GROUPS WITH IRREDUCIBLY UNFAITHFUL SUBSETS FOR UNITARY REPRESENTATIONS

PIERRE-EMMANUEL CAPRACE AND PIERRE DE LA HARPE

Abstract. Let G be a group and n a positive integer. We say G has Property $P(n)$ if, for every subset $F \subseteq G$ of size n, there exists an irreducible unitary representation π of G such that $\pi(x) \neq \mathrm{id}$ for all $x \in F \smallsetminus \{e\}$. Every group has $P(1)$ by a classical result of Gelfand and Raikov. Walter proved that every group has $P(2)$; it is easy to see that some groups do not have $P(3)$. We provide an algebraic characterization of the countable groups (finite or infinite) that have $P(n)$. We deduce that if a countable group G has $P(n-1)$ but does not have $P(n)$, then n is the cardinality of a projective space over a finite field.

1. Introduction

Fidèle, infidèle ?
Qu'est-ce que ça fait,
Au fait ?
Paul Verlaine, *Chansons pour elle*, 1891

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

Every group has Property $P(1)$. 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 [GeRa–43].

The starting point of this work is the following refinement of the Gelfand–Raikov Theorem due to Walter:

Every group has Property $P(2)$.

Date: July 13, 2018.
2000 *Mathematics Subject Classification.* 43A65, 22D10.
Key words and phrases. Countable group, unitary representation, irreducible representation, faithful representation.
P.-E.C. is a F.R.S.-FNRS senior research associate. This work was accomplished at the Bernoulli Center of EPFL, during the project *Descriptive set theory and Polish groups*; the authors are grateful for support and hospitality.

In other words, *in a group, every couple is irreducibly faithful(!)*. See [Walt–74, Proposition 2], as well as [Sasv–91] and [Sasv–95, 1.8.7].

It is clear that Property $P(3)$ 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 $P(3)$.

The goal of this note is to characterize groups with $P(n)$ for all $n \geq 3$. 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 [BeHa–08].

Before stating our main result, we need the following preliminaries. For any prime power q, we denote by $\mathbf{F}_q$ the finite field of order q. For a group G, we denote by $\mathbf{F}_q[G]$ its group algebra over $\mathbf{F}_q$. We recall that any abelian group V whose exponent is a prime p carries the structure of a vector space over $\mathbf{F}_p$, which is invariant under all elements of $\mathrm{Aut}(V)$. In other words, the group structure on V canonically determines a $\mathbf{F}_p$-linear structure. In particular, an abelian normal subgroup V of exponent p in a group G may be viewed, in a canonical way, as a $\mathbf{F}_p[G]$-module. We also recall that if W is a simple $\mathbf{F}_p[G]$-module, then Schur's Lemma ensures that the **commutant**

$$\mathrm{C}_{\mathrm{End}(W)}(G) = \{\alpha \in \mathrm{End}(W) \mid g.\alpha(w) = \alpha(g.w) \text{ for all } g \in G, \ w \in W\}$$

is a division algebra over $\mathbf{F}_p$. If in addition W is finite, then $\mathrm{C}_{\mathrm{End}(W)}(G)$ is a finite field by Wedderburn's Theorem. In that case, we may write $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$ for some power q of p. Moreover we may view W as a $\mathbf{F}_q[G]$-module.

Our main result reads as follows.

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

(1) *G does not have $P(n)$.*
(2) *There exist a prime p, a positive integer m, a finite abelian normal subgroup V in G of exponent p, and a finite simple $\mathbf{F}_p[G]$-module W of dimension m over $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$, enjoying the following properties:*
    (i) *V is isomorphic to the direct sum of $m+1$ copies of W, as a $\mathbf{F}_p[G]$-module;*
    (ii) *$q^m + q^{m-1} + \cdots + q + 1 \leq n$.*

To the best of our knowledge, Properties $P(n)$ have not been investigated for finite groups.

The following easy consequence of Theorem 1.1 shows that Klein's Vierergruppe is indeed the only obstruction to $P(3)$.

Corollary 1.2. *A countable group has $P(3)$ if and only if its center does not contain any subgroup isomorphic to $C_2 \times C_2$.*

Theorem 1.1 also has the following immediate consequence:

Corollary 1.3. *Let n be an integer, $n \geq 2$. Suppose that there is no prime power q and integer $m \geq 1$ such that $n = q^m + q^{m-1} + \cdots + q + 1$.*

Every countable group that has $P(n-1)$ also has $P(n)$.

Since 2 is not of the form $q^m + q^{m-1} + \cdots + q + 1$ for any prime power q and any $m \geq 1$, we recover, in the case of discrete groups, the fact that every countable group has $P(2)$.

On the other hand, when $n = q^m + q^{m-1} + \cdots + q + 1$, we have the following.

Example 1.4. Consider a prime p, a power q of p, an integer $m \geq 1$, the vector space $W = \mathbf{F}_q^m$, and the group $\mathrm{GL}(W) = \mathrm{GL}_m(\mathbf{F}_q)$. Let $V_0, V_1, \dots, V_m$ be $m+1$ copies of W; set $V = \bigoplus_{i=0}^m V_i$, viewed as a $\mathbf{F}_p[\mathrm{GL}(W)]$-module. Define the semi-direct product group

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

It is straightforward to check that every abelian normal subgroup of $G_{(q,m)}$ is contained in V, and that every minimal abelian normal subgroup of $G_{(q,m)}$ is isomorphic to W as a $\mathbf{F}_p[G_{(q,m)}]$-module.

