COMBINATORICA 1 (3) (1981) 243—256

ON THE FULL AUTOMORPHISM GROUP OF A GRAPH

by

C. D. GODSIL

Institut für Mathematik und Angewandte Geometrie
Mountanuniversität Leoben, Austria

Received 17 April 1980

While it is easy to characterize the graphs on which a given transitive permutation group G acts, it is very difficult to characterize the graphs X with $\mathrm{Aut}(X)=G$. We prove here that for the certain transitive permutation groups a simple necessary condition is also sufficient. As a corollary we find that, when G is a p-group with no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$, almost all Cayley graphs of G have automorphism group isomorphic to G.

1. Introduction

Let G be a finite permutation group acting faithfully and transitively on the set $I_n=\{1, \ldots, n\}$. In this paper we study the problem of characterizing the graphs and digraphs with automorphism group isomorphic, as permutation group, to G.

The first step is to characterize those digraphs on which G acts vertex-transitively. Let G_i denote the subgroup of G formed by those elements which fix i. We will see that there is a natural correspondence between the digraphs with vertex set I_n on which G acts vertex-transitively and subsets C of G such that $C=G_1CG_1$.

Given such a subset C of G we will find that any automorphism of G which fixes G_1 and C as sets induces an automorphism of the digraph $X=X(G, C)$ corresponding to C. Denote this group of automorphisms by $\mathrm{Aut}(G, C)$. In Section 2 of this paper we find that $\mathrm{Aut}(G, C)$ can be viewed as a subgroup of $\mathrm{Aut}(X)$ and we show that a necessary condition for the digraph $X(G, C)$ to have automorphism group isomorphic to G is that $G_1=\mathrm{Aut}(G, C)$ (see Corollary 2.3 and the remarks which follow it).

We are immediately faced with the problem of deciding when this necessary condition is also sufficient. Our main result (Corollary 3.9) is that this condition is both necessary and sufficient whenever G is a p-group with no homomorphism onto the abstract group $\mathbf{Z}_p$ wr $\mathbf{Z}_p$. We also obtain necessary and sufficient conditions for the occurence of the dihedral groups of order 2^k, and of certain Frobenius groups, as the full automorphism groups of vertex-transitive graphs and digraphs.

1.1. Terminology. This is generally standard. Most of the group theory we use can be found in [9], [10] or [12]. All groups considered are finite. We always denote

AMS subject classification (1980): 05 C 25; 05 B 25

the identity element of a group by e. If G is a permutation group then Aut (G) denotes the automorphism group of the abstract group G. If H is a subgroup or normal subgroup of G we write $H \leqq G$ or $H \trianglelefteq G$ respectively. If $S \subseteq G$ then $N_G(S)$, the normalizer of S in G, is the subgroup $\{g \in G | g^{-1}Sg = S\}$. We use $\langle S \rangle$ to represent the subgroup of G generated by the elements of S. Finally the letter p with always denote a prime number and G with always be a faithful transitive permutation group acting on the set I_n.

2. The necessary condition

In this section we characterize the digraphs X on which a given transitive group G acts and then establish a necessary condition for Aut (X) to be isomorphic to G.

The first task is easy since Sabidussi has already characterized the connected graphs on which G acts (in Theorem 2 of [13]) and his arguments require only minor changes to apply in our situation.

If G is a subset of G such that $C = G_1 C G_1$ then we define $X = X(G, C)$ to be the digraph with vertex set I_n and arc set

$$E(X) = \{(1g, 1cg) | c \in C, g \in G\}.$$

It is an immediate consequence of the definitions that G acts transitively by right multiplication on X.

On the other hand, suppose X is a digraph with vertex set I_n on which G acts transitively. If we define C to be the set of elements g in G such that $(1, 1g)$ is an arc of X then it is an routine task to verify that $C = G_1 C G_1$ and $X = (G, C)$.

Thus we have our required characterization. It is worth noting that $X(G, C)$ will be a graph if and only $c^{-1} \in C$ whenever $c \in C$ and that X has no loops if and only if $G_1 \cap C = \emptyset$. Since $C = G_1 C G_1$ is an union of cosets of G_1 the latter holds if and only if $G_1 \subsetneqq C$.

From the above discussion we see that if $X = X(G, C)$ then $G \leqq \text{Aut}(X)$. We now address ourselves to the task of establishing a necessary condition for G to coincide with Aut (X).

Henceforth C will denote a subset of G such that $C = G_1 C G_1$ and $G_1 \cap C = \emptyset$. If $S \subseteq G$ and $\varphi \in \text{Aut}(G)$ then S^φ is the set $\{g^\varphi | g \in S\}$. In the introduction we defined Aut (G, C) as

$$\{\varphi \in \text{Aut}(G) | G_1^\varphi = G_1, C^\varphi = C\}.$$

The next result shows that if $X = X(G, C)$ we can identify Aut (G, C) with a subgroup of Aut (X).

