\colon G \to \mathbb{Z}/2$ be the unique homomorphism such that the restriction of $\overline{s}$ onto F is trivial, and onto $\mathbb{B}(X)$ is b_s (as defined in Remark 6.3). Under $\overline{s}$ the images of $i_X(x)$ and $i_X(y)$ are not conjugate, so they are not conjugate in G either. Therefore j_X is injective. Since we may guarantee that $s(x)$ is not a unit, we get that j_X maps into $\mathcal{X}^*(G)$, too.

Now assume that there is a $y \in \mathcal{X}^*(G)$ which is not in the image of j_X. Since X is compact and $\mathcal{X}^*(G)$ is Hausdorff, the image of j_X is closed, so by Lemma 3.6 there is a continuous function $r\colon \mathcal{X}^*(G) \to \mathbb{Z}/2$ such that $r \circ j_X$ is zero, and $r(y)$ is non-zero. By Theorem 6.6, the pro-2 group G is real projective. Hence, by Scheiderer's theorem [8, Theorem 2.11], there is a continuous homomorphism $\overline{r}\colon G \to \mathbb{Z}/2$ whose image under the map

$$\pi_1\colon H^1(G, \mathbb{Z}/2) \to C(\mathcal{X}^*(G), \mathbb{Z}/2)$$

is r. Then the restriction of $\overline{r}$ onto $i_X(X)$ is zero, so by the universal property of $\mathbb{B}(X)$ the restriction of $\overline{r}$ onto $\mathbb{B}(X)$ is also zero, and hence this homomorphism factors through the surjective homomorphism $p_1\colon G \to F$ supplied by the universal property of free pro-2 products. But F is torsion-free (see [12, Corollary 3, part (a) on page 31]), so p_1 is zero on any involution $\overline{y}$ in the conjugacy class y. Therefore $r(y) = \overline{r}(\overline{y})$ is zero, which is a contradiction. □

Theorem 6.12. *Let G be isomorphic to the absolute Galois group of a field K. Then there is a continuous section $s\colon \mathcal{X}^*(G) \to \mathcal{Y}^*(G)$.*

Proof. Let $H \subseteq G$ be the open subgroup corresponding to the finite extension $K(\sqrt{-1})/K$. Then H is isomorphic to the absolute Galois group of $K(\sqrt{-1})$, and it is torsion-free. In particular, if $H = G$ then $\mathcal{X}^*(G)$ is empty and the claim is trivially true. Otherwise, H has index two in G. Then the theorem follows from Proposition 6.13 below and Theorem 4.7. □

Proposition 6.13. *With the above assumptions, the map $\mathcal{Y}^*(G) \to \mathcal{X}^*(G)$ is a profinite principal H-bundle with respect to the conjugation action of H on $\mathcal{Y}^*(G)$, and $\mathcal{X}^*(G)$ is Hausdorff.*

Proof. Clearly $\mathcal{Y}(G)$ is closed in G. Since H is torsion-free, the subset $\mathcal{Y}^*(G)$ is the intersection of $\mathcal{X}(G)$ and the complement of the open H in G, so it is closed, too. Since G is profinite, we get that $\mathcal{Y}^*(G)$ is profinite. As G is isomorphic to an absolute Galois group, for every $y \in \mathcal{Y}^*(G)$ we have $H \cap C_G(y) = \{1\}$, and hence H acts freely on $\mathcal{Y}^*(G)$. This action is also clearly continuous.

We claim that every $x \in G$ conjugate to y is already conjugate under H. Indeed, let $z \in G$ be such that $z^{-1}xz = y$. Since H has index 2 and $y \notin H$ we have $G = H \cup Hy$. If $z \in H$ the claim is clearly true. Otherwise $z = hy$ for some $h \in H$, and hence $x = zyz^{-1} = hyyy^{-1}h^{-1} = hyh^{-1}$, so x is conjugate to y under H in this case, too. So the map $\mathcal{Y}^*(G) \to \mathcal{X}^*(G)$ is the quotient map with respect to the action of H. Since $\mathcal{Y}^*(G)$ is open in $\mathcal{Y}(G)$ the subspace topology on $\mathcal{X}^*(G) \subset \mathcal{X}(G)$ is the quotient topology with respect to the map in the claim. Therefore, $\mathcal{X}^*(G)$ is Hausdorff by Proposition 4.5. □

Corollary 6.14. *Let G be a real projective profinite group. Then there is a continuous section $s\colon \mathcal{X}^*(G) \to \mathcal{Y}^*(G)$.*

Proof. Since every real projective profinite group is isomorphic to the absolute Galois group of a pseudo real closed field, the claim follows at once from Theorem 6.12. □

Remark 6.15. Note that Corollary 6.14 is also part (a) of [6, Lemma 3.5 on page 160]. We think, however, that our proof is more conceptual and derives a similar claim for a much larger class of groups.

Notation 6.16. For every pro-2 group G, let G_* denote the *maximal abelian* 2-*torsion quotient of* G and, for every homomorphism $b\colon G \to H$ of pro-2 groups, let $b_*\colon G_* \to H_*$ denote the homomorphism induced by b.

Theorem 6.17. *Let G be a real projective pro-2 group. Then G is quasi-Boolean.*

Proof. Let X denote $\mathcal{X}^*(G)$, and let $s\colon X \to \mathcal{Y}^*(G)$ be the section furnished by Theorem 6.12. Let B be the image of the homomorphism $(b_s)_*\colon \mathbb{B}(X)_* \to G_*$. Since $\mathbb{B}(X)_*$ is compact and G_* is Hausdorff, B is closed. Let $A \subseteq G_*$ be a complement of B, which exists by part (ii) of Lemma 6.10. By part (i) of Lemma 6.10, there is a set Y such that $A \cong \mathbb{Z}/2^Y$. Since $F(Z)_* \cong \mathbb{Z}/2^Y$, by part (a) of [12, Proposition 24 on page 30] and Pontryagin duality, there is a continuous homomorphism $h\colon F(Y) \to G$ such that $h_*\colon F(Y)_* \to G_*$ maps $F(Y)_*$ isomorphically onto A. We set $P = F(Y) *_2 \mathbb{B}(X)$ and let $\alpha\colon P \to G$ be the homomorphism $h *_2 b_s$. Since $(G_1 *_2 G_2)_* \cong (G_1)_* \oplus (G_2)_*$ for every pair of pro-2 groups G_1 and G_2, we get that $\alpha_*\colon P_* \to G_*$ is an isomorphism. Hence, by [12, Proposition 24, part (b), on page 30] and Pontryagin duality, the map α is surjective. To finish the proof we need the following