Therefore, if $n = q^m + q^{m-1} + \cdots + q + 1$, Theorem 1.1 implies that $G_{(q,m)}$ has property $P(n-1)$ but not $P(n)$.

Notice that the group $G_{(q,1)}$ is the semi-direct product $\mathbf{F}_q^* \ltimes (\mathbf{F}_q \oplus \mathbf{F}_q)$. The group $G_{(3,1)}$ appears in [Burn–11, Note F] as an example of a centerless finite group which does not admit any faithful irreducible representation. The group $G_{(4,1)}$ appears in [Isaa–76, Problem 2.19] for the same reason. Note that $G_{(2,1)}$ is Klein's Vierergruppe. Our group $G_{(q,1)}$ appear in the historical review section of [Szec–16], where they are denoted by $G(2,q)$.

Numerical note 1.5. The sequence of positive integers which are of the form $q^m + q^{m-1} + \ldots + q + 1$ for some prime power q and positive integer m is Sequence A258777 of [OEIS]; 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 start 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 45th tem and 46th term, i.e., between 91 and 98; it follows from Corollary 1.3 that a group with Property $P(91)$ has necessarily Property $P(97)$. It is a consequence of the Prime Number Theorem that the asymptotic density of this sequence is 0; in other words, if for $k \geq 1$ 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 [Radu–17, Appendix B]. Note 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 $x, y \geq 2$, $x \neq y$, and $M, N \geq 3$, 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 [Goor–17, BuSh–02, He–09].

1.2. **Irreducibly faithful groups.** Clearly, the existence of a faithful irreducible unitary representation for a group G implies that G has $P(n)$ for all $n \geq 1$. The problem of characterizing finite groups with a faithful irreducible unitary representation has been addressed by Burnside in [Burn–11, 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 overview in [Szec–16]).

Gaschütz [Gasc–54] 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.* That result was extended to the class of all countable groups in [BeHa–08, Theorem 2]; see Section 2 below. As a consequence of Theorem 1.1, we shall obtain the following supplementary characterization.

Corollary 1.6. *For a countable group G, the following conditions are equivalent:*

(i) G has a faithful irreducible unitary representation.

(ii) G has $P(n)$ for all $n \geq 1$.

(iii) For every prime p and every finite simple $\mathbf{F}_p[G]$-module W of dimension m over $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$, the group G does not contain any finite abelian normal subgroup V of exponent p which is isomorphic to the direct sum of $m+1$ copies of W as a $\mathbf{F}_p[G]$-module.

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 [Shod–31, Page 207]).

1.3. **Abelian groups.** In view of Theorem 1.1, a countable abelian group G does not have $P(n)$ if and only if G contains $C_p \times C_p$ for some prime $p \leq n-1$, where C_p denotes the cyclic group of order p. We shall offer a direct proof of that fact that does not rely on Theorem 1.1, and holds in particular without the hypothesis of countability:

Proposition 1.7. *An abelian group G does not have $P(n)$ if and only if G contains a subgroup isomorphic to $C_p \times C_p$ for some prime $p \leq n-1$.*

In order to establish that, we invoke the following result of M. Bhargava:

Proposition 1.8 ([Bhar–02, Theorem 4]). *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 $p \leq n-1$.

Proof of Proposition 1.7. Assume that G does not have Property $P(n)$. Let $F \subset G \smallsetminus \{e\}$ be an irreducibly unfaithful subset of G of size $\leq n$. Let $\widehat{G}$ be the Pontryagin dual of G, namely the group of all characters $G \to \{z \in \mathbf{C} \mid |z| = 1\}$. 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 $P(1)$, 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 Proposition 1.8 ensures that $\widehat{G}$ maps onto $C_p \times C_p$, for some prime $p \leq |F| - 1 \leq n-1$. By duality (see [Bourb–TS, chap. II, § 1, no 7, Th. 4]), it follows that G contains a subgroup isomorphic to $C_p \times C_p$.

Conversely, if G contains $V \simeq C_p \times C_p$ for some prime $p \leq n-1$, consider a set $F \subset G$ of size $p+1$ containing a generator of each of the $p+1$ non-trivial cyclic subgroups of V. Any character of G kills at least one of the elements of F. Thus F is irreducibly unfaithful, and G does not have $P(n)$. □

As a consequence, we observe that the condition of countability cannot be removed in Corollary 1.6. Indeed, any torsion-free abelian group G has $P(n)$ for all n by Proposition 1.7, but it cannot be irreducibly faithful if its cardinality is larger than that of the continuum.

2. Gaschütz Theorem and related facts

Theorem 2.2 below is due to Gaschütz in the case of finite groups [Gasc–54] (see also [Hupp–98, Theorem 42.7]), and has been generalized to countable groups in [BeHa–08, part of Theorem 2]. First we remind 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 $\mathrm{MS}(\mathbf{Z}) = \{0\}$. Note that $\mathrm{MS}(G)$ is contained in the FC-centre of G, which is the subgroup of G of elements having a finite conjugacy class.

