PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 4, December 1992

MULTIPLICATIVE SUBGROUPS OF FINITE INDEX IN A RING

VITALY BERGELSON AND DANIEL B. SHAPIRO

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. If G is a subgroup of finite index in the multiplicative group of an infinite field K then $G - G = K$. Similar results hold for various rings.

INTRODUCTION

Let R be an associative ring with 1 and let R^* denote the multiplicative group of units (invertible elements) of R. If G is a subgroup of R^*, the set $G - G$ consists of all differences $g_1 - g_2$ for $g_i \in G$. If this subgroup G is "big enough" then $G - G = R$. For example, if K is an infinite field and G is a subgroup of finite index in K^*, then we prove that $G - G = K$. The proof is valid for a wider class of rings, which we call $(G - G)$-*rings*. (Fields with this property were called *uniform fields* in [B].)

0.1. **Definition.** A ring R is a $(G - G)$-*ring* if $G - G = R$ whenever G is a subgroup of finite index in R^*.

We will show that if R is an infinite field then R is a $(G-G)$-ring. Generally if R^* is big enough then R is $(G - G)$-ring. For example, if R is any finite-dimensional algebra over an infinite field (Proposition 2.2), then R is a $(G-G)$-ring. Further examples are presented in §2.

These results are of interest because of the interplay of the additive and multiplicative structures in the ring R. See Proposition 2.14 for a complementary result. Although the theorem is a purely algebraic statement, it is proved using techniques of analysis (the amenability of abelian groups) and of combinatorics (Ramsey's Theorem).

The original motivation for this theorem came from the new elementary proof by Berrizbeitia of an old result about finite fields: if K is a finite field then every element of K can be expressed as $x^3 + y^3$ for some $x, y \in K^*$, except when $|K| = 4, 7, 13$, or 16. (References to this result are given in [LS].) Leep and Shapiro [LS] extended Berrizbeitia's idea to infinite fields K by replacing the subgroup of cubes by a subgroup G of index 3 in K^*. They gave an elementary argument proving that $G + G = K$ for any such subgroup G. The question for subgroups of index $n > 3$ in a field was left as a conjecture in [LS]. In the case of finite fields this question is settled by applying classical estimates to

Received by the editors August 1, 1990 and, in revised form, March 5, 1991.
1991 *Mathematics Subject Classification.* Primary 12E99, 16B99, 43A07, 05C55, 28D99.

show that for a given index n there are only finitely many exceptions among the finite fields. See [LS] Theorem 7 for further information and references.

To show that the question is not vacuous for infinite fields let us describe a few examples of subgroups of finite index in $\mathbb{Q}^*$. Every $r \in \mathbb{Q}^*$ can be expressed uniquely as $r = (-1)^{\nu_0(r)} \cdot \prod_p p^{\nu_p(r)}$ where $\nu_0(r) \in \{0, 1\}$, $\nu_p(r) \in \mathbb{Z}$, and $\nu_p(r) = 0$ for all but finitely many primes p. For any given positive integer n and $c_k \in \mathbb{Z}/n\mathbb{Z}$ ($k = 0$ or prime), define $f: \mathbb{Q}^* \to \mathbb{Z}/n\mathbb{Z}$ by setting $f(r) = c_0\nu_0(r) + \sum_p c_p\nu_p(r) \pmod n$. Then f is a homomorphism and $G = \ker f$ is a subgroup of index at most n. For example the set of all r where $\sum_p \nu_p(r) \equiv 0 \pmod 5$ is a subgroup of index 5 in $\mathbb{Q}^*$. This sort of construction applies to any field of fractions of a unique factorization domain. A different example is given at the end of §3.

The next step was another insight by Berrizbeitia, who noted that the set of differences $G - G$ is easier to work with than $G + G$; in fact, if $-1 \notin G$ he noted that $G + G$ need not be additively closed (see §3). Using the higher-dimensional version of van der Waerden's Theorem on arithmetic progressions, Berrizbeitia proved [B] that if G is a subgroup of finite index in a field K of characteristic zero then $G - G = K$. Our proof of the result for fields of arbitrary characteristic was inspired directly by a preprint of [B], although the methods we employ are substantially different. (Yet another proof for characteristic 0 is mentioned at the end of §1.) Since the same proof works for a wider class of rings, we deal with the more general context from the start.

1. $(G - G)$-RINGS

Throughout this note R denotes an associative ring with 1 and R^* is its group of units (invertible elements). Here are two necessary conditions for R to be a $(G - G)$-ring. We do not know whether these conditions are also sufficient.

1.1. **Lemma.** *If R is a $(G - G)$-ring then $R^* + R^* = R$ and every nontrivial homomorphic image of R is infinite.*

Proof. The first statement follows using $G = R^*$, noting that $-1 \in R^*$. For the second statement suppose there is a ring homomorphism $\varphi: R \to S$ where S is a finite ring. Let G be the kernel of the induced group homomorphism $\varphi': R^* \to S^*$; that is, $G = \varphi^{-1}(1) \cap R^*$. Then $R^*/G \cong \varphi(R^*) \subseteq S^*$ is finite and the hypothesis implies that $G - G = R$. Then $1_R \in G - G$ so that $1_S = \varphi(1_R) \in \varphi(G - G) = 1_S - 1_S = 0_S$. It follows that $S = \{0\}$. □

The proof of our theorem involves certain invariant measures on the additive group of the ring R. Since this additive group is abelian, it is amenable. (See [W, pp. 146–150] for a readable introduction to the subject of measures in groups. Another proof of amenability of abelian groups can be found in [G, p. 5].) Therefore there exists a finitely additive, invariant probability measure μ on $\mathcal{P}(R)$, the set of all subsets of R. This means that $\mu: \mathcal{P}(R) \to [0, \infty)$ is a mapping such that (i) if $A, B \in \mathcal{P}(R)$ with $A \cap B = \varnothing$ then $\mu(A \cup B) = \mu(A) + \mu(B)$; (ii) $\mu(x + E) = \mu(E)$ for every $x \in R$ and $E \in \mathcal{P}(R)$; and (iii) $\mu(R) = 1$. Throughout this paper an *invariant measure* will be a measure of this type on $\mathcal{P}(R)$.

