A NOTE ON DIFFERENCE SETS

D. R. HUGHES

1. **Introduction.** In [1] R. H. Bruck develops a theory of difference sets in groups that are not necessarily cyclic. In this note we shall present examples of such difference sets (where $\lambda = 1$) in not-abelian groups of countably infinite order; to do this we generalize a method used by M. Hall in [2]. (For terminology see [1].) The author wishes to thank R. H. Bruck and R. P. Goblirsch for helpful comments.

2. **Construction of difference sets.** Suppose G is a group, D a subset of G, and for every $g \in G$, $g \neq 1$, there exists exactly one pair $d_1, d_2 \in D$ such that $g = d_1 d_2^{-1}$, and there exists exactly one pair $d_3, d_4 \in D$ such that $g = d_3^{-1} d_4$. Then D is a 1-difference set, or merely a difference set, for the group G.

LEMMA. *Let G be a group and let S be a subset of G; then S satisfies* (i) *if and only if it satisfies* (ii).

(i) $\quad s_1 s_2^{-1} = s_3 s_4^{-1} \neq 1, \quad s_i \in S, \quad$ implies $\quad s_1 = s_3, s_2 = s_4.$

(ii) $\quad s_1^{-1} s_2 = s_3^{-1} s_4 \neq 1, \quad s_i \in S, \quad$ implies $\quad s_1 = s_3, s_2 = s_4.$

PROOF. Suppose S satisfies (i), and $s_1^{-1}s_2 = s_3^{-1}s_4 \neq 1$, where the s_i are in S. Then $s_3 s_1^{-1} = s_4 s_2^{-1}$. If $s_1 = s_3$, then $s_2 = s_4$, and we have (ii); if $s_1 \neq s_3$, then $s_3 s_1^{-1} \neq 1$, so by (i) we have $s_3 = s_4$, $s_1 = s_2$, which contradicts $s_1^{-1}s_2 \neq 1$. The other half of the proof is completely similar.

Now let B be a countably infinite group satisfying:

(a) any equation $x^2 = b$ has at most finitely many solutions $x \in B$ for a given $b \in B$;

(b) B contains no elements of order two;

(c) every element not in the center of B has infinitely many distinct conjugates.

Suppose D' is a finite subset of B such that all the quantities $d_1 d_2^{-1}$, for $d_1, d_2 \in D'$, $d_1 \neq d_2$, are distinct (whence all the quantities $d_1^{-1} d_2$, for $d_1, d_2 \in D'$, $d_1 \neq d_2$, are distinct). Then we shall call D' a partial difference set. Given a partial difference set D' (possibly empty) and given an element $b \in B$ such that $b \neq d_1 d_2^{-1}$ for any $d_1, d_2 \in D'$, we shall extend D' to a partial difference set D'' in which $b = d_1 d_2^{-1}$ holds for some pair $d_1, d_2 \in D''$. Then given an element $c \in B$ such that $c \neq d_1^{-1} d_2$ for any $d_1, d_2 \in D''$, we shall extend D'' to a partial difference set D''' in which $c = d_1^{-1} d_2$ holds for some pair $d_1, d_2 \in D'''$.

Received by the editors December 9, 1954.

If we show that this can be done, then we can clearly construct a difference set D for the group B, since B is countable.

Given $b \in B$ as in the above paragraph, note that $b \neq 1$. Letting x be an arbitrary element of B, consider the elements:

(1) $xd_1^{-1}, d_1x^{-1}, bxd_1^{-1}, d_1x^{-1}b^{-1}, b, b^{-1}, d_1d_2^{-1}$, where $d_1, d_2 \in D', d_1 \neq d_2$.

We note that $b \neq b^{-1}$, and $b \neq d_1d_2^{-1}$; thus the elements of (1) are distinct from one another and from the identity, unless at least one of the following holds:

(1.1) $xd_1^{-1}x = d_2$; (1.2) $xd_1^{-1}bx = d_2$;

(1.3) $xd_1^{-1}bx = b^{-1}d_2$; (1.4) $x = d_1d_2^{-1}d_3$;

(1.5) $x = b^{-1}d_1d_2^{-1}d_3$; (1.6) $x = bd_1$;

(1.7) $x = b^{-1}d_1$; (1.8) $x = d_1$;

(1.9) $x = b^{-2}d_1$; (1.10) $x^{-1}bx = d_1^{-1}d_2$;

where $d_i \in D'$.

