SELF-CENTRED SETS

H. KESTELMAN

1. Introduction. A subset S of an abelian group G is said to have a centre at a if whenever x belongs to S so does $2a - x$. This note is mainly concerned with *self-centred* sets, i.e. those S with the property that every element of S is a centre of S. Such sets occur in the study of space groups: the set of inversion centres of a space group is always self-centred. Every subgroup of G is self-centred, so is every coset in G: this is the reason why the set of points of absolute convergence of a trigonometric series is self-centred or empty **(1)**. A self-centred set of real numbers that is either discrete or consists of rational numbers must in fact be a coset (see §3); this does not hold for an arbitrary enumerable self-centred set of real numbers (§3.3). An enumerable discrete self-centred plane set is either a lattice or (in a suitable basis) it consists of all points having integral coordinates (m, n) with mn even (§3.2).

We discuss linear and plane sets from first principles (§3). This is followed (§4) by a more general discussion (applicable to abelian groups) which throws light on the earlier more restricted approach.

All groups to be considered are abelian, the group operation is denoted by $+$, and the neutral element by 0; kS denotes the set of kx with x in S, and $S + T$ the set of $s + t$ with s in S and t in T. When $S \subset R_n$, $m_i S$ and $m_e S$ denote respectively the interior and exterior Lebesgue measures of S.

It will be convenient to denote the set of centres of an arbitrary set S by $\mathfrak{Z}(S)$ and the set of differences of S ($x - y$ with x and y in S) by $\mathfrak{D}(S)$; $\mathfrak{T}(S)$ denotes the translation group of S, i.e. the set of a in G such that $S + a = S$, and $\mathfrak{G}(S)$ the subgroup of G generated by S, i.e. the set of elements

$$n_1 x_1 + n_2 x_2 + \ldots + n_q x_q$$

where $x_1, \ldots, x_q$ are in S and $n_1, \ldots, n_q$ are arbitrary integers. If S is a subgroup, we have $\mathfrak{Z}(S) \supset \mathfrak{T}(S) = \mathfrak{G}(S) = S$. It is plain that S and its complement in G, cS, have the same translation group; also that every centre of S is also a centre of cS, of the closure of S, and of the interior of S; equally obvious, $\mathfrak{Z}(S)$ is always self-centred or empty. If S and T are self-centred, so is $S \cap T$, and if $a \in G$, $S + a$ is self-centred.

I am grateful to Professor C. A. Rogers for some very helpful discussions and suggestions. I am also indebted to a referee who pointed out that there is a close connection between some of the results presented below and those which, in a greatly generalized form, are contained in T. S. Motzkin's memoir

Received August 20, 1965.

on endovectors (Proc. Symp. Pure Math. (7) (Convexity), Amer. Math. Soc. 1963).

2. Some examples. Before discussing the form of self-centred linear and plane sets, we list a few examples in vector spaces of self-centred sets that are not cosets.

(a) The set of real numbers $m + n\sqrt{2}$, where m and n are integers and mn is even, includes zero but is not a group since it includes 1 and $\sqrt{2}$ but not $1 + \sqrt{2}$.

(b) The set of number pairs (m, n) with m, n restricted as in (a) is self-centred but not a coset.

(c) In R_n, let G be the lattice of all points with integral coordinates. The group $2G$ has index 2^n in G, the points $(e_1, \ldots, e_n)$ with $e_r = 0$ or 1 being a set of representatives of the cosets of $2G$ in G; any union of these cosets is self-centred (see §4).

(d) Let G be the space of arbitrary sequences of real numbers and E any chosen set of natural numbers. Define X to be the subset of G consisting of all $(x_1, x_2, \ldots)$ with x_r integral whenever $r \in E$, and let $S = 2X$. Every point of X is a centre of S; thus S is self-centred.

(e) The set S of points $(m, n3^r)$ in R_2, where m, n, r are integers and mn is even, is self-centred. Those points with m and n even form a subgroup T of S, and S is the union of $\aleph_0$ cosets of T.