1.2. **Definition.** A ring R is in the class $\mathscr{U}$ if:

(1) R^* is additively big; that is, $\mu(R^*) > 0$ for some invariant measure μ on R.

(2) There is an infinite set in R having invertible differences; that is, there exist $a_1, a_2, a_3, \ldots$ in R such that $a_i - a_j \in R^*$ whenever $i \neq j$.

1.3. **Theorem.** *If a ring R is in the class $\mathscr{U}$ then R is a $(G-G)$-ring.*

In §2 we will describe algebraic conditions on R that imply that R is in $\mathscr{U}$. Furthermore we show in Proposition 2.12 that the converse of Theorem 1.3 is false. Theorem 1.3 remains true if $\mathscr{U}$ is enlarged to the class $\mathscr{U}_0$ defined by weakening condition (2) as follows:

(2′) There are arbitrarily large finite sets in R having invertible differences.

We do not know whether $\mathscr{U}_0$ is actually larger than $\mathscr{U}$.

In order to prove Theorem 1.3 we use a combinatorial lemma.

1.4. **Lemma.** *Suppose $S \subseteq R$ is an infinite subset having invertible differences. If G is a subgroup of index n in R^* then there exist an infinite set $B = \{b_1, b_2, \ldots\} \subseteq S$ and a coset dG such that $b_i - b_j \in dG$ whenever $i > j$.*

Proof. This lemma is a consequence of a version of Ramsey's Theorem. A "finite coloring" of a set T is a function $\rho: T \to C$ where $C = \{c_1, \ldots, c_n\}$ is a finite set of "colors." A subset $T_0 \subseteq T$ is *monochromatic* (relative to the given coloring) if $\rho(T_0) = \{c_i\}$ is a single color. If S is a set let $[S]^2$ denote the set of all 2-element subsets of S. We need the following version of Ramsey's Theorem:

> if S is an infinite set and $[S]^2$ is finitely colored then there exists an infinite subset $A \subseteq S$ such that $[A]^2$ is monochromatic.

For a proof see [GRS, Theorem 5, p. 16].

Let $S = \{a_1, a_2, \ldots\} \subseteq R$ be the given set where $a_i - a_j \in R^*$ whenever $i > j$. Define a coloring on $[S]^2$, using the cosets of G in R^* as the colors, in the following way: if $\{a_i, a_j\} \in [S]^2$ where $i > j$ assign it the color $(a_i - a_j)G$. Ramsey's Theorem then provides an infinite subset $B \subseteq S$ and a coset dG such that every element of $[B]^2$ has the same color dG. Writing $B = \{a_{k_1}, a_{k_2}, \ldots\}$ where $k_1 < k_2 < \cdots$, this says that $a_{k_i} - a_{k_j} \in dG$ whenever $i > j$. Setting $b_i = a_{k_i}$ we are done. □

Proof of Theorem 1.3. Let G be a subgroup of finite index in R^*. Since R^* is a finite union of cosets of G and $\mu(R^*) > 0$ by hypothesis, there must exist $c \in R^*$ with $\mu(cG) > 0$. Let $B = \{b_1, b_2, \ldots\}$ be the infinite set found in Lemma 1.4. For any $x \in R$ there must exist $i > j$ such that $xb_i + cG$ meets $xb_j + cG$. (For otherwise those translates are pairwise disjoint so that $m \cdot \mu(cG) = \mu\left(\bigcup_{i=1}^{m}(xb_i + cG)\right) \leq \mu(R) = 1$ for every positive integer m, contradicting the inequality $\mu(cG) > 0$.) Then $x(b_i - b_j) \in cG - cG$ and since $b_i - b_j \in dG$, it follows that $c^{-1}dx \in G - G$. Since x was arbitrary, we have $R = c^{-1}dR \subseteq G - G$. □

Appendix to §1. Sets of recurrence. The definition of the class $\mathscr{U}$ can be made more general by using an idea from ergodic theory.

1.5. **Definition.** Suppose H is a group (written additively), H acts on a set X, and μ is an H-invariant probability measure on X. A set $S \subseteq H - \{0\}$ is a *set of recurrence for H acting on (X, μ)* if for every $A \subseteq X$ with $\mu(A) > 0$

there exists $s \in S$ such that $\mu(A \cap (A+s)) > 0$. S is a *set of recurrence for* H if it is a set of recurrence for every such space (X, μ). If R is a ring then, a subset $S \subseteq R$ is a *dilatable set of recurrence* if for every nonzero $x \in R$ the set Sx is a set of recurrence for the additive group of R. A *partition dilatable set of recurrence* is a subset S such that whenever S is finitely colored there is a monochromatic subset that is a dilatable set of recurrence.

The usual application of these ideas in this paper is the case R acts on itself and the set S lies in R^*. If $B = \{b_1, b_2, \dots\}$ is any infinite set in R then the set of differences $B - B$ always contains a partition dilatable set of recurrence (by the Ramsey Theorem argument used in the proof of (1.3) and (1.4)).

Using these ideas we define a somewhat larger class of rings.

1.6. **Definition.** A ring R belongs to the class $\mathscr{U}'$ if there is a finitely additive, invariant, probability measure μ on R where (1) $\mu(R^*) > 0$ and (2) there exists $S \subseteq R^*$ that is a partition dilatable set of recurrence for R acting on (R, μ).

The arguments above establish the following stronger version of our result.

1.7. **Theorem.** *If R is in the class $\mathscr{U}'$ then R is a $(G-G)$-ring.*

A result of Bergelson (see [Ber, Theorem 4.11]) shows that if S is any set of recurrence that is finitely colored, then S contains a monochromatic set of recurrence. (*Question*: Is it true that every dilatable set of recurrence is partition dilatable?) Dilating by units is not a problem, at least in the commutative case, provided that we use a "doubly invariant" measure.