Lemma 6.18. *Let $\alpha\colon P \to G$ be a continuous surjective homomorphism of real projective profinite groups, and let $X \subseteq \mathcal{Y}^*(P)$ be a system of representatives of $\mathcal{X}^*(P)$. If α maps X bijectively onto a system of representatives of $\mathcal{X}^*(G)$, then there is a continuous injective homomorphism $\gamma\colon G \to P$ such that $\alpha \circ \gamma = \mathrm{id}_G$.*

Proof. This claim is part (b) of [6, Lemma 3.5 on page 160]. The proof relies on the projectivity of the Artin–Schreier structures attached to real projective groups (see [5, Proposition 7.7 on page 473]). □

We return to the proof of Theorem 6.17. By Theorem 6.6, the quasi-Boolean group P is real projective, while by Theorem 6.11 the subset $X \subseteq P$ is a system of representatives of $\mathcal{X}^*(P)$ mapped bijectively onto a system of representatives of $\mathcal{X}^*(G)$, so the conditions in Lemma 6.18 above hold. Therefore there is a continuous homomorphism $\gamma\colon G \to P$ such that $\alpha \circ \gamma = \mathrm{id}_G$. Then $\alpha_* \circ \gamma_* = (\alpha \circ \gamma)_* = (\mathrm{id}_G)_* = \mathrm{id}_{G_*}$ is the identity, and α_* is an isomorphism, so γ_* is an isomorphism, too. Therefore, γ is surjective by part (b) of [12, Proposition 24 on page 30] and Pontryagin duality. So γ is an isomorphism, and hence G is quasi-Boolean. This finishes the proof of Theorem 6.17. □

7. Quillen's theorems and their consequences

The goal of this section is to prove Corollary 7.23.

Definition 7.1. Following Quillen we say that a homomorphism $R \to S$ of graded anti-commutative rings is *finite* if S is a finitely generated module over R. This definition is a bit ambiguous since it does not specify whether we consider S as a left R-module or a right R-module. However, note that S is a finitely generated left R-module if and only if it is a finitely generated right R-module. Indeed if S is a finitely generated left R-module then it is also generated by a finite set $H \subset S$ of homogeneous elements. But the left R-module generated by H is the same as the right R-module generated by H since S is anti-commutative. Therefore S is also finitely generated as a right R-module. The converse could be proved similarly.

Theorem 7.2 (Quillen)**.** *Let G be a pro-p group and let $H \subseteq G$ be a finite subgroup. Then the homomorphism $H^\bullet(G, \mathbb{Z}/p) \to H^\bullet(H, \mathbb{Z}/p)$ is finite.*

Proof. Note that H is a closed subgroup, as G is Hausdorff, so the homomorphism $H^\bullet(G, \mathbb{Z}/p) \to H^\bullet(H, \mathbb{Z}/p)$ is well-defined. This theorem was proved by Quillen when G is finite [13, Corollary 2.4 on page 555], and the general case follows as an easy corollary. Indeed let $N \lhd G$ be an open normal subgroup such that the restriction of the quotient map $q \colon G \to G/N$ to H is injective. Then the homomorphism $H^\bullet(G/N, \mathbb{Z}/p) \to H^\bullet(H, \mathbb{Z}/p)$ induced by the composition of the inclusion map $H \to G$ and q is finite by the above. Since this homomorphism factors through $H^\bullet(G, \mathbb{Z}/p) \to H^\bullet(H, \mathbb{Z}/p)$, the latter is also finite. □

Corollary 7.3. *Let G be a pro-p group and let $H \subseteq G$ be a subgroup of order p. Then the homomorphism $H^n(G, \mathbb{Z}/p) \to H^n(H, \mathbb{Z}/p)$ is non-zero for infinitely many n.*

Proof. Assume that the claim is false and there is a natural number d such that the image of $H^n(G, \mathbb{Z}/p) \to H^n(H, \mathbb{Z}/p)$ is zero for $n \geqslant d$. Let $S \subset H^\bullet(H, \mathbb{Z}/p)$ be a finite subset of homogeneous elements which generate $H^\bullet(H, \mathbb{Z}/p)$ as a $H^\bullet(G, \mathbb{Z}/p)$-module. Let d' be the maximal degree of the elements of S. Then $H^n(H, \mathbb{Z}/p) = 0$ for every $n \geqslant d + d'$. But, since H has order p, $H^n(H, \mathbb{Z}/p) \neq 0$ for every n which is a contradiction. □

We now recall the following types of algebras from [8].

Definition 7.4. We call an $\mathbb{F}_2$-algebra $B^\bullet = \bigoplus_{i \geqslant 0} B^i$ a *graded Boolean algebra* if $B^0 = \mathbb{F}_2$ and there is a Boolean ring B such that, for every $i \geqslant 1$, we have $B^i = B$, and, for every pair $i, j \geqslant 1$, the multiplication $B^i \times B^j \to B^{i+j}$ is the multiplication in the ring $B = B^i = B^j = B^{i+j}$. We call an $\mathbb{F}_2$-algebra $D^\bullet = \bigoplus_{i \geqslant 0} D^i$ a *dual algebra* if $D^0 = \mathbb{F}_2$, and $D^i = 0$ for $i \geqslant 2$. The *connected sum* $D^\bullet \sqcap B^\bullet$ is the graded $\mathbb{F}_2$-algebra with $(D^\bullet \sqcap B^\bullet)^0 = \mathbb{F}_2$, $(D^\bullet \sqcap B^\bullet)^i = D^i \oplus B^i$ for $i \geqslant 1$ and multiplication $D^1 B^i$ and $B^i D^1$ is set to be zero for all $i \geqslant 1$.

Remark 7.5. In [8] we show that dual and graded Boolean algebras are Koszul algebras. In particular, they are quadratic algebras and their connected sum is their direct sum as quadratic algebras.