(f) Let H be a Hamel base for the real numbers over the rationals. Take β_1, β_2 in H and let A be the set of all real numbers whose β_1 and β_2 components in H are zero; define S as the set of all numbers $m\beta_1 + n\beta_2 + x$ where $x \in A$ and m, n are integers with mn even. S is self-centred and not a coset (as in (a)). S is non-measurable: $m_i S = 0$ (by Steinhaus' theorem) since

$$q^{-1}\beta_1 \,\bar{\in}\, \mathfrak{D}(S)$$

for $q = 1, 2, \ldots$, and $m_e S > 0$ since $\aleph_0$ translates of S cover R_1. In fact $m_i cS = 0$ (see §4), and S is of second category.

3. Self-centred linear and plane sets.

3.1. *Suppose that S is an infinite set of real numbers which is self-centred but not everywhere dense; then S is a linear lattice.*

Proof. Choose a and b $(= a + p)$ in S. Since S is self-centred, $a \pm 2p$ are in S and are centres of S, and by induction $a + np \in S$ for all integers n. Since S is not everywhere dense, this implies that S has no limit points and that there is a least positive p, say p_0, such that $a + p \in S$. Thus, for every integer n, S includes $a + np_0$ and $a + (n + 1)p_0$ but no intermediate number.

THEOREM 1. *Let S be an infinite set of rational numbers which is self-centred and includes zero; then S is a group* (*under addition*).

Proof. We prove that S is a group by defining an increasing sequence of groups whose union is S. Let $0, x_1, x_2, \ldots$ be the elements of S. As in 3.1, $\mathfrak{G}(x_1) \subset S$, and we define G_1 as $\mathfrak{G}(x_1)$. If $G_1 \neq S$, let n_1 be the least integer r for which $x_r \bar{\in} G_1$. Clearly H_1, the group generated by G_1 and x_{n_1}, is discrete and so G_2, defined as $H_1 \cap S$, is self-centred and discrete and therefore a group by 3.1. G_2 contains G_1 and includes x_1 and x_2. Now continue inductively. Having defined $G_1, \ldots, G_q$ as discrete groups with $G_1 \subset G_2 \subset \ldots \subset G_q$ and $x_1, \ldots, x_q$ in G_q, we may, if $G_q \neq S$, define n_q as the least r for which $x_r \bar{\in} G_q$, H_q as the discrete group generated by G_q and x_{n_q}, and G_{q+1} as $H_q \cap S$.

COROLLARY. *A self-centred set S of rational numbers is a coset of some group*; for if $a \in S$, the set $S - a$ is self-centred and includes zero; hence it is a group.

3.2. The next theorem shows that Example (b) of §2 is the prototype of discrete plane self-centred sets that are not lattices. It will be recalled that the inversion centres for the plane symmetry groups which include sixfold centres and inversion centres are of this type.

THEOREM 2. *Let S be a plane self-centred set that is discrete but not a lattice. Then S includes points U, V, W such that S consists of all points P given by $\overrightarrow{UP} = m\overrightarrow{UV} + n\overrightarrow{UW}$ where m and n are integers with mn even.*

Proof. If $v \in \mathfrak{D}(S)$, then, since S is self-centred, it follows (see §4) that $2v \in \mathfrak{T}(S)$, and so, S being discrete, the distances between points of S must have a positive least value, say δ. Choose U and V in S so that $UV = \delta$. As in §3.1, the points of S on UV form the lattice determined by U and V. Similarly, and since $2\overrightarrow{UV} \in \mathfrak{T}(S)$, the distances of points of S (not on UV) from the line UV have a least positive value δ'; let W be a point of S distant δ' from UV. If V' and W' are taken so that $\overrightarrow{UV'} = 2\overrightarrow{UV}$ and $\overrightarrow{UW'} = 2\overrightarrow{UW}$, it follows that $\overrightarrow{UV'}$ and $\overrightarrow{UW'}$ belong to $\mathfrak{T}(S)$ and S contains the lattice determined by U, V', W'. From the definitions of δ and δ', it follows that the points of S in the closed parallelogram with sides UV' and UW' are the vertices and mid-points of the sides of this parallelogram and possibly also the centre of the parallelogram. Since S is not a lattice, the second possibility is excluded and this proves the result required.