2.1. Lemma. *Let $X = X(G, C)$ and $A = \text{Aut}(X)$. Then $N_A(G) \cap A_1 \cong \text{Aut}(G, \mathscr{C})$.*

Proof. Set $\Gamma = \text{Aut}(G, C)$. Suppose $x, y \in G$ and $(1)x = (1)y$. Then $xy^{-1} = h \in G_1$. If $\varphi \in \Gamma$ we have

$$(1) \qquad (1)x^\varphi = (1)(hy)^\varphi = (1)h^\varphi y^\varphi.$$

Since $h\in G_1$ and $\varphi\in\Gamma$, $h^\varphi\in G_1$. Hence if $(1)x=(1)y$ then $(1)x^\varphi=(1)y^\varphi$. Accordingly the map $\bar{\varphi}$ defined by setting

$$((1)x)\bar{\varphi} = (1)x^\varphi \quad (x\in G)$$

is a well-defined permutation of $I_n=V(X)$.

Our next task is to show that $\bar{\varphi}\in A$. Assume $x, y\in G$ such that $(1)x$ and $(1)y$ are adjacent. Then we must have $xy^{-1}=c\in\mathscr{C}$. Arguing as in (1) we conclude that $(1)x^\varphi=(1)c^\varphi y^\varphi$ which implies, since $c\in\mathscr{C}$ and $\varphi\in\Gamma$, that $(1)x^\varphi$ and $(1)y^\varphi$ are adjacent. Consequently $\bar{\varphi}\in A$.

We now aim to show that the map $\varphi\to\bar{\varphi}$ is an isomorphism from Γ into A. If $\varphi, \psi\in\Gamma$ and $x\in G$ then

$$(1)x^{\varphi\psi} = (1)(x^\varphi)\bar{\psi} = (1)x\bar{\varphi}\bar{\psi}$$

and so our map is at least a homomorphism.

Assume φ lies in the kernel of this homomorphism. Let x and y be arbitrary elements of G. Then

$$(1)y = (1)y\bar{\varphi} = (1)y^\varphi$$

and so $y^\varphi y^{-1}=k\in G_1$. Further

$$\begin{aligned}(1)xy = (1)xy\bar{\varphi} = (1)x^\varphi y^\varphi &= (1)x\bar{\varphi}y^\varphi\\ &= (1)xy^\varphi\\ &= (1)xky\end{aligned}$$

and therefore $(1)x=(1)xk$. As our choice of x in G was arbitrary, it follows that k fixes each vertex in X. This implies that $k=e$. Consequently $y=y^\varphi$ and so, since our choice of y in G was arbitrary, we conclude that φ is the identity element of Γ.

Accordingly the map $\varphi\to\bar{\varphi}$ is an isomorphism of Γ into A_1. It only remains for us to show that the image of Γ is $N_A(G)\cap A_1$. Now we have, for $h\in G_1$ and $\varphi\in\Gamma$,

$$(1) = (1)h^\varphi = (1)h = (1)h\bar{\varphi} = (1)\bar{\varphi}$$

and so our isomorphism maps Γ onto a subgroup of A_1. Hence it will suffice to show that if $\varphi\in\Gamma$ then $\bar{\varphi}\in N_A(G)$.

Assume $x, y\in G$ and $\varphi\in\Gamma$. Let $i=(1)x$. We have

$$\begin{aligned}(i)\bar{\varphi}^{-1}y\bar{\varphi} = (1)x\bar{\varphi}^{-1}y\bar{\varphi} &= (1)x^{\varphi^{-1}}y\bar{\varphi}\\ &= (1)(xy^\varphi)^{\varphi^{-1}}y\bar{\varphi}\end{aligned} \tag{2}$$

Since $xy^\varphi\in G$,

$$(1)(xy^\varphi)^{\varphi^{-1}} = (1)xy^\varphi\bar{\varphi}^{-1},$$

whence (2) yields

$$(i)\bar{\varphi}^{-1}y\bar{\varphi} = (1)xy^\varphi = (i)y^\varphi. \tag{3}$$

Our choice of x in G was arbitrary, so we conclude that $\bar{\varphi}^{-1}y\bar{\varphi}=y\varphi$. As $\varphi\in\mathrm{Aut}\,(G)$, $y^\varphi\in G$, and therefore $\bar{\varphi}\in N_A(G)$ as required. ∎

From (3) in the above proof it follows that $\mathrm{Aut}\,(G,\mathscr{C})$ is isomorphic to $N_A(G)\cap A_1$ not only as an abstract group, but also when considered as a group

of operators on G. In view of this we will identify $\mathrm{Aut}(G, \mathscr{C})$ with $N_A(G) \cap A_1$. Thus elements of $\mathrm{Aut}(G, \mathscr{C})$ act on G by conjugation. We now derive further information from Lemma 2.1.

2.2. Lemma. *Let* $X = X(G, C)$, $\Gamma = \mathrm{Aut}(G, C)$ *and* $A = \mathrm{Aut}(X)$. *Then*

(a) $G_1 \trianglelefteq \Gamma$,

(b) $N_A(G) = \Gamma G$ *and*

(c) $\Gamma / G_1 \cong N_A(G)/G$

Proof. Clearly $G \leqq N_A(G)$. Therefore we have

$$G_1 = G \cap A_1 \leqq N_A(G) \cap A_1 = \Gamma$$

and so $G_1 \leqq \Gamma$. If $\varphi \in \Gamma$ then, by definition of $\mathrm{Aut}(G, C)$, $G_1^{\varphi} = G$. Hence $G_1 \trianglelefteq \Gamma$ and thus (a) is proved.

