ON SUBGROUPS OF FIXED INDEX

GEORGE K. WHITE

If $k\in\mathcal{K}$, where \mathcal{K} is a subgroup of a group \mathcal{S} , then closure implies $k^2,k^3,\cdots,\in\mathcal{K}$. Nonempty subsets $S\subset\mathcal{S}$ with the inverse property $s^m\in S$ implies $s,s^2,\cdots,s^m\in S$ $(m=1,2,\cdots)$ will be called stellar sets. Let p^α be a fixed prime power. If a stellar set S of an abelian group \mathcal{S} intersects every subgroup \mathcal{K} of index p^α in \mathcal{S} , and $0\not\in S$, then the cardinal |S| of S is bounded below by p^α (Theorem 3), when \mathcal{S} satisfies a mild condition.

Hence for instance a subset S of euclidean n-space E_n intersecting all sublattices of determinant p^{α} of the fundamental lattice will have at least p^{α} elements, and more if no element is divisible by p^{α} .

Henceforth $\mathcal S$ will always be an additive abelian group, so a $stellar\ set$ will be one with

(1)
$$\varnothing \neq S \subset \mathscr{S}$$
 $mg \in S \Rightarrow g, 2g, \dots, mg \in S(g \in \mathscr{S}, m = 1, 2, \dots)$.

Examples of stellar sets are \mathscr{S} itself, and its *periodic part* [5, p. 137]; and a star set [7] is a symmetric stellar set. There are stellar sets of one element s, i.e., those s for which $s = mg(m = 1, 2, \cdots)$ implies m = 1. Now let p be a fixed prime, and suppose S intersects every subgroup \mathscr{K} of \mathscr{S} of index p. Suppose also

$$(2) 0 \notin S$$

(if $0 \in S$ the intersection property is redundant). Then we can say the following (in this paper we denote |A| = cardinal of A, $mA = \{ma; a \in A\}$, for any set A and integer m):

THEOREM 1. Let p be a fixed prime, S an abelian group, and S a stellar set with $0 \in S$ which intersects all subgroups \mathcal{K} of index $S: \mathcal{K} = p$. Then

$$|S| \ge p.$$

When $S \cap p\mathscr{S} = \emptyset$ we have |S| > p.

A similar result holds for ordinary sets T:

Theorem 2. Suppose p is a fixed prime, $\mathcal S$ is an abelian group with more than one subgroup of index p, and T is any subset of $\mathcal S$ with

$$(4) T \cap p\mathscr{S} = \emptyset$$

which intersects all subgroups \mathcal{K} of index $\mathcal{S}:\mathcal{K}=p$. Then

$$|T| \geq p+1.$$

When $\mathscr S$ is the fundamental lattice Λ_0 [2, 4] in r-space E_r of all points with integral coordinates, Theorems 1 and 2 are immediate using Rogers' proof of his Theorem 1 [7] on starsets, the small adjustment needed being clear. He states his theorem with a slightly stronger hypothesis equivalent to "S intersects all subgroups of index $\leq p$ ", and for this more stringent requirement Cassels [3], replacing p by n, has made elegant use of a generalization of Bertrand's postulate due to Sylvester [9] and Schur [8] to show $|S| \geq n$ for $n = 1, 2, \cdots$ and any stellar set S of an abelian $\mathscr S$ with no periodic part. For $n = p^{\alpha}$ a prime power we shall extend this as follows:

THEOREM 3. Suppose that $n=p^{\alpha}$ is fixed, $\mathcal S$ is an abelian group containing no element of order p^{β} when $1 < p^{\beta} < p^{\alpha}$, and that S is a stellar set with $0 \notin S$ which intersects all subgroups $\mathscr K$ of index $\mathscr S: \mathscr K = p^{\alpha}$. Then

$$|S| \geq p^{\alpha}.$$

When $S \cap p^{\alpha} \mathscr{S} = \emptyset$, we have

$$|S| \geq p^lpha + egin{cases} p & if \, lpha > 1 \ if \, lpha = 1 \ . \end{cases}$$

Note the requirement "contains at least one subgroup of index p^{α} " is a natural one, but it is an unneeded restriction on S. Note also that Theorem 1 is an immediate consequence of Theorem 3.