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 $\bigcup_{H \in \mathcal{H}(G)} H$. We write $\prod'$ to indicate a restricted product of groups.

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 [Rema–30]. For general groups, finite or not, the structure of the mini-socle can be described similarly, as follows; we refer to [BeHa–08, Proposition 1] for the proof.

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

(1) Every abelian mini-foot A in $\mathcal{A}_G$ is isomorphic to $(C_p)^n$ for some prime p and positive integer n.
(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-abelain mino-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 direct product of the 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 $p \colon G \to H$ is a surjective homomorphism. Then for every foot X of G, either $p(X)$ is trivial or $p(X)$ is a foot of H. In particular p maps $\mathrm{MA}(G)$ [respectively $\mathrm{MH}(G)$, $\mathrm{MS}(G)$] to a subgroup of $\mathrm{MA}(H)$ [resp. $\mathrm{MH}(H)$, $\mathrm{MS}(H)$] which is normal in H.

The following result is a slight reformulation of the equivalence between (i) and (iv) in [BeHa–08, 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 established in [BeHa–08].

Given a group G and a normal subgroup N, a unitary character or a 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 $x \in N$.

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 countable group, N a normal subgroup of G, and π an irreducible unitary representation of G.*

If the restriction $\pi|_N$ is faithful, then N has an irreducible unitary representation σ which is G-faithful.

Proof. See [BeHa–08, Lemma 9]. The hypothesis 'π is faithful' there can be weakened to '$\pi|_N$ is faithful', and the same proof works. □

Lemma 2.4. *Let G be a countable group, N a normal subgroup of G, and σ an irreducible unitary representation of N.*

If σ 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.*

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

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

and

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

We claim that $\mu(\widetilde{\Omega}) = \mu(\widehat{\Omega}) = 0$; to show this, we argue as in the proof of [BeHa–08, 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 $\Omega_\ell = \{\omega \in \Omega \mid G_\ell \subset \mathrm{Ker}(\pi_\omega)\}$, such that $\mu(\Omega_\ell) > 0$. Then, as in 'Claim 1' in the proof of [BeHa–08, Lemma 10] we show that $G_\ell \cap N = \{e\}$, in contradiction with $G_\ell \subset N$.

To show that $\mu(\widehat{\Omega}) = 0$, also by contradiction, we assume now 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 $\Omega_m = \{\omega \in \Omega \mid G_m \subset \mathrm{Ker}(\pi_\omega)\}$, 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 is thus non-empty. For any $\omega \in \Omega \smallsetminus (\widetilde{\Omega} \cup \widehat{\Omega})$, the representation π_ω is an irreducible unitary representation of G that has the required properties. □

Lemma 2.5. *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 direct product of a collection $\{S_i\}$ of non-abelian finite simple 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 [BeHa–08]. □

The following consequence of all the facts above is not used below, but may be of independent interest (compare [BeHa–08, Proposition 11]). It shows that a countable group has an irreducible unitary representation π with a kernel which is 'very small', in the sense that the normal closure of any $g \in \mathrm{Ker}(\pi)$ is finite.

Proposition 2.6. *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 finite subgroup of G and its socle is abelian.*

Proof. Let $N = \mathrm{MH}(G)$ be the semi-simple part of the mini-socle of G. Since N is the restricted direct product of non-abelian finite simple groups (Proposition 2.1), Lemma 2.5 ensures that N has a faithful irreducible unitary representation σ. Let π be an irreducible unitary representation of G afforded by applying Lemma 2.4 to σ; given a non-trivial $g \in \mathrm{Ker}(\pi)$, the normal closure $\Gamma_g := \langle\langle g \rangle\rangle_G$ is finite.

Let $\mathrm{SocH}(\Gamma_g)$ be the semi-simple part of the socle of of Γ_g. Since $\mathrm{SocH}(\Gamma_g)$ is a characteristic subgroup of Γ_g, it is also a finite normal subgroup of G, which is a direct product of non-abelian finite simple groups. Therefore, if $\mathrm{SocH}(\Gamma_g)$ were non-trivial, then it would contain a non-abelian mini-feet of G.

Since $\pi|_N$ is faithful, i.e., since $N \cap \mathrm{Ker}(\pi) = \{e\}$, any mini-foot of G contained in $\mathrm{Ker}(\pi)$ is abelian. In particular any mini-foot of G contained in Γ_g is abelian.

It follows that $\mathrm{SocH}(\Gamma_g) = \{e\}$, so that the socle of $\Gamma_g = \langle\langle g \rangle\rangle_G$ is abelian. □

We end this section with the following two subsidiary facts. Given an abelian group A, the symbol $\widehat{A}$ denotes the **Pontrjagin dual** of A, namely the set of all unitary characters $A \to \mathcal{U}(1) := \{z \in \mathbf{C} \mid |z| = 1\}$. Lemma 2.8 will be needed in Section 4.

Lemma 2.7. *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 Pontrjagin duality: see the proof of the equivalence between (i) and (ii) in [BeHa–08, Lemma 14]. □

Lemma 2.8. *Let G be a group and A be a finite normal subgroup of G contained in $\mathrm{MA}(G)$.*

Then A has a G-faithful unitary character if and only if A is generated by a single conjugacy class.