3.3. It is clear that a plane self-centred set that has limit points (e.g. example (e),§2) could not be described by a formula like that in Theorem 2. If S is plane and self-centred and consists of points (x, y) with x and y both rational, and S includes $(0, 0)$ but is not a lattice, we can partially imitate the argument used in Theorem 1. First enumerate the points of S as $0, z_1, z_2, \ldots$, let $G_1 = \mathfrak{G}(z_1)$, and let z_{n_1} be the first in the sequence which is not in G_1. The extension of G_1 by z_{n_1} is a discrete group H_1; and G_2, defined as $H_1 \cap S$, is self-centred and discrete and includes z_1 and z_2. But G_2 need not be a group:

https://doi.org/10.4153/CJM-1966-098-3 Published online by Cambridge University Press

it could consist of $u_2 + mv_2 + nw_2$ where m and n are integers with mn even (Theorem 2). We could then continue and obtain a sequence $G_1 \subset G_2 \subset \ldots$ where G_q includes $z_1, \ldots, z_q$, and if G_q is not a group, it consists of all points $u_q + mv_q + nw_q$ where m and n are integers and mn is even. If S, which is the union of the G_q, is not a group, this formula will apply for arbitrarily large q.

The same considerations apply to a self-centred set of real numbers consisting of numbers of the form $a + b\xi$ where ξ is a fixed irrational and a and b are rational; we have only to map the point $a + b\xi$ onto the point (a, b).

4. Centres of subsets of an abelian group. For the discussion of non-enumerable self-centred sets in R_n and for subsets of general abelian groups, it is basic that a set that has more than one centre must have translational symmetry:

LEMMA 1. *For any subset S of an abelian group,* $2\mathfrak{D}\{\mathfrak{Z}(S)\} \subset \mathfrak{T}(S)$.

Proof. If a and b are centres of S, and $x \in S$, then

$$2(b - a) + x = 2b - (2a - x) \in S.$$

Thus $2(b - a) + S \subset S$, and if we interchange a and b we get

$$2(b - a) + S = S.$$

THEOREM 3. *Suppose that S is a self-centred subset of an abelian group G. Then S is a union of cosets of* $2\mathfrak{G}\{\mathfrak{D}(S)\}$ *in G.*

Proof. Since $S \subset \mathfrak{Z}(S)$, and $\mathfrak{T}(S)$ is a group, Lemma 1 implies that $2\mathfrak{G}\{\mathfrak{D}(S)\} \subset \mathfrak{T}(S)$, and so $a \in S$ implies $a + 2\mathfrak{G}\{\mathfrak{D}(S)\} \subset S$.

COROLLARY. *If G is a normed vector space, and S in Theorem* 3 *has interior points, then $S = G$* since $\mathfrak{D}(S)$ contains a sphere about the origin and so $\mathfrak{G}\{\mathfrak{D}(S)\} = G$; see also Theorem 5.

One can readily construct self-centred sets in a vector space by using

THEOREM 4. *If G is a subgroup of a vector space over the real numbers and S is the union of any aggregate of cosets of G in $\frac{1}{2}G$, then S is self-centred.*

Proof. If x and y belong to S, then $2x$ and $2y$ belong to G and so does $2x - 2y$; hence $2x - y$ and y are in the same coset of G. Since S contains the whole of the coset of G including y, this means that $2x - y \in S$ and so S is self-centred.

THEOREM 5. *If S in R_n is self-centred and $m_i S > 0$, then $S = R_n$.*

Proof. By a theorem of Steinhaus, $\mathfrak{D}(S)$ contains a sphere about the origin. Thus $\mathfrak{G}\{\mathfrak{D}(S)\} = R_n$ and so $S = R_n$ by Theorem 3.

THEOREM 6. *If $S \subset R_n$ and $\mathfrak{T}(S)$ is everywhere dense (e.g. in R_1 if S has arbitrarily close centres, in particular if $\mathfrak{Z}(S)$ is non-enumerable), then there are just two possibilities:*

either (*a*) *S is non-measurable with* $m_i S = m_i cS = 0$,
or else (*b*) *S is measurable and one of S and cS has measure zero.*

Proof. If $m_i S > 0$, it follows by elementary density arguments that almost all points of R_n have the form $s + t$ with s in S and t in $\mathfrak{T}(S)$. So, if S is measurable, $mS > 0$ implies $mcS = 0$. But if S is non-measurable, $m_i S$ must be zero. The same applies to cS, which has the same translation group as S.