1.8. **Lemma.** *If R is a commutative ring then there exists a finitely additive probability measure μ on R that is doubly invariant: for every $E \in \mathscr{P}(R)$, $\mu(aE+b) = \mu(E)$ for every $a \in R^*$ and $b \in R$.*

Proof. The affine group $\Gamma(R) = \{f: R \to R | f(x) = ax + b$ for some $a \in R^*$ and $b \in R\}$ is always amenable (since it is solvable). Use the fixed point property (see [W, Theorem 10.11(8)] or [G, §3.3]) for Γ acting on the space of normalized linear functionals on R. □

This $\mathscr{U}'$ seems to be a better class than $\mathscr{U}$ because sets of differences are such special types of sets of recurrence. There are many sets of recurrence that do not arise as differences. For example a theorem of Furstenberg-Sárközy states that if $f(x) \in \mathbb{Z}[x]$ is "intersective" (i.e., for every integer $m > 1$ there exists $n \in \mathbb{Z}$ with $f(n) \neq 0 \pmod m$), then the set $f(\mathbb{N})$ is a set of recurrence for $\mathbb{Z}$. (Further details are discussed in [Ber, pp. 80–82].) This provides a somewhat different proof of Berrizbeitia's result that fields of characteristic 0 are $(G-G)$-rings.

Proof. Suppose K is a field of characteristic 0 and $G < K^*$ is a subgroup of index n. Since $\mathbb{N} \subseteq K^*$ (because char $K = 0$) the set $S_n = \{k^n : k \in \mathbb{N}\}$ is in G. By the remarks above S_n is a set of recurrence for K (since $\mathbb{Z} \subseteq K$). If μ is a doubly invariant measure on F then S_n is a dilatable set of recurrence for K acting on (K, μ). The rest of the proof follows as before.

If R is a ring containing $\mathbb{Q}$, this argument shows only that if $G \subseteq R^*$ is a subgroup of finite index then $R^* \subseteq G - G$. To show that $G - G = R$ by this

method we require that $R^{*n} = \{u^n : u \in R^*\}$ be a dilatable set of recurrence for every n. We do not know whether this is true for every R containing $\mathbb{Q}$. For any c with $0 \leq c < 1$, there does exist a ring R containing $\mathbb{Z}$ with an invariant measure μ having $\mu(R^*) = c$ but where even R^* is not a set of recurrence. For instance if R has a finite nonzero homomorphic image then R^* is not a set of recurrence (because the group G considered in Lemma 1.1 has $\mu(aG) > 0$ for some $a \in R^*$ but $aG - aG$ does not meet R^*). Such a ring is described in Corollary 2.9.

1.9. *Remark.* It is true that if K is any infinite field then K^{*n} is a set of recurrence for every invariant measure on K. This result then implies that K is a $(G-G)$-ring. The proof uses ergodic theoretical techniques.

2. Examples of rings in the class $\mathscr{U}$

2.1. **Lemma.** *If R is tiled by translates of R^* (i.e., $R = \bigcup_{k=1}^{s}(x_k + R^*)$ for some $x_k \in R$) then $\mu(R^*) > 0$ for every finitely additive invariant probability measure μ on R.*

Proof. $1 = \mu(R) \leq \sum_{k=1}^{s} \mu(x_k + R^*) = s \cdot \mu(R^*)$ so that $\mu(R^*) > 0$. □

It is easy to see that any infinite field is in the class $\mathscr{U}$. Here are some further examples.

2.2. **Proposition.** (1) *Any infinite division ring is in the class $\mathscr{U}$.*

(2) *If R is a finite-dimensional algebra over an infinite field then R is in $\mathscr{U}$.*

Proof. (1) Easy. (2) Since $K \subseteq R$ an infinite set of distinct elements of K provides a set with invertible differences in R. Using the regular representation we view R as a subring of the matrix algebra $\mathbb{M}_n(K)$. If $r \in R$ then $r \in R^*$ if and only if $\det(r) \neq 0$.

Claim. If $x_1, x_2, \ldots, x_{n+1}$ in K are distinct, then $R = \bigcup_{k=1}^{n+1}(x_k + R^*)$. For if $r \in R$, the polynomial $\det(x \cdot I - r)$ has at most n roots in K. Therefore there exists k where $\det(x_k \cdot I - r) \neq 0$, so that $x_k \cdot I - r \in R^*$ and $r \in x_k \cdot I + R^*$. Then Lemma 2.1 applies. (Note. This result is a special case of Proposition 2.5.) □

In order to see how the class $\mathscr{U}$ and the class of $(G-G)$-rings behave under homomorphisms and products we need some information about the behavior of invariant measures.

2.3. **Lemma.** (1) *Suppose J is an ideal of R and $\pi: R \to R/J$ is the projection. An invariant measure μ on R induces invariant measures μ_0 on J and $\overline{\mu}$ on R/J. Conversely given μ_0 and $\overline{\mu}$ there is a unique measure μ inducing them. For such measures, if $\overline{A} \in \mathscr{P}(R/J)$ we have $\overline{\mu}(\overline{A}) = \mu(\pi^{-1}(\overline{A}))$.*

(2) *If $R = R_1 \times R_2$ is a direct product of rings and if μ_i is an invariant measure on R_i then there is an invariant "product measure" μ on R satisfying $\mu(A_1 \times A_2) = \mu_1(A_1)\mu_2(A_2)$ for every $A_i \in \mathscr{P}(R_i)$. Furthermore this construction can be done for infinite direct products $\prod_{k=1}^{\infty} R_k$ so that $\mu(\prod_{k=1}^{\infty} A_k) = \prod_{k=1}^{\infty} \mu_k(A_k)$.*

Proof. (1) The existence of an invariant measure μ on R is equivalent to the existence of an invariant mean $m: \mathscr{B}(R) \to \mathbb{R}$, where $\mathscr{B}(R)$ is the set of all bounded real-valued functions on R. (A linear functional m on $\mathscr{B}(R)$ is a *mean* if $\inf\{f\} \leq m(f) \leq \sup\{f\}$ for every $f \in \mathscr{B}(R)$. It is *invariant* if $m(f_c) = m(f)$ for every $f \in \mathscr{B}(R)$ and $c \in R$, where $f_c(x) = f(x + c)$.)