Since G acts transitively on $V(X)$, $A = A_1 G$. As $G \leqq N_A(G)$ we find that

$$N_A(G) = N_A(G) \cap A_1 G = \big(N_A(G) \cap A_1\big) G,$$

which yields (b). It also follows that

$$\frac{N_A(G)}{G} = \frac{\Gamma G}{G} \cong \frac{\Gamma}{\Gamma \cap G}.$$

as claimed in (c). ∎

2.3. Corollary. *We use the notation of Lemma 2.2. We then have:*

(a) $N_A(G) = G$ *if and only if* $\Gamma = G_1$.

(b) *If G is a p-group, then G is a Sylow p-subgroup of A if and only if G_1 is a Sylow p-subgroup of Γ.*

Proof. We note that (a) is an immediate consequence of Lemma 2.2 (c). We prove (b).

Suppose G is a Sylow p-subgroup of A. Then $N_A(G)/G$ has order coprime to p and so by Lemma 2.2 (c), the same is true of Γ/G_1. Since G_1 is a p-group it follows that it is a Sylow p-subgroup of Γ.

Assume conversely that G is a p-group and that G_1 is a Sylow p-subgroup of Γ. Then, as before, $N_A(G)/G$ has order coprime to p, since Γ/G_1 does. If G is not a Sylow p-subgroup of A, it is a maximal subgroup of some p-subgroup P of A. Now $G \trianglelefteq P$ and therefore $P \leqq N_A(G)$. Thus $N_A(G)/G$ has a non-trivial p-subgroup P/G, which is a contradiction. Accordingly G must be a Sylow p-subgroup of A. ∎

It follows from Corollary 2.3 (a) that if $\mathrm{Aut}(X) = G$ then $\mathrm{Aut}(G, C) = G_1$. Thus we have established the necessary condition given in the introduction. In the case that G acts regularly on I_n this necessary condition seems to have been used first by Frucht (Theorem 2.4 in [7]). It also occurs as Theorem 1 in Watkins [15].

3. p-groups

In this section we establish the existence of a class of p-groups G for which the condition $\mathrm{Aut}(G, C) = G_1$ is necessary and sufficient for us to have $\mathrm{Aut}\big(X(G, C)\big) = G$.

3.1. Definitions. The *Frattini subgroup* $\Phi(P)$ of the group P is defined to be the intersection of the maximal subgroups of P. Hence $\Phi(P)$ is a characteristic subgroup of P. If P is a finite p-group then the commutator subgroup P' of P lies in $\Phi(P)$.

A group B is said to be *p-nilpotent* if it has a normal subgroup M with order coprime to p such that B/M is a p-group. M is called a *normal p-complement* of B, since if Q is a Sylow p-subgroup of B then $B=QM$ and $Q\cap M=\langle e\rangle$.

The following group theoretic result is quite non-trivial.

3.2. Lemma. (J. Tate [14].) *Suppose H is a normal subgroup of K and P is a Sylow p-subgroup of K. If $H\cap P\leqq\Phi(P)$ then H is nilpotent.*

Lemma 3.2 is also proved in [10] (as IV. § 4.7 Satz). We will use 3.2 in conjunction with the next result.

3.3. Lemma. *Assume G is a finite p-group and let $X=X(G, C)$. If G is a Sylow p-subgroup of $A=\mathrm{Aut}(X)$ then any p-nilpotent subgroup of A normalized by G is contained in G.*

Proof. Let B be a p-nilpotent subgroup of A normalized by G. Let M be a normal p-complement of B. Since $|M|$ and $|B:M|$ are coprime, M is a characteristic subgroup of B.

As M is a characteristic subgroup of B and $B\trianglelefteq BG$ it follows that $M\trianglelefteq BG$. Let $D=BG$. Since G acts transitively on $V(X)$, $D=D_1G$. Hence

$$D = D_1 G = MD_1 G$$

and therefore

$$|D:G| = |D_1 : D_1\cap G| = |MD_1 : MD_1\cap G|. \tag{1}$$

Now G is a Sylow p-subgroup of A, so it is certainly a Sylow p-subgroup of D. This implies that $|D:D_1|$ is coprime to p. Consequently $D_1\cap G$ is a Sylow p-subgroup of D_1 and $MD_1\cap G$ is a Sylow p-subgroup of MD_1. (Note that since $M\trianglelefteq D$, MD_1 is in fact a subgroup and not subset of D.)

As $|M|$ is coprime to p the Sylow p-subgroups of D_1 and MD_1 have the same order. Consequently it follows from (1) that $|D_1|=|MD_1|$ and so $M\leqq D_1$. Therefore if $h\in M$ then $(1)h=(1)$ and if $g\in G$ then $(1)h^g=(1)$, since $M^g=M$. Hence

$$(1)g^{-1}h = (1)g^{-1}hg\cdot g^{-1} = (1)g^{-1}.$$

However our choice of g in G was arbitrary and so we conclude that $h=e$, which implies in turn that $M=\langle e\rangle$.

If $M=\langle e\rangle$ then B is a p-group and so some conjugate of B lies in the Sylow p-subgroup G. Since $B\trianglelefteq D$ we find then that $B\leqq G$, as claimed. ∎

Our next result is of independent interest since it asserts that under certain conditions some automorphisms of $X=X(G, \mathscr{C})$ must lie in G. We need one preliminary:

3.4. Definition. If $H\leqq K$ then

$$\mathrm{Core}_K(H) = \cap\{H^x | x\in K\}.$$

Thus $\mathrm{Core}_K(H)$ is the largest normal subgroup of K contained in H.

