CONFLUENTES MATHEMATICI

Pierre-Emmanuel CAPRACE and Pierre DE LA HARPE

Groups with irreducibly unfaithful subsets for unitary representations

Tome 12, n° 1 (2020), p. 31-68.

<http://cml.centre-mersenne.org/item?id=CML_2020__12_1_31_0>

Confluentes Math.
12, 1 (2020) 31-68

GROUPS WITH IRREDUCIBLY UNFAITHFUL SUBSETS FOR UNITARY REPRESENTATIONS

PIERRE-EMMANUEL CAPRACE AND PIERRE DE LA HARPE

Abstract. Let G be a group. A subset $F \subset G$ is called irreducibly faithful if there exists an irreducible unitary representation π of G such that $\pi(x) \neq \mathrm{id}$ for all $x \in F \smallsetminus \{e\}$. Otherwise F is called irreducibly unfaithful. Given a positive integer n, we say that G has Property $\mathcal{P}(n)$ if every subset of size n is irreducibly faithful. Every group has $\mathcal{P}(1)$, by a classical result of Gelfand and Raikov. Walter proved that every group has $\mathcal{P}(2)$. It is easy to see that some groups do not have $\mathcal{P}(3)$.

We provide a complete description of the irreducibly unfaithful subsets of size n in a countable group G (finite or infinite) with Property $\mathcal{P}(n-1)$: it turns out that such a subset is contained in a finite elementary abelian normal subgroup of G of a particular kind. We deduce a characterization of Property $\mathcal{P}(n)$ purely in terms of the group structure. It follows that, if a countable group G has $\mathcal{P}(n-1)$ and does not have $\mathcal{P}(n)$, then n is the cardinality of a projective space over a finite field.

A group G has Property $\mathcal{Q}(n)$ if, for every subset $F \subset G$ of size at most n, there exists an irreducible unitary representation π of G such that $\pi(x) \neq \pi(y)$ for any distinct x, y in F. Every group has $\mathcal{Q}(2)$. For countable groups, it is shown that Property $\mathcal{Q}(3)$ is equivalent to $\mathcal{P}(3)$, Property $\mathcal{Q}(4)$ to $\mathcal{P}(6)$, and Property $\mathcal{Q}(5)$ to $\mathcal{P}(9)$. For $m, n \geqslant 4$, the relation between Properties $\mathcal{P}(m)$ and $\mathcal{Q}(n)$ is closely related to a well-documented open problem in additive combinatorics.

Fidèle, infidèle ?
Qu'est-ce que ça fait,
Au fait ?
Puisque toujours dispose à couronner mon zèle
Ta beauté sert de gage à mon plus cher souhait.
(Paul Verlaine, *Chansons pour elle*, 1891.)

Contents

Math. classification: 43A65, 22D10.
Keywords: Countable group, unitary representation, irreducible representation, faithful representation, factor representation, finite elementary abelian normal subgroup.

1. Introduction

1.1. **Irreducibly unfaithful subsets.** A subset F of a group G is called **irreducibly faithful** if there exists an irreducible unitary representation π of G in a Hilbert space $\mathcal{H}$ such that $\pi(x) \neq \mathrm{id}$ for all $x \in F$ with $x \neq e$. (We denote by e the identity element of the group, and by id the identity operator on the space $\mathcal{H}$.) Otherwise F is called **irreducibly unfaithful**. For $n \geqslant 1$, we say that G has **Property** $\mathcal{P}(n)$ if every subset of size at most n is irreducibly faithful.

Every group has Property $\mathcal{P}(1)$*:* this is the particular case for discrete groups of a foundational result established for all locally compact groups and continuous unitary representations by Gelfand and Raikov [14] (see also the exposition in [10, 13.6.6], and another proof for second-countable locally compact groups in [23, Pages 109–110]).

The following refinement of the Gelfand–Raikov Theorem is due to Walter: *Every group has Property* $\mathcal{P}(2)$*.* In other words, *in a group, every couple is irreducibly faithful* (!). See [35, Proposition 2], as well as [30] and [31, 1.8.7].

It is clear that Property $\mathcal{P}(3)$ does not hold for all groups. Indeed, Klein's Vierergruppe, the direct product $C_2 \times C_2$ of two copies of the group of order 2, does not have $\mathcal{P}(3)$.

The property $\mathcal{P}(n)$ has been considered by Walter [35] for $n \leqslant 3$ (but without our terminology). As far as we know, it has not been considered for larger values of n.

The first goal of this article is to characterize groups with $\mathcal{P}(n)$ for all $n \geqslant 3$. We focus on *countable groups*, i.e., groups that are either finite or countably infinite. What follows can be seen as a quantitative refinement of results in [2], quoted in Theorem 2.2 below.

Before stating our main result, we need the following preliminaries. Let $\mathbf{k}$ be a finite field of order q; in case $q = p$ is a prime, we write $\mathbf{F}_p$ instead of $\mathbf{k}$. For a group G, we denote by $\mathbf{k}[G]$ its group algebra over $\mathbf{k}$. We recall that any abelian group U whose exponent is a prime p carries the structure of a vector space over $\mathbf{F}_p$, which is invariant under all group automorphisms of U. In other words, the group structure on U canonically determines an $\mathbf{F}_p$-linear structure. In particular, an abelian normal subgroup U of exponent p in a group G may be viewed, in a canonical way, as an $\mathbf{F}_p[G]$-module. Moreover, U is minimal as a normal subgroup of G if and only if U is simple as an $\mathbf{F}_p[G]$-module. (We rather use W instead of U when such a simple module appears below, and V for direct sums of particular numbers of copies of simple modules.)

Let G be a group and U an $\mathbf{F}_p[G]$-module. The **centralizer** of U is the $\mathbf{F}_p$-algebra

$$\mathcal{L}_{\mathbf{F}_p[G]}(U) = \{\alpha \in \mathrm{End}_{\mathbf{F}_p}(U) \mid g.\alpha(u) = \alpha(g.u) \text{ for all } g \in G,\ u \in U\}.$$

If W is a simple $\mathbf{F}_p[G]$-module, Schur's lemma ensures that $\mathcal{L}_{\mathbf{F}_p[G]}(W)$ is a division algebra over $\mathbf{F}_p$ [5, § 4, Proposition 2]. If in addition W is finite, then the algebra $\mathcal{L}_{\mathbf{F}_p[G]}(W)$ is a finite field extension of $\mathbf{F}_p$, by Wedderburn's Theorem [5, § 11, no. 1]. In this case, W is a vector space over $\mathcal{L}_{\mathbf{F}_p[G]}(W)$, and the dimension of W over $\mathcal{L}_{\mathbf{F}_p[G]}(W)$ is the quotient of $\dim_{\mathbf{F}_p}(W)$ by the degree of the extension $\mathcal{L}_{\mathbf{F}_p[G]}(W)$ of $\mathbf{F}_p$.

For example, consider a finite field extension $\mathbf{k}$ of $\mathbf{F}_p$, a positive integer m, the vector space $W = \mathbf{k}^m$, and the general linear group $\mathrm{GL}(W) = \mathrm{GL}_m(\mathbf{k})$ together with its natural action on W. View W as a vector space over $\mathbf{F}_p$, and as an $\mathbf{F}_p[\mathrm{GL}(W)]$-module. Then $\mathcal{L}_{\mathbf{F}_p[\mathrm{GL}(W)]}(W)$ and $\mathbf{k}$ can be identified, and $\dim_{\mathbf{k}}(W) = m$.

Our main result reads as follows; the proof is in Section 4.

THEOREM 1.1. — *Let G be a countable group and n a positive integer. The following assertions are equivalent.*

(1) G does not have $\mathcal{P}(n)$.

(2) There exist a prime p, a finite normal subgroup V in G which is an elementary abelian p-group, and a finite simple $\mathbf{F}_p[G]$-module W, such that the following properties hold, where $\mathbf{k}$ denotes the centralizer field $\mathcal{L}_{\mathbf{F}_p[G]}(W)$, $m = \dim_{\mathbf{k}}(W)$, and $q = |\mathbf{k}|$:

(i) V is isomorphic to the direct sum of $m+1$ copies of W, as an $\mathbf{F}_p[G]$-module;

(ii) q is a power of p and $q^m + q^{m-1} + \cdots + q + 1 \leqslant n$.

Notice that the inequality $q^m+q^{m-1}+\cdots+q+1 \geqslant 3$ always holds, since $q \geqslant p \geqslant 2$ and $m \geqslant 1$. Therefore, in the particular cases of $n = 1$ and $n = 2$, Theorem 1.1 recovers for countable groups the results of Gelfand–Raikov and Walter quoted above. In the particular case of $n = 3$, the theorem shows that the only obstruction to $\mathcal{P}(3)$ can be expressed in terms of Klein's Vierergruppe:

COROLLARY 1.2. — *A countable group has $\mathcal{P}(3)$ if and only if its centre does not contain any subgroup isomorphic to $C_2 \times C_2$.*

Proof. — For $n = 3$, we have $p = q = 2$ and $m = 1$ in (2) of Theorem 1.1. Hence $V = W \oplus W$ is an $\mathbf{F}_2[G]$-module of dimension 2 over $\mathbf{F}_2$. Moreover, the action of G is trivial on W, therefore also on V. This means that, as a normal subgroup of G, the group V is central. □

COROLLARY 1.3. — *Let n be a positive integer and G a countable group. Assume that every minimal finite abelian normal subgroup of G is central.*

Then G does not have $\mathcal{P}(n)$ if and only if G contains a central subgroup isomorphic to $C_p \times C_p$ for some prime $p \leqslant n-1$.

In the following proof, and later, we denote by $\mathbf{T}$ the group of complex numbers of modulus one. Recall that, for any irreducible unitary representation π of a group G with centre Z on a Hilbert space $\mathcal{H}$, there exists by Schur's Lemma a unitary character $\chi : Z \to \mathbf{T}$ such that $\pi(g) = \chi(g)\mathrm{id}$ for every $g \in Z$.

Proof. — Suppose that G does not have Property $\mathcal{P}(n)$. Let p be a prime and V, W as in Assertion (2) of Theorem 1.1. Since the action by conjugation of G on minimal finite abelian normal subgroups is trivial by hypothesis, the $\mathbf{F}_p[G]$-module W, which is simple, is of dimension 1 over $\mathbf{F}_p$. With the notation of Theorem 1.1, this implies that $m = 1$ and $\mathbf{k} = \mathbf{F}_p$. It follows that $V = W \oplus W \cong C_p \times C_p$.

Conversely, if G contains a central subgroup V isomorphic to $C_p \times C_p$ for some prime $p \leqslant n-1$, consider a subset F of G of size $p+1$ containing a generator of each of the $p+1$ non-trivial cyclic subgroups of V. As recalled just before the present proof, every irreducible unitary representation of G provides a unitary

character $\chi : C_p \times C_p \to \mathbf{T}$. Since every finite subgroup of $\mathbf{T}$ is cyclic, we have $F \cap \mathrm{Ker}\chi \not\subset \{e\}$, hence F is irreducibly unfaithful. □

Example 1.4. — There are several classes of groups which have the property that "every minimal finite abelian normal subgroup is central":

(1) Torsion-free groups have the property.
(2) Icc-groups, that is infinite groups in which all conjugacy classes distinct from $\{e\}$ are infinite, have the property.
(3) A group G without non-trivial finite quotient has the property. Indeed, if N is a finite normal subgroup of G, the action by conjugation of G on N provides a homomorphism from G to the group of automorphisms of N; since this homomorphism is trivial by hypothesis, N is central.
(4) In a connected algebraic group G, a Zariski-dense subgroup Γ has the property. To check this, it suffices to show that the FC-centre $\mathrm{FC}(\Gamma)$ of Γ coincides with the centre of Γ. Recall that the **FC-centre** of a group is the characteristic subgroup consisting of elements which have a finite conjugacy class; the FC-centre of a group contains every finite normal subgroup.

    Recall that the centraliser of an element in an algebraic group is a Zariski-closed subgroup. Given $\gamma \in \mathrm{FC}(\Gamma)$, the centralizer $C_G(\gamma)$ is Zariski-closed and contains a finite index subgroup of Γ. Since Γ is Zariski-dense, it follows that $C_G(\gamma)$ is of finite index in G. Therefore $C_G(\gamma) = G$ since G is connected. Hence γ is in the centre $Z(G)$ of G. It follows that $\gamma \in \Gamma \cap Z(G) = Z(\Gamma)$. This shows that $\mathrm{FC}(\Gamma)$ is central in Γ, and consequently that every finite normal subgroup of Γ is central.

    In particular, this applies to all lattices in connected semi-simple groups over non-discrete locally compact fields without compact factors, by the Borel Density Theorem.
(5) A nilpotent group has the property, because any non-trivial normal subgroup of a nilpotent group has a non-trivial intersection with the centre [4, Chap. I, § 6, no. 3].

Theorem 1.1 also has the following immediate consequence:

Corollary 1.5. — *Let n be an integer, $n \geqslant 2$. Suppose that there is no prime power q and integer $m \geqslant 1$ such that $n = q^m + q^{m-1} + \cdots + q + 1$.*
Every countable group that has $\mathcal{P}(n-1)$ also has $\mathcal{P}(n)$.

When $n = q^m + q^{m-1} + \cdots + q + 1$, we have the following.

Example 1.6. — Consider a prime p, a power q of p, an integer $m \geqslant 1$, a field $\mathbf{k}$ of order q, the vector space $W = \mathbf{k}^m$, and the group $\mathrm{GL}(W) = \mathrm{GL}_m(\mathbf{k})$. Let $V_0, V_1, \ldots, V_m$ be $m+1$ copies of W. The group $\mathrm{GL}(W)$ acts diagonally on $V := \bigoplus_{i=0}^m V_i$. Since V is an elementary abelian p-group, it can be viewed as an $\mathbf{F}_p[\mathrm{GL}(W)]$-module. Define the semi-direct product group

$$G_{(q,m)} = \mathrm{GL}(W) \ltimes V.$$

Let N be a normal subgroup of $G_{(q,m)}$. Assume that $N \cap V = \{e\}$. On the one hand, N commutes with V, hence acts trivially on V by conjugation. On the other hand, the triviality of $N \cap V$ implies that N maps injectively in the quotient $G_{(q,m)}/V \cong \mathrm{GL}(W)$, whose conjugation action on V is faithful. Hence

$N = \{e\}$. This shows that every non-trivial normal subgroup of $G_{(q,m)}$ has a non-trivial intersection with V. In particular, every minimal normal subgroup of $G_{(q,m)}$ is contained in V, and thus is abelian. Hence it corresponds to a simple $\mathbf{F}_p[G_{(q,m)}]$-submodule of V. Therefore, every minimal abelian normal subgroup of $G_{(q,m)}$ is isomorphic to W as an $\mathbf{F}_p[G_{(q,m)}]$-module.

We now set $n = q^m + q^{m-1} + \cdots + q + 1$. Then Theorem 1.1 implies that $G_{(q,m)}$ has Property $\mathcal{P}(n-1)$ but not $\mathcal{P}(n)$.

Notice that the group $G_{(q,1)}$ is the semi-direct product $\mathbf{k}^\times \ltimes (\mathbf{k} \oplus \mathbf{k})$, where $\mathbf{k}$ is a field of order q. The group $G_{(2,1)}$ is Klein's Vierergruppe. The group $G_{(3,1)}$ appears in [7, Note F] as an example of a finite group with trivial centre which does not admit any faithful irreducible representation. The group $G_{(4,1)}$ appears in [20, Problem 2.19] for the same reason. Our groups $G_{(q,1)}$ appear in the historical review section of [34], where they are denoted by $G(2, q)$. The tables

q	2	3	4	5	7	8	9	11
$\lvert G_{(q,1)}\rvert$	4	18	48	100	294	448	649	1110

and

q	2	3
$\lvert G_{(q,2)}\rvert$	384	34992

give the orders of the 8 smallest groups $G_{(q,1)}$ and the 2 smallest groups $G_{(q,2)}$.

Numerical note 1.7. — The sequence of positive integers which are of the form $q^m + q^{m-1} + ... + q + 1$ for some prime power q and positive integer m is Sequence A258777 of [25]; the first 25 terms are

$$3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 20, 21, 24, 26, 28, 30, 31, 32, 33, 38, 40$$

(note that we start with 3 whereas A258777 starts with 1). The first 10 000 terms appear on `https://oeis.org/A258777/b258777.txt` where the last term is 101 808. For terms below 100, the largest gap is between the 45th term and the 46th term, i.e., between 91 and 98; it follows from Corollary 1.5 that a group with Property $\mathcal{P}(91)$ has necessarily Property $\mathcal{P}(97)$.

It is a consequence of the Prime Number Theorem that the asymptotic density of this sequence is 0. In other words, if for $k \geqslant 1$ we denote by $R(k)$ the number of positive integers less than k which are terms of this sequence, then $\lim_{k\to\infty} R(k)/k = 0$. See [26, Appendix B].

Note also that the 21st term, which is 31, can be written in two ways justifying its presence in the sequence: $31 = 2^4 + 2^3 + 2^2 + 2 + 1 = 5^2 + 5 + 1$. It is a conjecture that there are no other terms with this property, but this is still open. Indeed, conjecturally, the Goormaghtigh equation

$$\frac{x^M - 1}{x - 1} = \frac{y^N - 1}{y - 1}$$

has no solution in integers x, y, M, N such that $x, y \geqslant 2$, $x \neq y$, and $M, N \geqslant 3$, except $31 = \frac{2^5-1}{2-1} = \frac{5^2-1}{5-1}$ and $8191 = \frac{2^{13}-1}{2-1} = \frac{90^3-1}{90-1}$. We are grateful to Emmanuel Kowalski and Yann Bugeaud for information on the relevant literature, which includes [27, 15, 8, 18].

In a group which has $\mathcal{P}(n-1)$ and not $\mathcal{P}(n)$, irreducibly unfaithful subsets of size n are contained in finite normal subgroups of a very particular kind, described in Theorem 4.5. Here is a partial statement of this theorem:

PROPOSITION 1.8. — *Let G be a countable group and n a positive integer. Assume that G has Property $\mathcal{P}(n-1)$. Let F be a finite subset of G of size n which is irreducibly unfaithful, and let U denote the smallest normal subgroup of G containing F.*

Then there exists a prime p such that U is a finite elementary abelian p-group, and U is contained in the mini-socle $\mathrm{MA}(G)$ *(as defined in Subsection 2.1 below).*

1.2. **Irreducibly faithful groups.** A group is **irreducibly faithful** if it has a faithful irreducible unitary representation. Clearly, an irreducibly faithful group G has $\mathcal{P}(n)$ for all $n \geqslant 1$. The problem of characterizing finite groups which are irreducibly faithful has been addressed by Burnside in [7, Note F], where a sufficient condition is given. Since then, various papers have been published on the subject, providing various answers to Burnside's question; see the historical review in [34].

