SOME MAPPINGS OF PFRIODIC GROUPS

BY

SHMUEL SCHREIBER

ABSTRACT

For the rational integer a and the rational prime b, let $P(a,b)$ be the set of primes p such that

$$\text{(i)} \qquad (p,\, a(a-1)) = 1,\; b \,|\, (p-1), \left(\exists c \in N,\; b \not| \, c, p \,\Big|\, \frac{a^{bc}-1}{a^c-1}\right).$$

A natural integer q satisfies (i) iff q is a power product from $P(a,b)$. In the (additively written) Abelian group G, $g \to ag$ permutes the elements of $G^{\#}$ in cycles whose lengths are multiples of b, but not of b^2, iff G is a π-group with $\pi \subset P(a,b)$. The case $a = -2, b = 2$ has combinational applications.

1. Introduction

Let G be an additively written periodic group with the following property: that there exist a rational integer a and a rational prime b such that the mapping $g \to ag$ permutes the elements of $G^{\#}$ in cycles, the length of each cycle being some multiple of b but not of b^2. It turns out that the presence or absence of this property depends not so much on the structure of G as on the set of primes dividing the orders of its elements. The cases $b = 2$ and $a = -2$, $b = 2$ are discussed further, the latter having combinatorial applications.

2. The general case

NOTATION. a is a rational integer, b is a rational prime, q and c are positive integers. G is an additively written group, $G^{\#}$ is the set of its nonzero elements, $|G|$ is the order of G (when finite).

DEFINITION 1. $q \in Z(a,b)$ if q satisfies the following (partly redundant) conditions:

Received June 14, 1973

(1) $$(q, a(a-1)) = 1$$

(2) $$b \mid q-1$$

(3) $$\exists c, b \nmid c, q \,\Big|\, \frac{a^{bc}-1}{a^c-1}.$$

The subset of $Z(a,b)$ consisting of primes will be denoted by $P(a,b)$.

Definition 2. The additively written group $G \in G(a,b)$ if the mapping $g \to ag$, $\forall g \in G$, permutes the elements of $G^{\#}$ in cycles, the length of each of which is divisible by b, but not by b^2. Thus, $G(a,b)$ can contain no group having elements of infinite order; hence we only discuss *periodic* or *torsion* groups, such as, finite ones.

Our main purpose is the proof of the following assertion.

Proposition 3. *G is in $G(a,b)$ if and only if every prime dividing the order of some element of $G^{\#}$ is in $P(a,b)$.*

Remark. Taking b composite, this is false. Let G be the cyclical group of order 31, take $a = 5$, $b = 6$. One verifies $(31,20) = 1$, $6 \mid (31-1)$, $31 \mid ((5^6-1)/(5-1)) = 3906 = 31 \times 126$. Thus, by Definition 1, $31 \in Z(5,6)$. But in G, $g \to 5g$ is an automorphism of order 3, not 6.

For the proof of Proposition 3 we need several lemmas.

Lemma 4. *$G \in G(a,b)$ if and only if every cyclical subgroup of G is in $G(a,b)$.*

The proof is immediate, since $g \to ag$ takes no element outside the cyclical group it generates.

Lemma 5. *Proposition 3 holds for cyclical groups of prime order q.*

Proof. Suppose first that $G \in G(a,b)$; then, whether $q = |G|$ is a prime or not conditions (1) and (2) of Definition 1 follow. For if $g \to ag$ is to permute the elements of $G^{\#}$, no element of $G^{\#}$ may have an order dividing a, since it would be mapped on zero. Nor may the order of an element divide $a-1$, since such an element would be mapped on itself (giving a cycle of length 1). Since a cyclical group of order q contains elements of every order dividing q, this gives (1, 1).

It also follows that $q - 1 = |G^{\#}|$ is divisible by b, since $G^{\#}$ is to be partitioned into cycles, the order of each being a multiple of b, and this is (1, 2).

Let now q be a prime number and let m be the least integer such that $a^m \equiv 1 \pmod{q}$ (that is, let a belong to the exponent m, modulo q), then obviously all cycles will be of length m. By hypothesis, m is a multiple of b, say $m = b \cdot c$ with $b \nmid c$; then $a^{bc} \equiv 1$ (modulo q), $a^c \not\equiv 1$ (modulo q), thus q divides the integer $(a^{bc} - 1)/(a^c - 1)$, which is (3).