2. A lemma. We find it useful, for Rogers' case $\mathscr{S} = \Lambda_0 \subset E^r$, to restate Theorem 3 in altered form. We denote $\overline{x} = (x_1, \dots, x_r)$ so that

$$\Lambda_0 = \{\bar{x}: \text{ all the } x_i \text{ are integers, } i=1,\cdots,r\}$$
,

and $\mathscr{S} = \Lambda_0$ is isomorphic to a direct sum of r infinite cyclic groups. When $\overline{x} \in \Lambda_0$ we define $p | \overline{x}$ to mean $p | x_1, \dots, p | x_r$, and

$$||x||_p = \max \{\alpha : p^{\alpha} | \overline{x}\}$$
.

Let T be any subset of Λ_0 satisfying

$$(7) p^{\alpha} \varLambda_{\scriptscriptstyle 0} \cap T = \varnothing (T \subset \varLambda_{\scriptscriptstyle 0}) ,$$

and a modified stellar condition

$$\begin{cases} p^{\beta}\overline{x}\in T & \text{implies} \quad \overline{x},\,2\overline{x},\,\cdots,\,p^{\beta}\overline{x}\in T \\ (1\leq\beta\leq\alpha,\,p^{\alpha} \text{ fixed}) \;, \end{cases}$$

and consider congruences

$$(9) \overline{l} \cdot \overline{x} = l_1 x_1 + \cdots + l_r x_r \equiv 0 (p^{\alpha}) (\overline{l} \in \Lambda_0, p \nmid \overline{l}).$$

LEMMA. If $T \subset \varLambda_0$ satisfies (7) and (8), $r \geq 2$ and the congruence (9) has for each \overline{l} a solution $\overline{x} \in T$, then T contains at least $p^{\alpha} + p^{\min(\alpha,2)-1}$ distinct elements mod p^{α} ,

$$| \ T \bmod p^\alpha | \geq p^\alpha + \begin{cases} p & \text{if } \alpha > 1 \text{ ,} \\ 1 & \text{if } \alpha = 1 \text{ .} \end{cases}$$

Proof. We consider two cases, (i) $\alpha = 1$ or $r \le \alpha$, and (ii) $r > \alpha \ge 2$. For the first case, a simple counting argument will suffice. Define

(11)
$$\theta(i, \alpha) = \frac{p^{(i-1)(\alpha-1)}(p^i-1)}{p-1}.$$

Then there are exactly

$$\sum_{k=1}^{k=r} p^{(\alpha-1)(k-1)+lpha(r-k)} = heta(r, lpha)$$

distinct congruences (9), representable by

$$\overline{l}=(pm_1,\cdots,pm_{k-1},1,l_{k+1},\cdots,l_r)$$
.

If $\bar{y} \equiv b\bar{x} \mod p^{\alpha}$ then clearly \bar{y} satisfies every congruence \bar{x} does, and hence we may construct a subset V of T which likewise satisfies every congruence (9), and also

(12)
$$\begin{cases} \overline{x} \in V, \ \overline{y} \in V, \ \overline{y} \equiv b\overline{x} \bmod p^{\alpha} \Rightarrow \overline{y} = \overline{x} \ , \\ \overline{x} \in V \Rightarrow \overline{x} \quad \text{satisfies some congruence (9) .} \end{cases}$$

Any $\bar{x} \in V$ may be expressed as

$$\bar{x} = \bar{x}' p^{\xi}(p \nmid \bar{x}'; 0 \leq \xi = ||\bar{x}||_{p} < \alpha)$$

by (7), since $V \subset T$. A fixed $\bar{x} \in V$ obeys (9) for at least one \bar{l} and in fact for precisely those \bar{l} satisfying $\bar{l} \cdot \bar{x}' \equiv 0(p^{\alpha-\ell})$; these correspond to exactly $p^{\ell}\theta(r-1,\alpha)$ congruences (consider, e.g., $\bar{x}'=(1,0,\cdots,0)$). Hence, counting over the $\theta(r,\alpha)$ congruences (9), we get