Gaschütz [13] obtained a short proof of the following simple criterion: *a finite group G admits a faithful irreducible representation over an algebraically closed field of characteristic* 0 *if and only if the abelian part of the socle of G is generated by a single conjugacy class*. For unitary representations, this result has been extended to the class of all countable groups in [2, Theorem 2]; see Subsection 2.1 below. As a consequence of Theorem 1.1, we shall obtain the following supplementary characterization (see also Item (iv) in Corollary 5.2).

COROLLARY 1.9. — *For a countable group G, the following conditions are equivalent:*

(i) G has a faithful irreducible unitary representation.
(ii) G has $\mathcal{P}(n)$ for all $n \geqslant 1$.
(iii) For any prime p, the group G does not contain any finite abelian normal subgroup V of exponent p with the following properties: there exists a finite simple $\mathbf{F}_p[G]$-module W, with associated centralizer $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$ and dimension $m = \dim_{\mathbf{k}}(W)$, such that V is isomorphic as an $\mathbf{F}_p[G]$-module to the direct sum of $m+1$ copies of W.

In the case of finite groups, the equivalence between (i) and (ii) is trivial, while the equivalence between (i) and (iii) is due to Akizuki (see [33, Page 207]).

Let G be a countable group in which every minimal finite abelian normal subgroup is central (see Corollary 1.3). For such a group, Condition (iii) above can be reformulated as follows.

(iii′) The group G does not contain any central subgroup isomorphic to $C_p \times C_p$ for some prime p.

For uncountable groups, some of the equivalences of Corollary 1.9 may fail. See Remark 1.13.

1.3. **Abelian groups.** Corollary 1.3 applies in particular to countable abelian groups. The following Proposition 1.11 shows that the conclusion holds for all abelian groups, countable or not. Our proof does not rely on Theorem 1.1, but uses the following result of Mira Bhargava, which is Theorem 4 of [3].

THEOREM 1.10 (Mira Bhargava). — *For any group G and any natural number n, the following conditions are equivalent:*

(i) G is the union of n proper normal subgroups.

(ii) G has a quotient isomorphic to $C_p \times C_p$, for some prime $p \leqslant n-1$.

PROPOSITION 1.11. — *Let n be a positive integer and let G be an abelian group. Then G does not have $\mathcal{P}(n)$ if and only if G contains a subgroup isomorphic to $C_p \times C_p$ for some prime $p \leqslant n-1$.*

Proof. — Assume that G does not have Property $\mathcal{P}(n)$. Let $F \subset G \smallsetminus \{e\}$ be an irreducibly unfaithful subset of G of size $\leqslant n$. Let $\widehat{G}$ be the Pontryagin dual of G, namely the group of all unitary characters $G \to \mathbf{T}$. For each $x \in F$, let $H_x = \{\chi \in \widehat{G} \mid \chi(x) = 1\}$; it is a subgroup of $\widehat{G}$. Since G has $\mathcal{P}(1)$, we have $H_x \neq \widehat{G}$. Since F is irreducibly unfaithful we have $\widehat{G} = \bigcup_{x \in F} H_x$. Since $\widehat{G}$ is abelian, every subgroup is normal, and Theorem 1.10 ensures that $\widehat{G}$ maps onto $C_p \times C_p$, for some prime $p \leqslant |F| - 1 \leqslant n-1$. By duality (see [6, chap. II, § 1, no 7, Th. 4]), it follows that G contains a subgroup isomorphic to the dual of $C_p \times C_p$, i.e., a subgroup isomorphic to $C_p \times C_p$ itself.

The proof of the converse implication is as in the proof of Corollary 1.3. □

It is easy to characterize abelian groups having faithful unitary characters, i.e., having faithful irreducible unitary representations. We denote by $\mathfrak{c}$ the cardinality of the continuum, i.e., of $\mathbf{T}$.

PROPOSITION 1.12. — *For an abelian group G, the following conditions are equivalent:*

(i) G has a faithful unitary character, i.e., G is isomorphic to a subgroup of $\mathbf{T}$.

(ii) The cardinality of G is at most $\mathfrak{c}$, and no subgroup of G is isomorphic to $C_p \times C_p$, for any prime p.

For a proof, see Subsection 2.6.

Remark 1.13. — Corollary 1.9 does not extend to groups of cardinality larger than $\mathfrak{c}$. Indeed, by Proposition 1.11, any torsion-free abelian group has $\mathcal{P}(n)$ for all $n \geqslant 0$ (Condition (ii) of Corollary 1.9), but cannot be isomorphic to a subgroup of $\mathbf{T}$ when its cardinality is larger than $\mathfrak{c}$ (negation of Property (i) of Corollary 1.9).

We have not been able to decide whether Conditions (i) and (ii) of Corollary 1.9 are equivalent for all groups of cardinality at most $\mathfrak{c}$. They are for abelian groups of cardinality at most $\mathfrak{c}$, this is Proposition 1.12.

Conditions (ii) and (iii) of Corollary 1.9 are equivalent for any abelian group, this is Proposition 1.11.

1.4. **Irreducible versus factor representations.** Recall that two unitary representations π, π' of a group G are called **disjoint** if there do not exist non-zero subrepresentations ρ of π and ρ' of π' which are equivalent. A unitary representation π of a group G is called a **factor representation** (or a **primary representation**) if it cannot be decomposed as the direct sum of two disjoint subrepresentations. Equivalently the unitary representation π is a factor representation if the von Neumann algebra generated by $\pi(G)$ is a factor. Every irreducible unitary representation is a factor representation. The direct sum of several copies of a given irreducible unitary representation is an example of a factor representation which is

not irreducible. However, some factor representations do not contain any irreducible subrepresentations. The notion of factor representation plays a key role in the theory of unitary representations on infinite-dimensional Hilbert spaces, see [10] and [23]. We record here the following observation, which implies that the results above remain unchanged if one replaces the class of irreducible unitary representations by the larger class of factor representations (proof in Subsection 2.4).

PROPOSITION 1.14. — *Let G be a countable group. For any factor representation π of G, there is an irreducible unitary representation σ of G such that* $\mathrm{Ker}(\sigma) = \mathrm{Ker}(\pi)$.

In particular, a countable group is irreducibly faithful if and only if it is factorially faithful.

1.5. **Irreducibly injective subsets.** A natural variation on the notion of irreducible (un)faithfulness can be defined as follows.

A subset F of a group G is called **irreducibly injective** if G has an irreducible unitary representation π such that the restriction $\pi|_F$ of π to F is injective. We say that G has Property $\mathcal{Q}(n)$ if every subset of G of size $\leqslant n$ is irreducibly injective. It is a tautology that every group has Property $\mathcal{Q}(1)$. Clearly, an irreducibly faithful group G has $\mathcal{Q}(n)$ for all $n \geqslant 1$.

Though we do not know a characterization of countable groups which have Property $\mathcal{Q}(n)$ for a given n in terms of the group structure (unless $n \leqslant 5$), some of the results we show in Section 5 can be summarized as follows.

PROPOSITION 1.15. — *Let G be a countable group and n a positive integer.*

(i) If G has $P\left(\binom{n}{2}\right)$, then G has $\mathcal{Q}(n)$; in particular, every countable group has $\mathcal{Q}(2)$.
(ii) If G has $\mathcal{Q}(n)$, then G has $\mathcal{P}(n)$.
(iii) G has $\mathcal{Q}(3)$ if and only if G has $\mathcal{P}(3)$.
(iv) G has $\mathcal{Q}(4)$ if and only if G has $\mathcal{P}(6)$.
(v) G has $\mathcal{Q}(5)$ if and only if G has $\mathcal{P}(9)$.

Understanding Property $\mathcal{Q}(n)$ for larger n is closely related to a well-documented open problem in additive combinatorics. See Subsection 5.5.

We are grateful to Yves Cornulier for his comments on a previous version of our text.

2. Irreducibly faithful groups and related facts

2.1. **Feet, mini-feet and Gaschütz' Theorem.** Theorem 2.2 below is due to Gaschütz in the case of finite groups [13] (see also [19, Theorem 42.7]), and has been generalized to countable groups in [2, part of Theorem 2]. First we recall some terminology.

In a group G, a **mini-foot** is a minimal non-trivial finite normal subgroup; we denote by $\mathcal{M}_G$ the set of all mini-feet of G. The **mini-socle** of G is the subgroup $\mathrm{MS}(G)$ generated by $\bigcup_{M\in\mathcal{M}_G} M$; the mini-socle is $\{e\}$ if $\mathcal{M}_G$ is empty, for example $\mathrm{MS}(\mathbf{Z}) = \{0\}$.

Let $\mathcal{A}_G$ denote the subset of $\mathcal{M}_G$ of abelian mini-feet, and $\mathcal{H}_G$ the complement of $\mathcal{A}_G$ in $\mathcal{M}_G$. The **abelian mini-socle** of G is the subgroup $\mathrm{MA}(G)$ generated

by $\bigcup_{A\in\mathcal{A}_G} A$, and the **semi-simple part** $\mathrm{MH}(G)$ of the mini-socle is the subgroup generated by $\bigcup_{H\in\mathcal{H}(G)} H$. For examples of $\mathrm{MA}(G)$, see 2.4 below.

In the context of finite groups, mini-foot and mini-socle are respectively called **foot** and **socle**. We denote the socle of a finite group G by $\mathrm{Soc}(G)$, the abelian socle by $\mathrm{SocA}(G)$, and the semi-simple part of the socle by $\mathrm{SocH}(G)$. The structure of the socle is due to Remak [28].

For general groups, finite or not, the structure of the mini-socle can be described similarly, as follows. We write $\prod'_{\iota\in I} G_\iota$ for the restricted sum of a family of groups $(G_\iota)_{\iota\in I}$; recall that it is the subgroup of the direct product consisting of elements $(g_\iota)_{\iota\in I} \in \prod_{\iota\in I} G_\iota$ such that g_ι is the identity of G_ι for all but finitely many $\iota \in I$.

Proposition 2.1. — *Let G be a group. Let $\mathcal{M}_G$, $\mathrm{MS}(G)$, $\mathcal{A}_G$, $\mathrm{MA}(G)$, $\mathcal{H}_G$ and $\mathrm{MH}(G)$ be as above.*

(1) Every abelian mini-foot A in $\mathcal{A}_G$ is an elementary abelian p-group $(\mathbf{F}_p)^m$ for some prime p and positive integer m.
(2) There exists a subset $\mathcal{A}'_G$ of $\mathcal{A}_G$ such that $\mathrm{MA}(G) = \prod'_{A\in\mathcal{A}'_G} A$. In particular $\mathrm{MA}(G)$ is abelian.
(3) Every non-abelian mini-foot H in $\mathcal{H}_G$ is a direct product of a finite number of isomorphic non-abelian simple groups, conjugate with each other in G.
(4) $\mathrm{MH}(G)$ is the restricted sum $\prod'_{H\in\mathcal{H}_G} H$ of the mini-feet in $\mathcal{H}_G$.
(5) $\mathrm{MS}(G)$ is the direct product $\mathrm{MA}(G) \times \mathrm{MH}(G)$.
(6) Each of the subgroups $\mathrm{MS}(G)$, $\mathrm{MA}(G)$, $\mathrm{MH}(G)$ is characteristic (in particular normal) in G.
(7) Let $r : G \twoheadrightarrow Q$ be a surjective homomorphism of G onto a group Q. Then, for every mini-foot X of G, either $r(X)$ is trivial or $r(X)$ is a mini-foot of Q. In particular r maps $\mathrm{MA}(G)$ [respectively $\mathrm{MH}(G)$, $\mathrm{MS}(G)$] to a subgroup of $\mathrm{MA}(Q)$ [respectively $\mathrm{MH}(Q)$, $\mathrm{MS}(Q)$] which is normal in Q.

We refer to [2, Proposition 1] for the proof.

The next result is a slight reformulation of the equivalence between (i) and (iv) in [2, Theorem 2].

Theorem 2.2. — *For a countable group G, the following assertions are equivalent.*

(i) G has a faithful irreducible unitary representation.
(ii) Every finite normal subgroup of G contained in the abelian mini-socle is generated by a single conjugacy class.

This result is a crucial tool for the proof of Theorem 1.1. Moreover, we shall also need subsidiary facts that we will extract from [2]. They will be presented in Section 2.4 below.

2.2. **On characteristic subgroups that are directed unions of finite normal subgroups.** The next lemma, whose straightforward proof is left to the reader, ensures that every group has a unique largest normal subgroup that is the directed union of all its finite normal subgroups [respectively all its soluble finite normal subgroups]. In particular these subgroups are characteristic.

For an element $g \in G$ and a subset $F \subset G$, we denote by $\langle\langle g\rangle\rangle_G$ the normal subgroup of G generated by $\{g\}$, and by $\langle\langle F\rangle\rangle_G$ that generated by F.

LEMMA 2.3. — *Let G be a group.*

(i) Let k be a positive integer and $N_1, \dots, N_k$ finite normal subgroups of G. The subgroup of G generated by $\bigcup_{j=1}^{k} N_j$ is the product $N_1 N_2 \dots N_k$, in particular it is a finite normal subgroup of G.

(ii) The subset

$$\mathrm{W}(G) = \{g \in G \mid \text{the normal subgroup } \langle\langle g \rangle\rangle_G \text{ is finite}\}$$

is a characteristic subgroup of G, and is the directed union of all finite normal subgroups of G.

(iii) The subset

$$\mathrm{Fsol}(G) = \{g \in G \mid \text{the normal subgroup } \langle\langle g \rangle\rangle_G \text{ is finite and soluble}\}$$

is a characteristic subgroup of G, and is the directed union of all soluble finite normal subgroups of G.

The FC-centre $\mathrm{FC}(G)$ has been defined in Example 1.4. The characteristic subgroup $\mathrm{W}(G)$ is the **torsion FC-centre** of G. According to Dicman's Lemma [29, 14.5.7], which ensures that every element of finite order in the FC-centre of G has a finite normal closure, $\mathrm{W}(G)$ is also the set of elements of finite order in $\mathrm{FC}(G)$. The inclusions

$$\mathrm{MA}(G) \leqslant \mathrm{Fsol}(G) \leqslant \mathrm{W}(G) \leqslant \mathrm{FC}(G)$$

and

$$\mathrm{MS}(G) \leqslant \mathrm{W}(G)$$

follow from the definitions.

We illustrate those notions by discussing several examples.

Example 2.4 (Abelian mini-socles and other characteristic subgroups). —

(1) Let p be a prime. In the cyclic group $\mathbf{Z}/p^2\mathbf{Z}$, the abelian socle $\mathbf{Z}/p\mathbf{Z}$ (which is also the socle) is a proper subgroup of $\mathrm{Fsol}(\mathbf{Z}/p^2\mathbf{Z}) = \mathbf{Z}/p^2\mathbf{Z}$.

More generally, for a torsion abelian group G, the abelian mini-socle (which is also the mini-socle) is generated by the elements of prime order, while $\mathrm{Fsol}(G) = G$.

(2) If G is the restricted sum of an infinite family $(G_n)_{n \geqslant 1}$ of soluble finite groups, then $\mathrm{Fsol}(G)$ is the whole group G; note that $\mathrm{Fsol}(G)$ is soluble if and only if the supremum over all n of the derived length of G_n is finite.

If G is a finite group, then $\mathrm{Fsol}(G)$ is the largest soluble normal subgroup of G, known as the **soluble radical** of G.

(3) Let G be a torsion-free group. Then $\mathrm{W}(G) = \{e\}$, so that $\mathrm{MA}(G) = \mathrm{MS}(G) = \mathrm{Fsol}(G) = \{e\}$.

(4) Let G be a group for which Assertion (2) in Theorem 1.1 holds true. Then, with the notation of this Theorem, the finite normal subgroup V of G is contained in the abelian mini-socle $\mathrm{MA}(G)$.

(5) Let p be a prime, d an integer, $d \geqslant 2$, and $q = p^d$. Let C_q be the cyclic group $\mathbf{Z}/q\mathbf{Z}$; denote by $c_q \in C_q$ the class modulo $q\mathbf{Z}$ of an integer $c \in \mathbf{Z}$. Let H_q be the group of triples $(a, b, c) \in \mathbf{Z} \times \mathbf{Z} \times C_q$ with the multiplication defined by

$$(a, b, c)(a', b', c') = (a + a', b + b', c + c' + (ab')_q).$$

We identify the cyclic group C_p of order p with a subgroup of C_q, and the group C_q to the subgroup of H_q of triples of the form $(0,0,c)$. Observe that all conjugacy classes in H_q are finite, i.e., H_q is its own FC-centre (it is a so-called FC-group). Moreover, the torsion FC-centre $W(H_q)$ coincides with the central subgroup C_q of H_q, and also with $\mathrm{Fsol}(H_q)$. The following five subgroups of H_q constitute a strictly ascending chain of characteristic subgroups:

the trivial group $\{e\}$,
the mini-socle $\mathrm{MS}(H_q) = \mathrm{MA}(H_q) = C_p$,
the group $\mathrm{Fsol}(H_q) = \mathrm{W}(H_q) = C_q$,
the centre $q\mathbf{Z} \times q\mathbf{Z} \times C_q$,
and the group H_q itself.

(6) Let G be a non-trivial nilpotent group. Since minimal normal subgroups of G are central, as recalled in Example 1.4(5), it follows that the mini-socle of G is the subgroup generated by the central elements of prime order.

Recall also that the set $\tau(G)$ of elements of finite order in G is a subgroup of G, indeed a characteristic subgroup, and that $G/\tau(G)$ is torsion-free. When G is moreover finitely generated then $\tau(G)$ is finite [32, Chapter 1, Corollary 10].

It follows that, for a finitely generated nilpotent group G, we have $\mathrm{Fsol}(G) = \mathrm{W}(G) = \tau(G)$, and $\mathrm{W}(G/\mathrm{W}(G)) = \{e\}$. The next example shows that the finite generation condition cannot be deleted.