This equivalence is explained in [G, pp. 14–15]. If invariant means m_0 on J and $\overline{m}$ on R/J are given, we construct m on R as follows. If $f \in \mathscr{B}(R)$ and $c \in R$ define $\varphi_c \in \mathscr{B}(J)$ by setting $\varphi_c(x) = f(x+c)$ for $x \in J$. Then $m_0(\varphi_c)$ is defined and, since m_0 is invariant, it depends only on the class $c+J$ in R/J. Define $m(f) = \overline{m}(m_0(\varphi_c))$. The rest of the properties are left to the reader.

(2) Suppose $R = R_1 \times R_2$ and m_j is an invariant mean on R_j. The product mean m on R is defined easily as in (1): if $f \in \mathscr{B}(R)$ and $x \in R_1$, define $\varphi_x \in \mathscr{B}(R_2)$ by $\varphi_x(y) = f(x, y)$. Then $m_2(\varphi) \in \mathscr{B}(R_1)$ and we define $m(f) = m_1(m_2(\varphi))$. (See [HR, §17.18].) This m is an invariant mean on R. The construction for infinite products is more sophisticated. Define a *cylinder* in $R = \prod_{k=1}^{\infty} R_k$ to be a set of the form $A = \prod_{k=1}^{\infty} A_k$ where $A_k = R_k$ for all but finitely many k. By the method above we can define an invariant measure μ' on the Boolean algebra generated generated by all the cylinders in R. This measure can be extended to an invariant measure μ on all of $\mathscr{P}(R)$ by invoking the Invariant Extension Theorem as in [W, Theorem 10.8]. □

2.4. **Proposition.** (1) *Suppose S is a homomorphic image of R. If R is in $\mathscr{U}$ then so is S. If R is a $(G-G)$-ring then so is S.*

(2) *Suppose $R \cong R_1 \times R_2$. Then R is in $\mathscr{U}$ (resp. is a $(G-G)$-ring) if and only if R_1 and R_2 are in $\mathscr{U}$ (resp. are $(G-G)$-rings).*

(3) *Here* $\operatorname{rad}(R)$ *denotes the Jacobson radical (the intersection of all the maximal left ideals). If $J \subseteq \operatorname{rad}(R)$ and R/J is in $\mathscr{U}$, then R is in $\mathscr{U}$.*

Proof. (1) Let $\varphi: R \to S$ be the given surjective homomorphism. Then $\varphi(R^*) \subseteq S^*$. If R is in the class $\mathscr{U}$ then S is too, by Lemma 2.3. Suppose R is a $(G-G)$-ring, and let G be a subgroup of S^* of finite index. Let $H = \varphi^{-1}(G) \cap R^* = \ker(R^* \to S^*/G)$. Then H has finite index in R^* so that $H - H = R$. Then $G - G \supseteq \varphi(H) - \varphi(H) = S$.

(2) If R is in $\mathscr{U}$ (resp. is a $(G-G)$-ring) then (1) implies R_1 and R_2 have the same property. Suppose R_1 and R_2 are in $\mathscr{U}$. Since $R^* = R_1^* \times R_2^*$ it is easy to get an infinite set with invertible differences. Suppose μ_i is an invariant measure on R_i with $\mu_i(R_i^*) > 0$. Using the product measure μ described in Lemma 2.3, we have $\mu(R^*) > 0$ so that R is in $\mathscr{U}$. Suppose R_1 and R_2 are $(G-G)$-rings, and let G be a subgroup of R^* with finite index. Define $A_1 = \{a \in R_1^* : (a, 1) \in G\}$. Then $A_1 = \ker(\alpha_1 : R_1^* \to R^*/G)$ where $\alpha_1(a) = (a, 1)G$ and it follows that A_1 has finite index in R_1^*. Similarly define A_2 of finite index in R_2^*. Since $A_i - A_i = R_i$ and $A_1 \times A_2 \subseteq G$, it follows that $G - G = R$.

(3) The radical $\operatorname{rad}(R)$ is characterized as the largest ideal M of R such that $1 + M \subseteq R^*$. (See, e.g., [J, vol. II, §4.2] for further details.) Let $S = R/J$ and let $\varphi: R \to S = R/J$ be the natural map. Since $J \subseteq \operatorname{rad}(R)$, we have $1 + J \subseteq R^*$, and the group homomorphism $\varphi^*: R^* \to S^*$ is surjective. Also, if $r \in R$ then $r \in R^*$ iff $\varphi(r) \in S^*$. Suppose S is in $\mathscr{U}$. If $a_1, a_2, \ldots$ is an infinite set with invertible differences in S choose $b_i \in \varphi^{-1}(a_i)$. Then $\varphi(b_i - b_j) = a_i - a_j \in S^*$ so that $b_i - b_j \in R^*$ whenever $i \neq j$. By Lemma 2.3 there is an invariant measure μ on R satisfying $\mu(\varphi^{-1}(\overline{E})) = \overline{\mu}(\overline{E})$ for any $\overline{E} \in \mathscr{P}(S)$. Then $\mu(R^*) = \mu(\varphi^{-1}(S^*)) = \overline{\mu}(S^*) > 0$. □

A *semilocal* ring is, by definition, a ring R such that $R/\operatorname{rad}(R)$ is semisimple artinian. (A ring is *artinian* if it satisfies the descending chain condition

on left ideals.) The Artin-Wedderburn Theorem implies that $R/\operatorname{rad}(R)$ is a direct product of a finite number of simple rings, and each simple component is isomorphic to a matrix ring over some division ring. (For details on these results see a graduate algebra text, e.g., [J, vol. II, §3.13, §4.4].) For example, every artinian ring is semilocal. A commutative ring is semilocal when it has only a finite number of maximal ideals.