If, as we are assuming, G acts transitively on I_n then there is a $1-1$ correspondence between subgroups of G containing G_1 and block systems for G in its action on I_n. In fact, a subset S of I_n which contains 1 is a block for G if and only if $S=(1)Q$ for some subgroup Q of G such that $G_1 \leqq Q$. It is easy to show that x in G fixes each block in the set $\{(1)Qg | g \in G\}$ if and only if $x \in \mathrm{Core}_G(Q)$.

3.5. Lemma. *Let G be a finite group. Let $X=X(G, \mathscr{C})$, $A=\mathrm{Aut}(X)$ and assume that G is a Sylow p-subgroup of A. Assume further that $Q \leqq G$ such that $G_1 \leqq Q$ and $\mathrm{Core}_G(Q) \leqq \Phi(G)$.*

Then an element x of A fixes each subset $(1)Qg$ $(g \in G)$ of $V(X)$ if and only if if lies in $\mathrm{Core}_G(Q)$.

Proof. As noted above the subsets $(1)Qg$ $(g \in G)$ form a complete block system for G in its action on X and the subgroup of G fixing each of these blocks is $C=\mathrm{Core}_G(Q)$.

Assume x is as given in the statement of the theorem. Then the subsets $(1)Qg$ $(g \in G)$ form a complete block system for $B=\langle G, x\rangle$. Let F be the subgroup of B fixing each of these blocks. Then $F \trianglelefteq B$ and it is also clear that $F \cap G \leqq C$, whence we conclude that $F \cap G \leqq \Phi(G)$.

It follows immediately from Lemma 3.2 that F is p-nilpotent. By Lemma 3.3 we then conclude that $F \leqq G$. As $F \cap G \leqq C$ we thus find finally that $F \leqq C = \mathrm{Core}_G(Q)$ as required. ∎

3.6. Notation. We use $\mathbf{Z}_p$ wr $\mathbf{Z}_p$ to denote the *wreath product* of $\mathbf{Z}_p$ by $\mathbf{Z}_p$. (Here, $\mathbf{Z}_p$ is the cyclic group of prime order p.) This group is isomorphic to a Sylow p-subgroup of the symmetric group on p^2 elements. For more information on this group, see I. § 15 of [10].

3.7. Theorem. (Yoshida [17]: Thm. 4.2.]) *Suppose that G is a Sylow p-subgroup of the group A and that G admits no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$. Then $G \cap A' = G \cap N_A(G)'$.*

3.8. Theorem. *Let G be a finite p-group, $X=X(G, \mathscr{C})$ and $A=\mathrm{Aut}(X)$. Assume $\mathrm{Aut}(G, \mathscr{C})=G_1$ and let Q be a subgroup of G such that*

(a) $G_1 \leqq Q$,
(b) $(1)Q$ *is a block for* A,
(c) $C=\mathrm{Core}_G(Q) \leqq \Phi(G)$,
(d) G/C *admits no homomorphism onto* $\mathbf{Z}_p$ wr $\mathbf{Z}_p$.

Then $A=G$.

Proof. Since G is a finite p-group and $\mathrm{Aut}(G, \mathscr{C})=G_1$ it follows from 2.4 that G is a Sylow p-subgroup of A and that $N_A(G)=G$.

As $(1)Q$ is a block for A, the sets $(1)Qg$ $(g \in G)$ form a complete block system for A. Let Γ be the subgroup of A fixing each of these blocks. By Theorem 3.6, $F=C$.

It is easily verified that

$$N_{A/C}(G/C) = G/C.$$

and consequently we may apply Theorem 3.7 to conclude that

$$G/C \cap (A/C)' \leqq (G/C)'.$$

Therefore, by I. § 8.4 of [10], we have

$$G/C \cap A'C/C \leqq G'C/C,$$

whence $G \cap A'C \leqq G'C$. As G is a p-group $G' \leqq \Phi(G)$. By hypothesis $C \leqq \Phi(G)$ and so $G'C \leqq \Phi(G)$. Hence

$$G \cap A' \leqq G \cap A'C \leqq \Phi(G).$$

Accordingly A' is p-nilpotent, by Lemma 3.2, and so $A' \leqq G$, by Lemma 3.3. But if $A' \leqq G$ then $G \trianglelefteq A$. As $G = N_A(G)$ it follows that we must have $G = A$. ∎

Since the statement of Theorem 3.8 is somewhat complicated we restate two special cases of it.

3.9. Corollary. *Let G be a finite p-group, $X = X(G, \mathscr{C})$ and $A = \mathrm{Aut}(X)$. Assume* $\mathrm{Aut}(G, \mathscr{C}) = G_1$. *If*

(a) *G admits no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$, or*

(b) *$G_1 \leqq \Phi(G)$ and $(1)\Phi(G)$ is a block for A,*

then $A = G$.

Proof. Since we are assuming G acts faithfully on I_n, $\mathrm{Core}_G(G_1) = \langle e \rangle$. Accordingly if we take $Q = G_1$ in Theorem 3.8 then (a) follows at once.