Conversely, suppose $q \in P(a, b)$. Then m, in the notation above, divides $b \cdot d$ where d is the greatest common denominator of c and $(q - 1)/b$. If $m \mid d$ then $a^d \equiv 1$ (modulo q). Hence $a^c \equiv 1$ (modulo q) and $(a^{bc-1})/(a^c - 1)$ is a sum of b terms, each congruent to 1 (modulo q) so, since $q \equiv 1$ (modulo b) by (2), q cannot divide that sum. Therefore $m \nmid d$, $m \mid bd \Rightarrow b \mid m$ (b being a prime). This completes the proof of Lemma 5.

Corollary 6. *The "only if" part of Proposition 3 holds in the general case, since a cyclical group G will contain elements of any prime order dividing $|G|$.*

Lemma 7. *Proposition 3 holds for cyclical groups of prime power order, $q = p^k$.*

Proof. By Corollary 6, we only have to show the "if" part. This might be verified directly, but it seems shorter to use a result of Le Veque [1, Th. 4-6, p. 52].

Theorem 8. *If a belongs to the exponent v, modulo p and if p^z is the largest power of p dividing $a^v - 1$, then a belongs, modulo p^k, to the exponent $v \cdot p^r$ where $r = \max(0, k - z)$.*

Let thus a belong to the exponent v, modulo p, where $v = b \cdot c$, $b \nmid c$; then, in the notation of Theorem 8, $p^z \mid (a^{bc} - 1)$, $p^z \nmid (a^c - 1)$ for some z, therefore $p^k \mid (a^{bc_1} - 1)$ with $c_1 = c \cdot p^r$, and $p \nmid (a^{c_1} - 1)$ since $b \nmid c_1$, thus

$$p^k \mid ((a^{bc_1} - 1)/(a^{c_1} - 1)).$$

Hence for a *primitive* or *generator* element $g_0 \in G$, the cycle will be of length $bc_1 = bcp^r$, while elements of the form $p^s g_0$ with $1 \leqq s \leqq r$ will permute in cycles of length bcp^{r-s}. This completes the proof of Lemma 7.

Lemma 9. *If $G_3 = G_1 \oplus G_2$, then $G_3 \in G(a, b)$ if and only if both summands belong to $G(a, b)$.*

Proof. Necessity follows from Lemma 4. (If one summand contains a cyclical subgroup violating the condition of Definition 2, the same will hold for the sum.) For sufficiency, we appeal again to Lemma 4. Let $g_3 = g_1 + g_2$, for $g_1 \in G_1$, $g_2 \in G_2$. If either term is zero, $\{g_3\}$ will still satisfy the condition, by the hypothesis on G_1 and G_2. Thus suppose $g_1 \in G_1^{\#}$, $g_2 \in G_2^{\#}$. If g_1 belongs to a cycle of length

bc_1 and g_2 to one of length bc_2, g_3 will belong to a cycle of length bc_3, where c_3 is the lcm of c_1 and c_2, and from $b \nmid c_1$, $b \nmid c_2$ we have $b \nmid c_3$. Thus the cyclical group $\{g_1 + g_2\}$ belongs to $G(a, b)$ and this, with Lemma 4, finishes the proof.

3. Proof of Proposition 3

By Corollary 6, all one has to check is that $p \in P(a,b)$ for every p dividing the order of an element, then G is indeed in $G(a,b)$. By Lemma 7, this will hold for every cyclical subgroup of prime power order. If $\{g\}$ is a cyclical subgroup of order n, where n is a power product of different primes, there exists a presentation (unique, up to isomorphism) of $\{g\}$ as direct sum of cyclical groups of the corresponding prime power orders, and a repeated application of Lemma 9 shows that $\{g\} \in G(a,b)$. Hence every cyclical subgrouo of G is in $G(a,b)$ and so, by Lemma 4, is G itself. This completes the proof.

Another formulation of Proposition 3 would be: G is in $G(a,b)$ if and only if G is a Π-group, with $\Pi \subseteq P(a,b)$.