(7) For each integer $n \geqslant 1$, let

$$H_n = \langle x_n, y_n, z_n \mid x_n^3,\ y_n^3,\ [x_n, y_n]z_n^{-1},\ [x_n, z_n],\ [y_n, z_n]\rangle$$

be a copy of the Heisenberg group over the field $\mathbf{F}_3$. We form the full direct product $P = \prod_{n\geqslant 1} H_n$ and, for each n, we identify x_n, y_n, and z_n with their natural images in P. We also set $x = (x_n)_{n\geqslant 1} \in P$, and define

$$G = \langle x, y_n \mid n \geqslant 1\rangle \leqslant P.$$

The group G is countable, of exponent 3, and nilpotent of class 2. Observe that $z_n = [x, y_n]$ is in G for all $n \geqslant 1$.

For $n \geqslant 1$, let A_n be the group generated by y_n and z_n. It is an abelian 3-group of order 9, which is normal in each of H_n, P, and G. Let A be the subgroup of G generated by $\bigcup_{n\geqslant 1} A_n$, which is normal in G. Observe that G/A is a cyclic group of order 3, generated by the class of x modulo A.

We have $A \leqslant \mathrm{Fsol}(G)$. Indeed, let $t = (t_n)_{n\geqslant 1} \in A$. There exists $C \geqslant 1$ such that $t_n = e$ whenever $n \geqslant C$, so that t is in the normal subgroup $\prod_{n=1}^{C} A_n$ of G, which is finite and abelian. Hence $t \in \mathrm{Fsol}(G)$.

For all $n \geqslant 1$, we have $[x, y_n] = z_n \in G$, so that the normal subgroup $\langle\langle x\rangle\rangle_G$ generated by x contains $\{z_n \mid n \geqslant 1\}$, and thus is infinite. It follows that x is not in the FC-centre of G, and in particular that x is not in $\mathrm{Fsol}(G)$.

We have shown that $A = \mathrm{Fsol}(G) \lneqq G$, and that $G/\mathrm{Fsol}(G)$ is a cyclic group of order 3. In particular, $\mathrm{Fsol}\big(G/\mathrm{Fsol}(G)\big) = G/\mathrm{Fsol}(G) \cong C_3$ is not trivial.

Since $\mathrm{W}(-)$ and $\mathrm{Fsol}(-)$ coincide for G and its quotients (indeed for any soluble group), this can be written $A = \mathrm{W}(G) \lneqq G$ and $\mathrm{W}(G/\mathrm{W}(G)) = G/\mathrm{W}(G) \cong C_3$.

The last example shows that $\mathrm{Fsol}(G)$ does not behave as a *radical* in general, in the sense that $\mathrm{Fsol}(G/\mathrm{Fsol}(G))$ can be non-trivial. Similarly $W(G/\mathrm{W}(G))$ can be non-trivial. However, it is easy to see that, if $\mathrm{W}(G)$ is finite [respectively $\mathrm{Fsol}(G)$ is finite], then $\mathrm{W}(G/\mathrm{W}(G)) = \{e\}$ [respectively $\mathrm{Fsol}(G/\mathrm{Fsol}(G)) = \{e\}$].

The following proposition will be used in Remark 2.19(2).

PROPOSITION 2.5. — *For any two groups G_1 and G_2, we have:*

(i) $\mathrm{MS}(G_1 \times G_2) = \mathrm{MS}(G_1) \times \mathrm{MS}(G_2)$.
(ii) $\mathrm{MA}(G_1 \times G_2) = \mathrm{MA}(G_1) \times \mathrm{MA}(G_2)$.
(iii) $\mathrm{Fsol}(G_1 \times G_2) = \mathrm{Fsol}(G_1) \times \mathrm{Fsol}(G_2)$.
(iv) $\mathrm{W}(G_1 \times G_2) = \mathrm{W}(G_1) \times \mathrm{W}(G_2)$.

Proof. — We identify G_1 and its subgroups with subgroups of $G_1 \times G_2$, and similarly for G_2 and its subgroups. For $j \in \{1, 2\}$, we denote by e_j the neutral element of G_j and by $r_j : G_1 \times G_2 \twoheadrightarrow G_j$ the canonical projection.

(i) The inclusion $\mathrm{MS}(G_1) \times \mathrm{MS}(G_2) \leqslant \mathrm{MS}(G_1 \times G_2)$ is straightforward, because any minimal non-trivial finite normal subgroup of G_1 or of G_2 is a minimal non-trivial finite normal subgroup of $G_1 \times G_2$.

To check the reverse inclusion, consider a minimal non-trivial finite normal subgroup N of $G_1 \times G_2$, and distinguish two cases. First, if $N \leqslant G_1$ or $N \leqslant G_2$, then $N \leqslant \mathrm{MS}(G_1) \times \mathrm{MS}(G_2)$. Second, if $N \not\leqslant G_1$ and $N \not\leqslant G_2$, then N does not contain any element of the form (x_1, e_2) or (e_1, x_2) with $x_1 \neq e_1$ and $x_2 \neq e_2$, by minimality. If N did contain an element $x = (x_1, x_2)$ with x_1 non central in G_1, then N would contain $(y_1, e_2)^{-1}x^{-1}(y_1, e_2)x = ([y_1, x_1], e_2)$ for some $y_1 \in G_1$ such that $[y_1, x_1] \neq e_1$, in contradiction with the hypothesis on N; and similarly for $N \ni (x_1, x_2)$ with x_2 non central in G_2; hence $r_1(N)$ is central in G_1 and $r_2(N)$ is central in G_2. It follows that N is central in $G_1 \times G_2$, and that there exists a prime p such that N is a cyclic group of order p. Hence N is of the form $\langle (x', x'') \rangle_{G_1 \times G_2}$ with x' of order p in G_1 and x'' of order p in G_2. In particular, $N \leqslant \langle\langle x' \rangle\rangle_{G_1} \times \langle\langle x'' \rangle\rangle_{G_2} \leqslant \mathrm{MS}(G_1) \times \mathrm{MS}(G_2)$. It follows that $\mathrm{MS}(G_1 \times G_2) \leqslant \mathrm{MS}(G_2) \times \mathrm{MS}(G_2)$.

An argument of the same kind shows that (ii) holds.

(iv) Given $x \in \mathrm{W}(G_1 \times G_2)$, the normal closure $\langle\langle x \rangle\rangle_{G_1 \times G_2}$ is finite by definition. Therefore $r_j(\langle\langle x \rangle\rangle_{G_1 \times G_2}) = \langle\langle r_j(x) \rangle\rangle_{G_j}$ is finite, so that $r_j(x) \in \mathrm{W}(G_j)$, for $j = 1, 2$. This proves that $x \in \mathrm{W}(G_1) \times \mathrm{W}(G_2)$, hence $\mathrm{W}(G_1 \times G_2) \leqslant \mathrm{W}(G_1) \times \mathrm{W}(G_2)$.

Let $j \in \{1, 2\}$ and $x_j \in G_j$. The group G_{3-j} commutes with x_j, so that $\langle\langle x_j \rangle\rangle_{G_1 \times G_2} = \langle\langle x_j \rangle\rangle_{G_j}$. Assume in addition that $x_j \in \mathrm{W}(G_j)$; then by definition $\langle\langle x_j \rangle\rangle_{G_j}$ is finite, hence $\langle\langle x_j \rangle\rangle_{G_1 \times G_2}$ is finite as well. Therefore $x_j \in \mathrm{W}(G_1 \times G_2)$. This proves that $\mathrm{W}(G_j) \leqslant \mathrm{W}(G_1 \times G_2)$. Therefore $\mathrm{W}(G_1) \times \mathrm{W}(G_2) \leqslant \mathrm{W}(G_1 \times G_2)$, which ends the proof of (iv).

An argument of the same kind shows that (iii) holds. □

2.3. **A basic property of factor representations.**

LEMMA 2.6. — *Let π be a unitary representation of a group G in a Hilbert space $\mathcal{H}$ and N a normal subgroup of G. Let π_1 [respectively π_2] be the subrepresentation of π given by the G-action on the subspace $\mathcal{H}^N$ of $\mathcal{H}$ consisting of the N-invariant vectors [respectively on its orthogonal complement].*

Then π_1 and π_2 are disjoint.

Proof. — Let ρ_1 be a non-zero subrepresentation of π_1 and ρ_2 a non-zero subrepresentation of π_2. On the one hand, the kernel of ρ_1 contains N. On the other hand, if the kernel of ρ_2 did contain N, the space of ρ_2 would be contained in $\mathcal{H}^N$, hence it would be $\{0\}$ by the definition of π_2. This is preposterous. Therefore the representations ρ_1 and ρ_2 have different kernels, and thus they are not equivalent. □

Two unitary representations π, π' of a group G are called **quasi-equivalent** if no non-zero subrepresentation of π is disjoint from π', and vice-versa.

PROPOSITION 2.7. — *Let π be a factor representation of a group G.*

For every non-zero subrepresentation $\rho \leqslant \pi$, we have $\mathrm{Ker}(\rho) = \mathrm{Ker}(\pi)$. In particular, if π' is any factor representation quasi-equivalent to π, then $\mathrm{Ker}(\pi) = \mathrm{Ker}(\pi')$.

Proof. — Set $N = \mathrm{Ker}(\rho)$. Denote by $\mathcal{H}_\pi$ the Hilbert space of π and by $\mathcal{H}_\rho$ that of ρ.

Since $\rho \leqslant \pi$, we have $\mathrm{Ker}(\pi) \leqslant N$. When $N = \{e\}$, there is nothing more to prove. We assume now that $N \neq \{e\}$.

The space $\mathcal{H}_\rho$ is contained in $\mathcal{H}_\pi^N$; in particular $\mathcal{H}_\pi^N \neq \{0\}$ since ρ is non-zero. Since π is a factor representation, $\mathcal{H}_\pi^N = \mathcal{H}_\pi$ by Lemma 2.6. It follows that $N \leqslant \mathrm{Ker}(\pi)$, hence that $N = \mathrm{Ker}(\pi)$.

Let π' be a factor representation of G which is quasi-equivalent to π. By [23, Theorem 1.7, Page 20], up to equivalence we have $\pi \leqslant \pi'$ or $\pi' \leqslant \pi$. Hence $\mathrm{Ker}(\pi) = \mathrm{Ker}(\pi')$ by the assertion that we have already established. □

2.4. **On G-faithful representations of subgroups of G.** Given a group G and a normal subgroup N, a unitary character or a unitary representation ρ of N is called **G-faithful** if the intersection over all $g \in G$ of the kernels $\mathrm{Ker}(\rho^g)$ is trivial, where $\rho^g(x) = \rho(gxg^{-1})$ for all $x \in N$.

The following lemma generalizes [2, Lemma 9]. More precisely, the statement from loc. cit. assumes that π is irreducible and faithful, whereas we only require that π is a factor representation and that the restriction $\pi|_N$ is faithful.

LEMMA 2.8. — *Let G be a countable group, N a normal subgroup of G, and π a factor representation of G such that the restriction $\pi|_N$ is faithful.*

Then N has an irreducible unitary representation ρ which is G-faithful.

Proof. — The proof is a small modification of that in [2, Lemma 9]. We reproduce the details since our hypotheses are slightly more general.

We assume that N is non-trivial, since otherwise there is nothing to prove. Set $\sigma := \pi|_N$ and let $\sigma = \int_\Omega^\oplus \sigma_\omega d\mu(\omega)$ be a direct integral decomposition of σ into irreducible unitary representations, implemented by an isomorphism $\mathcal{H}_\sigma \cong \int_\Omega^\oplus \mathcal{H}_\omega d\mu(\omega)$. Denote by $\{C_j\}_{j\in J}$ the family of G-conjugacy classes contained in

N distinct from $\{e\}$. For each j, let $N_j \leqslant N$ be the subgroup generated by C_j; note that N_j is normal in G. The family $\{C_j\}_{j\in J}$ is countable and non-empty. Every non-trivial normal subgroup of G contained in N must contain N_j for some $j \in J$. Therefore, given $\omega \in \Omega$, we see that σ_ω is not G-faithful if and only if $\mathrm{Ker}\big(\bigoplus_{g\in G}(\sigma_\omega)^g\big)$ contains N_j for some $j \in J$.

Set now $\Omega_j = \big\{\omega \in \Omega \mid N_j \leqslant \mathrm{Ker}\big(\bigoplus_{g\in G}(\sigma_\omega)^g\big)\big\}$ and $\widetilde{\Omega} = \bigcup_{j\in J} \Omega_j$. It follows that $\widetilde{\Omega}$ is the subset consisting of these $\omega \in \Omega$ such that σ_ω is not G-faithful. By [2, Lemma 8], each Ω_j is measurable. Since J is countable, $\widetilde{\Omega}$ is also measurable.

In order to finish the proof, it suffices to show that $\mu(\widetilde{\Omega}) = 0$. Suppose for a contradiction that $\mu(\widetilde{\Omega}) > 0$. Since J is countable, we have $\mu(\Omega_\ell) > 0$ for some $\ell \in J$. For each $\omega \in \Omega_\ell$, we have $N_\ell \leqslant \mathrm{Ker}(\sigma_\omega)$, so that the subspace $\int_{\Omega_\ell}^{\oplus} \mathcal{H}_\omega$ of $\mathcal{H}_\sigma$, which is non-zero since $\mu(\Omega_\ell) > 0$, consists of N_ℓ-invariant vectors. Since N_ℓ is normal in G, the set of N_ℓ-invariant vectors is G-invariant, and thus corresponds to a subrepresentation of π. Since π is a factor representation, we have $N_\ell \leqslant \mathrm{Ker}(\pi)$ by Proposition 2.7. Since $N_\ell \leqslant N$, this contradicts the hypothesis that $\pi|_N$ is faithful.

We have just shown that almost all irreducible unitary representations σ_ω of N occurring in a direct integral decomposition of σ are G-faithful. In particular there exists $\omega \in \Omega$ such that the irreducible unitary representation $\rho := \sigma_\omega$ is G-faithful. □

Proof of Proposition 1.14. — Let π be a factor representation of the countable group G. View π as a faithful representation of the group $H := G/\mathrm{Ker}(\pi)$. By Lemma 2.8 applied to H and its trivial normal subgroup $N = H$, the group H has an irreducible unitary representation ρ which is faithful. We may now view ρ as a representation of G and the proposition follows. □

LEMMA 2.9. — *Let G be a countable group, N a normal subgroup of G, and σ an irreducible unitary representation of N which is G-faithful.*

Then G has an irreducible unitary representation π with the following properties: the restriction $\pi|_N$ is faithful, and every element of $\mathrm{Ker}(\pi)$ *is contained in a finite normal subgroup of G, i.e.,* $\mathrm{Ker}(\pi)$ *is contained in the torsion FC-centre* $\mathrm{W}(G)$ *of G.*

Proof. — Let $\rho = \mathrm{Ind}_N^G(\sigma)$ be the unitary representation of G induced from σ. Let $\rho = \int_\Omega^{\oplus} \rho_\omega d\mu(\omega)$ be a direct integral decomposition of ρ into irreducible unitary representations. Set

$$\widetilde{\Omega} = \{\omega \in \Omega \mid \rho_\omega|_N \text{ is not faithful}\}$$

and

$$\widehat{\Omega} = \{\omega \in \Omega \mid \text{there exists } \ g \in \mathrm{Ker}(\rho_\omega) \ \text{ such that } \ \langle\langle g\rangle\rangle_G \ \text{ is infinite}\}.$$

We claim that $\mu(\widetilde{\Omega}) = \mu(\widehat{\Omega}) = 0$; to show this, we argue as in the proof of [2, Lemma 10].

To show that $\mu(\widetilde{\Omega}) = 0$, we proceed by contradiction. We assume that there exists a conjugacy class $C_\ell \neq \{e\}$ of G contained in N, generating a subgroup G_ℓ of G which is normal and contained in N, and defining a measurable subset $\Omega_\ell = \{\omega \in \Omega \mid G_\ell \leqslant \mathrm{Ker}(\rho_\omega)\}$, such that $\mu(\Omega_\ell) > 0$. Then, as in 'Claim 1' in the proof of [2, Lemma 10] we show that $G_\ell \cap N = \{e\}$, in contradiction with $G_\ell \leqslant N$.

To show that $\mu(\widehat{\Omega}) = 0$, also by contradiction, we assume this time that there exists a conjugacy class $C_m \neq \{e\}$ of G generating an infinite subgroup G_m of G, and defining a measurable subset $\Omega_m = \{\omega \in \Omega \mid G_m \leqslant \mathrm{Ker}(\rho_\omega)\}$, such that $\mu(\Omega_m) > 0$, and we arrive at a contradiction. Indeed, 'Claim 1' in the proof already quoted shows that $G_m \cap N = \{e\}$, and 'Claim 2' in the same proof shows that G_m is finite, in contradiction with the hypothesis.

Consequently, the complement of $\widetilde{\Omega} \cup \widehat{\Omega}$ in Ω has full measure, and thus is non-empty. For any $\omega \in \Omega \smallsetminus (\widetilde{\Omega} \cup \widehat{\Omega})$, the representation $\pi := \rho_\omega$ is an irreducible unitary representation of G that has the required properties. □

A strengthening of Lemma 2.9 will be established in Lemma 2.20 below.

LEMMA 2.10. — *Let G be a group and N, A, S normal subgroups of G such that $N = A \times S$. Assume that A is abelian, and that S is the restricted sum of a collection $\{S_i\}$ of non-abelian simple finite groups. Then:*

(i) S has a faithful irreducible unitary representation;
(ii) N has a G-faithful irreducible unitary representation if and only if A has a G-faithful unitary character.

Proof: see Lemma 13 and its proof in [2]. □

We end this section with some subsidiary facts. Given an abelian group A, denote by $\widehat{A}$ the **Pontryagin dual** of A, namely the space of all unitary characters $A \to \mathbf{T}$, with the compact open topology. Recall that $\widehat{A}$ is a compact abelian group.

LEMMA 2.11. — *Let G be a discrete group, A an abelian normal subgroup of G, and χ a unitary character of A.*

Then χ is G-faithful if and only if the subgroup generated by $\chi^G = \{\chi^g \mid g \in G\}$ is dense in $\widehat{A}$.

Proof. — This follows from Pontryagin duality. See the proof of the equivalence between (i) and (ii) of Lemma 14 in in [2]. □

Before the last proposition of this subsection, we recall the natural module structure on abelian normal subgroups, the definition of cyclic modules, and we state a lemma which is helpful for translating from the language of abelian groups to that of modules.