2.5. **Proposition.** *If R is a semilocal ring with no finite nonzero homomorphic images, then R is in $\mathscr{U}$.*

Proof. By the discussion above and Proposition 2.4 it suffices to consider the case $R = \mathbb{M}_n(D)$, the ring of $n \times n$ matrices over an infinite division ring D. Since $D \subseteq R$, there does exist an infinite set with invertible differences. To prove the measure property we verify the tiling condition of Lemma 2.1. We work with D^n viewed as the right D-vector space of column vectors. Let $e_i \in D^n$ be the column vector with 1 in the ith position and 0's elsewhere. Define $e_0 = 0$.

Claim. If $v_1, \ldots, v_r \in D^n$ where $r \leq n$ then there exist $i_1, \ldots, i_r \in \{0, 1, \ldots, n\}$ such that the vectors $v_1 + e_{i_1}, \ldots, v_r + e_{i_r}$ are right D-linearly independent.

The case $r = 1$ is easy, so we assume inductively that $r > 1$ and the claim is true for smaller values. Then there exist i_j for $1 \leq j < r$ where $v_1 + e_{i_1}, \ldots, v_{r-1} + e_{i_{r-1}}$ are right D-independent. Let W be the span: $W = \sum_{j=1}^{r-1}(v_j + e_{i_j})D$. Then $\dim W = r - 1 < n$ so there must exist an index k with $e_k \notin W$. If $v_r \notin W$ let $i_r = 0$ while if $v_r \in W$ let $i_r = k$. In either case we have $v_r + e_{i_r} \notin W$ and the independence follows, proving the claim.

If $\alpha \in R$ is given, let $v_1, \ldots, v_n$ be the columns of α. Apply the claim to these vectors to find the indices $i_1, \ldots, i_n$, and define a matrix β where the jth column of β is e_{i_j}. Then the columns of $\alpha + \beta$ are right D-independent, so that $\alpha + \beta \in R^*$. Since these β's vary in a finite set, the tiling condition of Lemma 2.1 is verified. □

For example suppose R is a ring that contains an infinite division ring D and such that R is finite-dimensional as a right D-vector space. Then Proposition 2.5 implies that R is in the class $\mathscr{U}$.

The analog of Proposition 2.4(3) for $(G - G)$-rings, seems harder. We can prove it in the following special case.

2.6. **Proposition.** *If $1 + J$ is a divisible group and R/J is a $(G-G)$-ring, then R is a $(G - G)$-ring. This condition on J is fulfilled whenever J is a nil ideal and $\mathbb{Q} \subseteq R$.*

Proof. By Lemma 2.7 below, $1 + J$ has no proper subgroup of finite index. If G is a subgroup of R^* of finite index then $G \cap (1 + J)$ has finite index in $1 + J$, so that $1 + J \subseteq G$. If $H = \varphi(G)$ then $\varphi^{-1}(H) = G(1 + J) = G$. Therefore $S^*/H \cong R^*/\varphi^{-1}(H) \cong R^*/G$ so that H has finite index in S. Since S is a $(G - G)$-ring, $H - H = S$, so that $G - G = \varphi^{-1}(H) - \varphi^{-1}(H) = R$. Finally, if J is a nil ideal (i.e., every element of J is nilpotent) and $\mathbb{Q} \subseteq R$, then $1 + J$ must be divisible. For if $j \in J$ and n is a positive integer, the binomial series for $(1 + j)^{1/n}$ is a finite sum in R. □

If Γ is a group and $n > 1$, define Γ_n to be the subgroup generated by the

nth powers of elements of Γ. Define Γ to be *predivisible* if $\Gamma_n = \Gamma$ for every positive integer n.

2.7. **Lemma.** *If Γ is predivisible then it has no proper subgroups of finite index. If Γ is abelian the converse also holds.*

Proof. If G is a subgroup of Γ of finite index, let N be a largest subgroup of G that is normal in Γ. Then $[\Gamma: N]$ is also finite. (In fact, if $[\Gamma: G] = n$ the action of Γ on the n left cosets of G provides a homomorphism $\varphi: \Gamma \to S_n$. Then $N = \ker\varphi$ and $[\Gamma: N]$ divides $n!$.) If $k = [\Gamma: N]$ and $x \in \Gamma$, Lagrange's theorem implies that $x^k N = N$ in Γ/N. Therefore $\Gamma_k \subseteq N$. If Γ is predivisible this implies that $N = G = \Gamma$. Conversely, suppose Γ is abelian and has no proper subgroups of finite index. For any prime number p the group Γ/Γ_p (written additively) is an $\mathbb{F}_p$ vector space. If this space is nonzero there exists a subspace of codimension 1. Pulling this subspace up to Γ yields a subgroup of index p, contrary to hypothesis. Therefore $\Gamma = \Gamma_p$ for every prime p, and it follows that Γ is predivisible. If Γ is noncommutative, this argument shows only that $\Gamma_n \cdot [\Gamma, \Gamma] = \Gamma$. □

Consequently, if R^* is a divisible abelian group then R is a $(G-G)$-ring if and only if $R^* + R^* = R$. For example, if $R = \prod_{k=0}^{\infty} \mathbb{C}$ then R^* is divisible and R is a $(G-G)$-ring, but it does not have the finite tiling property of Lemma 2.1. However this R does still lie in $\mathscr{U}$ as we see from the next result.

2.8. **Proposition.** (1) *Suppose $E \subseteq R$. There exists an invariant measure μ on R such that $\mu(E) = 1$ if and only if for every finite set $F \subseteq R$ there exists $r \in R$ such that $r + F \subseteq E$.*

(2) *If there exists an invariant measure μ on R such that $\mu(R^*) = 1$, then R is in $\mathscr{U}$.*

(3) *Suppose $R = \prod_{k=0}^{\infty} A_k$. There exists an invariant μ with $\mu(R^*) = 1$ if and only if for every k there exists an invariant measure μ_k with $\mu_k(A_k^*) = 1$.*

Proof. (1) This is a special case of Lemma A.1.2 of [G, pp. 91–93].