(13)
$$\theta(r,\alpha) \leq \sum_{\bar{x} \in V} p^{||\bar{x}||} p \theta(r-1,\alpha) .$$

Now $\overline{x} \in V$ obeys (8), since $V \subset T$. Hence to each $\overline{x} = \overline{x}'p^{\epsilon}$ in V there correspond p^{ϵ} elements

Moreover,

(15)
$$\bar{x}_1 \neq \bar{x}_2$$
 implies $T(\bar{x}_1) \cap T(\bar{x}_2) = \emptyset$ $(\bar{x}_1, \bar{x}_2 \in V)$,

for otherwise $\lambda_1 \overline{x}_1 = \lambda_2 \overline{x}_2$, $\lambda_i = \lambda_i' p^{\theta i}(p \nmid \lambda_i')$, without loss of generality $\theta = \theta_1 - \xi_1 - (\theta_2 - \xi_2) \geq 0$, and $\lambda_2' \overline{x}_2 = \lambda_1' p^{\theta} \overline{x}_1$, $\overline{x}_2 \equiv (\lambda_2')^{-1} \lambda_1' p^{\theta} \overline{x}_1 \mod p^{\alpha}$, $\overline{x}_2 = \overline{x}_1$ by (12). Thus by (13), (15),

$$egin{align} |T|&\geqq\sum_{ec{x}\in V}p^{||ec{x}|+p}\geqq heta(r,lpha)/ heta(r-1,lpha)\ &=p^lpha+rac{p^{lpha-1}(p-1)}{p^{r-1}-1}\,. \qquad (r\geqq2) \end{align}$$

If $\alpha=1$ we have $|T|\geq p+(p-1)(p^{r-1}-1)^{-1}>p$, so $|T|\geq p+1$; if $r\leq \alpha>1$ then

$$|T| - p^{\alpha} \ge p^{\alpha-1}(p-1)(p^{\alpha-1}-1)^{-1} > p-1$$
 ,

 $|T| - p^{\alpha} \ge p$, and case (i) is verified.

For our second case $r > \alpha \ge 2$ we employ induction on r. Let r = j, define $V \subset T$ as in case (i), and denote

(16)
$$\overline{x} = (x_1, \cdots, x_{j-1}, x_j) = (\overline{x}_0, x_j).$$

There are $p^{j-1}+\cdots+p+1\geqq p^{\alpha}+p+1$ subgroups

$$H(\bar{a}') = \{\lambda \bar{a}' \bmod p : \lambda = 1, \dots, p \equiv 0\}$$

 $(\bar{a}' \text{ fixed}, \ p \nmid \bar{a}')$, any two of which intersect in a point \bar{x} divisible by p. So if V contains a primitive $(p \nmid \bar{x})$ point from each subgroup, we have $|V| \geq p^{\alpha} + p + 1$ and our result follows. Hence we may assume that V does not intersect some $H(\bar{a}')$, where without loss of generality $\bar{a}' = (0, \dots, 0, 1)$; then V contains no point of type $\bar{x} = \lambda(p\bar{y}_0, 1) \mod p$ when $p \nmid \lambda$, and hence by (8) no such point for any $\lambda = 1, 2, \dots$,

(17)
$$\bar{x} \in V \Rightarrow \bar{x} = p^{\beta}(\bar{y}'_0, y_i)$$
. $(p \nmid \bar{y}'_0, 0 \leq \beta < \alpha)$.

Now define sets $T(\bar{x})$ as in (14) and denote their union by W,

$$W = \bigcup \{T(\overline{x}) : \overline{x} \in V\}$$
 ,

so that $V \subset W \subset S$, and W is the (smallest) set generated by V which satisfies the modified stellar condition (8). Denote

(18)
$$W_0 = \{ \overline{x}_0 : (\overline{x}_0, x_j) \in W \text{ for some } x_j \}.$$

Then by (17), (18), points $\overline{x}'_0 p^{\epsilon}(p \nmid \overline{x}'_0)$ of W_0 correspond to points $p^{\epsilon}(\overline{x}'_0, x_j)$ of W and so clearly W_0 satisfies (7) and (8). But V and

hence W satisfies every congruence \bar{l} in (9); thus W and hence W_0 satisfies every \bar{l} with $l_j = 0$ for some $\bar{x}_0 = (x_1, \dots, x_{j-1}) \in W_0$ such that

$$l_1x_1 + \cdots + l_{j-1}x_{j-1} \equiv 0(p^{\alpha})$$
 $(l_1, \cdots, l_{j-1}, p) = 1$.