Equations (1.4)–(1.9) are satisfied for only finitely many x. Equations (1.1)–(1.3) are all of the form $xax = c$, or $(ax)^2 = ac$; by hypothesis on B, only finitely many x satisfy (1.1)–(1.3).

Now consider (1.10). If b is in the center of B, this becomes $b = d_1^{-1}d_2$, or $d_1b = bd_1 = d_2$, or $b = d_2d_1^{-1}$; so (1.10) is not satisfied at all if b is in the center. If b is not in the center, then b has infinitely many distinct conjugates, so (1.10) is false for infinitely many values of x.

Thus we can choose x (in infinitely many ways) so that all the elements of (1) are distinct, and none is the identity. If, for such an x, we let D'' be the set union of D' and x and bx, then (1) is the set of all differences $d_1d_2^{-1}$, for $d_1, d_2 \in D''$, $d_1 \neq d_2$. Hence D'' is a partial difference set, and $b = d_1d_2^{-1}$ holds for a pair $d_1, d_2 \in D''$.

Now if $c \neq d_1^{-1}d_2$ for any $d_1, d_2 \in D''$, we can use a similar process to construct a partial difference set D''' in which $c = d_1^{-1}d_2$ holds for some pair $d_1, d_2 \in D'''$.

Thus we can construct a difference set D for the group B.

Condition (b) is necessary in any group B which contains a difference set D. For if $b^2 = 1$, $b \neq 1$, then $b = d_1d_2^{-1}$ for a unique pair $d_1, d_2 \in D$; thus $b = b^{-1} = d_2d_1^{-1}$, so $d_1 = d_2$ and $b = 1$, a contradiction.

3. **Not-abelian free groups.** We now show that the not-abelian free group G with n generators ($n \geqq 2$) satisfies the conditions (a), (b), (c) of the preceding section.

Suppose $x = g$, where g is a generator or the inverse of a generator, and $x^2 = c \neq 1$. If $y = h_1h_2 \cdots h_m$ is a reduced form for y, and $y^2 = c$, then if $m>1$, there must be a reduction in $h_1h_2 \cdots h_mh_1h_2 \cdots h_m$; in particular, $h_mh_1=1$. The reduction must lead to $y^2=h_1h_m=gg$, so $h_1=h_m=g$, which contradicts $h_mh_1=1$. So $m=1$, whence clearly $y=x$.

Now suppose $x=g_1g_2$ is a reduced form for x, where each g_i is a generator or the inverse of a generator, and $x^2=c\neq 1$. Then $c=g_1g_2g_1g_2$ and if this is not a reduced form for c, then $g_2g_1=1$ and $x=1$, a contradiction.

If $y=h_1h_2 \cdots h_m$ is a reduced form for y, and if $y^2=c$, then $h_1h_2 \cdots h_mh_1h_2 \cdots h_m=g_1g_2g_1g_2$; this must reduce to $h_1h_2h_{m-1}h_m =g_1g_2g_1g_2$, whence $h_1=h_{m-1}=g_1$ and $h_2=h_m=g_2$. If $m=2$ then it is clear that $y=x$. If $m>2$, then there was a reduction in the first expression for y^2, and in particular, $h_mh_1=1$; thus $g_2g_1=1$ and $x=1$, a contradiction.

Inductively, assume that if the equation $z^2=c$, for any $c\in G$, $c\neq 1$, has a solution x of length $<k$, then the solution is unique. Suppose $x=g_1g_2 \cdots g_k$ is a reduced form for x, and $x^2=c\neq 1$. Suppose $y=h_1h_2 \cdots h_m$, where $m\geqq k$, is a reduced form for y, and $y^2=c$. Then:

$$h_1h_2 \cdots h_mh_1h_2 \cdots h_m = g_1g_2 \cdots g_kg_1g_2 \cdots g_k. \tag{2}$$

In all cases, this implies $h_1=g_1$, $h_m=g_k$.