(2) If A, B are subsets of measure 1 in R then $\mu(A \cap B) = 1$ so that $A \cap B \neq \varnothing$. Then for any $r_1 \in R^*$ there exists $r_2 \in R^* \cap (R^* - r_1)$. Similarly there exists $r_3 \in R^* \cap (R^* - r_1) \cap (R^* - r_2) \cap (R^* - r_1 - r_2)$. Continuing in this way we get an infinite sequence $r_1, r_2, \ldots$ in R such that all finite sums of the r_j's are in R^*. Then $a_j = r_1 + r_2 + \cdots + r_j$ provides an infinite sequence in R having invertible differences.

(3) By (1) the existence of μ says that for any $x_1, x_2, \ldots, x_n \in R$ there exists $r \in R$ with $r + x_1, \ldots, r + x_n \in R^*$. Equivalently, for every i and any $x_{1i}, x_{2i}, \ldots, x_{ni} \in A_i$ there exists $r_i \in A_i$ with $r_i + x_{1i}, \ldots, r_i + x_{ni} \in A_i^*$. By (1) this is equivalent to the existence of μ_i. □

2.9. **Corollary.** *For every $c \in [0, 1)$ there exists a ring R with an invariant measure μ such that $\mu(R^*) = c$, but there is no measure μ' with $\mu'(R^*) = 1$.*

Proof. Let $R = \prod_{k=1}^{\infty} \mathbb{F}_{p_i}$ where $p_1, p_2, \ldots$ is a sequence of primes. Let μ be the invariant product measure as described in Lemma 2.3. Since the Haar measure is unique on each component (since it is finite), we see that $\mu(R^*) = \prod_{k=1}^{\infty} \mu(\mathbf{F}_{p_i}^*) = \prod_{k=1}^{\infty} (p_i - 1)/p_i$. For the given $c \in [0, 1)$ choose the primes p_i so that this product converges to c. Since R has a finite homomorphic image, Lemma 1.1 implies that R is not a $(G-G)$-ring, so by Theorem 1.3 it cannot

be in $\mathscr{U}$. There is no invariant measure μ' with $\mu'(R^*) = 1$ by Proposition 2.8(3). Even though there exists an invariant measure μ with $\mu(R^*)$ arbitrarily close to 1, there does not exist an infinite set with invertible differences (and, in fact, R^* is not even a set of recurrence). □

The ring $R = \mathbb{R}[x]$ is not a $(G-G)$-ring since there are certainly not enough units: $R^* + R^* = \mathbb{R}$. If we expand the ring by adjoining more units there is a better chance that it will become a $(G-G)$-ring. Here is one example.

2.10. **Proposition.** *Let* $R = \Delta^{-1}\mathbb{R}[x]$ *where* $\Delta = \{g \in \mathbb{R}[x]: g$ *has no nonreal roots*$\}$; *that is,* $R = \{f/g: f, g \in \mathbb{R}[x]$ *and* $g \in \Delta\}$. *Then* R *is in* $\mathscr{U}$.

Sketch of proof. We verify the condition in Proposition 2.8(1). It suffices to show that if $f_1, \ldots, f_k \in \mathbb{R}[x]$ are given then there exists $g \in \mathbb{R}[x]$ such that $g + f_j \in \Delta$ for every j. To do this suppose $n > \max\{\deg f_j\}$ and let $g = c(x-1)(x-2)\cdots(x-n)$ where c is a large constant. Then each $g + f_j$ has degree n. Choose c so large that the f_j's are tiny compared to g so that each $g + f_j$ has n real roots (which are near to the roots $1, 2, \ldots, n$ of g). □

Finally we show that there exist $(G-G)$-rings that are not in $\mathscr{U}$. We use a criterion for telling when a set has measure 0 with respect to all invariant measures.

2.11. **Lemma.** *Let* G *be an infinite amenable group (written multiplicatively) and* $E \subseteq G$. *Suppose that there exists an infinite sequence* $f_1, f_2, \ldots$ *in* G *and an integer* $k \geq 1$ *such that the intersection of any* k *of the translates* f_jE *is empty. Then* $\mu(E) = 0$ *for every invariant measure on* G.

Proof. Let μ be an invariant measure on G and consider the invariant mean m on $\mathscr{B}(G)$ that corresponds to μ (as in the proof of Lemma 2.3). For a large integer n, let $\varphi_n = \sum_{j=1}^{n} 1_{f_jE}$, where 1_{f_jE} is the characteristic function for the set f_jE. By hypothesis $\varphi_n < k \cdot 1_G$. Therefore $n \cdot \mu(E) = m(\varphi_n) \leq m(k \cdot 1_G) = k\mu(G) = k$ so that $\mu(E) \leq k/n$. Since this holds for every n, it follows that $\mu(E) = 0$. □

This criterion for measure 0 is similar to the condition for measure 1 used in Proposition 2.8. In fact, they are both consequences of the following criterion for a subset E of an infinite amenable group G and a number $c \in [0, 1]$: There exists an invariant measure μ on G such that $\mu(E) \geq c$ if and only if for every finite set $F \subseteq G$ there exists $\alpha \in G$ such that $|\alpha F \cap E| \geq c|F|$.

2.12. **Proposition.** *Suppose* $R = \mathbb{M}_n(K[x])$ *where* $n \geq 2$ *and* K *is a field of characteristic* 0. *Then* R *is a* $(G-G)$*-ring and* R *does not lie in the class* $\mathscr{U}$.