If $G \leqq \Phi(G)$ then we take $Q = \Phi(G)$ in Theorem 3.8. Since $G' \leqq \Phi(G)$, $G/\Phi(G)$ is abelian and so certainly admits no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$. Hence (b) follows. ∎

It is not difficult to show that if $X = X(G, \mathscr{C})$ has more than two vertices then, in order for us to have $\mathrm{Aut}(X) = G$, it is necessary that both X and its complement be connected. Since we have not explicitly assumed this in Theorem 3.8, it must follow from our hypotheses. It is, in fact, possible to show that if G is a finite p-group and X is not connected then $\mathrm{Aut}(G, \mathscr{C})$ contains p-elements which do not belong to G_1. We will not prove this here, since we make no further use of the claim.

We also point out that the class of finite p-groups with no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$ is quite large. It contains in particular all groups of exponent p and all groups with nilpotency class less than p.

The remainder of this section is devoted to an application of Corollary 3.9 (a).

3.10. Definitions. If H is a group then H^* denotes the set $H \setminus \{e\}$. We use $\pi(G)$ to denote the proportion of subsets $\mathscr{C}$ of G^* such that $\mathrm{Aut}(G, \mathscr{C})_1 = G_1$ and let $\pi^{\pm}(G)$ denote the corresponding proportion of inverse-closed subsets of G. (A subset S of G is *inverse closed* if, whenever $g \in S$, $g^{-1} \in S$.)

We say that a group H is *generalized dicyclic* if it is non-abelian and has an abelian subgroup A and an element x in $H \setminus A$ such that $|H:A| = 2$, $|x| = 4$ and $a^x = a^{-1}$ for each element a in A.

Generalized dicyclic groups are relevant here because they admit an automorphism which fixes or inverts each element (see [15]). Hence if G is generalized dicyclic with an inverse-closed subset $\mathscr{C}$ then $\mathrm{Aut}(G, \mathscr{C})$ strictly contains G_1. It is

easy to see that the same statement holds if G is abelian with exponent greater than two.

3.11. Theorem. *Assume that G is a finite p-group with no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$ and which acts regularly on I_n. Then the proportion of Cayley digraphs $X=X(G,\mathscr{C})$ such that $\mathrm{Aut}(X)=G$ is $\pi(G)$. The corresponding proportion of Cayley graphs is $\pi^{\pm}(G)$. As $|G|$ increases, $\pi(G)$ tends to 1, and if G is neither generalized dicyclic nor abelian with exponent greater than two, then $\pi(G^{\pm})$ also tends to 1.*

Given Corollary 3.9 (a), we see that this theorem is an immediate consequence of the following result.

3.12. Lemma. (L. Babai [1].) *Let G be a group with $g+1$ elements. Then*

$$\log_2(1-\pi(G)) < (\log_2 g)^2 - g/4$$

and if G is not generalized dicyclic, or abelian with exponent greater than two

$$\log_2(1-\pi^{\pm}(G)) < (\log_2 g)^2 - g/32.$$

Proof (of 3.12). Suppose $0 \leqq \varrho \leqq 1$ and that exactly $\varrho 2^g$ of the subsets of G^* are fixed by some non-trivial automorphism of G. Hence there are at least $\varrho 2^g$ ordered pairs (α, S) where $S \subseteq G^*$ and α is a non-trivial automorphism of G which fixes S.

We now obtain an upper bound for the number of such ordered pairs. If α in $\mathrm{Aut}(G)$ fixes f elements of G^* then it has at most $(g-f)/2$ orbits on the remaining elements. Thus it has at most

$$f+(g-f)/2 = (g+f)/2$$

orbits on G^*. The set of elements of G fixed by α form a subgroup of G and this subgroup is proper if $\alpha \neq e$. Consequently a non-identity element of $\mathrm{Aut}(G)$ has less than $3g/4$ orbits on G^*, since it fixes less than $g/2$ elements of G^*.

If $|\mathrm{Aut}(G)| = a+1$, there are therefore less than $a2^{3g/4}$ ordered pairs of the type described. Accordingly

$$\tau 2^g < a 2^{3g/4},$$

whence $\tau < a2^{-g/4}$. A routine argument (as in the proof of Theorem 2 in [1]) yields the conclusion that $\log_2 a \leqq (\log_2 g)^2$. Substituting this in our bound for g yields the first part of the lemma.

The second part of the lemma follows, using similar arguments, from Lemma 3 in [1]. (This lemma asserts that if G admits an automorphism φ which fixes or inverts more $7(g+1)/8$ of the elements of G then G is either abelian with exponent greater than two or generalized dicyclic.) We omit the details. ∎

The fact that Lemma 3.12 is implicit in the results in [1] was pointed out to the author by L. Babai. The bounds given for $\pi(G)$ and $\pi^{\pm}(G)$ should not be taken too seriously since they are far from best possible. The point is that they yield the conclusion that if $|G|$ is large then for a typical subset $\mathscr{C}$ of G, $\mathrm{Aut}(G,\mathscr{C}) = \langle e \rangle$, and that subject to the exceptions listed, this is still true if we require additionally that $\mathscr{C}$ be inverse-closed.