The results in [8] are the motivation for the following terminology which we recall from the introduction.

Definition 7.6. We say that a pro-2 group is a *cohomologically Boolean group* if its mod 2 cohomology is a graded Boolean algebra. We say that a pro-2 group is a *cohomologically quasi-Boolean group* if its mod 2 cohomology is the connected sum of a dual algebra and a graded Boolean algebra.

For every commutative ring R, let $\mathcal{N}(R)$ denote the nilradical of R.

Lemma 7.7. *Let G be a cohomologically quasi-Boolean pro-2 group. Then the quotient $H^\bullet(G, \mathbb{Z}/2)/\mathcal{N}(H^\bullet(G, \mathbb{Z}/2))$ is a graded Boolean algebra.*

Proof. Let $H^*(G, \mathbb{Z}/2)$ be the connected sum of a dual algebra D^* and a graded Boolean algebra B^*. Then the nilradical of $H^\bullet(G, \mathbb{Z}/2)$ is D^1, so the quotient $H^\bullet(G, \mathbb{Z}/2)/\mathcal{N}(H^\bullet(G, \mathbb{Z}/2))$ is isomorphic to B^*. □

Definition 7.8. Let G be a cohomologically quasi-Boolean pro-2 group. Let B denote the up to isomorphism unique Boolean ring such that the associated graded Boolean algebra B^* is isomorphic to $H^\bullet(G,\mathbb{Z}/2)/\mathcal{N}(H^\bullet(G,\mathbb{Z}/2))$. We say that a continuous homomorphism $k\colon G \to \mathbb{Z}/2$ is a *quasi-canonical homomorphism* if the image of the associated cohomology class $k \in H^1(G,\mathbb{Z}/2)$ under the quotient map

$$H^\bullet(G,\mathbb{Z}/2) \to H^\bullet(G,\mathbb{Z}/2)/\mathcal{N}(H^\bullet(G,\mathbb{Z}/2))$$

is the unit of B.

Remark 7.9. Quasi-canonical homomorphisms $k \in H^1(G,\mathbb{Z}/2)$ can be characterised by the following property: for every $n > 0$ and $c \in H^n(G,\mathbb{Z}/2)$ we have $c^2 = c \cup k^n$.

Definition 7.10. An *elementary p-group* H is a group isomorphic to $(\mathbb{Z}/p)^n$ for some n. The rank of H is n, that is, its dimension as a vector space over $\mathbb{Z}/p$. The *elementary rank* of a pro-p group G is the supremum of all natural numbers r such that G has a subgroup isomorphic to an elementary p-group of rank r.

Proposition 7.11. *Let G be a cohomologically quasi-Boolean pro-2 group. Then the following holds:*

(i) *every involution $x \in G$ is not in the kernel of any quasi-canonical homomorphism,*
(ii) *the elementary rank of G is at most one.*

Proof. To prove (i), let $x \in G$ be an involution, let $H \subseteq G$ be the subgroup generated by x and let $i\colon H \to G$ be the inclusion map. Assume that there is a quasi-canonical homomorphism $k \in H^1(G,\mathbb{Z}/2)$ whose restriction to H is zero, or equivalently $i^*(k) = 0$. By Corollary 7.3, there is an $n > 0$ and a $c \in H^n(G,\mathbb{Z}/2)$ such that $i^*(c) \in H^n(H,\mathbb{Z}/2)$ is non-zero. Then

$$0 \neq i^*(c)^2 = i^*(c^2) = i^*(c \cup k^n) = i^*(c) \cup i^*(k)^n = 0$$

using that $H^\bullet(H,\mathbb{Z}/2)$ is isomorphic to a polynomial ring in one variable over $\mathbb{Z}/2$, but this is a contradiction. Therefore (i) holds.

To prove (ii), assume to the contrary that G contains a subgroup H isomorphic to an elementary 2-group of rank 2. Then the kernel of the restriction of a quasi-canonical homomorphism of H is non-trivial. This contradicts part (i), so claim (ii) is true. □

Definition 7.12. Let p be a prime number and let $h\colon R \to S$ be a homomorphism of graded anti-commutative algebras over $\mathbb{F}_p$. We say that h is an F-isomorphism if

(i) for every homogeneous element r in the kernel of h we have $r^n = 0$ for some n,
(ii) for every homogeneous element s in S the power s^{p^n} is in the image of h for some n.

Lemma 7.13. *Let $f\colon B^\bullet \to C^\bullet$ be an F-isomorphism between graded Boolean algebras. Then f is an isomorphism.*

Proof. Since graded Boolean algebras have no nilpotent elements, we get that f is injective by condition (i) of Definition 7.12. Next we show that f is surjective. Since f is clearly an isomorphism in degree zero, it will be sufficient to show that for every positive integer n and $x \in C^n$ there is a $y \in B^n$ such that $f(y) = x$. By assumption, there is a positive integer m and a $z \in B^{nm}$ such that $f(z) = x^m$. Because $B^\bullet$ is a graded Boolean algebra the m-th power map $B^n \to B^{nm}$ is an isomorphism, so there is a $y \in B^n$ such that $y^m = z$, and hence $f(y)^m = f(y^m) = f(z) = x^m$. Since $C^\bullet$ is also a graded Boolean algebra the m-th power map $C^n \to C^{nm}$ is an isomorphism, so $f(y) = x$. □

Definition 7.14. For every profinite group G, let $\mathfrak{A}(G)$ denote the set of all subgroups of G which are finite elementary abelian p-groups. Note that all such subgroups are closed, since G is Hausdorff. Also note that $\mathfrak{A}(G)$ form a category where morphisms are maps $f\colon A \to B$ such that there is an $x \in G$ such that $f(y) = x^{-1}gx$ for every $y \in A$. Note that the assignment $G \mapsto \mathfrak{A}(G)$ is functorial, that is for every continuous homomorphism $h : G \to H$ there is an induced functor $\mathfrak{A}(h)\colon \mathfrak{A}(G) \to \mathfrak{A}(H)$. For every open normal subgroup $N \lhd G$, let $\mathfrak{A}(G, N)$ denote the image of $\mathfrak{A}(G)$ under the functor $\mathfrak{A}(\pi_N)\colon \mathfrak{A}(G) \to \mathfrak{A}(G/N)$ induced by the quotient map $\pi_N : G \to G/N$.