The following purely arithmetical result might be proved, very much on the same lines as Lemmas 5, 7, and 9.

Lemma 10. *$q \in Z(a,b)$ if and only if every prime factor of q is in $P(a,b)$.*

This leads immediately to two alternative formulations of Proposition 3, (the second one, for finite groups only).

Proposition 3′. *The periodic group G is in $G(a,b)$ if and only if the order of each element of $G^{\#}$ is in $Z(a,b)$.*

Proposition 3″. *The finite group G is in $G(a,b)$ if and only if $|G| \in Z(a,b)$.*

(This is so since, following Lagrange, the order of every element divides the group order.)

4. The case $b = 2$

Definition 11. We call the cycle generated by $g \to ag$ of the first kind if it contains $-x$ for every $x \in G$ in it; otherwise, it is of the second kind. It is readily seen that a cycle of the first kind is of even length, and that cycles of the second kind occur in pairs. Both kinds of cycle may appear in the same group, as for instance in the cyclical group of order 15 with $a = 2$.

Proposition 12. *If $g \in G(a,2)$, every cycle generated by $g \to ag$ is of the first kind.*

PROOF. If $p \in P(a, 2)$, p is odd and divides an integer of the form

$$(a^{2c} - 1)/(a^c - 1) = a^c + 1$$

with c odd. If $(p - 1, c) = d$, a will belong, modulo p, to the exponent $2d$, and we shall have $a^d \equiv -1$ (modulo p). Thus, in the cyclical group $C(p)$, $g \to ag$ will always yield $-g$ after d iterations. In any case, $p \mid (a^d + 1)$ and, as in the proof of Lemma 7, p^k will divide $a^{d_1} + 1$ where d_1 $(= d \cdot p^r$ for some $r \geqq 0)$ is again an odd number. Therefore, if g generates a cyclical group of order p^k, $g \to ag$ will take g into $-g$ after d_1 iterations.

Lastly, consider $g_3 = g_1 + g_2$, where g_1 belongs to a cycle of length $2d_1$ and g_2 to one of length $2d_2$, d_1, d_2 odd. Then d_3, the lcm of d_1 and d_2, is an odd multiple of each, thus d_3 iterations will take both g_1 into $-g_1$ and g_2 into $-g_2$, hence g_3 into $-g_3$. Since every element in a cyclical group is (uniquely) the sum of elements of prime power orders, this completes the proof.

REMARK. The elements of $P(a, 2)$ are obviously connected with the quadratic residue character of a. (Thus, if $p \equiv 1$ (modulo 4) and a is a non residue, or if $p \equiv -1$ (modulo 4) and a is a residue, $p \notin P(a, 2)$.) We shall further elaborate this connection in the subcase discussed in Section 5.

5. The subcase $a = -2$, $b = 2$

The groups of $G(-2, 2)$ are of independent interest since the Abelian ones appear in some combinatorial designs (refer to [2], [3]). They include, as we shall see presently, all groups of prime order p where p is a Mersenne prime. These have been used by Shaugnessy [3] in combinatorial constructions.

A prime $p \in P(-2, 2)$ if and only if p divides an integer of the form $(-2)^c + 1$ where c is odd, or equivalently, $2^c - 1$, c odd. If this integer itself is a prime, it is called a Mersenne prime $(7, 31, 127 \cdots)$. In any case, $p \in P(-2, 2)$ if 2 belongs (modulo p) to an odd exponent $d \mid p - 1$. Since $p - 1$ is an even number for $p > 2$, 2 has to be a quadratic residue of p, and this excludes all primes of the form $8t \pm 3$ (refer to [1, p. 68]).

If $p = 8t + 7$, 2 is a residue and its exponent is a factor of $4t + 3$, thus $p \in P(-2, 2)$. There remains the case $p = 8t + 1$. Here, if $t = 2^n \cdot h$, $n \geqq 0$, with h odd, then $p - 1 = 2^m h$, for $m = n + 3$ and we know a priori that 2, being a residue, belongs to the (unique) multiplicative cyclical subgroup of order $2^{n+2} \cdot h$. For $p \in P(-2, 2)$ we require 2 to belong to the smaller multiplicative subgroup of order h.