Cayley digraphs $X=X(G,\mathscr{C})$ such that $\mathrm{Aut}(X)=G$ are known as *digraphical regular representations* of G. The analogous term for Cayley graphs is *graphical*

regular representations. These expressions are usually abbreviated to *DRR* and *GRR* respectively. The problem of determining which finite groups admit a GRR was first raised in [15]. This problem, and the corresponding one for DRR's, has now been settled — see [8] for GRR's and [2] for DRR's.

Theorem 3.11 provides some evidence for the following conjecture.

3.13. Conjecture. *Suppose G acts regularly on I_n. Then, for almost all subsets $\mathscr{C}$ of G^*, $X(G, \mathscr{C})$ is a* DRR. *If G is not generalized dicyclic or abelian with exponent greater than two then, for almost all inverse-closed subsets $\mathscr{C}$ of G^*, $X(G, \mathscr{C})$ is a* GRR.

We do not conjecture that the condition that $\mathrm{Aut}(G, \mathscr{C})$ be trivial is sufficient, when G is regular, to ensure that $\mathrm{Aut}(X) = G$. For suppose G is isomorphic as an abstract group to the symmetric group S_m on m letters. If $m \geqq 4$ then (by [16]) G has a GRR $X(G, \mathscr{C})$. Hence $|\mathrm{Aut}(G, \mathscr{C})| = 1$. Now G can be viewed in the obvious way as a subgroup of S_{m+1}. It is not difficult to show that $|\mathrm{Aut}(S_{m+1}, \mathscr{C})| = 1$. However $X' = X(S_{m+1}, \mathscr{C})$ is not connected, since $\langle b \rangle = G \neq S_{m+1}$ and accordingly $\mathrm{Aut}(X') \neq S_{m+1}$.

4. Abelian p-groups

We will now study the automorphism group of $X(G, \mathscr{C})$ when G is an abelian p-group. It is well known that an abelian group which acts faithfully and transitively on a set must act regularly on that set. Therefore in this section our digraphs $X(G, \mathscr{C})$ will always be Cayley digraphs and G_1 will be the identity group.

4.1. Preliminaries. A group F is called a *Frobenius group* if it acts faithfully and transitively, but not regularly, on a set (I_n, say) and the only element of F fixing two or more points is the identity. It is known that, together with the identity, the set of elements of F with no fixed points form a regular normal subgroup of G. This subgroup is called the *kernel* of F and is always a nilpotent group.

If X is a digraph and $A = \mathrm{Aut}(X)$ is a Frobenius group with kernel K then X is a Cayley digraph with respect to K, since K acts regularly on $V(X)$. Suppose $X = X(K, \mathscr{C})$. If $a \in A_1$ and $k \in K$ then $k^a \in K$, since $K \trianglelefteq A$. Hence if $k^a = k$ we have

$$1ka = 1ak = 1k$$

and so α fixes $1k$. Since A is a Frobenius group this implies that $a = e$. From Lemma 2.1 we see that $A_1 = \mathrm{Aut}(K, \mathscr{C})$ and so we conclude that no non-identity element of K is fixed by any automorphism in $\mathrm{Aut}(K, \mathscr{C})$. We describe this by saying that $\mathrm{Aut}(K, \mathscr{C})$ acts *fixed-point freely* on K.

Conversely, suppose $\mathrm{Aut}(K, \mathscr{C})$ acts fixed-point freely on K and that $X = X(K, \mathscr{C})$, $A = \mathrm{Aut}(X)$. Then it is routine to show that $N_A(K)$ is a Frobenius group with kernel K.

A graph X such that $A = \mathrm{Aut}(X)$ is a Frobenius group is sometimes referred to as a *graphical Frobenius representation* of A. We abbreviate this term to GFR. These graphs have been studied in [6]. Our next result characterizes those GFR's X such that the kernel of $\mathrm{Aut}(X)$ is an abelian p-group.

4.2. Theorem. *Assume G is an abelian p-group and let $\mathscr{C}$ be a non-empty subset of G such that $\Gamma = \mathrm{Aut}(G, \mathscr{C})$ acts fixed-point freely on G. Let X be the digraph $X(G, \mathscr{C})$.*

Then either $C=G^*$ (and so X is the complete graph on $n=|G|$ vertices) or $A=\mathrm{Aut}(X)$ is a Frobenius group with kernel G and A_1 equals Γ.

Proof. We will show first that under the hypotheses of the theorem G is a Sylow p-subgroup of A. By Lemma 2.3 (b) it will suffice to prove that $|\Gamma|$ is coprime to p, since in this case $G_1=\langle e\rangle$ is a Sylow p-subgroup of Γ.

Assume $\varphi\in\Gamma$ such that $|\varphi|=p$. Then the orbits of the elements of G under the action of φ have length 1 or p. Since the orbits of φ partition the elements of the p-group G and since φ fixes the identity of G, we conclude that Γ fixes at least p elements of G. This is a contradiction to our assumption that Γ acts fixed-point freely on G. We conclude therefore that Γ contains no elements of order p and accordingly that $|\Gamma|$ is coprime to p.