Remark 2.12. — Let G be a group, V an abelian normal subgroup of G, and $\mathbf{Z}[G]$ the group ring of G over the integers. Then V has a canonical structure of $\mathbf{Z}[G]$-module. Moreover, V is simple as a $\mathbf{Z}[G]$-module if and only if V is minimal as abelian normal subgroup of G.

Compare with the reminder on simple $\mathbf{F}_p[G]$-modules just before Theorem 1.1.

For a ring R and a module V, the module V is **cyclic** if there exists $v \in V$ such that $V = Rv$. This terminology is used below for R the group ring $\mathbf{Z}[G]$ and V an abelian normal subgroup of G, and for R the group algebra $\mathbf{F}_p[G]$ and V a p-elementary abelian normal subgroup of G for some prime p.

The proof of the next lemma is straightforward, and left to the reader.

LEMMA 2.13. — *Let G be a group and V an abelian normal subgroup of G.*

Then V is generated as a group by one G-conjugacy class if and only if V as a $\mathbf{Z}[G]$-module is cyclic.

Suppose moreover that V is an elementary abelian p-group. Then V is generated as a group by one G-conjugacy class if and only if V as an $\mathbf{F}_p[G]$-module is cyclic.

The following classical result will be frequently used in the sequel, without further notice. For a proof, see [5, § 3, no. 3].

PROPOSITION 2.14. — *Let R be a ring and U a R-module. The following conditions are equivalent:*

(i) U is generated by simple submodules.
(ii) U is a direct sum of a family of simple submodules.
(iii) Every submodule of U is a direct summand.

If U satisfies these conditions, then

(a) every submodule of U satisfies Conditions (i) to (iii),
(b) every quotient module of U satisfies Conditions (i) to (iii).

A module U satisfying Conditions (i) to (iii) is called **semi-simple**.

Proposition 2.15 will be needed in Section 4.

PROPOSITION 2.15. — *Let G be a group, A a finite normal subgroup of G contained in* $\mathrm{MA}(G)$*, and p a prime.*
The following properties are equivalent:

(i) The group A has a G-faithful unitary character.
(ii) The group A is generated by a single conjugacy class.
(iii) The $\mathbf{Z}[G]$-module A is cyclic.

Suppose moreover that A is an elementary abelian p-group. Then Properties (i) to (iii) are equivalent to:

(iv) The $\mathbf{F}_p[G]$-module A is cyclic.

Proof. — For the equivalence of (i) and (ii), we follow the arguments of the proof of Lemma 14 in [2] (whose formal statement is however insufficient for our purposes).

By (2) in Proposition 2.1, A is a finite abelian group and is therefore a direct sum $A = \bigoplus_{p\in P} A_p$, where P is the set of primes p for which A has elements of order p, and where A_p is the p-Sylow subgroup of A. Moreover A_p is an elementary abelian p-group for each $p \in P$, by (1) of the same proposition. Notice that A_p is semi-simple by Proposition 2.14, since A is contained in $\mathrm{MA}(G)$. (For comparison with [2, Lemma 14], note that it follows from Proposition 2.14 applied to each A_p that there exists a finite set $\{A_i\}_{i\in E}$ of abelian mini-feet in G such that $A = \bigoplus_{i\in I} A_i$; each A_i is isomorphic to $(\mathbf{F}_p)^n$ for some prime p and some $n \geqslant 1$.) Observe that the Pontryagin dual of $A = \bigoplus_{p\in P} A_p$ is canonically isomorphic to $\bigoplus_{p\in P} \widehat{A}_p$.

We know by Lemma 2.11 that A has a G-faithful unitary character if and only if $\widehat{A}$ is generated by one G-orbit. By the Chinese Remainder Theorem, the group $\widehat{A} = \bigoplus_{p\in P} \widehat{A}_p$ is generated by a single G-orbit if and only each of its p-Sylow subgroups $\widehat{A}_p$ is generated by a single G-orbit (this can alternatively be deduced from Lemma 2.13 together with Lemma 3.8 below). Using Lemma 2.11 again, we deduce that A has a G-faithful unitary character if and only if A_p has a G-faithful character for each $p \in P$.

Consequently, it suffices to prove the equivalence of (i) and (ii) when $A = A_p$ for one prime p. By Lemma 2.13, the group A_p is generated by a single conjugacy class if and only if A_p is cyclic as an $\mathbf{F}_p[G]$-module. Under the natural identification of $\widehat{A}_p$ with the dual $A_p^* := \mathrm{Hom}_{\mathbf{F}_p}(A_p, \mathbf{F}_p)$, the G-action on $\widehat{A}_p$ corresponds to the dual (or contragredient) action of G on A_p^*. Thus we may identify $\widehat{A}_p$ with A_p^* as $\mathbf{F}_p[G]$-modules. A finite semi-simple $\mathbf{F}_p[G]$-module is cyclic if and only if its dual is cyclic (see Lemma 3.2 in [34]). Since the dual A_p^* is canonically isomorphic to the Pontryagin dual $\widehat{A}_p$, and since A_p is semi-simple, we deduce from Lemma 2.11 that A_p is generated by a single conjugacy class if and only if A_p has a G-faithful unitary character.

The equivalence of (ii) and (iii) holds by Lemma 2.13.

In the particular case of A an elementary abelian p-group, similarly, the equivalence of (ii) and (iv) holds by Lemma 2.13. □

2.5. **Irreducible representations whose kernel is contained in** $\mathrm{Fsol}(G)$**.** The goal of this subsection is to establish the following result of independent interest.

Proposition 2.16. — *Any countable group G admits an irreducible unitary representation π such that, for every element $g \in \mathrm{Ker}(\pi)$, the normal closure $\langle\langle g \rangle\rangle_G$ is a soluble finite subgroup of G.*

In other words, G has an irreducible unitary representation whose kernel is contained in the characteristic subgroup $\mathrm{Fsol}(G)$*.*

We need the following.

Lemma 2.17. — *Let G be a countable group and K a normal subgroup of G contained in the torsion FC-centre* $\mathrm{W}(G)$*.*

If G/K is irreducibly faithful, then $G/(K \cap \mathrm{Fsol}(G))$ is also irreducibly faithful.

Proof. — Set $S = \mathrm{Fsol}(G)$. In order to show that $G/(K \cap S)$ is irreducibly faithful, it suffices by Theorem 2.2 to consider an arbitrary finite normal subgroup A of $G/(K \cap S)$ contained in $\mathrm{MA}\big(G/(K \cap S)\big)$ and to show that A is generated by a single conjugacy class.

Let $r_1 : G \twoheadrightarrow G/(K \cap S)$ and $r_2 : G/(K \cap S) \twoheadrightarrow G/K$ be the canonical projections. We claim that the restriction $r_2|_A$ is injective. Indeed, let $x \in G$ be such that $r_1(x) \in \mathrm{Ker}(r_2|_A) = A \cap \mathrm{Ker}(r_2)$; note that $r_1(x) \in A$ and $x \in K$. We have

$$\langle\langle r_1(x) \rangle\rangle_{G/(K \cap S)} \cong \langle\langle x \rangle\rangle_G / \big(\langle\langle x \rangle\rangle_G \cap (K \cap S)\big) = \langle\langle x \rangle\rangle_G / \big(\langle\langle x \rangle\rangle_G \cap S\big).$$

Since $K \leqslant \mathrm{W}(G)$ by hypothesis, the normal closure $\langle\langle x \rangle\rangle_G$ is finite. By the definition of S, every finite normal subgroup of G contained in S is soluble; hence $\langle\langle x \rangle\rangle_G \cap S$ is soluble. Moreover $\langle\langle r_1(x) \rangle\rangle_{G/K \cap S}$ is abelian because $r_1(x) \in A$ and A is abelian normal in $G/(K \cap S)$. It follows that $\langle\langle x \rangle\rangle_G$ is soluble-by-abelian, hence soluble. We infer that $x \in S$. Therefore $r_1(x) = e$, which proves the claim.

Since $G/(K \cap S)$ is a quotient of G, we may view A as a $\mathbf{Z}[G]$-module, and we must show that this module is cyclic (see Proposition 2.15). The claim implies that r_2 induces an isomorphism of $\mathbf{Z}[G]$-modules $A \to r_2(A)$. Since G/K is irreducibly faithful by hypothesis, and since $r_2(A) \leqslant \mathrm{MA}(G/K)$ by Proposition 2.1(7), we deduce from Theorem 2.2 that $r_2(A)$ is generated by a single conjugacy class in

G/K. Thus $r_2(A)$ is a cyclic $\mathbf{Z}[G]$-module by Proposition 2.15, from which it finally follows that A is a cyclic $\mathbf{Z}[G]$-module, as required. □

Proof of Proposition 2.16. — The group G has an irreducible unitary representation whose kernel K is contained in $\mathrm{W}(G)$, by Lemma 2.9 applied with $N = \{e\}$. By Lemma 2.17, it follows that G also has an irreducible unitary representation whose kernel is contained in $\mathrm{Fsol}(G)$. □

Remark 2.18. — For a finite group G, Proposition 2.16 implies that G has an irreducible representation with soluble kernel. This falls quite short of a theorem due to Broline and Garrison [20, Corollary 12.20] which establishes that G has an irreducible representation with nilpotent kernel. More precisely:

Let G be a finite group and let π be an irreducible representation of G over $\mathbf{C}$ satisfying either of the following conditions: (i) the degree of π is maximal among the degrees of all irreducible representations of G, (ii) the kernel of π is minimal among the kernels of all irreducible representations of G. Then the kernel of π is nilpotent.

There are groups without any irreducible representation having abelian kernel. This is well-known to experts, and we are convinced that examples exist in the literature, but we have not been able to find a precise reference; one specific example can be found in Appendix A.

Remark 2.19. — Let G be a countable group.

(1) It follows from Proposition 2.16 that the complement $G \smallsetminus \mathrm{Fsol}(G)$ of $\mathrm{Fsol}(G)$ in a countable group G is irreducibly faithful. (A refinement of that statement will be established in Proposition 4.2.)

(2) However, the quotient $G/\mathrm{Fsol}(G)$ need not have a faithful irreducible unitary representation.

Indeed, let H be a countable group such that $H/\mathrm{Fsol}(H) \cong C_3$ is cyclic of order 3; see Example 2.4(7). Set $G = H \times H$. By Proposition 2.5, we have

$$G/\mathrm{Fsol}(G) \cong (H \times H)/(\mathrm{Fsol}(H) \times \mathrm{Fsol}(H)) \cong C_3 \times C_3,$$

so that $G/\mathrm{Fsol}(G)$ does not have any faithful irreducible unitary representation.

(3) In [2, Corollary 3], it is noted that each of the following conditions on G is sufficient to imply that G has a faithful irreducible unitary representation:

(i) G is torsion-free,

(ii) all conjugacy classes in G distinct from $\{e\}$ are infinite.

Proposition 2.16 shows that the following condition, weaker than both (i) and (ii), is also sufficient:

(iii) $\mathrm{Fsol}(G) = \{e\}$.

Here are two families of groups for which (iii) holds, but neither (i) nor (ii) does.

(a) Any restricted sum H of finite non-abelian simple groups. More generally, any direct product $G \times H$ of an irreducibly faithful group G with a restricted sum H of finite non-abelian simple groups.

(b) Let G be one of the groups defined by B.H. Neumann in 1937 to show that there are uncountably many pairwise non-isomorphic groups

which are finitely generated and not finitely presented; see [24], as well as [17, Section III.B and in particular no 35]. Recall that, in G, the FC-centre is a restricted sum $N := \prod'_n H_n$, where each H_n is a finite simple alternating group, and $|H_1| < \cdots < |H_n| < |H_{n+1}| < \ldots$, and the quotient G/N is the permutation group of $\mathbf{Z}$ generated by translations and even finitely supported permutations. Observe that G is neither torsion-free, nor with all conjugacy classes other than $\{e\}$ infinite. The subgroup $\mathrm{Fsol}(G)$ is trivial, and therefore G has a faithful irreducible unitary representation.

We finish by recording the following strengthening of Lemma 2.9, which will be needed in Section 4.

LEMMA 2.20. — *Let G be a countable group, N a normal subgroup of G, and σ an irreducible unitary representation of N which is G-faithful.*

Then G has an irreducible unitary representation π such that $\mathrm{Ker}(\pi) \cap N = \{e\}$ *and* $\mathrm{Ker}(\pi) \leqslant \mathrm{Fsol}(G)$.

Proof. — Let K be the kernel of the irreducible unitary representation of G afforded by applying Lemma 2.9 to σ. Thus $K \cap N = \{e\}$ and $K \leqslant \mathrm{W}(G)$. The desired conclusion now follows from Lemma 2.17. □

2.6. **On abelian groups.** We recall here some standard definitions and results concerning an abelian group G, before giving a proof of Proposition 1.12. In the rest of this subsection, the abelian group G is written additively.

A subset L of G is **independent** if $0 \notin L$ and if, for any finite subset $\{g_1, \ldots, g_k\}$ of L and any integers $n_1, \ldots, n_k \in \mathbf{Z}$, such that $n_1 g_1 + \cdots + n_k g_k = 0$, we have $n_1 g_1 = \cdots = n_k g_k = 0$; equivalently if the subgroup of G generated by L is the direct sum over $g \in L$ of the cyclic groups $\langle g \rangle$. The **torsion-free rank** $r_0(G)$ of G is the cardinality of an independent subset L of G which contains elements of infinite order only and which is maximal with respect to this property (this cardinality is independent of the choice of L). For a prime p, the p-**rank** of G is the cardinality of an independent subset L of G which contains elements whose orders are powers of p only and which is maximal with respect to this property (this cardinality is independent of the choice of L). For example, if G is a subgroup of $\mathbf{Q}$, then $r_0(G) \leqslant 1$ and $r_p(G) = 0$ for all p. For a prime p and the quasi-cyclic group $\mathbf{Z}(p^\infty) := \mathbf{Z}[1/p]/\mathbf{Z}$, we have $r_0(\mathbf{Z}(p^\infty)) = 0$, $r_p(\mathbf{Z}(p^\infty)) = 1$, and $r_\ell(\mathbf{Z}(p^\infty)) = 0$ for a prime $\ell \neq p$. For the group $\mathbf{T}$, we have $r_0(\mathbf{T}) = \mathfrak{c}$ (the cardinality of the continuum) and $r_p(T) = 1$ for every prime p.

An abelian group E is **divisible** if, for every $g \in E$ and every positive integer n, there exists $h \in E$ such that $g = nh$. For example, $\mathbf{Q}$ and $\mathbf{T}$ are divisible, and $\mathbf{Z}$ is not. It is a fact that any abelian group G can be embedded as a subgroup of a divisible group E, minimal in the sense that no proper divisible subgroup of E contains G; moreover two such E are isomorphic over G. Such a group E, with its subgroup G, is called a **divisible hull** of G [12, Section 24].

Any divisible group E is isomorphic to a direct sum

$$(*) \qquad E \cong \Big(\bigoplus_{r_0(E)} \mathbf{Q} \Big) \oplus \Big(\bigoplus_{p} \Big(\bigoplus_{r_p(E)} \mathbf{Z}(p^\infty) \Big) \Big).$$

In particular, we have

$$(**) \qquad \mathbf{T} \cong \Big(\bigoplus_{\mathfrak{c}} \mathbf{Q}\Big) \oplus \Big(\bigoplus_{p} \mathbf{Z}(p^\infty)\Big).$$

See [12, Theorem 23.1]. A divisible group (for example $\mathbf{T}$) has a subgroup isomorphic to some abelian group G if and only if it has a subgroup isomorphic to the divisible hull E of G; furthermore, we have

$$(***) \qquad r_0(E) = r_0(G) \quad \text{and} \quad r_p(E) = r_p(G) \ \text{ for all primes } p;$$

see [12, Section 24].

Proof of Proposition 1.12. — It follows from (**) and (***) that G satisfies Condition (i) if and only if $r_0(G) \leqslant \mathfrak{c}$ and $r_p(G) \leqslant 1$ for all primes p, that is if and only if G satisfies Condition (ii) □

3. Cyclic semi-simple $\mathbf{F}_p[G]$-modules

Let R be a ring. The following lemma is the module version of a result often stated for groups and known as Goursat's Lemma. The module version appears, for example, in [22, Page 171]. More on this lemma can be consulted in [1].

Lemma 3.1. — *Let $A = A_0 \oplus A_1$ be the direct sum of two R-modules. For $i = 0, 1$, let $r_i : A \twoheadrightarrow A_i$ be the canonical projection. Let $M \leqslant A$ be a submodule such that $r_i(M) = A_i$ for $i = 0, 1$. Set $M_i = M \cap A_i$.*

Then the R-modules A_0/M_0 and A_1/M_1 are isomorphic, and the canonical image of M in $A_0/M_0 \oplus A_1/M_1$ is the graph of an isomorphism of R-modules $A_0/M_0 \to A_1/M_1$.

Let now p be a prime and G a group. The main goal of this section is to characterize when a finite semi-simple $\mathbf{F}_p[G]$-module is cyclic. This will be achieved in Proposition 3.9 below, after some preparatory steps. Proposition 3.9 is well-known to experts: see Lemma 3.1 in [34]. It can be seen as a version over $\mathbf{F}_p$ of a result for cyclic unitary representations of compact groups which appears in Greenleaf and Moskowitz [16, Proposition 1.8].

Along the way, we count the number of simple $\mathbf{F}_p[G]$-submodules of a direct sum $V_0 \oplus \cdots \oplus V_\ell$ of mutually isomorphic simple $\mathbf{F}_p[G]$-modules (Lemma 3.5). This count is an important ingredient for the proof of the last inequality of Theorem 1.1.

Lemma 3.2. — *Let W be a finite simple $\mathbf{F}_p[G]$-module. Let $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$ be its centralizer, which is a finite field extension of $\mathbf{F}_p$. Let V_0, V_1 be two copies of W.*

Every simple $\mathbf{F}_p[G]$-submodule M of $V_0 \oplus V_1$ such that $M \cap V_0 = \{0\}$ is of the form

$$M = \{(\lambda x, x) \mid x \in V_1\}$$

for some $\lambda \in \mathbf{k}$.

Proof. — This is a straightforward consequence of Lemma 3.1. □

The following extension to a direct sum of $\ell + 1$ components will be useful.