If the right side of (2) is a reduced form for c, and if $m=k$, then clearly $y=x$. If $m>k$ then there must be a reduction on the left side of (2), and in particular, $h_mh_1=1$. But this implies $g_kg_1=1$, contradicting the assumption that the right side of (2) is a reduced form for c. So in this case, $y=x$.

If the right side of (2) is not a reduced form for c, then there is a reduction on the right side of (2), so $g_kg_1=h_mh_1=1$. Let $x'=g_2 \cdots g_{k-1}$, $y'=h_2 \cdots h_{m-1}$. Equation (2) becomes $x'^2=y'^2$, where x' has length $k-2$. By the induction hypothesis this implies $x'=y'$, so $x=g_1x'g_k =h_1y'h_m=y$.

Thus (a) holds in G.

If b is any element of G, $b\neq 1$, then $b=g_1$, $b=g_1g_2$, or $b=g_1wg_2$, where each g_i is a generator or the inverse of a generator, and where b is in reduced form.

If $b=g_1$, then there is a generator g such that $g\neq g_1$, $g\neq g_1^{-1}$. All the elements $g^{-k}bg^k$, as k ranges over the integers, are distinct and so b has infinitely many distinct conjugates.

If $b=g_1g_2$ or $b=g_1wg_2$, and if $g_1=g_2$ or $g_1=g_2^{-1}$, then there is a generator g such that $g\neq g_1$, $g\neq g_2$, and hence all the elements $g^{-k}bg^k$, as k ranges over the integers, are distinct; so b has infinitely many distinct conjugates. If $g_1\neq g_2$, $g_1\neq g_2^{-1}$, then all the elements $g_2^{-k}bg_2^k$, as

k ranges over the positive integers, are distinct, so b has infinitely many distinct conjugates.

Thus (c) holds in G; it is well known that G satisfies (b).

Bibliography

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. vol. 78 (1955) pp. 464–481.

2. M. Hall, *Cyclic projective planes*, Duke Math. J. vol. 14 (1947) pp. 1079–1090.

The University of Wisconsin

MAXIMAL SUBALGEBRAS OF GROUP-ALGEBRAS

JOHN WERMER

A closed subalgebra of a Banach algebra is called *maximal* if it is not contained in any larger proper closed subalgebra. Let G be a discrete abelian topological group and L its group-algebra, i.e. L is the Banach algebra of functions f on G with $\sum_{\lambda\in G} |f(\lambda)| < \infty$ and multiplication defined as convolution. What are the maximal subalgebras of L? The complete answer is not known even when G is the group of integers.

Here we assume that G is ordered. Let G^+ be the semi-group of non-negative elements of G and L^+ the subset of L consisting of functions which vanish outside of G^+. Then L^+ is a proper closed subalgebra of L.

Theorem 1.[1] *L^+ is a maximal subalgebra of L if and only if the ordering of G is archimedean.*

Proof. Suppose the ordering is non-archimedean. Then we can find a, b in G^+ with $na<b$ for $n=1, 2, \cdots$. Consider the set G_1 of all elements of G of the form $g^+ + n(-a)$, where $n=0, 1, 2, \cdots$ and g^+ is in G^+. Clearly G_1 is a semi-group containing G^+ and also $-a$ is in G_1 and $-b$ is not in G_1. Let L_1 be the closed subalgebra of L consisting of all functions vanishing outside G_1. Then L_1 lies properly between L^+ and L, whence L^+ is not maximal.

Suppose now that the ordering of G is archimedean. Let $\mathfrak{A}'$ be a proper closed subalgebra of L with L^+ included in $\mathfrak{A}'$. We shall show $\mathfrak{A}'=L^+$.

Let E_λ be the function in L with $E_\lambda(g)=0$, $g\neq\lambda$, $E_\lambda(\lambda)=1$. Then

Received by the editors December 27, 1954.

[1] A proof of this theorem has also been found by I. M. Singer. See the note below.