Definition 7.15. Let $\mathbf{DGAC}_p$ denote the category of graded anti-commutative algebras over $\mathbb{Z}/p$. For every profinite group G, let $F_G\colon \mathfrak{A}(G) \to \mathbf{DGAC}_p$ be the functor given by the rule $A \to H^\bullet(A, \mathbb{Z}/p)$. For every open normal subgroup $N \lhd G$, let $F_{G,N}\colon \mathfrak{A}(G, N) \to \mathbf{DGAC}_p$ denote the restriction of $F_{G/N}$ onto $\mathfrak{A}(G, N)$. For every G and N as above, let $\underline{H^\bullet}_{\mathfrak{A}}(G, \mathbb{Z}/p)$ and $\underline{H^\bullet}_{\mathfrak{A}}(G, N, \mathbb{Z}/p)$ denote the inductive limit of the functor F_G and $F_{G,N}$, respectively.

Definition 7.16. Let G and N be as above. Then for every $A \in \mathfrak{A}(G, N)$, let $\pi_{A,N}\colon A \to \pi_N(A)$ be the map induced by the restriction of π_N onto A. Note that for every

$$\underline{c} = \{c_A \in H^\bullet(A, \mathbb{Z}/p) \mid A \in \mathfrak{A}(G, N)\} \in \underline{H^\bullet}_{\mathfrak{A}}(G, N, \mathbb{Z}/p)$$

the collection

$$\mathfrak{a}_N(\underline{c}) = \{\pi^*_{N,A}(c_{\pi_N(A)}) \in H^\bullet(A, \mathbb{Z}/p) \mid A \in \mathfrak{A}(G)\}$$

lies in $\underline{H^\bullet}_{\mathfrak{A}}(G, \mathbb{Z}/p)$ and the map $\mathfrak{a}_N\colon \underline{H^\bullet}_{\mathfrak{A}}(G, N, \mathbb{Z}/p) \to \underline{H^\bullet}_{\mathfrak{A}}(G, \mathbb{Z}/p)$ is a homomorphism of graded anti-commutative algebras over $\mathbb{Z}/p$. Let $H^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ denote the union of the images of these homomorphisms as N ranges over the set of all open normal subgroups of G. Since these images form an inductive system, $H^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ is a graded subalgebra of $\underline{H^\bullet}_{\mathfrak{A}}(G, \mathbb{Z}/p)$. Clearly, when G is finite, we have $H^\bullet_{\mathfrak{A}}(G, \mathbb{Z}/p) = \underline{H^\bullet}_{\mathfrak{A}}(G, \mathbb{Z}/p)$.

Proposition 7.17. *Let G be a profinite group of elementary rank at most* 1 *such that there is an open normal subgroup of G without p-torsion. Then $H^n_{\mathfrak{A}}(G, \mathbb{Z}/p) = C(\mathcal{X}^*_p(G), \mathbb{Z}/p)$ for every $n > 0$.*

Proof. Let $F(\mathcal{X}^*_p(G), \mathbb{Z}/p)$ denote the group of all $\mathbb{Z}/p$-valued functions on $\mathcal{X}^*_p(G)$. Since for every non-zero $A \in \mathfrak{A}(G)$, we have $A \cong \mathbb{Z}/p$. Hence $H^n(A, \mathbb{Z}/p) = \mathbb{Z}/p$, every element $c \in \underline{H}^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ gives rise to a function $\mathcal{Y}^*_p(G) \to \mathbb{Z}/p$ which is conjugation-invariant, and hence descends to a function $f(c)\colon \mathcal{X}^*_p(G) \to \mathbb{Z}/p$. The map $f\colon \underline{H}^n_{\mathfrak{A}}(G, \mathbb{Z}/p) \to F(\mathcal{X}^*_p(G), \mathbb{Z}/p)$ is an isomorphism. So the precise meaning of our claim is that the image of $H^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ under f and $C(\mathcal{X}^*_p(G), \mathbb{Z}/p)$ are equal as subgroups of $F(\mathcal{X}^*_p(G), \mathbb{Z}/p)$.

First let $c \in H^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ be arbitrary. Then there is an open normal subgroup $N \lhd G$ and a $d \in \underline{H}^n_{\mathfrak{A}}(G, N, \mathbb{Z}/p)$ such that $c = \mathfrak{a}_N(d)$. Since for every pair M, N of open, normal subgroups of G such that $M \subseteq N$ the image of $\mathfrak{a}_M$ contains the image of $\mathfrak{a}_N$, we may assume that N does not contain p-torsion without the loss of generality by shrinking N if it is necessary. Then π_N induces a map $\pi_N^{\#}\colon \mathcal{X}_p^*(G) \to \mathcal{X}_p^*(G/N)$, and $f(c)$ is the composition of $\pi_N^{\#}$ with the function $\mathrm{Im}(\pi_N^{\#}) \to \mathbb{Z}/p$ corresponding to d. Since both $\pi_N^{\#}$ and the latter function are continuous, we get that $f(c)$ is continuous, too.

Now let $c \in C(\mathcal{X}_p^*(G), \mathbb{Z}/p)$ be arbitrary, and let $g\colon \mathcal{Y}_p^*(G) \to \mathbb{Z}/p$ be the continuous function we get by composing the quotient map $\mathcal{Y}_p^*(G) \to \mathcal{X}_p^*(G)$ with c. Since the translates of normal open subgroups of G form a sub-basis for its topology, for every $x \in \mathcal{Y}_p^*(G)$ there is a normal open subgroup $N_x \lhd G$ such that g is constant on $xN_x \cap \mathcal{Y}_p^*(G)$. Since there is an open normal subgroup of G without p-torsion, the subspace $\mathcal{Y}_p^*(G)$ is closed, and hence compact, so there is a finite subset $S \subseteq \mathcal{Y}_p^*(G)$ such that $\mathcal{Y}_p^*(G) \subseteq \bigcup_{x\in S} xN_x$.