Lemma 3.3. — *Let W be a finite simple $\mathbf{F}_p[G]$-module. Let $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$. Let $\ell \geqslant 0$; for each $i = 0, \ldots, \ell$, let V_i be a copy of W. Set $U = V_0 \oplus V_1 \oplus \cdots \oplus V_\ell$.*

Every maximal $\mathbf{F}_p[G]$-submodule $M \lneqq U$ such that $M \cap V_0 = \{0\}$ is of the form

$$M = \Big\{ \Big(\sum_{i=1}^{\ell} \lambda_i x_i, x_1, x_2, \dots, x_\ell \Big) \;\Big|\; (x_1, \dots, x_\ell) \in V_1 \oplus \cdots \oplus V_\ell \Big\}$$

for some $(\lambda_1, \dots, \lambda_\ell) \in \mathbf{k}^\ell$.

Proof. — Let $r : U \twoheadrightarrow V_1 \oplus \cdots \oplus V_\ell$ be the canonical projection. Let $M \lneqq U$ be a maximal $\mathbf{F}_p[G]$-submodule such that $M \cap V_0 = \{0\}$. Then the restriction $r|_M$ is injective. Since M is maximal, we have $U = V_0 \oplus M$, so that $r|_M : M \to V_1 \oplus \cdots \oplus V_\ell$ is an isomorphism of $\mathbf{F}_p[G]$-modules.

Given $i \in \{1, \dots, \ell\}$, let $M_i = (r|_M)^{-1}(V_i)$. Then M_i is isomorphic to V_i, hence it is a simple $\mathbf{F}_p[G]$-submodule of M contained in $V_0 \oplus V_i$. Moreover $M_i \cap V_0 = \{0\}$. By Lemma 3.2, there exists $\lambda_i \in \mathbf{k}$ such that $M_i \cong \{(\lambda_i x_i, x_i) \mid x_i \in V_i\} \leqslant V_0 \oplus V_i$. Since $r|_M : M \to V_1 \oplus \cdots \oplus V_\ell$ is an isomorphism, we deduce that

$$\begin{aligned} M &= M_1 \oplus \cdots \oplus M_\ell \\ &= \Big\{ \Big(\sum_{i=1}^{\ell} \lambda_i x_i, x_1, x_2, \dots, x_\ell \Big) \;\Big|\; (x_1, \dots, x_\ell) \in V_1 \oplus \cdots \oplus V_\ell \Big\} \end{aligned}$$

as required. □

We can now characterize when a direct sum of copies of a given simple $\mathbf{F}_p[G]$-module is cyclic.

Lemma 3.4. — *Retain the notation of Lemma 3.3.*
The $\mathbf{F}_p[G]$-module U is cyclic if and only if $\ell < \dim_{\mathbf{k}}(W)$.

Proof. — Assume first that $\ell \geqslant \dim_{\mathbf{k}}(W)$. Let $(v_0, \dots, v_\ell) \in U$. Since $V_i = W$ for all i, we may view v_i as an element of W. Then, upon reordering the summands $V_0, \dots, V_\ell$, we may assume that there exists $(\lambda_1, \dots, \lambda_\ell) \in \mathbf{k}^\ell$ such that $v_0 = \sum_{i=1}^{\ell} \lambda_i v_i$. It follows that $(v_0, \dots, v_\ell)$ belongs to

$$\Big\{ \Big(\sum_{i=1}^{\ell} \lambda_i x_i, x_1, x_2, \dots, x_\ell \Big) \;\Big|\; (x_1, \dots, x_\ell) \in V_1 \oplus \cdots \oplus V_\ell \Big\},$$

which is a proper $\mathbf{F}_p[G]$-submodule of U. Hence U is not cyclic. (In a context of characteristic zero, an argument of this kind is used for the proof of [10, Lemma 15.5.3].)

In order to prove the converse, we proceed by induction on ℓ. In case $\ell = 0$, we have $0 = \ell < \dim_{\mathbf{k}}(W)$ and $U = V_0 = W$ is simple, hence cyclic.

We now assume that $0 < \ell < \dim_{\mathbf{k}}(W)$. The induction hypothesis ensures that the $\mathbf{F}_p[G]$-module $V_1 \oplus \cdots \oplus V_\ell$ is cyclic. Let $(v_1, \dots, v_\ell)$ be a generator. Viewing all v_i as elements of W, the hypothesis that $\ell < \dim_{\mathbf{k}}(W)$ ensures the existence of an element $v_0 \in W$ which does not belong to the $\mathbf{k}$-subspace of W spanned by $\{v_1, \dots, v_\ell\}$. Let M be the $\mathbf{F}_p[G]$-submodule of U spanned by $(v_0, v_1, \dots, v_\ell)$. Let $r : U \twoheadrightarrow V_1 \oplus \cdots \oplus V_\ell$ denote the canonical projection. The image $r(M)$ coincides with the $\mathbf{F}_p[G]$-submodule generated by $(v_1, \dots, v_\ell)$, i.e., with $V_1 \oplus \cdots \oplus V_\ell$. If one had $M \cap V_0 = \{0\}$, then M would be a maximal proper $\mathbf{F}_p[G]$-submodule of U, and Lemma 3.3 would then ensures that v_0 is a $\mathbf{k}$-linear combination of $\{v_1, \dots, v_\ell\}$, a contradiction. Hence $M \cap V_0 \neq \{0\}$. Since V_0 is simple, M contains V_0, so that $U = M$; this shows that U is indeed cyclic. □

The following basic counting lemma will also be useful.

LEMMA 3.5. — *Retain the notation of Lemma 3.3. Moreover, set $q = |\mathbf{k}|$. The number of simple $\mathbf{F}_p[G]$-submodules of U is*

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

Proof. — We proceed by induction on ℓ. In case $\ell = 0$, the $\mathbf{F}_p[G]$-module $U = V_0$ is simple, so the result is clear. Assume now that $\ell \geqslant 1$. Consider

the collection $\mathcal{S}$ of all simple $\mathbf{F}_p[G]$-submodules of U,

the complement $\mathcal{S}_0$ of V_0 in $\mathcal{S}$, i.e., $\mathcal{S}_0 = \{S \in \mathcal{S} \mid S \cap V_0 = \{0\}\}$,

and the collection $\mathcal{S}'$ of all simple $\mathbf{F}_p[G]$-submodules of $V_1 \oplus \cdots \oplus V_\ell$.

Denote by r the canonical projection $U \twoheadrightarrow V_1 \oplus \cdots \oplus V_\ell$. Each $S \in \mathcal{S}_0$ determines its image $S' = r(S) \in \mathcal{S}'$, which can be viewed as a submodule of U contained in $V_1 \oplus \cdots \oplus V_\ell$, and there exists by Lemma 3.1 an element $\lambda \in \mathbf{k}$ such that $S = \{(\lambda x, x) \mid x \in S'\} \leqslant V_0 \oplus S'$. Conversely, $S' \in \mathcal{S}'$ and $\lambda \in \mathbf{k}$ determine S. This shows that $|\mathcal{S}| = |\mathcal{S}_0| + 1 = q|\mathcal{S}'| + 1$. Since $|\mathcal{S}'| = q^{\ell-1} + \cdots + q + 1$ by the induction hypothesis, this ends the proof. □

LEMMA 3.6. — *Retain the notation of Lemma 3.3. Moreover, set $q = |\mathbf{k}|$, denote by m the dimension of W over $\mathbf{k}$, and assume that $\ell \geqslant m$. Let $\mathcal{Z}$ be a set of simple $\mathbf{F}_p[G]$-submodules of U of cardinality $|\mathcal{Z}| < q^m + \cdots + q + 1$.*

There is an $\mathbf{F}_p[G]$-submodule $B \leqslant U$ with $B \cap Z = \{0\}$ for all $Z \in \mathcal{Z}$, and such that U/B is cyclic.

Proof. — Let $\mathcal{B}$ be the collection of all $\mathbf{F}_p[G]$-submodules B of U such that $B \cap Z = \{0\}$ for all $Z \in \mathcal{Z}$. Let also $B \in \mathcal{B}$ be an element which is maximal for the inclusion relation. Note that the $\mathbf{F}_p[G]$-module U/B is semi-simple. If U/B were not cyclic, then U/B would be isomorphic to a direct sum of at least $m + 1$ copies of W by Lemma 3.4. Therefore U/B would contain at least $q^m + \cdots + q + 1$ simple $\mathbf{F}_p[G]$-submodules by Lemma 3.5. In particular U/B would contain at least one simple $\mathbf{F}_p[G]$-submodule C which is different from the canonical image of Z in U/B for all $Z \in \mathcal{Z}$. Denoting by B' the preimage of C in U, we obtain $B \lneqq B'$ and $B' \in \mathcal{B}$. This contradicts the maximality of B. Hence U/B is cyclic. □

Given an additive group V and a subset $F \subseteq V$, we set

$$F - F = \{c \in V \mid c = a - b \text{ for some } a, b \in F\}.$$

The following result will be needed in Section 5.

LEMMA 3.7. — *Retain the notation from Lemma 3.5.*

If $\ell \geqslant 1$, there is a subset $F \subseteq U$ of size $q^\ell + q^{\ell-1} + \cdots + q + 1$ such that $F - F$ contains a non-zero element of each of the simple $\mathbf{F}_p[G]$-submodules of U.

Proof. — For each subset $I \subseteq \{0, 1, \ldots, \ell\}$, we view the direct sum $\bigoplus_{i \in I} V_i$ as a submodule of U.

Let $\mathcal{S}$ be the collection of all simple submodules of U and $\mathcal{S}'$ be the subcollection consisting of those $S \in \mathcal{S}$ which are contained in $V_0 \oplus V_1$. By Lemma 3.5, we have $|\mathcal{S}| = q^\ell + q^{\ell-1} + \cdots + q + 1$ and $|\mathcal{S}'| = q + 1$.

By definition, each element of $\mathcal{S}$ is a simple module, so that any two distinct elements of $\mathcal{S}$ have intersection $\{0\}$. Choosing a non-zero element in each member of $\mathcal{S} \smallsetminus \mathcal{S}'$, we obtain a set E of size $q^\ell + q^{\ell-1} + \cdots + q^2$.

Choose now a non-zero $x \in V_1$, and set $E' = \{(\lambda x, x) \mid \lambda \in k\} \subseteq V_0 \oplus V_1$. Thus $|E'| = |\mathbf{k}| = q$. By Lemma 3.2, the set E' contains a non-zero element in each member of $\mathcal{S}' \smallsetminus \{V_0\}$.

Finally, we set $F = E \cup E' \cup \{0\}$. Observe that $|F| = q^\ell + q^{\ell-1} + \cdots + q + 1$. Moreover, we have $E \cup E' \subset F \smallsetminus \{0\} \subset F - F$, so that $F - F$ contains a non-zero element of each member of $\mathcal{S} \smallsetminus \{V_0\}$. Since

$$V_0 \ni (x, 0) = (x, x) - (0, x) \in E' - E' \subset F - F,$$

we see that $F - F$ also contains a non-zero element of V_0. Thus the set F has the required properties. □

Given a semi-simple R-module U and a simple R-module W, the submodule of U generated by all simple submodules isomorphic to W is called the **isotypical component of type** W of U. Every semi-simple R-module is the direct sum of its isotypical components [5, § 3, Proposition 9].

LEMMA 3.8. — *Let R be a ring and $U = M_1 \oplus \cdots \oplus M_\ell$ be a finite direct sum of semi-simple R-modules. Assume that for all $i \neq j$, the modules M_i and M_j are disjoint, i.e., they do not contain any non-zero isomorphic summands. Then U is cyclic if and only if M_i is cyclic for all $i = 1, \ldots, \ell$.*

In particular, a semi-simple R-module with finitely many isotypical components is cyclic if and only if each of its isotypical components is cyclic.

Proof. — The 'only if' part is clear since any quotient of a cyclic module is cyclic.

Assume that M_i is cyclic for all $i \in \{1, \ldots, \ell\}$ and let $v_i \in M_i$ be a generator. We claim that $v = (v_1, \ldots, v_\ell)$ is a generator of U. We prove this by induction on ℓ. The base case $\ell = 1$ is trivial. Assume now that $\ell \geqslant 2$ and let M be the submodule generated by v. The induction hypothesis ensures that the canonical projection of M to $A_0 = \bigoplus_{i=1}^{\ell-1} M_i$ is surjective. Clearly, the projection of M to $A_1 = M_\ell$ is surjective. Since A_0 and A_1 are disjoint, it follows from Lemma 3.1 that $M = A_0 \oplus A_1 = U$. □

PROPOSITION 3.9. — *Let U be a finite semi-simple $\mathbf{F}_p[G]$-module. The following properties are equivalent:*

(i) U is not cyclic.

(ii) There exist a finite simple $\mathbf{F}_p[G]$-module W of dimension $m \geqslant 1$ over $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$, and a submodule $V \leqslant U$ isomorphic to a direct sum of $m + 1$ copies of W.

Proof. — Assume that Property (ii) holds. In view of Lemma 3.4, the module V afforded by (ii) is not cyclic. Since V is a direct summand of U, and therefore isomorphic to a quotient of U, it follows that U is not cyclic.

Assume conversely that U is not cyclic. Then U has a non-cyclic isotypical component by Lemma 3.8, and it follows from Lemma 3.4 that Condition (ii) holds. □

4. On the structure of minimal unfaithful subsets

The goal of this section is to prove Theorem 1.1. In fact, we shall establish a finer statement that describes precisely the structure of the normal closure of an irreducibly unfaithful subset of size n in a countable group with Property $\mathcal{P}(n-1)$, see

Theorem 4.5 below. We shall however start with the proof of the easier implication in Theorem 1.1.

4.1. **Proof of (2) ⇒ (1) in Theorem 1.1.**

LEMMA 4.1. — *Let G be a countable group. Suppose that there exist a prime p, a finite normal subgroup V of G which is an elementary abelian p-group, and a finite simple $\mathbf{F}_p[G]$-module W, with centralizer field $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$ and dimension $m = \dim_{\mathbf{k}}(W)$, such that V is isomorphic as $\mathbf{F}_p[G]$-module to a direct sum of $m+1$ copies of W. Set $q = |\mathbf{k}|$. Then:*

(i) For every irreducible unitary representation π of G, the kernel $\mathrm{Ker}(\pi)$ contains at least one of the $q^m + \cdots + q + 1$ simple submodules of V.

(ii) A subset $F \subset V$ is irreducibly faithful in G if and only if $F \cap K \subset \{e\}$ for some simple $\mathbf{F}_p[G]$-submodule K of V.

(iii) There is a subset $F \subset V$ of size $q^m + \cdots + q + 1$ which is not irreducibly faithful.

Proof. — (i) Since V is not cyclic as an $\mathbf{F}_p[G]$-module by Lemma 3.4, it follows that V has no G-faithful character by Proposition 2.15. In view of Lemma 2.8, for every irreducible unitary representation π of G, the restriction $\pi|_V$ cannot be faithful. In particular $\mathrm{Ker}(\pi)$ contains at least one of the simple $\mathbf{F}_p[G]$-submodules of V.

(ii) Let F be a subset of V. If F contains a non-trivial element in each of the simple $\mathbf{F}_p[G]$-submodules of V, it follows from (i) that F is not irreducibly faithful in G. Conversely, if there is a simple $\mathbf{F}_p[G]$-submodule K in V such that $F \cap K \subset \{e\}$, then every non-trivial element of F has a non-trivial image in the quotient V/K. Since V/K is a cyclic $\mathbf{F}_p[G]$-module by Lemma 3.4, it follows from Proposition 2.15 and Lemma 2.9 that G/K has an irreducible unitary representation whose restriction to V/K is faithful. Therefore F is irreducibly faithful in G.

(iii) By Lemma 3.5, the number of simple submodules in V equals $q^m+\cdots+q+1$. Thus V contains a subset of size $q^m+\cdots+q+1$ which is not irreducibly faithful. □

Proof of (2) ⇒ (1) in Theorem 1.1. — If G satisfies (2) in Theorem 1.1, then G contains a set $F \subseteq V$ of size $q^m + \cdots + q + 1$ which is not irreducibly faithful by Lemma 4.1, so that G does not have Property $\mathcal{P}(q^m + \cdots + q + 1)$. Since $n \geqslant q^m + \cdots + q + 1$, the group G does not have Property $\mathcal{P}(n)$. □

4.2. **Minimal unfaithful subsets are contained in** $\mathrm{Fsol}(G)$**.**

The following result shows that, in a countable group G, the irreducible faithfulness of a subset F can be checked on the intersection of F with $\mathrm{Fsol}(G)$.

PROPOSITION 4.2. — *Let G be a countable group and F a subset of G. If $F \cap \mathrm{Fsol}(G)$ is finite and irreducibly faithful, then F is irreducibly faithful.*

In particular, a finite subset $F \subseteq G$ is irreducibly faithful if and only if the intersection $F \cap \mathrm{Fsol}(G)$ is irreducibly faithful.

Note : We know already the particular case of this proposition for F disjoint from $\mathrm{Fsol}(G)$, for example for $F = G \smallsetminus \mathrm{Fsol}(G)$, see Remark 2.19(1).

Proof. — Set $S = \mathrm{Fsol}(G)$. Let $F \subseteq G$ be such that $F \cap S$ is finite and irreducibly faithful. We aim at proving that F is irreducibly faithful. To this end, we partition F into three subsets, $F = F_S \sqcup F_H \sqcup F_\infty$, where:

$$F_S = \{x \in F \mid \langle\langle x\rangle\rangle_G \text{ is finite soluble}\} = F \cap S,$$
$$F_H = \{x \in F \mid \langle\langle x\rangle\rangle_G \text{ is finite non-soluble}\} = (F \cap \mathrm{W}(G)) \smallsetminus S,$$
$$F_\infty = \{x \in F \mid \langle\langle x\rangle\rangle_G \text{ is infinite}\} = F \smallsetminus (F_S \sqcup F_H).$$

By hypothesis, there exists an irreducible unitary representation ρ of G such that $\rho(x) \neq \mathrm{id}$ for all $x \in F_S \smallsetminus \{e\}$. Since F_S is finite by hypothesis, the normal subgroup $A = \langle\langle F_S\rangle\rangle_G$ is finite soluble (Lemma 2.3). Let $K = A \cap \mathrm{Ker}(\rho)$, which is a finite soluble normal subgroup of G, and let $r : G \twoheadrightarrow Q = G/K$ be the canonical projection. Note that $r(x) \neq e$ for all $x \in F_S \smallsetminus \{e\}$.

Since A is soluble, its image $\rho(A)$ is soluble as well. Therefore the socle $\mathrm{Soc}(\rho(A))$ is abelian. Since $\rho(G)$ is irreducibly faithful, the socle $\mathrm{Soc}(\rho(A))$ has a $\rho(G)$-faithful irreducible unitary character by Lemma 2.8.