Thus by our induction hypothesis $(r=j-1, \alpha \ge 2)$ there are at least $p^{\alpha}+p$ such $\bar{x}_0 \in W_0$, and

$$|S| \geq |W| \geq |W_0| \geq p^{lpha} + p$$
 .

As our result is already established for $r=\alpha$ (case (i)), this completes the proof of the lemma.

3. Proof of Theorems 2 and 3. Consider the homomorphism η :

$$(19) \mathscr{S} \xrightarrow{\eta} \overline{\mathscr{S}} \cong \mathscr{S}/p^{\alpha}\mathscr{S}$$

(cf. Cassels [3] for his case s=1); for Theorem 2 we take $\alpha=1$.

We see easily that if $\mathscr{S}: \mathscr{K}=p^{\alpha}$ then $p^{\alpha}\mathscr{S}\subset \mathscr{K}$ and so there is a one-to-one correspondence between all \mathscr{K} , \mathscr{K} of index p^{α} in \mathscr{S} , \mathscr{S} respectively; and any subset V of \mathscr{S} intersects all such \mathscr{K} if and only if \overline{V} intersects all such \mathscr{K} (index p^{α}). If V has the stellar set property this may, however, be lost under η . Since $p^{\alpha}\mathscr{S}=0$ we have by a result of Prüfer [1] that \mathscr{S} is a direct sum of cyclic groups C_i of orders $p^{\beta_i} \leq p^{\alpha}$; in fact, $\beta_i = \alpha$ since in all our 3 theorems \mathscr{S} has no element of order $p^{\beta}(0 < \beta < \alpha)$ and hence $p^{\beta_i}c_i = 0$ implies $\beta_i \geq \alpha$. Thus

(20)
$$\overline{\mathscr{S}} = \sum_{i \in I}^{\oplus} C_i(C_i \cong \langle e : p^{\alpha}e = 0 \rangle) .$$

Note that all $s \in S$ have infinite period,

(21)
$$ms \neq 0$$
 $(s \in S, m = \pm 1, \pm 2, \cdots)$

since otherwise |m|s=0, $s=(|m|+1)s\in S$ so $0=|m|s\in S$ contrary to (2). Now suppose $\bar{0}\in \bar{S}$. Then $p^{\alpha}g\in S$ so $g,2g,\cdots,p^{\alpha}g\in S,|S|\geq p^{\alpha}$ since otherwise ig=jg(i< j) and $g\in S$ has finite period. It remains therefore to settle the matter when

(22)
$$\bar{0} \notin \bar{S}$$
 (i.e., $S \cap p^{\alpha} \mathscr{S} = \varnothing$).

The cases |I|=0,1 in (20) correspond to groups $\mathscr S$ with no, exactly one subgroup of index p^{α} . In the latter event we have $\overline{0} \in \overline{S}$, a case already settled. If |I|=0 in Theorem 3 then $\mathscr S=p^{\alpha}\mathscr S$ and all stellar sets S vacuously satisfy the intersection condition. No stellar set is empty, so we have $s \in S$, $s=p^{\alpha}s_1$, $s_1=p^{\alpha}s_2$, ..., and $|S|=\infty$ since otherwise $s_i=s_j$ (i< j) and $s_j \in S$ has finite period, contrary to (21).

The case $|I| \leq 1$ does not occur for Theorem 2, since here $\mathscr S$ has ≥ 2 subgroups of index p^{α} . Hence we may assume

$$(23) |I| \ge 2.$$

From (23) it is immediate that \mathcal{S} contains more than one subgroup of index p^{α} . We consider only Theorem 3 from now on; Theorem 2 will follow by the same reasoning $(\alpha = 1)$.