Proof. We follow the arguments from the proof of Lemma 14 in [BeHa–08] (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 A_p is the p-Sylow subgroup of A. Moreover A_p is a p-elementary abelian group for each $p \in P$, by (1) of the same proposition. (For comparison with [BeHa–08, Lemma 14], note that it follows from Proposition 3.1 below 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 $p \in P$ and some $n \geq 1$.) 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 2.7 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. Using Lemma 2.7 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 Lemma when $A = A_p$ for one prime p. Notice that A_p is generated by a single conjugacy class if and only if A_p is cyclic as a $\mathbf{F}_p[G]$-module. Under the natural identification of $\widehat{A}_p$ with A_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 [Szec–16]). Since the dual A_p^* is canonically isomorphic to the Pontrjagin dual $\widehat{A}_p$, we deduce from Lemma 2.7 that A_p is generated by a single conjugacy class if and only if A_p has a G-faithful unitary character. $\square$

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

Let R be a ring. The following classical result will be frequently used in the sequel, without further notice.

Proposition 3.1. *For a R-module V, the following conditions are equivalent:*

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

Proof. See [Bourb–A, §3, Proposition 7]. $\square$

A module V satisfying those equivalent conditions is called **semi-simple**.

The following basic fact is the module version of a result often stated for groups and known as Goursat's Lemma. The module version appears, for example, in [Lamb–76, Page 171]; more on this lemma in [BaSZ–15].

Lemma 3.2. *Let $A = A_1 \oplus A_2$ be the direct sum of two R-modules, and for $i = 1, 2$, let $p_i \colon A \to A_i$ be the canonical projection. Let $M \leq A$ be a submodule such that $p_i(M) = A_i$ for $i = 1, 2$, and set $M_i = M \cap A_i$.*

Then the canonical image of M in $A_1/M_1 \oplus A_2/M_2$ is the graph of an isomorphism $A_1/M_1 \to A_2/M_2$ of R-modules.

We say that a R-module V is **cyclic** if there exists $v \in V$ such that $V = Rv$. Let now p be a prime and G a group. The 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 3.8 below, after some preparatory steps. Proposition 3.8 is well-known to experts: see Lemma 3.1 in [Szec–16]. It can be seen as a version over $\mathbf{F}_p$ of a result for cyclic unitary representations of compact groups due to Greenleaf and Moskowitz [GrMo–71, Proposition 1.8].

Lemma 3.3. *Let W be a finite simple $\mathbf{F}_p[G]$-module and let $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$. 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 $\lambda \in \mathbf{F}_q$.

Proof. This is a straightforward consequence of Lemma 3.2. □

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

Lemma 3.4. *Let W be a finite simple $\mathbf{F}_p[G]$-module and let $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$. Let $m \geq 0$; for each $i = 0, \dots, m$, let V_i be a copy of W. Set $V = V_0 \oplus V_1 \oplus \cdots \oplus V_m$.*

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

$$M = \left\{ \Big(\sum_{i=1}^{m} \lambda_i x_i, x_1, x_2, \dots, x_m \Big) \;\Big|\; (x_1, \dots, x_m) \in V_1 \oplus \cdots \oplus V_m \right\}$$

for some $(\lambda_1, \dots, \lambda_m) \in \mathbf{F}_q^m$.

Proof. Let $p \colon V \to V_1 \oplus \cdots \oplus V_m$ be the canonical projection. Let $M \subsetneq V$ be a maximal $\mathbf{F}_p[G]$-submodule such that $M \cap V_0 = \{0\}$. Then the restriction $p|_M$ is injective. Since M is maximal, we have $V = V_0 \oplus M$, so that $p|_M \colon M \to V_1 \oplus \cdots \oplus V_m$ is an isomorphism of $\mathbf{F}_p[G]$-modules.

Given $i \in \{1, \dots, m\}$, let $M_i = (p|_M)^{-1}(V_i)$. 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 3.3, there exists $\lambda_i \in \mathbf{F}_q$ such that $M_i \simeq \{(\lambda_i x_i, x_i) \mid x_i \in V_i\} \leq V_0 \oplus V_i$. Since $p|_M \colon M \to V_1 \oplus \cdots \oplus V_m$ is an isomorphism, we deduce that

$$\begin{aligned} M &= M_1 \oplus \cdots \oplus M_m \\ &= \left\{ \Big(\sum_{i=1}^{m} \lambda_i x_i, x_1, x_2, \dots, x_m \Big) \;\Big|\; (x_1, \dots, x_m) \in V_1 \oplus \cdots \oplus V_m \right\} \end{aligned}$$

as required. □

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

Lemma 3.5. *Let W be a finite simple $\mathbf{F}_p[G]$-module and let $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$. Let $m \geq 0$; for each $i = 0, \dots, m$, let V_i be a copy of W; set $V = V_0 \oplus \cdots \oplus V_m$.*

Then the $\mathbf{F}_p[G]$-module V is cyclic if and only if $m < \dim_{\mathbf{F}_q}(W)$.