We prove next that if $k\in G^*$ then $C_A(k)=G$. Assume $k\in G^*$. Since G is abelian, $G\leqq C_A(k)$. Suppose $x\in C_A(k)\cap N_A(G)$. Because G acts transitively on $V(X)$, there must be an element h in G such that $1x=1h$. Thus $y=xh^{-1}\in A_1$. Since both x and h lie in $N_A(G)$ we therefore find that $y\in N_A(G)\cap A_1=\Gamma$. Now Γ acts fixed-point freely on G but $y\in C_A(k)$ and therefore fixes k. It follows that $y=e$ and hence that $x=h\in G$.

Consequently $C_A(k)\cap N_A(G)=G$. Setting $C=C_A(k)$, we therefore find that $N_A(G)=G$. Thus G is a self-normalizing abelian p-subgroup of C and so, by a well-known theorem of Burnside (see IV. § 2.6 of [10]), it follows that C is p-nilpotent. As $G\leqq C$, C is normalized by G and so, by Lemma 3.3, $C\leqq G$. Thus $C=G$ as required.

We have now established that G is an abelian Sylow p-subgroup of A and that if $k\in G^*$ then $C_A(k)=G$. By Lemma 2.5 of [3] this implies that either A is 2-transitive or $G\trianglelefteq A$. If A is 2-transitive then X must be a complete graph or a graph with no edges. The second possibility is excluded since b is non-empty, by hypothesis.

Thus we may assume $G\trianglelefteq A$. It follows from Lemma 2.2 (b) that $A=G\Gamma$. From our remarks preceding the statement of the theorem we conclude that A is a Frobenius group with kernel G and with A_1 isomorphic to Γ. ∎

If G is an abelian group with exponent greater than two then the map $\tau\colon g\to g^{-1}$ $(g\in G)$ is an automorphism of G. If $A=X(G,\mathscr{C})$ is a Cayley graph for G then $\mathscr{C}=\mathscr{C}^{-1}$ and so $\tau\in\mathrm{Aut}(G,\mathscr{C})$. Hence $|\mathrm{Aut}(X)_1|>1$ and therefore $\mathrm{Aut}(X)\neq G$. It is natural to ask under what conditions is it true that $\mathrm{Aut}(X)_1=\langle\tau\rangle$.

If $p>2$ and G is an abelian p-group then τ acts fixed-point freely on G. In this case our question is then answered by Theorem 4.2. However if $p=2$ then G contains elements of order two and these are fixed by τ. Thus Theorem 4.2 cannot be applied. If G is cyclic we can remedy this situation by using the next theorem.

4.3. Theorem. *Assume G is dihedral of order 2^k and let $X=X(G,C)$, $A=\mathrm{Aut}(X)$. If $\mathrm{Aut}(G,C)=G_1$ then either $A=G$ or $n=3$, $|V(X)|=4$ and $A=S_4$.*

(Note that since G is transitive and faithful we have either $n=2^{k-1}$ or $n=2^k$.)

4.4. Corollary. *Suppose that G is either an abelian p-group with p odd or a cyclic 2-group with order at least four. Let τ denote the automorphism of G mapping each element onto its inverse. Let $\mathscr{C}$ be a subset of G such that $\mathrm{Aut}(G,\mathscr{C})=\langle\tau\rangle$ and set $X=X(G,\mathscr{C})$, $A=\mathrm{Aut}(X)$. Then $A_1=\langle\tau\rangle$ and $G\trianglelefteq A$.*

Proof (of 4.4). If G is an abelian p-group (p odd) then the result is an immediate

consequence of Theorem 4.2 and our remarks following its proof. We assume then that G is a cyclic 2-group and that $|G| \geqq 4$.

By Lemma 2.1, $N_A(G) \cap A_1 = \langle \tau \rangle$. Clearly $H = \langle G, \tau \rangle$ is dihedral and since $|G| \geqq 4$, G is the unique cyclic subgroup of index two in H. Accordingly we have $N_A(H) \leqq N_A(G)$. Now $A = A_1 G$, so

$$\begin{aligned} N_A(G) &= N_A(G) \cap A_1 G \\ &= G(N_A(G) \cap A_1) \qquad (1) \\ &= G\langle \tau \rangle, \end{aligned}$$

where (1) follows since $G \leqq N_A(G)$. Thus $N_A(G) = H$, whence we have $N_A(H) = H$. Since H acts transitively on X we must also have $X = X(H, D)$ for some suitable subset $D = H_1 D H_1$ of H and as $N_A(H) = H$, $\mathrm{Aut}(H, D) = H_1$. Hence we may apply Theorem 4.3 to conclude that $A = H$. ∎

Note that, under the hypotheses of Corollary 4.4, we have $\mathscr{C} = \mathscr{C}^\tau = \mathscr{C}^{-1}$ and so $X(G, \mathscr{C})$ is actually a graph. If G is abelian with exponent greater than two then any Cayley graph of G will admit the inverting automorphism τ, i.e. we always have $\langle \tau \rangle \leqq A_1$. The problem of determining which abelian groups with exponent greater than two have a Cayley graph with $A_1 = \langle \tau \rangle$ has been settled by W. Imrich and M. E. Watkins [11].

Corollary 4.4 can also be used to derive results analogous to Theorem 3.11. Thus it can be shown that if G is an abelian p-group (p odd) or a cyclic 2-group then, for "almost all" inverse-closed subsets $\mathscr{C}$ of G^*, the vertex-stabilizer of $\mathrm{Aut}(X(G, \mathscr{C}))$ is $\langle \tau \rangle$.