The homomorphism ρ induces an isomorphism $\rho_A : A/K \xrightarrow{\cong} \rho(A)$, and similarly r induces an isomorphism $r_A : A/K \xrightarrow{\cong} r(A)$. Moreover, the action by conjugation of G on A induces G-actions on $\rho(A)$ and $r(A)$, and the isomorphism $r_A\rho_A^{-1} : \rho(A) \xrightarrow{\cong} r(A)$ is G-equivariant. Hence the group $N = \mathrm{Soc}(r(A))$, which is normal in Q, is abelian and has a Q-faithful unitary character, say σ.

We now invoke Lemma 2.20, which affords an irreducible unitary representation π of Q whose restriction to N is faithful, and such that $\mathrm{Ker}(\pi)$ is contained in $\mathrm{Fsol}(Q)$.

The composite map $\pi' = \pi \circ r$ is an irreducible unitary representation of G.

We claim that $\pi'(x) \neq \mathrm{id}$ for all $x \in \big(F_S \smallsetminus \{e\}\big)$. We know that the representation $\pi|_N$ is faithful. Since $N = \mathrm{Soc}(r(A))$, it follows that $\pi|_{r(A)}$ is also faithful. As noted above, for every $x \in F_S \smallsetminus \{e\}$, we have $r(x) \neq e$, and therefore $\pi'(x) = \pi(r(x)) \neq \mathrm{id}$.

We next claim that $\pi'(x) \neq \mathrm{id}$ for all $x \in F_H$. Indeed, for $x \in F_H$, we have $x \neq e$ and $\langle\langle x\rangle\rangle_G \not\leqslant S$, since $\langle\langle x\rangle\rangle_G$ is not soluble. But $K \cap \langle\langle x\rangle\rangle_G$ is finite soluble, because K is so. Therefore $\langle\langle r(x)\rangle\rangle_Q = r(\langle\langle x\rangle\rangle_G) \cong \langle\langle x\rangle\rangle_G/(K \cap \langle\langle x\rangle\rangle_G)$ is not soluble, hence $r(x) \notin \mathrm{Fsol}(Q)$. Since the kernel of π is contained in $\mathrm{Fsol}(Q)$, this shows that $r(x) \notin \mathrm{Ker}(\pi)$, and therefore that $x \notin \mathrm{Ker}(\pi')$, as claimed.

Given $x \in F_\infty$, the normal closure $\langle\langle x\rangle\rangle_G$ is infinite. Since K is finite, it follows that $\langle\langle r(x)\rangle\rangle_Q$ is infinite as well. In particular $r(x)$ is not contained in the kernel of π, which is contained in $\mathrm{Fsol}(Q) \leqslant \mathrm{W}(Q)$. Hence $\pi'(x) \neq 1$. This proves that $\pi'(x) \neq 1$ for all $x \in F \smallsetminus \{e\}$.

Thus F is irreducibly faithful, as required. □

Corollary 4.3. — *Let G be a countable group and $F \subseteq G$ be a finite subset which is irreducibly unfaithful.*

If every proper subset of F is irreducibly faithful, then F is contained in $\mathrm{Fsol}(G)$.

Proof. — Let F be a finite subset of G of which every proper subset is irreducibly faithful. If F was not contained in $\mathrm{Fsol}(G)$, then F would be irreducibly faithful by Proposition 4.2. Therefore $F \subseteq \mathrm{Fsol}(G)$. □

4.3. **Unfaithful subsets of size n in countable groups with $\mathcal{P}(n-1)$.**

Lemma 4.4. — *Let n be a positive integer and G a countable group. Let $F \subset G$ be an irreducibly unfaithful subset of size n such that:*

(a) every proper subset of F is irreducibly faithful;
(b) every element of F is contained in an abelian mini-foot of G.

Let $U = \langle\langle F \rangle\rangle_G$ the normal subgroup of G generated by F.

Then there exist a prime p, and a simple $\mathbf{F}_p[G]$-module W, such that the following assertions hold, where $\mathbf{k}$ denotes the centralizer field $\mathcal{L}_{\mathbf{F}_p[G]}(W)$, and $m = \dim_{\mathbf{k}}(W)$, and $q = |\mathbf{k}|$:

- *(i) U is a finite elementary abelian p-group, contained in the abelian mini-socle $\mathrm{MA}(G)$;*
- *(ii) U is isomorphic as an $\mathbf{F}_p[G]$-module to the direct sum of a number $\ell + 1$ of copies of W, and $\ell \geqslant m$;*
- *(iii) $q^m + q^{m-1} + \cdots + q + 1 \leqslant n$.*

Proof. — The hypothesis (a) on F implies that F does not contain the neutral element e, since otherwise F would be irreducibly faithful.

By Proposition 2.1, the normal subgroup U is abelian and finite. The conjugation action of G on U allows us to view U as a $\mathbf{Z}[G]$-module. Since U is generated by mini-feet of G, it follows from Proposition 2.14 that U is a semi-simple $\mathbf{Z}[G]$-module. Let $\mathcal{Y}$ denote the set of isomorphism classes of simple $\mathbf{Z}[G]$-submodules of U. For each $Y \in \mathcal{Y}$, let U_Y be the submodule of U generated by the simple submodules isomorphic to Y; note that U_Y is a finite abelian normal subgroup of U. We have the isotypical direct sum decomposition $U = \bigoplus_{Y \in \mathcal{Y}} U_Y$.

For $x \in F$, the normal closure $\langle\langle x \rangle\rangle_G \leqslant U$ is an abelian mini-foot of G by hypothesis, hence a simple $\mathbf{Z}[G]$-module. Thus it is isomorphic to some $Y \in \mathcal{Y}$ and $\langle\langle x \rangle\rangle_G \leqslant U_Y$. Setting $F_Y = F \cap U_Y$ for all $Y \in \mathcal{Y}$, we obtain a partition of F as $F = \bigsqcup_{Y \in \mathcal{Y}} F_Y$.

We claim that $\mathcal{Y}$ contains a single element. Indeed, assume this is not the case. For each $Y \in \mathcal{Y}$, the subset F_Y is strictly contained in F, hence is irreducibly faithful by the hypotheses made on F. Let π_Y be an irreducible unitary representation of G witnessing the faithfulness of F_Y, and set $K_Y = U_Y \cap \mathrm{Ker}(\pi_Y)$. Thus every element of F_Y has a non-trivial image in U_Y/K_Y. Moreover, we may view π_Y as an irreducible unitary representation of G/K_Y whose restriction to U_Y/K_Y is faithful. By Lemma 2.8, U_Y/K_Y has a G/K_Y-faithful unitary character. Therefore it is a cyclic $\mathbf{F}_p[G/K_Y]$-module by Proposition 2.15, where p is the exponent of Y. In particular it is a cyclic $\mathbf{Z}[G]$-module

Let now $K = \big\langle \bigcup_{Y \in \mathcal{Y}} K_Y \big\rangle$. Thus K is a normal subgroup of G, and we have a natural direct sum decomposition $K \cong \bigoplus_{Y \in \mathcal{Y}} K_Y$ (see Lemma 2.3). In particular $K \cap U_Y = K_Y$ for all $Y \in \mathcal{Y}$. Moreover, we have $K \cap F = \varnothing$, since otherwise $K \cap F_Y$ would be non-empty for some $Y \in \mathcal{Y}$, which would imply that K_Y contains an element of F_Y. This contradicts the definition of K_Y. Therefore, every element of F has a non-trivial image in G/K.

We may view the quotient U/K as a $\mathbf{Z}[G]$-module. It is semi-simple by Proposition 2.14, as a quotient module of U. Moreover, the direct sum decomposition $U/K \cong \bigoplus_{Y \in \mathcal{Y}} U_Y/K_Y$ is the isotypical decomposition of U/K. We have seen above that the isotypical component U_Y/K_Y of U/K is a cyclic $\mathbf{Z}[G]$-module for each $Y \in \mathcal{Y}$. It follows from Lemma 3.8 that U/K is cyclic. By Proposition 2.15, this means that U/K has a G/K-faithful unitary character. By Lemma 2.9, G/K has an irreducible unitary representation π whose restriction to U/K is faithful. Since every element of F has a non-trivial image in G/K, precomposing π with

the projection $G \twoheadrightarrow G/K$ yields an irreducible unitary representation of G mapping every element of F to a non-trivial operator. Thus F is irreducibly faithful, a contradiction. This proves the claim.

We denote the single element of $\mathcal{Y}$ by W. From now on, denote by p the exponent of W. Since the $\mathbf{Z}[G]$-module W is simple, p is a prime. Thus W is a simple $\mathbf{F}_p[G]$-module, and $U = U_W$ is isomorphic to a direct sum of $\ell + 1$ copies of W for some integer $\ell \geqslant 0$. Since F is not irreducibly faithful, it follows that the restriction to U of every irreducible unitary representation of G cannot be faithful. Therefore U has no G-faithful character by Lemma 2.9. Hence U is not a cyclic $\mathbf{F}_p[G]$-module by Proposition 2.15. In view of Proposition 3.9, this implies that $\ell \geqslant m$, where m is the dimension of W over $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$. This proves (i) and (ii).

It remains to prove that $n = |F| \geqslant q^m + \cdots + q + 1$. Recall from the hypothesis that $\langle\langle x \rangle\rangle_G$ is a simple $\mathbf{F}_p[G]$-submodule of U for all $x \in F$. Assume for a contradiction that $n < q^m + \cdots + q + 1$. Then, by Lemma 3.6, there is an $\mathbf{F}_p[G]$-submodule $B \leqslant U$ with $B \cap \langle\langle x \rangle\rangle_G = \{e\}$ for all $x \in F$, such that U/B is cyclic. It then follows from Lemma 2.9 and Proposition 2.15 that G/B has an irreducible unitary representation whose restriction to U/B is faithful. Viewing that representation as a representation of G, we obtain a contradiction with the fact that F is irreducibly unfaithful. This proves (iii). □

In the introduction, Property $\mathcal{P}(n)$ was defined for all $n \geqslant 1$. For the sake of uniformity in the forthcoming arguments, we extend the definition to the case $n = 0$. Thus every group has Property $\mathcal{P}(0)$, tautologically. The main result of this section is the following.

THEOREM 4.5. — *Let n be a positive integer and G a countable group with Property $\mathcal{P}(n-1)$. Let $F \subset G$ be an irreducibly unfaithful subset of size n, and $U = \langle\langle F \rangle\rangle_G$ the normal subgroup of G generated by F.*

Then there exist a prime p and a finite simple $\mathbf{F}_p[G]$-module W such that the following assertions hold, where $\mathbf{k}$ denotes the centralizer field $\mathcal{L}_{\mathbf{F}_p[G]}(W)$, and $m = \dim_{\mathbf{k}}(W)$, and $q = |\mathbf{k}|$:

(i) U is a finite elementary abelian p-group, contained in the abelian mini-socle $\mathrm{MA}(G)$;
(ii) U is isomorphic as an $\mathbf{F}_p[G]$-module to the direct sum of a number $\ell + 1$ of copies of W, and $\ell \geqslant m$;
(iii) q is a power of p and $q^m + q^{m-1} + \cdots + q + 1 = n$.

Proof. — It follows from the hypotheses that every proper subset of F is irreducibly faithful; in particular $e \notin F$. Hence $F \leqslant \mathrm{Fsol}(G)$ by Corollary 4.3. For every $x \in F$, it follows that the group $\langle\langle x \rangle\rangle_G$ is finite soluble, and therefore has an abelian socle. Since socles are characteristic subgroups, this socle is a finite abelian normal subgroup of G, hence it contains an abelian mini-foot of G. We may therefore choose $b_x \in \langle\langle x \rangle\rangle_G$ such that $\langle\langle b_x \rangle\rangle_G$ is an abelian mini-foot of G.

We set $F' = \{b_x \mid x \in F\}$, so that $|F'| \leqslant |F| = n$. Since $b_x \in \langle\langle x \rangle\rangle_G$, we see that F' is irreducibly unfaithful, because F itself has that property. If $|F'| < n$, then F' would be faithful since G has $\mathcal{P}(n-1)$, a contradiction. Thus $|F'| = n$, and every proper subset of F' is irreducibly faithful. We may therefore apply Lemma 4.4 to the set F'. We denote by p, $U' = \langle\langle F' \rangle\rangle_G$, W, m, q the various objects afforded

in that way. Then Properties (i) and (ii) are satisfied by U'. Moreover we have $q^m + q^{m-1} + \cdots + q + 1 \leqslant n$. Observe that $m \geqslant 1$ and $q \geqslant p \geqslant 2$, so that $n \geqslant 3$. If we had $q^m + q^{m-1} + \cdots + q + 1 \leqslant n-1$, then G would not have Property $\mathcal{P}(n-1)$ by Lemma 4.1. Therefore Property (iii) is also satisfied by U'. It remains to show that $U' = U$, i.e., that $U' = \langle\langle F \rangle\rangle_G$.

Since $b_x \in \langle\langle x \rangle\rangle_G$ for all $x \in F$, we have $U' = \langle\langle F' \rangle\rangle_G \leqslant \langle\langle F \rangle\rangle_G$. Thus it suffices to show that F is contained in U'. Assume for a contradiction that this is not the case, and let $y \in F$ be such that $y \notin U'$. Since $F' \smallsetminus \{b_y\}$ is irreducibly faithful, there exists an irreducible unitary representation ρ of G such that $\rho(b_x) \neq 1$ for all $x \in F \smallsetminus \{y\}$. Let $B = U' \cap \mathrm{Ker}(\rho)$. By Lemma 2.8 and Proposition 2.15, the $\mathbf{F}_p[G]$-module U'/B is cyclic. In particular, it is isomorphic to a direct sum of j copies of W, for some $j \in \{1, \ldots, m\}$, by Lemma 3.4. (The case $j = 0$ is excluded since $n \geqslant 3$.)

Let $r : G \twoheadrightarrow G/B = Q$ be the canonical projection. We have seen that $r(U') = U'/B$ is a cyclic $\mathbf{F}_p[Q]$-module. Thus U'/B has a Q-faithful unitary character by Proposition 2.15.

Since $y \notin U'$, we have $r(y) \notin r(U')$. Since F is contained in $\mathrm{Fsol}(G)$, it follows that $\langle\langle r(y) \rangle\rangle_Q$ is soluble finite, i.e., $r(y) \in \mathrm{Fsol}(Q)$. In particular the socle of $\langle\langle r(y) \rangle\rangle_Q$ is abelian. We may therefore choose $b'_y \in \langle\langle r(y) \rangle\rangle_Q$ such that $\langle\langle b'_y \rangle\rangle_Q$ is an abelian mini-foot of Q. Now we discuss the structure of $\langle\langle b'_y \rangle\rangle_Q$, in order to achieve a contradiction.

Since $\langle\langle b'_y \rangle\rangle_Q$ is a mini-foot of Q, it follows that $\langle\langle b'_y \rangle\rangle_Q$ may be viewed as a simple $\mathbf{Z}[Q]$-module (see Remark 2.12). In particular the normal subgroup

$$N = r(U') \langle\langle b'_y \rangle\rangle_Q$$

is a semi-simple $\mathbf{Z}[Q]$-module, by Proposition 2.14.

We claim that N is not cyclic as a $\mathbf{Z}[Q]$-module. Suppose by contradiction that N is cyclic. Then N has a Q-faithful unitary character by Proposition 2.15. Therefore Q has an irreducible unitary representation whose restriction to N is faithful, by Lemma 2.9. It follows that the set $r(F' \smallsetminus \{b_y\}) \cup \{b'_y\}$ is irreducibly faithful in Q. Notice that, if the kernel of a unitary representation of Q contains $r(x)$ for some x in $F \smallsetminus \{y\}$, then it contains $r(b_x)$ since $b_x \in \langle\langle x \rangle\rangle_G$. Similarly, if that kernel contains $r(y)$, then it contains b'_y. Since $r(F' \smallsetminus \{b_y\}) \cup \{b'_y\}$ is irreducibly faithful in Q, we infer that the set $r(F)$ is irreducibly faithful in Q. Hence F is irreducibly faithful in G, a contradiction. This confirms that the $\mathbf{Z}[Q]$-module N is not cyclic. Since $r(U') = U'/B$ is cyclic, we deduce that $b'_y \notin r(U')$. In particular, we have $N = r(U') \times \langle\langle b'_y \rangle\rangle_Q$.

Since Q is a quotient of G, we may view any $\mathbf{Z}[Q]$-module as a $\mathbf{Z}[G]$-module. We have seen above that $r(U')$ is a cyclic $\mathbf{F}_p[Q]$-module, hence a cyclic $\mathbf{Z}[G]$-module. Since $r(U')$ is a quotient of U', it is isomorphic, as a $\mathbf{Z}[G]$-module, to a direct sum of copies of W. If $\langle\langle b'_y \rangle\rangle_Q$ were not isomorphic to W as a $\mathbf{Z}[G]$-module, it would follow that the decomposition $N = r(U') \times \langle\langle b'_y \rangle\rangle_Q$ would be the isotypical decomposition of N. Since $\langle\langle b'_y \rangle\rangle_Q$ is a simple module, it is cyclic, and it would follow from Lemma 3.8 that N is a cyclic $\mathbf{Z}[G]$-module as well. This contradicts the claim above. We infer that $\langle\langle b'_y \rangle\rangle_Q$ is abelian of exponent p, and isomorphic to W as an $\mathbf{F}_p[G]$-module.