Proof. Assume first that $m \geq \dim_{\mathbf{F}_q}(W)$. Let $(v_0, \dots, v_m) \in V$. Since $V_i = W$ for all i, we may view v_i as an element of W. Then, upon reordering the summands

$V_0, \dots, V_m$, we may assume that there exists $(\lambda_1, \dots, \lambda_m) \in \mathbf{F}_q^m$ such that $v_0 = \sum_{i=1}^m \lambda_i v_i$. It follows that $(v_0, \dots, v_m)$ belongs to

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

which is a proper submodule of V. Hence V is not cyclic.

In order to prove the converse, we proceed by induction on m. In the base case $m = 0$, we have $0 = m < \dim_{\mathbf{F}_q}(W)$ and $V = V_0 = W$ is simple, hence cyclic. We now assume that $0 < m < \dim_{\mathbf{F}_q}(W)$. The induction hypothesis ensures that the module $V_1 \oplus \cdots \oplus V_m$ is cyclic. Let $(v_1, \dots, v_m)$ be a generator. Viewing all v_i as elements of W, the hypothesis that $m < \dim_{\mathbf{F}_q}(W)$ ensures the existence of an element $v_0 \in W$ which does not belong to the $\mathbf{F}_q$-subspace of W spanned by $\{v_1, \dots, v_m\}$. Let M be the submodule of V spanned by $(v_0, v_1, \dots, v_n)$. The image of M under the canonical projection $V \to V_1 \oplus \cdots \oplus V_m$ is surjective, since it coincides with the submodule generated by $(v_1, \dots, v_m)$. If $M \cap V_0 = \{0\}$, then M is a maximal proper submodule. Lemma 3.4 then ensures that v_0 is a $\mathbf{F}_q$-linear combination of $\{v_1, \dots, v_m\}$, a contradiction. Therefore M contains V_0 since V_0 is simple. Hence $V = M$, so that V is indeed cyclic. □

The following basic counting lemma will also be useful.

Lemma 3.6. *Let W be a finite simple $\mathbf{F}_p[G]$-module and let $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$. Let $m \geq 0$; for each $i = 0, \dots, m$, let V_i be a copy of W. Set $V = V_0 \oplus V_1 \oplus \cdots \oplus V_m$. The number of simple $\mathbf{F}_p[G]$-submodules of V is*

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

Proof. We proceed by induction on m. In case $m = 0$, the module $V = V_0$ is simple, so the result is clear.

Assume now that $m \geq 1$. Let $\mathcal{S}$ be the collection of all simple submodules of V. For each $S \in \mathcal{S}$ such that $S \cap V_0 = \{0\}$, there is a simple submodule $S' \leq V_1 \oplus \cdots \oplus V_m$ and a scalar $\lambda \in \mathbf{F}_q$ such that $S \simeq \{(\lambda x, x) \mid x \in S'\} \leq V_0 \oplus S'$ (see Lemma 3.2). By induction, there are $q^{m-1} + \cdots + q + 1$ such modules S', and the scalar λ can take q different values. Since the only $S \in \mathcal{S}$ with $S \cap V_0 \neq \{0\}$ is $S = V_0$, we deduce that

$$|\mathcal{S}| = q(q^{m-1} + \cdots + q + 1) + 1 = q^m + q^{m-1} + \cdots + q + 1,$$

as required. □

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

Lemma 3.7. *A finite semi-simple $\mathbf{F}_p[G]$-module V 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.

Let $V = M_1 \oplus \cdots \oplus M_\ell$ be the decomposition of V as the direct sum of its isotypical components. Assume that M_k is cyclic for all $k \in \{1, \ldots, \ell\}$ and let $v_k \in M_k$ be a generator. We claim that $v = (v_1, \ldots, v_\ell)$ is a generator of V. We prove this by induction on ℓ. The base case $\ell = 1$ is trivial. Assume now that $\ell \geq 2$ and let M be the submodule generated by v. The induction hypothesis ensures that the canonical projection of M to $A_1 = \bigoplus_{k=1}^{\ell-1} M_k$ is surjective. Clearly, the projection of M to $A_2 = M_\ell$ is surjective. Since A_1 and A_2 are disjoint (i.e., they do not contain any non-zero isomorphic summands), it follows from Lemma 3.2 that $M = A_1 \oplus A_2 = V$. □

Proposition 3.8. *Let V be a finite semi-simple $\mathbf{F}_p[G]$-module. The following assertions are equivalent:*

- *(i) V is not cyclic.*
- *(ii) There exist a simple $\mathbf{F}_p[G]$-module W of dimension $m \geq 1$ over $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$ and a submodule $V' \leq V$ isomorphic to a direct sum of $m+1$ copies of W.*

Proof. In view of Lemma 3.5, the module V' afforded by Condition (ii) is not cyclic. Since that module is a direct summand of V, it follows that V is not cyclic.

Assume conversely that V is not cyclic. Then V has a non-cyclic isotypical component by Lemma 3.7. It then follows from Lemma 3.5 that Condition (ii) holds. □

4. Proof of Theorem 1.1

The proof of (1) ⇒ (2) rests on the following two lemmas.

Lemma 4.1. *Let n be an integer, $n \geq 2$, and G a countable group with $P(n-1)$ but not $P(n)$.*

For every irreducibly unfaithful subset F of size n of G and for every $x \in F$, the normal subgroup $\langle\langle x \rangle\rangle_G$ of G is finite and its socle is abelian. In particular all mini-feet of G contained in $\langle\langle x \rangle\rangle_G$ are abelian.