We can illustrate (a) by taking a Hamel base for the real numbers over the rationals and assuming that it includes 1. If J is the set of elements of the base other than 1, and S is the group generated by the rational multiples of elements of J, then R_1 is covered by $\aleph_0$ translates of S. This implies that $m_e S > 0$, and since $rS = S$ for all non-zero rational numbers r, S and therefore $\mathfrak{T}(S)$ are everywhere dense in R_1. Any non-enumerable group S of real numbers with $mS = 0$ is plainly everywhere dense and illustrates (b).

4.2. The special property of self-centred sets of rational numbers described in Theorem 1 is a consequence of Theorem 3 and the following

THEOREM 7. *If G is a group of rational numbers* (*under addition*), *then either 2G has index 2 in G or else* $2G = G$ (*in which case* $x \in G$ *implies* $x/2^n \in G$ *for all integers n*).

Proof. Suppose $2G \neq G$ and let a be a number in G which is not in $2G$. Write the elements of G as $a = x_1, x_2, x_3, \ldots$; G_n, the group generated by $x_1, x_2, \ldots, x_n$, is discrete and we write it as $\mathfrak{G}(\gamma_n)$. $2G$ consists of the even multiples of γ_n and so a must be an odd multiple of γ_n and

$$G_n = 2G_n \cup (2G_n + a).$$

Since G is the union of the G_n, and $2G$ the union of the $2G_n$, this proves that $G = 2G \cup (2G + a)$.

By contrast, we note that if G is the group generated by 1 and $\sqrt{2}$, then $2G$ has index 4 in G, a set of representatives of $G/2G$ being $0, 1, \sqrt{2}, 1 + \sqrt{2}$. In general,

THEOREM 8. *If G is an abelian group and* $pG \neq G$ *for some prime p, then the index of pG in G is either infinite or else an integral multiple of p.*

Proof. Suppose pG has finite index k in G. Let a be an element of G not in pG. Then $ka \in pG$; if k is not a multiple of p, and its residue (mod p) is s, then clearly $sa \in pG$. Since p is prime, there exist integers μ and ν such that $1 = \mu s + \nu p$ and so $a = \mu sa + \nu pa \in pG$, which is a contradiction.

Example (e) in §2 shows that the index can be $\aleph_0$.

The following is an analogue of Theorem 7.

THEOREM 9. *Suppose G is an abelian group which is the union of a sequence of cyclic groups* $G_1 \subset G_2 \subset \ldots$, *and p is a prime such that* $pG \neq G$. *Then pG has index p in G.*

https://doi.org/10.4153/CJM-1966-098-3 Published online by Cambridge University Press

Proof. If G is finite, it follows from Theorem 8 that its order is a multiple of p, say ph. G is then cyclic and generated by some element g of order ph, and $prg = psg$ if and only if $p(r - s)$ is a multiple of ph, i.e. $r - s$ is a multiple of h. Hence pG is composed of $pg, 2pg, \ldots, hpg$, i.e. pG has order h and G/pG has p members.

Now suppose G is infinite. We know from Theorem 8 that the index of pG is at least p. Suppose if possible that the index exceeds p, and that $x_1, x_2, \ldots, x_{p+1}$ are in different cosets of pG. Take n so large that $x_1, x_2, \ldots, x_{p+1}$ all belong to G_n; then it follows that the index of pG_n in G_n exceeds p. Hence, from the first case considered, G_n cannot be finite. Suppose $G_n = \mathfrak{G}(g)$; then rg and sg are in the same coset of pG if and only if $r - s$ is a multiple of p; this means that pG_n has as many cosets in G_n as there are residue classes (mod p): in other words, pG_n has index p in G_n, which is a contradiction.