Since $N = \bigcap_{x\in S} N_x$ is the intersection of finitely many normal open subgroups, it is a normal open subgroup, too. We may even assume that N does not contain p-torsion without the loss of generality by shrinking N if it is necessary, as above. Then g is constant on $xN \cap \mathcal{Y}_p^*(G)$ for every $x \in \mathcal{Y}_p^*(G)$, and hence c is the composition of $\pi_N^{\#}$ above with a function $d\colon \mathrm{Im}(\pi_N^{\#}) \to \mathbb{Z}/p$. □

Definition 7.18. Let G be as above, and, for every $A \in \mathfrak{A}(G)$, let $i_A\colon A \to G$ be the inclusion map. For every $c \in H^\bullet(G, \mathbb{Z}/p)$, the collection

$$q_G(c) = \{i_A^*(c) \in H^\bullet(A, \mathbb{Z}/p) \mid A \in \mathfrak{A}(G)\}$$

lies in $\underline{H}_{\mathfrak{A}}^\bullet(G, \mathbb{Z}/p)$, since every conjugation of G induces the identity on $H^\bullet(G, \mathbb{Z}/p)$. The resulting map $q_G\colon H^\bullet(G, \mathbb{Z}/p) \to \underline{H}_{\mathfrak{A}}^\bullet(G, \mathbb{Z}/p)$ is a homomorphism of graded anti-commutative algebras over $\mathbb{Z}/p$.

Lemma 7.19. *The homomorphism q_G maps $H^\bullet(G, \mathbb{Z}/p)$ into $H_{\mathfrak{A}}^\bullet(G, \mathbb{Z}/p)$.*

Proof. Let $c \in H^n(G, \mathbb{Z}/p)$ be arbitrary. Then there is an open normal subgroup $N \lhd G$ and a $d \in H^n(G/N, \mathbb{Z}/p)$ such that $c = \pi_N^*(d)$. Let $\phi_N\colon \underline{H}_{\mathfrak{A}}^n(G/N, \mathbb{Z}/p) \to \underline{H}_{\mathfrak{A}}^n(G, N, \mathbb{Z}/p)$ be the map induced by the inclusion functor $\mathfrak{A}(G, N) \to \mathfrak{A}(G/N)$. Clearly $q_G(c) = \mathfrak{a}_N(\phi_N(q_{G/N}(d)))$, and hence the claim holds. □

Theorem 7.20 (Quillen–Scheiderer)**.** *For every profinite group G, the homomorphism*

$$q_G\colon H^\bullet(G, \mathbb{Z}/p) \to H_{\mathfrak{A}}^\bullet(G, \mathbb{Z}/p)$$

is an F-isomorphism.

Proof. This theorem was proved by Quillen when G is finite (see [13, Theorem 7.1 on page 567] which is actually a more general result). At the end of [11] (see 8.6 and 8.7 on pages 279–80) Scheiderer pointed out that there is an easy limit argument to derive the theorem above as a corollary. In fact, he proved that q_G satisfies property (i) in Definition 7.12. We complete his argument by showing (ii) for the convenience of the reader.

Definition 7.21. For every pair M, N of open, normal subgroups of G such that $M \subseteq N$ let $\pi_{M,N}\colon G/M \to G/N$ be the quotient map, and let $\mathfrak{A}(G, M, N)$ denote the image of the functor $\mathfrak{A}(\pi_{M,N})\colon \mathfrak{A}(G/M) \to \mathfrak{A}(G/N)$.

Lemma 7.22. *For every open, normal subgroup $N \lhd G$ there is open, normal subgroup $M \lhd G$ such that $M \subseteq N$ and $\mathfrak{A}(G, M, N) = \mathfrak{A}(G, N)$.*

Proof. This is the Claim on page 280 of [11]. □

Now let $c \in H^n_{\mathfrak{A}}(G, \mathbb{Z}/p)$ be arbitrary, and let $N \lhd G$ be an open normal subgroup such that there is a

$$\underline{d} = \{d_A \in H^\bullet(A, \mathbb{Z}/p) \mid A \in \mathfrak{A}(G,N)\} \in \underline{H}^n_{\mathfrak{A}}(G,N,\mathbb{Z}/p)$$

with the property $c = \mathfrak{a}_N(\underline{d})$. By Lemma 7.22, there is an open, normal subgroup $M \lhd G$ such that $M \subseteq N$ and $\mathfrak{A}(G,M,N) = \mathfrak{A}(G,N)$. For every $A \in \mathfrak{A}(G/M)$, let $\pi_{M,N,A} \colon A \to \pi_{M,N}(A)$ be the map induced by the restriction of $\pi_{M,N}$ onto A. The fact $\mathfrak{A}(G,M,N) = \mathfrak{A}(G,N)$ means that the collection

$$e = \left\{\pi^*_{M,N,A}(d_{\pi_{M,N}(A)}) \in H^\bullet(A,\mathbb{Z}/p) \mid A \in \mathfrak{A}(G/M)\right\}$$

is a well-defined element of $H^n_{\mathfrak{A}}(G/M, \mathbb{Z}/p) = \underline{H}^n_{\mathfrak{A}}(G/M, \mathbb{Z}/p)$. Applying Quillen's theorem to e we get that there is a positive integer m and an $f \in H^n(G/M, \mathbb{Z}/p)$ such that $e^{p^m} = q_{G/M}(f)$. Let $\phi_M \colon \underline{H}^n_{\mathfrak{A}}(G/M, \mathbb{Z}/p) \to \underline{H}^n_{\mathfrak{A}}(G, M, \mathbb{Z}/p)$ be the map induced by the inclusion functor $\mathfrak{A}(G,M) \to \mathfrak{A}(G/M)$ as above. Then $\mathfrak{a}_M(\phi_M(e)) = \mathfrak{a}_N(\underline{d})$, and hence

$$c^{p^m} = \mathfrak{a}_M(\phi_M(e))^{p^m} = \mathfrak{a}_M(\phi_M(e^{p^m})) = \mathfrak{a}_M(\phi_M(q_{G/M}(f))) = q_G(\pi^*_N(f)).$$

This finishes the proof of Theorem 7.20. □

As a consequence we get the following

Corollary 7.23. *Let G be a cohomologically quasi-Boolean pro-2 group. Then for every $i > 0$, there is a natural homomorphism*

$$\pi_i \colon H^i(G, \mathbb{Z}/2) \to C(\mathcal{X}^*(G), \mathbb{Z}/2)$$

which is an isomorphism for $i > 1$ and surjective for $i = 1$.