Proof. We start with a preliminary observation. Let N be a finite normal subgroup of G. If the socle $\mathrm{Soc}(N)$ is abelian, then $\mathrm{Soc}(N)$ is a non-trivial finite abelian normal subgroup of G and thus contains an abelian mini-foot of G.

Similarly, if $\mathrm{Soc}(N)$ is non-abelian, then its semi-simple part $\mathrm{SocH}(N)$ is a non-trivial characteristic subgroup of N that splits as a direct product of non-abelian finite simple groups, and hence N contains a non-abelian minifoot of G. Conversely, if N contains a non-abelian minifoot of G, say M, then M is a normal subgroup of N that is a direct product of non-abelian finite simple groups. Thus

M contains a foot of N which is *a fortiori* a direct product of non-abelian finite simple groups. In particular the socle of N is non-abelian.

Let now F be an irreducibly unfaithful subset of G of size n. Note that $e \notin F$, otherwise G would contain an irreducibly unfaithful subset $F \smallsetminus \{e\}$ of size $n-1$. We partition F into three subsets, $F = F_A \sqcup F_H \sqcup F_\infty$, where:

$$\begin{aligned}
F_A &= \{x \in F \mid \langle\!\langle x \rangle\!\rangle_G \text{ is finite with abelian socle}\},\\
F_H &= \{x \in F \mid \langle\!\langle x \rangle\!\rangle_G \text{ is finite with non-abelian socle}\},\\
F_\infty &= \{x \in F \mid \langle\!\langle x \rangle\!\rangle_G \text{ is infinite}\} = F \smallsetminus (F_A \sqcup F_H).
\end{aligned}$$

By the preliminary observation above, we may, for each $x \in F_A$ [respectively F_H], choose an abelian mini-foot A_x of G inside $\langle\!\langle x \rangle\!\rangle_G$ and $y_x \neq e$ in A_x [respectively a non-abelian mini-foot H_x of G inside $\langle\!\langle x \rangle\!\rangle_G$ and $y_x \neq e$ in H_x]. We have $A_x = \langle\!\langle y_x \rangle\!\rangle_G$ [respectively $H_x = \langle\!\langle y_x \rangle\!\rangle_G$]. Define

$$\begin{aligned}
F'_A &= \{y_x \in G \mid x \in F_A\}, \quad G_A = \langle\!\langle F'_A \rangle\!\rangle_G,\\
F'_H &= \{y_x \in G \mid x \in F_H\}, \quad G_H = \langle\!\langle F'_H \rangle\!\rangle_G,\\
F' &= F'_A \cup F'_H \cup F_\infty.
\end{aligned}$$

By Proposition 2.1, the finite normal subgroup G_A of G is abelian, the finite normal subgroup G_H of G is a direct product of non-abelian simple finite groups, and the subgroup of G generated by G_A and G_H is their direct product $G_A \times G_H$.

Observe that $|F'| \leq |F|$. Moreover, by construction, for all $x \in F_A \cup F_H$, we have $\langle\!\langle y_x \rangle\!\rangle_G \leq \langle\!\langle x \rangle\!\rangle_G$, so that F' cannot be irreducibly faithful. Since G has $P(n-1)$, it follows that $|F'| = |F| = n$.

We claim that $F' = F'_A$. Indeed, assume the contrary. Then $|F'_A| \leq n-1$, and since G has $P(n-1)$ we may find an irreducible unitary representation π of G with $\pi(y_x) \neq \mathrm{id}$ for all $y_x \in F'_A$. Set $K = G_A \cap \mathrm{Ker}(\pi)$ and $Q = G/K$. Observe that the image N of $G_A \times G_H$ in Q is a normal subgroup which is the direct product of the image G_A/K of G_A in Q, which is abelian, and the image of G_H in Q, which is isomorphic to G_H since $K \cap G_H = \{e\}$.

By construction, all elements of F'_A have a non-trivial image in Q. Moreover, since $K \leq \mathrm{Ker}(\pi)$, we may view π as an irreducible unitary representation of Q, whose restriction to G_A/K is faithful. By Lemma 2.3, we know that G_A/K has a Q-faithful irreducible unitary representation. Since $N = (G_A/K) \times G_H$ is a normal subgroup of Q satisfying the hypothesis of Lemma 2.5, we see that N has a Q-faithful irreducible unitary representation. Hence, by Lemma 2.4, we conclude that Q has an irreducible unitary representation ρ such that every element in $\mathrm{Ker}(\rho)$ has a normal closure which is finite and intersects N trivially. We may view π as an irreducible unitary representation of G. Since K is finite, we have $\pi(z) \neq \mathrm{id}$ for all $x \in F_\infty$. Therefore $\pi(z) \neq \mathrm{id}$ for all $z \in F'$, a contradiction because F' is not irreducibly faithful.