For each $x \in F \smallsetminus \{y\}$, the image $r(b_x)$ is contained in a simple $\mathbf{F}_p[G]$-submodule of N contained in $r(U')$. Since $r(U') = U'/B$ is a direct sum of $j \leqslant m$ copies of W, we deduce from Lemma 3.5 that $r(U')$ contains $q^{j-1}+\cdots+q+1$ simple submodules. Since N is a direct sum of $j+1$ copies of W, it contains $q^j+q^{j-1}+\cdots+q+1$ simple submodules. Since $q^j \geqslant 2$, we deduce that N contains a simple $\mathbf{F}_p[G]$-submodule C which is neither contained in $r(U')$ nor equal to $\langle\langle b'_y \rangle\rangle_Q$. The quotient N/C is a direct sum of at most $j \leqslant m$ copies of W, and thus is cyclic by Lemma 3.4. Therefore Q/C has an irreducible unitary representation whose restriction to N/C is faithful, by Lemma 2.9 and Proposition 2.15. By construction, every element of $r(F' \smallsetminus \{b_y\}) \cup \{b'_y\}$ has a non-trivial image in N/C. We conclude that the set $r(F' \smallsetminus \{b_y\}) \cup \{b'_y\}$ is irreducibly faithful in Q. Therefore, as in the proof of the claim above, we deduce that the set $r(F)$ is also irreducibly faithful in Q. In particular F is irreducibly faithful in G. This final contradiction finishes the proof. □

4.4. **End of proof of Theorem 1.1 and proof of Corollary 1.9.**

Proof of (1) ⇒ (2) in Theorem 1.1. — Let n be a positive integer and G a countable group for which (1) of Theorem 1.1 holds, i.e., a group which does not have Property $\mathcal{P}(n)$. Upon replacing n by a smaller integer, we may assume that G has Property $\mathcal{P}(n-1)$. (Recall that Property $\mathcal{P}(0)$ holds for any group.)

Let $F \subset G$ be an irreducibly unfaithful subset of size n. We invoke Theorem 4.5. This shows that $U = \langle\langle F \rangle\rangle_G$ is a finite normal subgroup which is an elementary abelian p-group, and which is isomorphic to a direct sum of $\ell+1$ copies of a simple $\mathbf{F}_p[G]$-module W of dimension m over $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$, where $\ell \geqslant m$. In particular U has a submodule V which is isomorphic to a direct sum of $m+1$ copies of W. This proves that (2) holds. □

Proof of Corollary 1.9. — That (i) implies (ii) is clear. That (ii) implies (iii) follows from Theorem 1.1.

Assume that (iii) holds. If $\mathrm{MA}(G) = \{e\}$, then (i) holds by Theorem 2.2. If not, let A be a non-trivial finite abelian normal subgroup of G contained in the mini-socle. Let p be a prime dividing $|A|$; let A_p be the p-Sylow subgroup of A. Then A_p is a finite $\mathbf{F}_p[G]$-module, which is semi-simple because A, hence also A_p, is generated by mini-feet of G. Since (iii) holds, A_p is a finite simple $\mathbf{F}_p[G]$-module. By Lemma 2.13 and Proposition 3.9, A_p is generated by a single conjugacy class. Since that holds for all p dividing $|A|$, it follows that A is generated by a single conjugacy class (see Lemmas 2.13 and 3.8). Therefore G is irreducibly faithful by Theorem 2.2. Thus (i) holds. □

5. Irreducibly injective sets

5.1. **Property $\mathcal{Q}(n)$.** Recall from Subsection 1.5 that a subset F of a group G is called **irreducibly injective** if G has an irreducible unitary representation π such that the restriction $\pi|_F$ is injective. We say that G has Property $\mathcal{Q}(n)$ if every subset of G of size $\leqslant n$ is irreducibly injective.

As mentioned earlier, the fact that every group has $\mathcal{P}(1)$ is a classical result of Gelfand–Raikov. That every group has $\mathcal{Q}(1)$ is a trivial fact.

The goal of this section is to compare properties $\mathcal{P}(m)$ and $\mathcal{Q}(n)$. For a group G written multiplicatively and for a subset F of G, we define

$$FF^{-1} = \{z \in G \mid z = xy^{-1} \text{ for some } x, y \in F\}.$$

(When G is abelian and written additively, this is the same as the subset $F - F$ defined in Section 3.) To a subset F of G, we associate a subset $\binom{F}{2}$ of $G \smallsetminus \{e\}$ defined as follows. Let $F^2_{\neq}$ be a subset of $F \times F$ consisting of exactly one of each (x, y), (y, x), for $x, y \in F$ with $x \neq y$. Then

$$\binom{F}{2} = \{z \in G \smallsetminus \{e\} \mid z = xy^{-1} \text{ for some } (x, y) \in F^2_{\neq}\}.$$

In particular, if F is a singleton, then $\binom{F}{2}$ is empty; if F is finite of some size $n \geqslant 2$, then $|\binom{F}{2}| \leqslant \binom{n}{2}$. Note that $\binom{F}{2}$ involves an arbitrary choice (its dependence on F is not canonical), even though it is not apparent in the notation.

The following lemma records the most straightforward implications between Properties P and Q.

LEMMA 5.1. — *Let G be a group and n a positive integer.*

(i) Let F be a finite subset of G of size n; let E be a finite subset of the form $\binom{F}{2}$. Then F is irreducibly injective if and only if E is irreducibly faithful.

(ii) If G has $P\left(\binom{n}{2}\right)$, then G has $\mathcal{Q}(n)$. In particular G has $\mathcal{Q}(2)$.

(iii) If G has $\mathcal{Q}(n+1)$, then G has $\mathcal{P}(n)$.

Proof. — Claim (i) follows from the definitions.

For (ii), let $F \subset G$ be a subset of size at most n. Let $E \subset G \smallsetminus \{e\}$ be a subset of the form $\binom{F}{2}$. Since G has $P\left(\binom{n}{2}\right)$, and as $|E| \leqslant \binom{n}{2}$, there exists an irreducible unitary representation π of G such that $\pi(z) \neq \mathrm{id}$ for all $z \in E$. It follows that $\pi(xy^{-1}) \neq \mathrm{id}$ for all $(x, y) \in F^2_{\neq}$, i.e., $\pi(x) \neq \pi(y)$ for all $(x, y) \in F^2$ with $x \neq y$. Hence G has $\mathcal{Q}(n)$. Applying this fact to $n = 2$, and recalling that every group has $\mathcal{P}(1)$, we deduce that every group has $\mathcal{Q}(2)$.

For (iii), let $F \subset G$ be a subset of size at most n. Since G has $\mathcal{Q}(n+1)$, the set $F \cup \{e\}$ is irreducibly injective. □

Claim (iii) will be strengthened in Proposition 5.3.

Lemma 5.1 implies that a group has Property $\mathcal{Q}(n)$ for all $n \geqslant 1$ if and only if it has Property $\mathcal{P}(n)$ for all $n \geqslant 1$. Observe moreover that a group which has a faithful irreducible unitary representation has Property $\mathcal{Q}(n)$ for all $n \geqslant 1$. Therefore, our Corollary 1.9 can be completed as follows:

COROLLARY 5.2. — *For a countable group G, the equivalent assertions (i)–(iii) from Corollary 1.9 are also equivalent to:*

(iv) G has $\mathcal{Q}(n)$ for all $n \geqslant 1$.

5.2. **$\mathcal{Q}(n)$ implies $\mathcal{P}(n)$.** Using Theorem 1.1, we obtain for countable groups the following small improvement of Lemma 5.1(iii).

PROPOSITION 5.3. — *If a countable group has $\mathcal{Q}(n)$ for some $n \geqslant 1$, then it also has $\mathcal{P}(n)$.*

Proof. — Since every group has $\mathcal{Q}(1)$ and $\mathcal{P}(1)$, we may assume that $n \geqslant 2$. Let G be a countable group satisfying $\mathcal{Q}(n)$. By Lemma 5.1(iii), the group G has $\mathcal{P}(n-1)$.

Suppose for a contradiction that G does not have $\mathcal{P}(n)$. We may then invoke Theorem 1.1. Let V, m, q be as in Theorem 1.1(2); in particular V is a finite

abelian normal subgroup of G and we have $q^m + \cdots + q + 1 \leqslant n$. If we had $q^m + \cdots + q + 1 < n$, then the other implication of Theorem 1.1 would imply that G does not have $\mathcal{P}(n-1)$, in contradiction with the previous paragraph. We conclude that $q^m + \cdots + q + 1 = n$.

By Lemma 3.7, the group V has a subset F of size $q^m + \cdots + q + 1$ such that the set $F - F$ contains a non-zero element of each abelian mini-foot of G contained in V. By Lemma 4.1, given an irreducible unitary representation π of G, the kernel $\mathrm{Ker}(\pi)$ intersects V non-trivially. More precisely, $\mathrm{Ker}(\pi)$ contains an abelian mini-foot of G contained in V, and hence a non-zero element of $F - F$. Therefore $\pi(x) = \pi(y)$ for some $x \neq y \in F$. This proves that F is not irreducibly injective. Since $|F| = n$, we deduce that G does not have $\mathcal{Q}(n)$, a contradiction. □

5.3. **The constant $\alpha_{(q,m)}$.** Theorem 5.8, which is the main result of this section, depends on technical results for which we introduce the following notation. Let q be a power of some prime p and $m \geqslant 1$ be an integer. Let $G_{(q,m)} = \mathrm{GL}(W) \ltimes V$ be the group defined in Example 1.6, whose notation is retained here. We define

$$\alpha_{(q,m)}$$

as the smallest cardinality of a subset $F \subset V$ such that the difference set $F - F$ contains a non-zero vector of each of the $q^m + \cdots + q + 1$ simple $\mathbf{F}_p[G_{(q,m)}]$-submodules of V. Lemma 3.7 implies that the inequality

$$\alpha_{(q,m)} \leqslant q^m + \cdots + q + 1$$

holds for all q and m. The following result shows that the constant $\alpha_{(q,m)}$ is somehow independent of the group $G_{(q,m)}$.

Lemma 5.4. — *Let G be a group. Suppose that there exist a prime p, a positive integer m, a finite simple $\mathbf{F}_p[G]$-module W of dimension m over $\mathbf{k} = \mathcal{L}_{\mathbf{F}_p[G]}(W)$, and a finite normal subgroup V of G which is an elementary abelian p-group and which is isomorphic as $\mathbf{F}_p[G]$-module to the direct sum of $m+1$ copies of W.*

Then $\alpha_{(q,m)}$ is equal to the smallest cardinality of a subset $F \subset V$ such that $F - F$ contains a non-zero element of each of the simple $\mathbf{F}_p[G]$-submodules of V.

Proof. — We start with a preliminary observation. Consider a ring R, a simple R-module S, and a semi-simple R-module U which is a direct sum of ℓ copies of S. Then every simple submodule of U is isomorphic to S, as an R-module. This follows by a straightforward induction on ℓ, using Goursat's lemma (Lemma 3.1).

We return now to the situation of the lemma. The fact that W is a $\mathbf{k}[G]$-module yields a homomorphism $G \to \mathrm{GL}_m(\mathbf{k}) = \mathrm{GL}(W)$. Set $L = \mathrm{GL}(W)$, where W is viewed as a vector space over $\mathbf{k}$. We may view V both as an $\mathbf{F}_p[G]$-module and as an $\mathbf{F}_p[L]$-module. Note that $\mathcal{L}_{\mathbf{F}_p[G]}(W) = \mathbf{k} = \mathcal{L}_{\mathbf{F}_p[L]}(W)$.

By the preliminary observation, every simple $\mathbf{F}_p[L]$-submodule of V is isomorphic to W, as an $\mathbf{F}_p[L]$-module. In particular, each of them is also a simple $\mathbf{F}_p[G]$-submodule of V. In view of Lemma 3.5, we deduce that the additive subgroups of V which are simple $\mathbf{F}_p[G]$-submodules of V are exactly the additive subgroups of V which are simple $\mathbf{F}_p[L]$-submodules of V. The required assertion follows. □

Clearly, we have

$$\binom{\alpha_{(q,m)}}{2} \geqslant q^m + \cdots + q + 1.$$

The following lemma provides the values of $\alpha_{(q,m)}$ for some small q and m. The proof of the last item was computer-aided. We are grateful to Max Horn for having independently checked the result.

LEMMA 5.5. — *With the notation $\alpha_{(q,m)}$ defined above, we have:*

(i) $\alpha_{(2,1)} = 3$.
(ii) $\alpha_{(3,1)} = \alpha_{(4,1)} = \alpha_{(5,1)} = 4$.
(iii) $\alpha_{(7,1)} = \alpha_{(8,1)} = \alpha_{(2,2)} = 5$.
(iv) $\alpha_{(9,1)} = 6$.

Proof. — Consider as above the group $G_{(q,m)} = \mathrm{GL}(W) \ltimes V$. Recall that $q = |\mathbf{k}|$, $m = \dim_{\mathbf{k}}(W)$, and $V = W \oplus \cdots \oplus W$ ($m+1$ times).

If $m = 1$, the simple $\mathbf{F}_p[\mathbf{k}^\times]$-submodules of V coincide with the 1-dimensional subspaces of $V = \mathbf{k}^2$. As noticed above, we have $\binom{\alpha_{(q,1)}}{2} \geqslant q+1$. For $q = 2$ [respectively, $3 \leqslant q \leqslant 5$, $7 \leqslant q \leqslant 9$], this implies $\alpha_{(2,1)} \geqslant 3$ [respectively $\alpha_{(q,1)} \geqslant 4$, $\alpha_{(q,1)} \geqslant 5$]. For $q \in \{2,3,4,5,7,8\}$, to show that this lower bound on $\alpha_{(q,1)}$ is attained, it suffices to exhibit a subset $F \subset V$ of the corresponding size such that $F - F$ has the required property. One can check that the following sets do the job, where the elements of the prime field $\mathbf{F}_p$ are denoted by $0, 1, \ldots, p-1$.

For $q = 2$, we set $F = \{(0,0), (1,0), (0,1)\}$.

For $q = 3$, we set $F = \{(0,0), (0,1), (1,0), (1,1)\}$.

For $q = 4$, we set $F = \{(0,0), (1,0), (0,1), (1,x)\}$, where $\mathbf{k}$ has been identified with $\mathbf{F}_2[x]/(x^2+x+1)$.

For $q = 5$, we set $F = \{(0,0), (1,0), (0,1), (3,4)\}$.

For $q = 7$, we set $F = \{(0,0), (1,0), (0,1), (2,3), (5,2)\}$.

For $q = 8$, we set $F = \{(0,0), (1,0), (0,1), (1,x), (x^2+x, x^2)\}$, where $\mathbf{k}$ has been identified with $\mathbf{F}_2[x]/(x^3+x+1)$.

For $q = 9$, the situation is different. We know that $\binom{\alpha_{(9,1)}}{2} \geqslant 10$, so that $\alpha_{(9,1)} \geqslant 5$. With the help of a computer, we checked that no subset F in V of size 5 is such that $F - F$ contains a non-zero vector of each of the 10 one-dimensional subspaces of V. On the other hand, one verifies that the set

$$F = \{(0,0), (1,0), (0,1), (0,2), (0,x), (2,2x+1)\}$$

has this property, where $\mathbf{k}$ has been identified with $\mathbf{F}_3[x]/(x^2-x-1)$. Thus $\alpha_{(9,1)} = 6$.

Finally, consider the case of $m = 2$ and $q = 2$. Since $\binom{\alpha_{(2,2)}}{2} \geqslant 2^2+2+1 = 7$, we have $\alpha_{(2,2)} \geqslant 5$. Let a be a non-zero vector in W. One checks that the set

$$F = \{(0,0,0), (a,0,0), (0,a,0), (0,0,a), (a,a,a)\}$$

satisfies the required condition, so that $\alpha_{(2,2)} = 5$. □

5.4. $\mathcal{P}(\binom{n}{2}-1)$ **sometimes implies** $\mathcal{Q}(n)$**.** We are now ready to present the main technical result of this section. It may be viewed as a supplement to Lemma 5.1(ii).

PROPOSITION 5.6. — *Let n be an integer, $n \geqslant 3$. Let G be a countable group with Property $P\left(\binom{n}{2}-1\right)$. Assume that, for all pairs (q,m) consisting of a prime power q and an integer m such that $q^m + \cdots + q + 1 = \binom{n}{2}$, we have $\alpha_{(q,m)} > n$.*

Then G has $\mathcal{Q}(n)$.

Proof. — Suppose for a contradiction that G does not have $\mathcal{Q}(n)$. Let $F \subset G$ be a subset of size $\leqslant n$ which is not irreducibly injective in G. Upon replacing F by Fx^{-1} for some $x \in F$, we may assume without loss of generality that F contains the neutral element e.

Let $E \subset G \smallsetminus \{e\}$ be a subset of the form $\binom{F}{2}$; recall that $|E| \leqslant \binom{n}{2}$. Since $e \in F$, we may choose E in such a way that E contains $F \smallsetminus \{e\}$. It follows from Lemma 5.1(i) that E is irreducibly unfaithful. Since G has $P\left(\binom{n}{2} - 1\right)$ by hypothesis, we deduce that $|E| = \binom{n}{2}$. Set $U = \langle\langle E \rangle\rangle_G$. Since $F \smallsetminus \{e\} \subset E$, we have $F \subset U$.

We invoke Theorem 4.5 and use its notation, except for F there being E here. In particular, there exist a prime p and a simple $\mathbf{F}_p[G]$-module W such that U is isomorphic as an $\mathbf{F}_p[G]$-module to the direct sum of $\ell + 1$ copies of W for some $\ell \geqslant m$. By Theorem 4.5(iii), we have $q^m + \cdots + q + 1 = \binom{n}{2}$. Set $V = \bigoplus_0^m W$.

We next claim that there exists a surjective map of $\mathbf{F}_p[G]$-modules $r : U \twoheadrightarrow V$ whose restriction to F is injective. If $\ell = m$, then $U = V$ and r can be defined as the identity map. If $\ell > m$, we proceed by induction on $\ell - m$. Lemma 3.5 ensures that the number of simple $\mathbf{F}_p[G]$-submodules of U is strictly larger than $\binom{n}{2}$. Since $\binom{n}{2} = |E|$, there exists a simple $\mathbf{F}_p[G]$-submodule U_0 of U such that $U_0 \cap E = \{0\}$. If $r_0 : U \twoheadrightarrow U/U_0$ denotes the quotient map, we have $\mathrm{Ker}(r_0) \cap E = \{0\}$, and it follows that the restriction of r_0 to F is injective. Since U/U_0 is isomorphic to a direct sum of ℓ copies of W, the induction hypothesis guarantees the existence of a surjective map of $\mathbf{F}_p[G]$-modules $r_1 : U/U_0 \twoheadrightarrow V$ whose restriction to $r_0(F)$ is injective. The map $r = r_1 \circ r_0 : U \twoheadrightarrow V$ satisfies the required property. This proves the claim.