Proof. For the first statement we prove more generally that if A is a commutative euclidean domain containing $\mathbb{Q}$ then $R = \mathbb{M}_n(A)$ is a $(G-G)$-ring. Let ε_{ij} be the matrix with 1 in the (i, j)-position and 0's elsewhere. For $a \in A$ and $i \neq j$ let $e_{ij}(a) = I + a\varepsilon_{ij}$. Define $E_n(A)$ to be the subgroup of $R^* = \mathrm{GL}_n(A)$ generated by all these "elementary" matrices $e_{ij}(a)$. The following 3 steps imply that R is a $(G-G)$-ring.

Step 1. If G is a subgroup of $R^* = \mathrm{GL}_n(A)$ of finite index, then $E_n(A) \subseteq G$.

Proof of Step 1. If $a \in A$ and k is a positive integer then $a/k \in A$ (since $\mathbb{Q} \subseteq A$) and therefore $e_{ij}(a) = e_{ij}(a/k)^k$ is a kth power. Hence $E_n(A)$ is predivisible and Lemma 2.7 applies to the subgroup $G \cap E_n(A)$.

Step 2. $E_n(A) - E_n(A)$ contains all diagonal matrices.

Proof of Step 2. An elementary row operation on a matrix α is done by adding a multiple of one row to another. Elementary column operations are defined similarly. Any sequence of elementary row and column operations on α produces a matrix $p\alpha q$ for some p, $q \in E_n(A)$. If τ is a triangular (upper or lower) matrix with 1's on the diagonal, then $\tau \in E_n(A)$, since τ can be reduced to I by a sequence of elementary row operations. Consequently, if β is a matrix with all 0's on the diagonal then $\beta \in E_n(A) - E_n(A)$. Similarly, every permutation matrix of determinant 1 is in $E_n(A)$. If δ is a diagonal matrix there is a permutation matrix $p \in E_n(A)$ where $p\delta$ has 0's on the diagonal. Therefore $\delta \in E_n(A) - E_n(A)$.

Step 3. If A is euclidean then $E_n(A) - E_n(A) = R$. Moreover $E_n(A) = \mathrm{SL}_n(A)$.

Proof of Step 3. For any matrix α in R there is a sequence of elementary row and column operations reducing α to a diagonal matrix δ. (See, e.g., [J, vol. I, Theorem 3.8], noting that only operations of type I are needed in the reduction.) As in Step 2 there exist p, $q \in E_n(A)$ such that $p\alpha q = \delta \in E_n(A) - E_n(A)$. The equality follows. Finally if $\alpha \in \mathrm{SL}_n(A)$ then α can be reduced to some $\delta = \mathrm{diag}(d_1, \ldots, d_n)$ where $d_1 d_2 \cdots d_n = 1$. To reduce δ to the identity matrix it suffices to note that if u, $v \in A^*$ then the matrix $\mathrm{diag}(u, v)$ can be reduced to $\mathrm{diag}(1, uv)$ by a sequence of elementary row and column operations. (Note. Those groups $E_n(A)$ appear in algebraic K-theory, as seen for example in [HO, §1.2C].)

Finally suppose $A = K[x]$ where K is a field of characteristic 0. We will prove that $R^* = \mathrm{GL}_n(K[x])$ has measure 0 relative to every invariant measure. This will show that R is not in the class $\mathscr{U}$. By Lemma 2.11 it suffices to show that the set of translates $R^* - jx$ for $j \in \mathbb{Z}$ has the property that any $n+1$ of them have empty intersection. To do this suppose $J \subseteq \mathbb{Z}$ is a subset with $|J| = n+1$ and there exists $\alpha \in \bigcap_{j \in J}(R^* - jx)$. Then $jx + \alpha \in R^*$ for every $j \in J$ so that $\det(jx + \alpha) \in K[x]^* = K^*$. Let T be a new indeterminate and define $p(T) = \det(Tx + \alpha) = (Tx)^n + c_{n-1}(Tx)^{n-1} + \cdots + c_0$ where $c_i \in K[x]$. Then for every $j \in J$ the polynomial $p(j) - c_0$ is in K and is a multiple of x in $K[x]$. Therefore $p(j) - c_0 = 0$. But then $p(T) - c_0$ is a polynomial of degree n in $K(x)[T]$ having $n+1$ roots, which is absurd. Therefore no such α can exist and the intersection is empty. □

A number of basic questions concerning $(G-G)$-rings remain unanswered. Here are some examples:

2.13. **Questions.** (1) Does the converse of Lemma 1.1 hold? That is, if $R^* + R^* = R$ and every proper homomorphic image of R is infinite must R be a $(G-G)$-ring?

(2) Is there a commutative $(G-G)$-ring that is not in $\mathscr{U}$? Noncommutative examples are given in Proposition 2.12.

(3) Suppose $R = \mathbb{M}_n(A)$ where $n \geq 2$ and A is an integral domain containing $\mathbb{Q}$. For which A does it follow that $\mathrm{SL}_n(A) - \mathrm{SL}_n(A) = R$? For which A is R a $(G-G)$-ring?

(4) Suppose R is a finite-dimensional algebra over an infinite field K. Let $G = \ker N$ where N is the norm homomorphism $N: R^* \to K^*$ (e.g., if $r \in R$

we can define $N(r) = \det(\lambda_r)$ where $\lambda: R \to \mathrm{End}_K(R)$ is the regular representation (defined $\lambda_r(x) = rx$).) When does it happen that $G - G = R$? For example it holds when $R = \mathbb{M}_2(\mathbb{R})$ (by Proposition 2.12), but it fails when R is the quaternion division algebra over $\mathbb{R}$.

We end this section by answering a twisted version of the original question, where the roles of multiplication and addition are switched.