It remains, then, to verify Theorem 3 when (22), (23) hold. Assume now then

$$|S| < \infty ,$$

since if $|S| = \infty$ we have nothing to prove. Then if we decompose $\overline{s} = \sum_{s_i}$ in (20) we have $s_i \neq 0$ for some $\overline{s} \in \overline{S}$ for only a finite number of $i \in I$, which we may include in a finite set $i = 1, \dots, j$ $(2 \leq j \leq |I|)$. Then

$$ar{S}\subset \mathscr{S}^{\scriptscriptstyle(0)}\cong arLambda_0 mod p^lpha \quad (ext{in j-space E^j}) \;, \qquad (2 \leqq j) \;, \ ar{\mathscr{S}}=\mathscr{S}^{\scriptscriptstyle(0)} igoplus \mathscr{S}^* \;,$$

and we may represent any $\bar{x} \in \mathcal{F}$ uniquely by

$$\bar{x} = x^{(0)} + x^* = (x_1, \dots, x_j; x^*) \mod p^{\alpha}$$
.

The following subgroups $\overline{\mathscr{K}}$ have index p^{α} in $\overline{\mathscr{S}}$ and hence are intersected by \overline{S} :

$$\widehat{\mathscr{K}}=\{\overline{x}\colon l_{\scriptscriptstyle 1}x_{\scriptscriptstyle 1}+\,\cdots\,+\,l_{\scriptscriptstyle j}x_{\scriptscriptstyle j}\equiv\,0(p^{\scriptscriptstylelpha})\}\qquad (l_{\scriptscriptstyle 1},\,\cdots,\,l_{\scriptscriptstyle j},\,p)=1$$
 ,

where $(l_i, p) = 1$ for some i and l_1, \dots, l_j are fixed for each $\widetilde{\mathcal{K}}$ (cf. [3, preceding (10)]); we have $p \nmid l_i$ for at least one i and so for each $\overline{x} \in \widetilde{\mathcal{K}}$, $x_i = -\sum_{j \neq i} l_i^{-1} l_j x_j$. Hence $|\mathscr{K}_0| = p^{\alpha(j-1)}$,

$$\mathscr{S}:\mathscr{K}=\mathscr{S}_{\scriptscriptstyle{0}}:\mathscr{K}_{\scriptscriptstyle{0}}=p^{\scriptscriptstyle{lpha j}}/p^{\scriptscriptstyle{lpha(j-1)}}=p^{\scriptscriptstyle{lpha}}$$
 .

Elements \bar{s} of \bar{S} are of type $\bar{s}=(s_1,\cdots,s_j;0^*);$ since S is a stellar set the modified property (8) holds for $T=\bar{S};$ also, $0=(0,\cdots,0,0^*)\notin \bar{S}$ and $r=j\geq 2$ by (22), (23). So we may apply the lemma to find there are at least $p^{\alpha}+p^{\min(\alpha,2)-1}$ distinct points $(s_1,\cdots,s_j,0^*)$ in $\bar{S};$ hence

$$|S| \geq |ar{S}| \geq p^{lpha} + p^{\min(lpha,2)-1}$$
 ,

and our proof of Theorems 2, 3 is complete.

4. Remarks. 1. In our proof of Theorem 3 we utilize the stellar property of S only through its consequence in \bar{S} , a condition of type (8) with $T = \bar{S}$ which would clearly follow from imposing

condition (8) on S, along with $S \neq \emptyset$. Hence we may make the following extension:

THEOREM 4. Theorem 3 holds for S not a stellar set, if S satisfies (8) $(T = S \subset \mathcal{S}, \bar{x} \in \mathcal{S})$, and $S \neq \emptyset$.

2. When \mathscr{S} is not abelian, Theorems 1-4 need not hold; e.g., the direct sum $\mathscr{S}=C^\infty \oplus A_5$ of the infinite cyclic group and alternating group of 60 elements has only one subgroup of index 3, $\mathscr{K}=3C^\infty \oplus A_5$, and \mathscr{K} is intersected by the stellar set of one element,

$$S = \{3 + \text{cycle (123)}\} \neq 3g$$
 .