It follows that $F' = F'_A$, and therefore $F = F_A$. By the preliminary observation above, this implies that for all $x \in F$, every mini-foot of G contained in $\langle\langle x \rangle\rangle_G$ is abelian. $\square$

Lemma 4.2. *Let G be a countable group and $F \subset G$ be an irreducibly unfaithful subset of size n such that every non-trivial element of F is contained in an abelian mini-foot of G.*

Then there exist a prime p, an integer $m \geq 1$, a finite abelian normal subgroup V of G of exponent p, and a simple $\mathbf{F}_p[G]$-module W of dimension m over $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$, enjoying the following properties:

(i) V is isomorphic to the direct sum of $m+1$ copies of W, as a $\mathbf{F}_p[G]$-module;
(ii) $q^m + q^{m-1} + \cdots + q + 1 \leq n$.

Proof. Let A be the normal closure of F in G.

Let K be a maximal normal subgroup of G contained in A and such that $F \cap K \subseteq \{e\}$. Let $G' = G/K$ and let A' and F' be the images of A and F in G'. Notice that every abelian mini-foot of G' contained in A' must contain an element of F'. In particular A' contains at most n mini-feet of G'.

Since every element of F' is contained in an abelian mini-foot of G', and since any two feet commute, we see that A' is a finite abelian normal subgroup of G'. Since F is irreducibly unfaithful in G, it follows that F' and A' are irreducibly unfaithful in G'. Therefore, by Lemma 2.4, it follows that no irreducible unitary representation of A' is G'-faithful. By Lemma 2.8, this implies that A' is not generated by a single conjugacy class.

Let $\mathcal{P}$ be the set of all prime divisors of $|A'|$, and let A'_p be the p-Sylow subgroup of A'. Then A'_p is G'-invariant, and we have a G'-equivariant decomposition $A' \simeq \bigoplus_{p \in \mathcal{P}} A'_p$. Each A'_p may be viewed as a $\mathbf{F}_p[G']$-module. Moreover A'_p is semi-simple since it is generated abelian by mini-feet, each of which is a simple $\mathbf{F}_p[G']$-module (see Proposition 3.1).

If each A'_p were generated by a single conjugacy class, then A' would have the same property. Thus there exists p such that A'_p is not generated by a single conjugacy class. In other words the $\mathbf{F}_p[G']$-module A'_p is not cyclic. We may therefore invoke Lemma 3.8. This yields a simple $\mathbf{F}_p[G]$-module W of dimension $m \geq 1$ over $\mathbf{F}_q = \mathrm{C}_{\mathrm{End}(W)}(G)$ and a submodule V' of A'_p which is isomorphic to a direct sum of $m+1$ copies of W.

Since A' contains at most n mini-feet of G', it follows that V' contains at most n simple submodules. In view of Lemma 3.6, we deduce that $q^m + q^{m-1} + \cdots + q + 1 \leq n$.

Let now A_p be the p-Sylow subgroup of A. Observe that the restriction of the G-equivariant surjective homomorphism $A \to A'_p$ to A_p is still G-equivariant and surjective. We may view A_p as a $\mathbf{F}_p[G]$-module. Since A is generated by abelian mini-feet of G, the same holds for A_p, so that A_p is a semi-simple $\mathbf{F}_p[G]$-module. Therefore, the short exact sequence $0 \to K \cap A_p \to A_p \to A'_p \to 0$, which is

G-equivariant, admits a G-equivariant section (see Proposition 3.1). Thus G has an abelian normal subgroup V of exponent p which is isomorphic to V' as a $\mathbf{F}_p[G]$-module. The required conclusions follow. □

Proof of Theorem 1.1. Let G be a group for which (1) of Theorem 1.1 holds, i.e., a group which does not have Property $P(n)$. Upon replacing n by a smaller integer, we may assume that G has Property $P(n-1)$. Let F be an irreducibly unfaithful subset of G of size n. We invoke Lemma 4.1. This ensures that for each $x \in F$ we may find a non-trivial element $y_x \in \langle\!\langle x \rangle\!\rangle_G$ such that $\langle\!\langle y_x \rangle\!\rangle_G$ is an abelian mini-foot of G. Since $\langle\!\langle y_x \rangle\!\rangle_G \leq \langle\!\langle x \rangle\!\rangle_G$ for all $x \in F$, it follows that the set $F' = \{y_x \mid x \in F\}$ is irreducibly faithful. Notice that F' satisfies Lemma 4.2; moreover we have $|F'| \leq |F| = n$. We deduce that (2) indeed holds.

For the reverse implication (2) $\Rightarrow$ (1) in Theorem 1.1, we pick a non-trivial element in each of the $q^m + q^{m-1} + \cdots + q + 1$ simple $\mathbf{F}_p[G]$-submodules of V (see Lemma 3.6). In that way we obtain a subset F of G of size $q^m + q^{m-1} + \cdots + q + 1$. Since V is not cyclic as a $\mathbf{F}_p[G]$-module by Lemma 3.5, it follows that V is not generated by a single conjugacy class. In view of Theorem 2.2, 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. Hence F is irreducibly unfaithful. This shows that G does not have Property $P(q^m + \cdots + q + 1)$, hence also not $P(n)$ since $n \geq q^m + \cdots + q + 1$. The proof is complete. □

5. Groups with $P(n)$ for all n

Proof of Corollary 1.6. That (i) implies (ii) is clear. That (ii) implies (iii) follows from Theorem 1.1.