Proof. Let $C^\bullet(\mathcal{X}^*(G), \mathbb{Z}/2)$ denote the graded Boolean algebra associated to the Boolean ring $C(\mathcal{X}^*(G), \mathbb{Z}/2)$. By Proposition 7.11, the conditions of Proposition 7.17 apply to G. Hence, by Theorem 7.20, there is an F-isomorphism:

$$\pi_* \colon H^\bullet(G, \mathbb{Z}/2) \to C^\bullet(\mathcal{X}^*(G), \mathbb{Z}/2).$$

This map is zero on the nilradical of $H^\bullet(G,\mathbb{Z}/2)$, so it induces an F-isomorphism:

$$H^\bullet(G,\mathbb{Z}/2)/\mathcal{N}(H^\bullet(G,\mathbb{Z}/2)) \to C^\bullet(\mathcal{X}^*(G), \mathbb{Z}/2) \tag{7.23.1}$$

of graded Boolean algebras by Lemma 7.7, which must be an isomorphism by Lemma 7.13. Since the nilradical of $H^\bullet(G,\mathbb{Z}/2)$ consists of degree one elements, the claim follows. □

8. Proof of the main theorem and some consequences

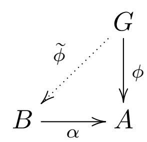
Now we are ready to give the proofs of our main results.

Proof of Theorem 1.6. The implication $(i) \Rightarrow (ii)$ is Theorem 6.6, while the implication $(ii) \Rightarrow (i)$ is Theorem 6.17. We already saw that (ii) trivially implies (iii) in the proof of Theorem 5.4. Now assume that G is the maximal pro-2 quotient of a real projective profinite group H. As explained in [8, Section 10], $H^\bullet(H,\mathbb{Z}/2)$ is the connected sum of a dual algebra and a graded Boolean algebra. The pull-back map $H^\bullet(H,\mathbb{Z}/2) \to H^\bullet(G,\mathbb{Z}/2)$ is an isomorphism by the Rost–Voevodsky norm residue theorem [14], so we get that G is cohomologically quasi-Boolean. Therefore the implication $(iii) \Rightarrow (iv)$ holds. To finish the proof of Theorem 1.6, we show the remaining implication $(iv) \Rightarrow (i)$ in the following

Theorem 8.1. *Every cohomologically quasi-Boolean pro-2 group G is real projective.*

Proof. Since G has an open subgroup without 2-torsion by part (i) of Proposition 7.11, it will be sufficient to show that every real embedding problem for G has a solution. By Proposition 5.2, we need to show that any real 2-embedding problem for G has a solution. In fact we will prove something stronger.

Definition 8.2. For every group G, let $G^{\#}$ denote the set of its conjugacy classes, for every $x \in G$, let $x^{\#} \in G^{\#}$ denote the conjugacy class of x, and, for every homomorphism $h\colon G \to H$ of groups, let $h^{\#}\colon G^{\#} \to H^{\#}$ denote the map on conjugacy classes induced by h. Now let G be a profinite group. An embedding problem with *lifting data* $(\mathbf{E}, f)$ for G is an embedding problem $\mathbf{E}$:



and a continuous map $f\colon \mathcal{X}^*(G) \to \mathcal{X}(B)$ such that $\alpha^{\#} \circ f = \phi^{\#}|_{\mathcal{X}^*(G)}$. A *solution* to this embedding problem with lifting data is a solution $\widetilde{\phi}$ to the embedding problem $\mathbf{E}$ such that $\widetilde{\phi}^{\#}|_{\mathcal{X}^*(G)} = f$.

Proposition 8.3. *Let G be a quasi-Boolean pro-2 group G. Then every 2-embedding problem with lifting data for G has a solution.*

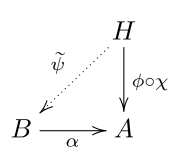
Proof. In order to prove the claim in a first significant case, we need to recall some basic definitions and results.

Definition 8.4. The *kernel*, denoted $\mathrm{Ker}(\mathbf{E})$, of an embedding problem $\mathbf{E}$ as one in Definition 5.1 is the kernel of α. We say that $\mathbf{E}$ is *central* if $\mathrm{Ker}(\mathbf{E})$ lies in the centre of B. In this case the conjugation action of G makes $\mathrm{Ker}(\mathbf{E})$ into a constant abelian G-module. Assume now that the embedding problem $\mathbf{E}$ is central. Let $\widehat{\phi}\colon G \to B$ be a continuous map such that $\alpha \circ \widehat{\phi} = \phi$. Then the map $c\colon G \times G \to \mathrm{Ker}(\mathbf{E})$ given by the rule:

$$c(x, y) = \widehat{\phi}(xy)\widehat{\phi}(y)^{-1}\widehat{\phi}(x)^{-1} \in \mathrm{Ker}(\mathbf{E}), \quad (x, y \in G)$$

is a cocycle, and its cohomology class $o(\mathbf{E}) \in H^2(G, \mathrm{Ker}(\mathbf{E}))$, called the *obstruction class* of $\mathbf{E}$, does not depend on the choice of $\widehat{\phi}$, only on $\mathbf{E}$. Moreover, $\mathbf{E}$ has a solution if and only if $o(\mathbf{E})$ is zero.

Remark 8.5. The obstruction class has the following important naturality property: Let $\mathbf{E}$ be an embedding problem for G as above, and suppose that $\mathbf{E}$ is central. Let $\chi\colon H \to G$ be a continuous homomorphism of profinite groups. Then



is a central embedding problem $\mathbf{E}(\chi)$ for H with the same kernel as $\mathbf{E}$, and we have

$$\chi^*(o(\mathbf{E})) = o(\mathbf{E}(\chi)),$$

where $\chi^*\colon H^\bullet(G, \mathrm{Ker}(\mathbf{E})) \to H^\bullet(H, \mathrm{Ker}(\mathbf{E}))$ is the pull-back map.