5. The relation between $\mathfrak{G}(S)$ and $\mathfrak{G}\{\mathfrak{D}(S)\}$. It is of interest to examine the relation between $\mathfrak{G}(S)$ and its subgroup $\mathfrak{G}\{\mathfrak{D}(S)\}$ for arbitrary sets S. Since $S - b \subset \mathfrak{D}(S)$ for every b in S, we have

$$\text{(1)} \qquad \mathfrak{G}(S - b) \subset \mathfrak{G}\{\mathfrak{D}(S)\} = \mathfrak{G}\{\mathfrak{D}(S - b)\} \subset \mathfrak{G}(S - b),$$
$$\mathfrak{G}\{\mathfrak{D}(S)\} = \mathfrak{G}(S - b).$$

Also

$$\text{(2)} \qquad \mathfrak{G}(S) = \mathfrak{G}(S - b) + \mathfrak{G}(b) = \mathfrak{G}\{\mathfrak{D}(S)\} + \mathfrak{G}(b).$$

It follows that $\mathfrak{G}(S) = \mathfrak{G}\{\mathfrak{D}(S)\}$ if S includes an element of $\mathfrak{G}\{\mathfrak{D}(S)\}$; in particular, if $0 \in S$, or if S includes an element x and also $2x$.

However, if S and $\mathfrak{G}\{\mathfrak{D}(S)\}$ are disjoint, we see from (2) that $\mathfrak{G}(S)$ is generated by $\mathfrak{G}\{\mathfrak{D}(S)\}$ and any one element of S and that $\mathfrak{G}(S)/\mathfrak{G}\{\mathfrak{D}(S)\}$ is cyclic. In particular, if G is a normed space and $\mathfrak{G}(S)$ is of second Baire category, then so is $\mathfrak{G}\{\mathfrak{D}(S)\}$ since a countable union of translates of the latter compose $\mathfrak{G}(S)$. Finally, $\mathfrak{G}(S) = \mathfrak{G}\{\mathfrak{D}(S)\}$ whenever $\mathfrak{G}(S)$ is a subfield of R_1; this follows from (1) and

THEOREM 10. *If $S \subset R_1$ and $\mathfrak{G}(S)$ is a field, then $\mathfrak{G}(S + a) = \mathfrak{G}(S)$ for all a in $\mathfrak{G}(S)$.*

Proof. Since $\mathfrak{G}(S + a) = a\mathfrak{G}(a^{-1}S + 1)$ if $a \neq 0$, it is enough to prove that $\mathfrak{G}(S + 1) = \mathfrak{G}(S)$. If $x \in \mathfrak{G}(S)$, then clearly

$$\text{(3)} \qquad x = y_0 + n_0$$

for some y_0 in $\mathfrak{G}(S + 1)$ and some integer n_0. By taking $x = \frac{1}{2}$ it follows that $\mathfrak{G}(S + 1)$ includes non-zero integers; these (with zero) form a group, say $\mathfrak{G}(k)$. Hence the integer n_0 in (3) can be restricted so that $0 \leqslant n_0 < k$, and so $\mathfrak{G}(S + 1)$ has finite index in $\mathfrak{G}(S)$, say j. This means that for every x in $\mathfrak{G}(S)$, $jx \in \mathfrak{G}(S + 1)$ and hence $\mathfrak{G}(S) \subset \mathfrak{G}(S + 1) \subset \mathfrak{G}(S)$.

It is clear that Theorem 10 has an analogue for abelian groups in general.

THEOREM 11. *Suppose that S is a subset of an abelian group and that $\mathfrak{G}(S)$ has no proper subgroup of finite index. Let a be any element of $\mathfrak{G}(S)$ and r an integer, $r \geqslant 2$. Then $\mathfrak{G}(S + ra) = \mathfrak{G}(S)$.*

Proof. As in the proof of Theorem 10, $x \in \mathfrak{G}(S)$ implies that $x = y_0 + n_0 ra$ for some y_0 in $\mathfrak{G}(S + ra)$ and some integer n_0. By taking $x = a$, we get $y_0 = a - n_0 ra$, and since $r \geqslant 2$, this means that $\mathfrak{G}(S + ra)$ includes non-zero integral multiples of a and consequently a group $\mathfrak{G}(ka)$ where k is some positive integer; thus every x in $\mathfrak{G}(S)$ can be written as $y_0 + m_0 a$ with $0 \leqslant m_0 < k$; this implies that $\mathfrak{G}(S + ra)$ has finite index in $\mathfrak{G}(S)$ and is therefore identical with $\mathfrak{G}(S)$.

REFERENCE

1. J. Arbault, *Sur l'ensemble de convergence absolue d'une série trigonométrique*, Bull. Soc. Math. France, *80* (1952), 253–317.

University College, London