2.14. **Proposition.** *Let K be an infinite field and $G \subseteq K$ a subgroup of finite index in the additive group. Then $G^* \cdot (G^*)^{-1} = K^*$ where $G^* = G - \{0\}$; that is, for every $c \in K^*$ there exist $g_1, g_2 \in G^*$ such that $c = g_1/g_2$.*

Proof. If $\mathrm{char}\, K = 0$ then the additive group is divisible, $G = K$, and the claim is trivial. Suppose $\mathrm{char}\, K = p > 0$. Then K is an infinite-dimensional $\mathbb{F}_p$-vector space (where $\mathbb{F}_p$ is the field of p elements). Since G and cG are $\mathbb{F}_p$-subspaces of finite codimension, we must have $G \cap cG \neq \{0\}$ and the result follows. □

3. Behavior of $G + G$ in a field

Suppose K is an infinite field and G is a subgroup of finite index n in K^*. The questions raised in [LS] concerned the set $G+G$. Theorem 1.3 above implies that if $-1 \in G$ (e.g., if the index n is odd), then $G + G = K$. What happens if $-1 \notin G$?

Let $m \cdot G$ denote the sum of m copies of G (for example, $2 \cdot G = G + G$). Let ΣG be the smallest additively closed set containing G, so that ΣG is the union of all the $m \cdot G$. If $-1 \notin G$ then $G + G \subseteq \Sigma G \cap K^*$, and it is tempting to conjecture that this is an equality. When $n = 2$ the equality does follow [LS, Proposition 2]. However, at the end of [B] Berrizbeitia described examples when $K = \mathbb{Q}$ showing that this conjecture is false and discussed the number of summands needed to make $G + \cdots + G = \Sigma G$. Here is a summary of those results.

3.1. **Proposition** (Berrizbeitia). *Let K be an infinite field and $G < K^*$ a subgroup of index n.*

(1) *$m \cdot G \subseteq (m+1) \cdot G$ with equality if and only if $m \cdot G = \Sigma G$.*

(2) *If $0 \in \Sigma G$ then $\Sigma G = K$. In fact, $0 \in m \cdot G$ if and only if $m \cdot G = K$. Moreover, $n \cdot G \supseteq K^*$ so that $(n+1) \cdot G = K$.*

(3) *If $0 \notin \Sigma G$ then K is a formally real field and ΣG is the intersection of finitely many "orderings of higher level" in K. The index $d = [K^* : \Sigma G]$ is even and $(n/d) \cdot G = \Sigma G$.*

Sketch of Proof (following [B, §3]). (1) By Theorem 1.3, $1 = g - g'$ for some $g, g' \in G$. Then $G = (1 + g')G \subseteq G + G$ and the remaining statements follow.

(2) If $0 \in m \cdot G$ then $-1 \in (m-1) \cdot G$ and $K = G - G \subseteq G + (m-1) \cdot G = m \cdot G$. If m_0 is the smallest index with $m_0 \cdot G = \Sigma G$ then for each $k < m$ the set $(k+1) \cdot G$ contains some element (and hence some coset of G) not contained in $k \cdot G$. Hence $k \cdot G$ contains at least k cosets and the claim follows.

(3) If $0 \notin \Sigma G$ then ΣG is a torsion preordering in the sense of [Bec], and therefore K is formally real. As noted in [Bec], every torsion preordering is the intersection of some orderings of higher level. The index d is even since $-1 \notin \Sigma G$. The equality follows as before since ΣG contains n/d cosets. □

Moreover Berrizbeitia proved that the bound in (2) cannot be improved in general. For any odd prime p he found a subgroup $G_p < \mathbb{Q}^*$ of index $n = p-1$ such that $(p-1) \cdot G_p \neq \mathbb{Q}$ but $p \cdot G_p = \mathbb{Q}$. This G_p is the kernel of the homomorphism $\varphi: \mathbb{Q}^* \to (\mathbb{Z}/p\mathbb{Z})^*$ defined as follows: Every $r \in \mathbb{Q}^*$ can be expressed uniquely as $r = p^m \cdot r_0$ where $m \in \mathbb{Z}$ and r_0 is a p-adic unit. Define $\varphi(r) = [r_0]$, the class of r_0 in $\mathbb{Z}/p\mathbb{Z}$.

3.2. **Question.** If n is even, is there a subgroup G of index n in $\mathbb{Q}^*$ such that $n \cdot G \neq \mathbb{Q}$ but $(n+1) \cdot G = \mathbb{Q}$? If such G exists, must the factor group $\mathbb{Q}^*/G$ be cyclic?

Acknowledgments

We are grateful to P. Berrizbeitia for sending us a preliminary version of his work. It is also a pleasure to thank J. Rosenblatt for several interesting conversations about invariant means.

Added in proof

F. Kalhoff has noted that these ideas also apply in the following nonassociate case: If K is a quasifield and $G < K^*$ is a subloop of finite index then $G - G = K$.

References

[Bec] E. Becker, *Extended Artin-Schreier theory of fields*, Rocky Mountain J. Math. **14** (1984), 881–897.

[Ber] V. Bergelson, *Ergodic Ramsey theory*, Logic and Combinatorics (S. G. Simpson, ed.), Contemp. Math., vol. 65, Amer. Math. Soc., Providence, RI, 1987, pp. 63–87.

[B] P. Berrizbeitia, *Additive properties of multiplicative subgroups of finite index in fields*, Proc. Amer. Math. Soc. **112** (1991), 365–369.

[F] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory*, Princeton Univ. Press, Princeton, NJ, 1981.

[GRS] L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey theory*, John Wiley & Sons, New York, 1980.

[G] F. Greenleaf, *Invariant means on topological groups and their applications*, van Nostrand, New York, 1969.

[HO] A. J. Hahn and O. T. O'Meara, *The classical groups and K-theory*, Springer-Verlag, Berlin, 1989.

[HR] E. Hewitt and K. A. Ross, *Abstract harmonic analysis*, vol. 1, Springer-Verlag, Berlin, 1963.

[J] N. Jacobson, *Basic algebra*. I, II, Freeman, San Francisco, 1974, 1980.

[LS] D. B. Leep and D. B. Shapiro, *Multiplicative subgroups of index three in a field*, Proc. Amer. Math. Soc. **105** (1989), 802–807.

[W] S. Wagon, *The Banach-Tarski paradox*, Cambridge, Univ. Press, Cambridge, 1985.

Department of Mathematics, Ohio State University, Columbus, Ohio 43210-1174