Lemma 8.6. *Let G be a quasi-Boolean pro-2 group G. Then every 2-embedding problem with lifting data for G and with a kernel isomorphic to $\mathbb{Z}/2$ has a solution.*

Proof. Let $(\mathbf{E}, f)$ be an embedding problem with lifting data for G as in Definition 8.2, and assume that its kernel is isomorphic to $\mathbb{Z}/2$. Since the automorphism group of the latter is trivial, we get that $\mathbf{E}$ is central. Because $\mathbf{E}$ is equipped with lifting data, it is real, that is, for every subgroup $H \subseteq G$ of order 2 the embedding problem $\mathbf{E}(i_H)$ has a solution, where $i_H \colon H \to G$ is the inclusion map. Therefore, by Remark 8.5, the image of $o(\mathbf{E})$ under the homomorphism:

$$\pi_2 \colon H^2(G, \mathbb{Z}/2) \to C(\mathcal{X}^*(G), \mathbb{Z}/2)$$

is zero. So by Corollary 7.23, the obstruction class $o(\mathbf{E})$ vanishes, and hence $\mathbf{E}$ has a solution.

Let $s \colon G \to B$ be such a solution. Let $r \colon \mathcal{X}^*(G) \to \mathbb{Z}/2 = \mathrm{Ker}(\alpha)$ be the map given by the rule:

$$r(x) = \begin{cases} 0 & \text{, if } s^{\#}(x) = f(x), \\ 1 & \text{, otherwise.} \end{cases}$$

Since $s^{\#} \times f \colon \mathcal{X}^*(G) \to B^{\#} \times B^{\#}$ is continuous with finite image, and $r(x)$ only depends on $s^{\#}(x)$ and $f(x)$ for every $x \in \mathcal{X}^*(G)$, we get that r is continuous. Therefore, by Corollary 7.23, there is a continuous homomorphism $\chi \colon G \to \mathbb{Z}/2 = \mathrm{Ker}(\alpha)$ whose image of under the homomorphism:

$$\pi_1 \colon H^1(G, \mathbb{Z}/2) \to C(\mathcal{X}^*(G), \mathbb{Z}/2)$$

is r. Let $\widetilde{\phi} \colon G \to B$ be the function given by the rule $\widetilde{\phi}(g) = s(g)\chi(g)$. Since it is the product of two continuous functions, $\widetilde{\phi}$ is continuous. Moreover,

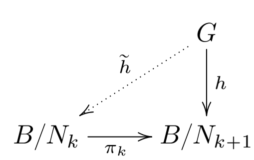
$$\widetilde{\phi}(gh) = s(gh)\chi(gh) = s(g)s(h)\chi(g)\chi(h) = s(g)\chi(g)s(h)\chi(h) = \widetilde{\phi}(g)\widetilde{\phi}(h)$$

using that s, χ are homomorphisms and $\mathrm{Ker}(\alpha)$ is central. Therefore $\widetilde{\phi}$ is a homomorphism. Since $\alpha \circ \widetilde{\phi} = \alpha \circ s = \phi$, we get that $\widetilde{\phi}$ is a solution to $\mathbf{E}$. Now let $y \in \mathcal{Y}^*(G)$ be arbitrary. If $s^{\#}(y^{\#}) = f(y^{\#})$, then $\widetilde{\phi}(y) = s(y)$, and hence $\widetilde{\phi}(y)^{\#} = s(y)^{\#} = s^{\#}(y^{\#}) = f(y^{\#})$. If $s^{\#}(y^{\#}) \neq f(y^{\#})$, then $\widetilde{\phi}(y) \neq s(y)$, so $\widetilde{\phi}(y)$ is the unique element of $\alpha^{-1}(\phi(y))$ different from $s(y)$. Since $\alpha^{-1}(\phi(y))$ contains an element of $f(y^{\#})$, as α is surjective, and this element is not $s(y)$, it must be $\widetilde{\phi}(y)$. So $\widetilde{\phi}(y)^{\#} = f(y^{\#})$ in this case, too. □

Now we are going to show Proposition 8.3 in the general case. Let $(\mathbf{E}, f)$ be an embedding problem with lifting data for G as in Definition 8.2. Since B is a 2-group, it has a filtration by normal subgroups:

$$\{1\} = N_0 \subset N_1 \subset \cdots \subset N_n = \mathrm{Ker}(\alpha)$$

such that the kernel of the quotient map $\pi_k \colon B/N_k \to B/N_{k+1}$ is isomorphic to $\mathbb{Z}/2$ for every $k = 0, 1, \ldots, n-1$. Let $q_k \colon B \to B/N_k$ be the quotient map. Note that it will be sufficient to show that for every continuous homomorphism $h : G \to B/N_{k+1}$ such that $h^{\#}|_{\mathcal{X}^*(G)} = q^{\#}_{k+1} \circ f = \pi^{\#}_k \circ q^{\#}_k \circ f$ the embedding problem $\mathbf{E}_k$:



with lifting data $q_k^{\#} \circ f$ has a solution for every $k = 0, 1, \ldots, n$. Indeed let $r_k \colon B/N_k \to A = B/N_n$ be the quotient map; then we would get by descending induction on the index k that the embedding problem:

$$\begin{array}{ccc} & & G \\ & \overset{\tilde{\phi}}{\swarrow} & \downarrow \phi \\ B/N_k & \xrightarrow[r_k]{} & A \end{array}$$

with lifting data $q_k^{\#} \circ f$ has a solution. The claim is now clear from the case $k = 0$. However $\mathbf{E}_k$ has a kernel isomorphic to $\mathbb{Z}/2$, so $(\mathbf{E}_k, q_k^{\#} \circ f)$ has a solution by Lemma 8.6. □

In order to conclude the proof of Theorem 8.1 it will be sufficient to show that every real 2-embedding problem $\mathbf{E}$ for G as above can be equipped with lifting data. By assumption, for every $x \in \mathcal{X}(A)$ in the image $\mathrm{Im}(\phi^{\#}|_{\mathcal{X}*(G)})$, there is a $y \in \mathcal{X}(B)$ such that $\alpha^{\#}(y) = x$, i.e., there is a section $g \colon \mathrm{Im}(\phi^{\#}|_{\mathcal{X}*(G)}) \to \mathcal{X}(B)$ of the restriction $\alpha^{\#}|_{\mathcal{X}(B)}$. Since g is a map between discrete spaces, it is continuous, therefore the composition $f = g \circ \phi^{\#}|_{\mathcal{X}*(G)}$ is also continuous, and hence $(\mathbf{E}, f)$ is a 2-embedding problem with lifting data. □