- 3. In the excluded case $0 \in S$ the least stellar set containing 0 is the periodic part of \mathcal{S} , and $|S| \ge p$ need not follow.
- 4. When $\mathscr{S}=\varLambda_0(r\geq 2)$, the set of all $(1, x_2, 0, \dots, 0), (px_1, 1, 0, \dots, 0) \mod p^{\alpha}$ is a stellar set of $p^{\alpha}+p^{\alpha-1}$ elements intersecting all congruences (9) mod p^{α} . So our bounds are best possible, for the lemma, when $\alpha=1,2$. $(r\geq 2)$.
- 5. In Theorem 3 we must exclude elements of order $p^{\beta}(\beta < \alpha)$. For consider ,e.g., $\mathscr{S} = C^{\infty} \oplus C^{(p)}$ (any α). Here the bound is $p^{\alpha} + 1$.
- 6. Let $\alpha \geq 2$, S be a stellar set in Euclidean n-space $\{\bar{x} = (x_1, \dots, x_n)\}$ with fewer than $p^{\alpha} + p$ elements, and no element $p^{\alpha}\bar{x}$. Then there is a sublattice of the fundamental lattice of determinant p^{α} (see [2], p. 10) which is not intersected by S.
- 7. Our condition (A)''S intersects all subgroups of index n'' is equivalent to $(B)''\cdots$ index $d\colon d\mid n''$ though weaker than $(C)''\cdots$ index $m\colon m< n''$. The latter remark follows from the example $S=\{(4,1),\,(2,1),\,(2,0),\,(1,0)\}$ in $\mathscr{S}=C^{\infty}\oplus C^{(2)}$ (n=4). For the former prove first for d=n/p and then iterate: if $\mathscr{S}:\mathscr{H}=n/p$ $(p\mid n)$ and (A) holds then $\mathscr{H}\neq p\mathscr{H}$, there exist \mathscr{M} in \mathscr{H} with $\mathscr{H}:\mathscr{M}=p$ so $\mathscr{S}:\mathscr{M}=n,\,\mathscr{H}\cap S\neq\varnothing$.
- 8. Theorem 3 does not hold for all $n=1,2,\cdots$. Mr. George M. Bergman of Cambridge, Mass. has kindly furnished me with a set of counterexamples for $\mathscr{S}=C^{\infty}\oplus C^{\infty}$, which includes a stellar set S of 76 elements that intersects every subgroup of index 77.
- 9. Finally, we should like to acknowledge here some parallel though independent work of Mr. Bergman who in unpublished cor-

respondence proves a simpler version of Theorem 4, obtaining a slightly lower bound (p^{α} rather than $p^{\alpha}+p$, 1). His proof is in essence similar to ours, except there is no induction step: a homomorphism η (19) reduces the problem to Rogers' case $\mathscr{S}=\varLambda_0$, and a version of our lemma is proved by arguments resembling ours for $\alpha=1$ or $r\geq\alpha$, Mr. Bergman in effect considering congruences (9) with $l_1=1$ to obtain his bound p^{α} for (10) for all r,α , without induction. We thank Mr. Bergman for the material communicated; among other things it helped remind us to include Theorem 4. We thank him also for welcome suggestions concerning our final draft.

REFERENCES

- 1. J. L. Brenner, The decomposition theorem for abelian groups Bull. Amer. Math. Soc. 47 (1941), 116-117.
- 2. J. W. S. Cassels, An introduction to the geometry of numbers Grund d. Mat. Wiss 99 (Berlin, 1959).
- 3. ———, On the subgroups of infinite abelian groups, J. London Math. Soc. 33 (1958), 281-284.
- 4. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford, 1954.
- 5. A.C. Kurosh, *The theory of groups* I (Trans. K.A. Hirsch), Chelsea, New York, 1955.
- 6. H. Prüfer, Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, Math. Zeit. 17 (1923), 35-61.
- 7. C. A. Rogers, The number of lattice points in a star body J. London Math. Soc. 26 (1951), 307-310.
- 8. I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I, II Sitzungsberichte der Preuss. Akad. Wiss. (1929), 125-136, 370-391.
- 9. J. Sylvester, On arithmetical series, Mess of Math. 21 (1892), 1-19, 87-120. (Reprinted in Collected Works IV, 687-731.)

Received October 13, 1967.

University of British Columbia and Dalhousie University