ESTIMATE. About one sixth of the primes of the form $8t+1$ belong to $P(-2,2)$. That is to say, of a large number N of primes of this form we expect about $\frac{1}{6}N$ to be in $P(-2,2)$.

HEURISTIC PROOF.

(i) In the sequence of primes of the form $2^{3+n}\cdot h+1$, h odd, we expect to find $n=0$ in one half of the cases, $n=1$ in one fourth of them and, generally, the event $n=k$ to occur with relative frequency 2^{-k-1}.

(ii) For $n=k$, 2 belongs to the subgroup of order $2^{k+2}\cdot h$ and we expect 2 to belong to the smaller subgroup of order h once in 2^{k+2} times.

Thus for each k we expect a contribution of $N\cdot 2^{-2k-3}$, and altogether $\frac{1}{8}N\sum_{k=0}^{\infty}2^{-2k}=\frac{1}{6}N$.

Of the first 295 primes of the form $8t+1$, 42 belong to $P(-2,2)$. The first few are 73, 89, 233, 337, 601.

To sum up: $Z(-2,2)$ consists of all the primes of the form $8t-1$, of about one sixth of the primes of the form $8t+1$, and of their power products.

Lastly, let us see how information on the residue character of 2 allows us to obtain more details on $P(-2,2)\cap\{8t+1\}$. For this, we appeal to the investigations of Whiteman [4]. Note that each prime of the form $8t+1$ may be written uniquely in the form $p=a^2+b^2=c^2+2d^2$, b and d even [1, p. 128, Cor. and Prob.]. Then, if 2 is at least an octic residue:

(5.1) $(2/p)_8=1\Rightarrow 2^{\frac{1}{8}(p-1)}\equiv(-1)^{\frac{1}{8}(p-1)}\cdot(-1)^{\frac{1}{8}b}$ (modulo p) [4, Th. 2].

(5.2) $(2/p)_{16}=1\Rightarrow 2^{(p-1)^{16}}\equiv(-1)^{b/16+d/4}$(modulo p) [4, Th. 3].

These congruences are valid whenever the relevant exponents are integers.

From this we obtain:

(5.3) For $n=3$, $p=16t+9$, $p\in P(-2,2)$ if and only if $b\equiv 8$ (modulo 16); then $\frac{1}{8}(p-1)$ is odd. Thus, from the right-hand side of (5.1), $\frac{1}{8}b$ should be odd as well.

(5.4) For $n\geqq 4$, $p\in P(-2,2)$ only if $b\equiv 0$ (modulo 16) and $b+4d\equiv 0$ (modulo 32). This follows again from the right-hand side of (5.1) where $\frac{1}{8}(p-1)$ is even, hence $\frac{1}{8}b$ should be even as well, and from the right-hand side of (5.2). If $n=4$, $p=32t+17$, this condition is also sufficient, because then the exponent of the left-hand side of (5.2) is an odd integer. A case in point is $p=337=9^2+16^2=7^2+2\cdot 12^2$, with $16\equiv 0$ (modulo 16) and $16+4\cdot 12\equiv 0$ (modulo 32).

Observe finally that (5.3) gives us a convenient construction of some primes with the desired property: list all sums $a^2 + b^2$ with $a = 8a_1 + 3$, $b = 16b_1 + 8$ (to ensure $p \equiv 9$ (modulo 16)) and select the prime values.

Acknowledgement

The author thanks the referee of [2] for formulating Proposition 3, and Professor J. B. Muskat for many helpful suggestions and discussions, not least for acquainting him with the relevant material of [1] and [4].

References

1. W. J. Le Veque, *Topics in Number Theory*, Volume 1, Addison-Wesley, Reading, Mass., 1956.

2. S. Schreiber, *Covering all triples on n mark by disjoint Steiner systems*, J. Combinatorial Theory Ser. A **15** (1973), 347–350.

3. E. P. Shaugnessy, *On disjoint Steiner systems* (to appear in J. Comb. Theory, Series A).

4. A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math. **6** (1954), 346–373.

Department of Mathematics
Bar-Ilan University
Ramat Gan, Israel