Proof of Corollary 1.7. First assume that G is Boolean, i.e., G is isomorphic to $\mathbb{B}(X)$ for some profinite space X. Then it is cohomologically quasi-Boolean by Theorem 1.6, so $H^\bullet(G, \mathbb{Z}/2)$ is the connected sum of a dual algebra $D^\bullet$ and a graded Boolean algebra $B^\bullet$. Assume that $D^\bullet$ is non-trivial, so there there is a non-zero $c \in D^1 \subset \mathrm{Hom}(G, \mathbb{Z}/2)$. Then $c \cup c = 0$ as $D^2 = 0$, so the restriction of c onto every involution in the image of $i_X \colon X \to \mathcal{Y}(\mathbb{B}(X))$ is zero. Therefore, by the universal property of $\mathbb{B}(X)$ of Remark 6.3, the homomorphism corresponding to c is also zero, a contradiction, and hence G is cohomologically Boolean.

Next assume that G is cohomologically Boolean. Then it is quasi-Boolean by Theorem 1.6, so G is the free product of a free pro-2 group F and a Boolean group $\mathbb{B}(X)$ for a profinite space X. Assume that F is non-trivial; then there is a non-zero $c \in \mathrm{Hom}(F, \mathbb{Z}/2)$. Let $\pi_1 \colon G \to F$ be the surjective homomorphism supplied by the universal property of free pro-2 products, and let $\overline{c}$ be the composition of π_1 and c. Then $c \cup c = 0$, and hence $\overline{c} \cup \overline{c} = 0$. Since $H^\bullet(G, \mathbb{Z}/2)$ is a graded Boolean algebra, this implies that $\overline{c}$ is zero, a contradiction. Therefore G is Boolean. □

Remark 8.7. Let G be a Boolean group and let $f \colon G \to \mathbb{Z}/2$ be a quasi-canonical homomorphism. By Remark 7.9, the homomorphism f is characterised by the property that, for every $n > 0$ and $c \in H^n(G, \mathbb{Z}/2)$, we have $c^2 = c \cup k^n$. But $H^\bullet(G, \mathbb{Z}/2)$ is a graded Boolean algebra by Corollary 1.7, and hence f is unique. Therefore, it is justified to call it the canonical homomorphism of the Boolean group G.

Proof of Theorem 1.8. By assumption, G is isomorphic to $F(Y') *_2 \mathbb{B}(X')$ for a set Y' and a profinite space X'. We are actually going to show something stronger, namely, that the profinite spaces X and X' are homeomorphic, and the sets Y' and Y are bijective. By Theorem 6.11, the profinite spaces X' and $\mathcal{X}^*(G)$ are homeomorphic, and, as we saw in the proof of Corollary 7.23, the graded Boolean algebras $B^\bullet$ and $C^\bullet(\mathcal{X}^*(G), \mathbb{Z}/2)$ are isomorphic (see (7.23.1)). Therefore, by Stone duality Theorem 2.10, the profinite spaces X and X' are homeomorphic, too. Using Notation 6.16, we have $G_* = F(Y')_* \oplus \mathbb{B}(X')_*$. Hence we have $H^1(G, \mathbb{Z}/2) = H^1(F(Y'), \mathbb{Z}/2) \oplus H^1(\mathbb{B}(X'), \mathbb{Z}/2)$. But $H^1(G, \mathbb{Z}/2) = D^1 \oplus B^1$, as since $H^1(\mathbb{B}(X'), \mathbb{Z}/2) \cong B^1$ by the above, we get that $H^1(F(Y'), \mathbb{Z}/2) \cong D^1$. Therefore, $\mathbb{Z}/2^{\oplus Y'} \cong \mathbb{Z}/2^{\oplus Y}$, and hence there is a bijection between Y' and Y. □

References

[1] M. Atiyah and I. Macdonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, Addison-Wesley, 1969.

[2] D. Gildenhuys and L. Ribes, *A Kurosh subgroup theorem for free Pro-$\mathcal{C}$-products of pro-$\mathcal{C}$-groups*, Trans. Amer. Math. Soc. **186** (1973), 309–329.

[3] A. Gleason, *Projective topological spaces*, Illinois J. Math. **2** (1958), 482–489.

[4] D. Haran, *On the cohomological dimension of Artin–Schreier structures*, J. Algebra **156** (1993), 219–236.

[5] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field*, Ann. Sc. Norm. Sup. Pisa **12** (1985), 449–489.

[6] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of* $\mathbb{R}(t)$, J. Pure Appl. Algebra **37** (1985), 155–165.

[7] F. Morel, *Ensembles profinis simpliciaux et interprétacion géometrique du foncteur T*, Bull. Soc. math. France **124** (1996), 347–373.

[8] A. Pál and G. Quick, *Real projective groups are formal*, arXiv:2206.14645v2, 38 pages.

[9] L. Positselski, *Koszulity of cohomology = $K(\pi, 1)$-ness + quasi-formality*, J. Algebra **483** (2017), 188–229.

[10] C. Scheiderer, *Real and étale cohomology*, Lecture Notes in Mathematics **1588**, Springer, Berlin-New York, 1994.

[11] C. Scheiderer, *Farell cohomology and Brown theorems for profinite groups*, Manuscripta Math. **91** (1996), 247–281.

[12] J.-P. Serre, *Galois cohomology*, Springer Monographs in Mathematics, Springer, Berlin-New York, 1997.

[13] D. Quillen, *The spectrum of an equivariant cohomology ring: I*, Ann. Math. **94** (1971), 549–572.

[14] V. Voevodsky, *Motivic cohomology with $\mathbb{Z}/2$-coefficients*, Publ. Math. Inst. Hautes Études Sci. **98** (2003), 59–104.

Department of Mathematics, 180 Queen's Gate, Imperial College, London, SW7 2AZ, United Kingdom
Email address: a.pal@imperial.ac.uk

Department of Mathematical Sciences, NTNU, NO-7491 Trondheim, Norway
Email address: gereon.quick@ntnu.no