Set $E' = r(E)$, $F' = r(F)$ and $K = \mathrm{Ker}(r)$. Since K is an $\mathbf{F}_p[G]$-submodule of U, we may view it as a normal subgroup of G. We view E', F' and V as subsets of the quotient group $G' = G/K$; observe that $E' \subset G' \smallsetminus \{e\}$ is of the form $\binom{F'}{2}$. Since F is not irreducibly injective in G, it follows that F' is not irreducibly injective in G'. Hence E' is not irreducibly faithful in G'. Therefore E' contains a non-zero element in each of the simple submodules of V, by Lemma 4.1. Recalling that $E' \subset F' - F'$, we deduce from Lemma 5.4 that $\alpha_{(q,m)} \leqslant |F'|$. Since $|F'| = |F| = n$, this contradicts the hypothesis that $\alpha_{(q,m)} > n$. □

Remark 5.7. — As mentioned in Section 1.1, the Goormaghtigh Conjecture predicts that for every integer ℓ, there exists at most one prime power q and one positive integer m such that $q^m + \cdots + q + 1 = \ell$, except for $\ell = 31$. Since 31 is not of the form $\binom{n}{2}$, that conjecture predicts that the condition from Proposition 5.6 needs to be checked for at most one value of q and m, once the integer n is fixed.

THEOREM 5.8. — *Let G be a group. Then G has Properties $\mathcal{P}(2)$ and $\mathcal{Q}(2)$. Suppose moreover that G is countable; then:*

(i) G has $\mathcal{Q}(3)$ if and only if G has $\mathcal{P}(3)$.
(ii) G has $\mathcal{Q}(4)$ if and only if G has $\mathcal{P}(6)$.
(iii) G has $\mathcal{Q}(5)$ if and only if G has $\mathcal{P}(9)$.

Proof. — By Lemma 5.1(ii), Property $\mathcal{P}(\binom{n}{2})$ implies $\mathcal{Q}(n)$. For $n = 3$, and 4, this yields $\mathcal{P}(3) \Rightarrow \mathcal{Q}(3)$ and $\mathcal{P}(6) \Rightarrow \mathcal{Q}(4)$. By Proposition 5.3, we have $\mathcal{Q}(3) \Rightarrow \mathcal{P}(3)$.

Among other things, this proves (i).

Let now G be a countable group that does not satisfy $\mathcal{P}(6)$. To show (ii), it remains to show that G does not have $\mathcal{Q}(4)$. We may assume that G has $\mathcal{Q}(3)$, since otherwise we are already done. Hence, G has $\mathcal{P}(3)$ by (i). Let n be the least integer such that G does not have $\mathcal{P}(n)$. Hence n is one of 4, 5, or 6.

If $n = 4$, we deduce from Theorem 1.1 that G contains a normal subgroup V isomorphic to $\mathbf{F}_3 \oplus \mathbf{F}_3$, on which the G-action is by scalar multiplication. Let π be an irreducible unitary representation of G. Set $Q = G/\mathrm{Ker}(\pi)$ and let $r : G \twoheadrightarrow Q$ be the canonical projection. By Proposition 2.1(7), the subgroup $r(V) \leqslant Q$ is generated by abelian mini-feet of Q, and it is an elementary abelian 3-group. Suppose that $r(V)$ were isomorphic to V; note that Q would act on V by scalar multiplication; since Q is irreducibly faithful, hence has Property $\mathcal{P}(4)$, this would contradict Theorem 1.1. Hence the restriction of r to V cannot be faithful. (Note moreover that, for each of the simple $\mathbf{F}_3[G]$-modules W contained in V, the restriction to W of the projection r is either injective or the zero map.) Therefore $\mathrm{Ker}(r) = \mathrm{Ker}(\pi)$ contains at least one of the 4 cyclic subgroups of order 3 of V. Lemma 5.5 yields a subset F of V of size 4 such that $F - F$ contains a non-trivial element of each of the 4 cyclic subgroups of order 3 of V. Therefore $\pi(a) = \pi(b)$ for some a, b distinct in F. This shows that G does not have Property $\mathcal{Q}(4)$.

If $n = 5$ and $n = 6$, similar arguments using Lemmas 5.4 and 5.5 apply, each time with $|F| = 4$. This confirms that (ii) holds.

Arguing similarly using Theorem 1.1 and Lemma 5.5, we see that $\mathcal{Q}(5)$ implies $\mathcal{P}(9)$. Conversely, invoking Proposition 5.6 for $n = 5$, we deduce that $\mathcal{P}(9)$ implies $\mathcal{Q}(5)$ since $\alpha_{(9,1)} = 6$ by Lemma 5.5. This proves (iii). □

5.5. **From $\mathcal{Q}(n)$ to additive combinatorics.** Theorem 5.8 suggests the following question.

Question 5.9. — *Can we characterize Property $\mathcal{Q}(n)$ by an algebraic property of G, in the same vein as in Theorem 1.1 ?*

In particular, is it true that, for each $n \geqslant 1$, there exists an integer $f(n) \geqslant 1$ such that a countable group G has Property $\mathcal{Q}(n)$ if and only if it has Property $\mathcal{P}(f(n))$?

The proof of Theorem 5.8 suggests that an answer to Question 5.9 might require to compute the numbers $\alpha_{(q,m)}$ for all (q, m). This is confirmed by the following observation.

Observation 5.10. — *The group $G_{(q,m)}$ from Example 1.6 has the Property $\mathcal{Q}(\alpha_{(q,m)} - 1)$, but not $\mathcal{Q}(\alpha_{(q,m)})$.*

Proof. — That $G = G_{(q,m)}$ does not have $\mathcal{Q}(\alpha_{(q,m)})$ follows from the definition and from Lemma 5.1, in view of Theorem 1.1.

In order to show that $G_{(q,m)}$ has $\mathcal{Q}(\alpha_{(q,m)} - 1)$, we fix a subset F of G such that $|F| < \alpha_{(q,m)}$. We shall prove that FF^{-1} is irreducibly faithful. This implies that F is irreducibly injective, as required. Modules below refer to the ring $\mathbf{F}_p[G]$.

Notice that FF^{-1} remains unchanged when F is replaced by a translate Fg, for some $g \in G$. Without loss of generality we may thus assume that F contains e. In particular $F \subseteq FF^{-1}$.

Let $\{g_1, \ldots, g_k\} \subset G$ be a set of minimal cardinality such that $F \subset \bigcup_{i=1}^{k} Vg_i$. For each i, set $F_i = F \cap Vg_i$. Notice that if $x \in F_i$ and $y \in F_j$ with $i \neq j$, then

$xy^{-1} \notin V$ because $g_i g_j^{-1} \notin V$. Therefore the intersection $FF^{-1} \cap V$ coincides with $\bigcup_{i=1}^k F_i F_i^{-1}$. For each i, we set $F_i' = F_i g_i^{-1}$, and set $F' = \bigcup_{i=1}^k F_i'$. Hence

$$(\sharp) \qquad |F'| \leqslant |F|, \ \ F' \subseteq V \ \text{ and } \ F'(F')^{-1} \supseteq FF^{-1} \cap V.$$

We next observe that, if W is any simple submodule of V, then the quotient group G/W is irreducibly faithful. This follows from Theorem 1.1 and Corollary 1.9 (using a similar argument as in the discussion of Example 1.6). Therefore, if FF^{-1} were not irreducibly faithful, then it would contain a non-zero element of each simple submodule of V. By $(\sharp)$, $F'(F')^{-1}$ would also contain a non-zero element of each simple submodule of V. This would contradict the sequence of inequalities $|F'| \leqslant |F| < \alpha_{(q,m)}$. It follows that FF^{-1} is irreducibly faithful, and this ends the proof. □

In particular, answering Question 5.9 for $C_p \times C_p = G_{(p,1)}$ amounts to compute $\alpha_{(p,1)}$. This happens to be an open problem in additive combinatorics, see Question 5.2 in [9]. As pointed out in this reference, the value of $\alpha_{(p,1)} = n_p$ can be estimated as follows. On the one hand, since

$$\frac{n_p^2}{2} > \binom{n_p}{2} \geqslant p + 1 > p,$$

we have $n_p > \sqrt{2p}$. On the other hand, using Theorems 1.2 and 2.1 from [11], we obtain the upper bound

$$n_p \leqslant 2\lceil \sqrt{p} \rceil + 1.$$

However, determining the exact value of n_p remains an open problem. We are grateful to Ben Green for point out the reference [9] and for discussing it with us.

Appendix A. A finite group all of whose irreducible representations have non-abelian kernels

We know from Proposition 2.16 that every countable group G has an irreducible unitary representation whose kernel is contained in $\mathrm{Fsol}(G)$, and we have cited in Remark 2.18 the result according to which every finite group has an irreducible representation with nilpotent kernel. Short of having found in the literature appropriate references for groups without irreducible representations having abelian kernels, we indicate here an example, long known to experts.

Let D_8 denote the dihedral group of order 8. The centre of D_8 is cyclic of order 2. For $i = 1, 2, 3$, let H_i be a group isomorphic to D_8, and let z_i be the non-trivial element of the centre of H_i. We set

$$G = (H_1 \times H_2 \times H_3)/\langle z_1 z_2 z_3 \rangle.$$

Thus G is a nilpotent group of order $2^8 = 256$. Its centre $Z(G)$ is isomorphic to $C_2 \times C_2$. The socle of G coincides with its centre, and $\mathrm{Fsol}(G)$ is the group G itself (see Example 2.4(6)).

Proposition A.1. — *For every abelian normal subgroup N in G, the centre of the quotient G/N is not cyclic.*

Proof. — The natural homomorphism $H_1 \times H_2 \times H_3 \to G$ induces an embedding $H_i \to G$ for each i. We identify H_i with its image in G. In particular we view z_1, z_2, z_3 as elements of G. The centre of G is $Z(G) = \{e, z_1, z_2, z_3\}$.

We assume for a contradiction that N is an abelian normal subgroup of G such that G/N has a cyclic centre. Since the centre of G is not cyclic, we have $N \neq \{e\}$. Let $r : G \twoheadrightarrow G/N$ be the canonical projection.

Let $i \in \{1,2,3\}$. Since N is abelian and H_i is not, $r(H_i) \cong H_i/H_i \cap N$ is non-trivial. In particular $r(H_i)$ has a non-trivial centre. We may thus choose an element $h_i \in H_i$ such that $r(h_i)$ is a non-trivial element of the centre $Z(r(H_i))$. Since H_1, H_2 and H_3 commute pairwise in G, and since G is generated by these subgroups, we have $Z(H_i) \leqslant Z(G)$ and $Z(r(H_i)) \leqslant Z(r(G))$. In particular $r(h_i) \in Z(G/N)$.

Since G is a 2-group, every non-trivial normal subgroup has a non-trivial intersection with the centre $Z(G)$. Thus there exists $j \in \{1,2,3\}$ such that $z_j \in N$. Since $Z(G/N)$ is cyclic and $Z(r(H_j)) \leqslant Z(G/N)$, it follows that $Z(r(H_j))$ is cyclic. Since $N \cap H_j$ is a non-trivial normal subgroup of $H_j \cong D_8$, the quotient $r(H_j) \cong H_j/(N \cap H_j)$ is abelian. Therefore, it coincides with its centre, hence it is cyclic. The only abelian normal subgroups of $H_j \cong D_8$ affording a cyclic quotient group are its subgroups of index 2. Thus $r(H_j) \cong H_j/(N \cap H_j)$ is of order 2. In particular $N \cap H_j$ is a maximal subgroup of H_j, and $r(h_j)$ is of order 2. Moreover we have $H_j = \langle h_j \rangle (N \cap H_j)$ since $r(h_j) \neq e$ and hence $h_j \notin N \cap H_j$.

Let now $i \in \{1,2,3\}$ such that $i \neq j$. We know that $Z(G/N)$ is cyclic, and that $r(h_i)$ and $r(h_j)$ are two non-trivial elements in $Z(G/N)$. Since moreover $r(h_j)$ is of order 2, we infer that $r(h_i)^k r(h_j) = e$ for some integer k. In other words $h_i^k h_j \in N$. Since N is abelian, it follows that $h_i^k h_j$ commutes with $N \cap H_j$. Moreover h_i commutes with H_j, hence h_i^k commutes with $N \cap H_j$. It follows that h_j commutes with $N \cap H_j$. Since N is abelian and since $H_j = \langle h_j \rangle (N \cap H_j)$, it follows that $H_j \cong D_8$ is abelian, which is absurd. □

By Schur's Lemma, the image $\pi(G)$ of G under any irreducible representation π has cyclic centre. It follows from Proposition A.1 that the kernel of π cannot be abelian. Thus we obtain:

Corollary A.2. — *Every irreducible representation of G has a non-abelian kernel.*

Here is another proof of Corollary A.2. Let z denote the non-trivial element of the centre of D_8. The group D_8 has 4 irreducible representations of degree 1, of which the kernels contain z, and one irreducible representation π of degree 2, such that $\pi(z) = -\mathrm{id}$. Consequently, the group $H_1 \times H_2 \times H_3$ has

- 64 irreducible representations of degree 1,
- 48 irreducible representations of degree 2,
- 12 irreducible representations of degree 4,
- 1 irreducible representation of degree 8,

and the irreducible representations having kernels containing $z_1 z_2 z_3$ are precisely those of dimensions 1 and 4. It follows that G has 64 irreducible representations of degree 1, none of them with abelian kernel, and 12 irreducible representations of degree 3, each having a kernel isomorphic to D_8.

Acknowledgements

P.-E.C. is a F.R.S.-FNRS senior research associate. This work was started at the Bernoulli Center of EPFL, during the project *Descriptive set theory and Polish groups*; the authors are grateful for support and hospitality.

References

[1] K. Bauer, D. Sen, and P. Zvengrowski, *A generalized Goursat lemma*. Tatra Mt. Math. Publ. **64** (2015), 1–19.

[2] B. Bekka and P. de la Harpe, *Irreducibly represented groups*. Comment. Math. Helv. **83** (2008), 847–868.

[3] M. Bhargava, *When is a group the union of proper normal subgroups?* Amer. Math. Monthly **109** (2002), no. 5, 471–473.

[4] N. Bourbaki, *Algèbre, Chapitres 1 à 3*. Bourbaki, 1970.

[5] N. Bourbaki, *Algèbre, Chapitre VIII, Modules et anneau semi-simples*. Hermann, 1958.

[6] N. Bourbaki, *Théories spectrales, Chapitres 1 et 2*. Hermann, 1967.

[7] W. Burnside, *The theory of groups of finite order*, 2nd Edition. Cambridge Univ. Press, 1911. Reprint, Dover, 1955.

[8] Y. Bugeaud and T.N. Shorey, *On the Diophantine equation* $\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1}$. Pacific J. Math. **207** (2002), no. 1, 61–75.

[9] E.E. Croot, E. Samuel III, and V.F. Lev, *Open problems in additive combinatorics*. Amer. Math. Soc., Proc. Lecture Notes **43** (2007), 207–233.

[10] J. Dixmier, *Les C*-algèbres et leurs représentations*, deuxième édition. Gauthier–Villars, 1969 [First Edition 1964, English translation North-Holland 1977].

[11] M. Fitch, and R. Jamison, *Minimum sum covers of small cyclic groups*. Proceedings of the Thirty-first Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 2000). Congr. Numer. **147** (2000), 65–81.

[12] L. Fuchs, *Infinite abelian groups. Vol. I*. Academic Press, 1970.

[13] W. Gaschütz, *Endliche Gruppen mit treuen absolut–irreduziblen Darstellungen*. Math. Nach. **12** (1954), 253–255.

[14] I. Gelfand and D. Raikov, *Irreducible unitary representations of locally bicompact groups*. Rec. Math. [Mat. Sbornik] N.S. **13(55)** (1943), 301–316. I.M. Gelfand, *Collected papers*, Volume II, 3–17.

[15] R. Goormaghtigh. L'intermédiaire des Mathématiciens **24** (1917), 88.

[16] F. Greenleaf and M. Moskowitz, *Cyclic vectors for representations of locally compact groups*. Math. Ann. **190** (1971), 265–288.

[17] P. de la Harpe, *Topics in geometric group theory*. The University of Chicago Press, 2000.

[18] B. He, *A remark on the Diophantine equation* $\frac{x^3-1}{x-1} = \frac{y^n-1}{y-1}$. Glas. Mat. Ser. III **44**(**64**), no. 1 (2009), 1–6.

[19] B. Huppert, *Character theory of finite groups*. W. de Gruyter, 1998.

[20] I.M. Isaacs, *Character theory of finite groups*. Academic Press, 1976.

[21] E. Kowalski, *An introduction to the representation theory of groups*. Graduate Studies in Mathematics **155**, Amer. Math. Soc., 2014.

[22] J. Lambek, *Lectures on rings and modules*, Second Edition. Chelsea, 1976. [First Edition, Blaisdell, 1966.]

[23] G.W. Mackey, *The theory of unitary group representations*. University of Chicago Press, 1976.

[24] B.H. Neumann, *Some remarks on infinite groups*, J. London Math. Soc. **12** (1937), 120–127.

[25] *The On-Line Encyclopedia of Integer Sequences*. On line: `https://oeis.org`

[26] N. Radu, *A classification theorem for boundary 2-transitive automorphisms of trees*. Invent. Math. **209** (2017), no. 1, 1–60.

[27] R. Ratat. L'intermédiaire des Mathématiciens **23** (1916), 150.

[28] R. Remak, *Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen*. J. reine angew. Math. **162** (1930), 1–16.

[29] D.J.S. Robinson, *A course in the theory of groups*, Second Edition. Graduate Texts in Math. **80**, Springer, 1996.

[30] Z. Sasvári, *On a refinement of the Gel'fand–Raikov theorem*. Math. Nachr. **150** (1991), 185–187.

[31] Z. Sasvári, *Positive definite and definitizable functions*. Academic Verlag, 1994.

[32] D. Segal, *Polycyclic groups*. Cambridge Univ. Press, 1983.

[33] K. Shoda, *Bemerkungen über vollständig reduzible Gruppen*. J. Fac. Sci., Univ. Tokyo, Sect. I **2** (1931), 203–209.

[34] F. Szechtman, *Groups having a faithful irreducible representation*. J. Algebra **454** (2016), 292–307.

[35] M.E. Walter, *A duality between locally compact groups and certain Banach algebras*. J. Functional Analysis **17** (1974), 131–160.

Manuscript received October 18, 2019,
revised March 31, 2020,
accepted April 1, 2020.

Pierre-Emmanuel CAPRACE
UCLouvain – IRMP, Chemin du Cyclotron 2, box L7.01.02, B-1348 Louvain-la-Neuve
pe.caprace@uclouvain.be

Pierre DE LA HARPE
Section de mathématiques, Université de Genève, C.P. 64, CH-1211 Genève 4
Pierre.delaHarpe@unige.ch