Assume that (iii) holds. Let A be a finite abelian normal subgroup of G contained in the mini-socle. Let p be a prime dividing $|A|$ and 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, it follows from Lemma 3.8 that 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. Therefore G is irreducibly faithful by Theorem 2.2. Thus (i) holds. □

6. Irreducibly injective sets

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 $Q(n)$ if every subset of G of size $\leq n$ is irreducibly injective. Observe that $C_2 \times C_2$ does not have $Q(2)$, yet has $P(2)$, as does any group.

Properties $P(n)$ and $Q(m)$ are clearly related; the following observations are straightforward:

- If G has $P(\binom{n}{2})$, then G has $Q(n)$.

- If G has $Q(n+1)$, then G has $P(n)$.

Can we characterize $Q(n)$ by an algebraic property of G, in the same vein as in Theorem 1.1?

In particular, we need to determine, for each prime p, the number n such that the group $C_p \times C_p$ (and more generally any group $G_{(q,m)}$ from Example 1.4) has $Q(n-1)$ but does not have $Q(n)$. This leads us to additive combinatorics, through the following questions:

Question 6.1. Let $G = C_p \times C_p$. What is the smallest size of a subset $F \subset G$ such that the set $\{xy^{-1} \mid x, y \in F\}$ contains a generator of each of the $p+1$ cyclic subgroups of G?

Similarly, let $V \leq G_{(q,m)}$ as in Example 1.4. What is the smallest size of a subset $F \subset V$ such that the set $\{x - y \mid x, y \in F\}$ contains a non-zero vector in each of the $q^m + \cdots + q + 1$ simple submodules of V?

References

[BaSZ–15] K. Bauer, D. Sen, and P Zvengrowski, *A generalized Goursat lemma*. Tatra Mt. Math. Publ. **64** (2015), 1–19. 9

[BeHa–08] B. Bekka and P. de la Harpe, *Irreducibly represented groups*. Comment. Math. Helv. **83** (2008), 847–868. 2, 4, 5, 6, 7, 8

[Bhar–02] M. Bhargava, *When is a group the union of proper normal subgroups?* Amer. Math. Monthly **109** (2002), no. 5, 471–473. 5

[Bourb–A] N. Bourbaki, *Algèbre, Chapitre VIII, Modules et anneau semi-simples*. Hermann, 1958. 9, 11

[Bourb–TS] N. Bourbaki, *Théories spectrales, Chapitres 1 et 2*. Hermann, 1967. 5

[Burn–11] W. Burnside, *The theory of groups of finite order*, 2nd Edition. Cambridge Univ. Press, 1911. Reprint, Dover, 1955. 3, 4

[BuSh–02] 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. 4

[Gasc–54] W. Gaschütz, *Endliche Gruppen mit treuen absolut–irreduziblen Darstellungen*. Math. Nach. **12** (1954),253–255. 4, 5

[GeRa–43] 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. 1

[Goor–17] R. Goormaghtigh. L'intermédiare des Mathématiciens **24** (1917), 88. 4

[GrMo–71] F. Greenleaf and M. Moskowitz, *Cyclic vectors for representations of locally compact groups*. Math. Ann. **190** (1971), 265–288. 10

[He–09] 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. 4

[Hupp–98] B. Huppert, *Character theory of finite groups*. W. de Gruyter, 1998. 5

[Isaa–76] I.M. Isaacs, *Charater theory of finite groups*. Academic Press, 1976. 3

[Lamb–76] J. Lambek, *Lectures on rings and modules*, Second Edition. Chelsea, 1976. [First Edition, Blaisdell, 1966.] 9

[OEIS] *The On-Line Encyclopedia of Integer Sequences*. On line: `https://oeis.org` 3

[Radu–17] N. Radu, *A classification theorem for boundary 2-transitive automorphisms of trees*. Invent. Math. **209** (2017), no. 1, 1–60. 3

[Rema–30] R. Remak, *Über minimale invariante Ungtergruppen in der Theorie der endlichen Gruppen*. J. reine angew. Math. **162** (1930), 1–16. 5

[Sasv–91] Z. Sasvári, *On a refinement of the Gel'fand-Raikov theorem*. Math. Nachr. **150** (1991), 185–187. 2

[Sasv–95] Z. Sasvári, *Positive definite and definitizable functions*. Academic Verlag, 1994. 2

[Shod–31] K. Shoda, *Bemerkungen über vollständig reduzible Gruppen*. J. Fac. Sci., Univ. Tokyo, Sect. I **2** (1931), 203–209. 4

[Szec–16] F. Szechtman, *Groups having a faithful irreducible representation*. J. Algebra **454** (2016), 292–307. 3, 4, 9

[Walt–74] M.E. Walter, *A duality between locally compact groups and certain Banach algebras*. J. Functional Analysis **17** (1974), 131–60. 2

Pierre-Emmanuel Caprace: UCLouvain – IRMP, Chemin du Cyclotron 2, box L7.01.02, B-1348 Louvain-la-Neuve.

E-mail address: pe.caprace@uclouvain.be

Pierre de la Harpe: Section de mathématiques, Université de Genève, C.P. 64, CH–1211 Genève 4.

E-mail address: Pierre.delaHarpe@unige.ch