Our proof of Theorem 4.3 depends on the following special case of the Brauer—Suzuki—Wall theorem [5], as formulated in [4].

4.5. Theorem. *Assume B is a finite group with a dihedral subgroup H of order at least four. Let T be a cyclic subgroup of index two in H. If*

(a) *all involutions in B are conjugate and*

(b) *for all elements a in $B \setminus H$, $T^a \cap T = \langle e \rangle$*

then $B = \mathrm{PSL}(2, q)$ for some prime power q.

4.6. Proof of 4.3. We have $X = X(G, \mathscr{C})$ and $A = \mathrm{Aut}(X)$, where G is dihedral of order 2^k and $\mathrm{Aut}(G, \mathscr{C}) = G_1$. We aim to show that either $A = G$ or $|G| = 8$, $|V(X)| = 4$ and $A = S_4$.

If $|G| = 2$ then the result is trivial. If $|G| = 4$ then there is no subset $\mathscr{C}$ of G^* such that $\mathrm{Aut}(G, \mathscr{C}) = G_1 (= \langle e \rangle)$. Hence the theorem holds vacuously. We assume henceforth that $|G| \geqq 8$.

By Corollary 2.3 (a) we see that $G = N_A(G)$ and by Corollary 2.3 (b) we see that G is a Sylow 2-subgroup of A. Let B denote the subgroup of A generated by its elements of odd order. Since B is generated by a set of elements which is closed under conjugation it is easy to prove that $B \trianglelefteq A$. We let S denote the unique cyclic subgroup of index two in G and set $H = B \cap G$, $T = B \cap S$.

We assume further that our theorem fails for the given group G and subset $\mathscr{C}$. We will now proceed, in a number of steps, to derive the contradictory conclusion that G is not a Sylow 2-subgroup of A.

(a) *We claim that $|A : B| = |G : H|$ and H is a Sylow 2-subgroup of B.*

We have noted already that $B \trianglelefteq A$. For any odd prime p the Sylow p-subgroups of A must all lie in B. Hence the corresponding Sylow subgroups of A/B are trivial and so A/B is a 2-group. Since $B \trianglelefteq A$, $H = B \cap G$ is a Sylow 2-subgroup of B. As $|A:B|$ is a power of two and G is a Sylow 2-subgroup of A, we conclude that $|A:B| = |G:H|$.

(b) $|A:B| = 2$ *and* H *is dihedral with order at least four.*

As $B \trianglelefteq A$, $H = B \cup G$ is a normal subgroup of G. Since G is dihedral it follows that either H is cyclic or $|G:H| = 2$ and H is dihedral. If the Sylow 2-subgroups of B are cyclic then it is 2-nilpotent. (This follows, for example, from exercise 21 on page 32 of [10] or from Theorem 7.6.1 of [9].) It follows readily that A is 2-nilpotent, whence we conclude using Lemma 3.3 that $A = G$. Thus we may assume that H is dihedral and $|G:H| = 2$. Since $|A:B| = |G:H|$ and $|G| \geqq 8$, both our claims hold.

(c) *All involutions in* B *are conjugate.*

We first show that B has no subgroups of index two. For suppose $F \leqq B$ and $|B:F| = 2$. Then $F \trianglelefteq B$ and the natural homomorphism from B onto B/F maps each element of B with odd order onto the identity. Hence F contains all elements of odd order in B. By definition, these elements generate B and so we have $F = B$.

Since B has dihedral Sylow 2-subgroups and no subgroups of index two it follows now from Proposition 12.3 of [12] that all involutions in B are conjugate.

(d) *For all elements* a *in* H/B, $T^a \cap T = \langle e \rangle$.

We prove that $S^a \cap S = \langle e \rangle$ for all elements a in $A \setminus G$, from which it follows that $S^a \cap S = \langle e \rangle$ for all elements a in $B \setminus G = B \setminus H$.

Since S is cyclic it contains a unique involution t. As $S \trianglelefteq G$, $\langle t \rangle \trianglelefteq G$ and so $G \leqq C_A(t)$ (since if $t^g \in \langle t \rangle$ for g in G, $t^g = t$). By 7.7.3 of [9], $C_A(t)$ is 2-nilpotent. By our Lemma 3.3 then, $C_A(t) \leqq G$, implying that $C_A(t) = G$. Suppose now that $a \in A$ and $S^a \cap S = \langle e \rangle$. Then $t \in S^a \cap S$, so $t \in S^a$ and therefore $t = t^a$, since the latter element is the only involution in S^a. Hence $a \in C_A(t) = G$.

(e) $B = \mathrm{PSL}(2, q)$ *where* $q = p^r$ *for some odd prime* p *and positive integer* r.

From (b), (c) and (d) we see that the hypotheses of Theorem 4.5 are satisfied by B, H and T. Hence $B \cong \mathrm{PSL}(2, q)$ for some prime power $q = p^r$. If $p = 2$ then $\mathrm{PSL}(2, q) = \mathrm{SL}(2, q)$ has elementary abelian Sylow 2-subgroups of order q (see II. § 8.10 of [10]). Hence either $q = 4$ or q is odd. As $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5)$ we may assume the latter.

(f) *The orbits of* B *have length* $q+1$ *and either* $q = 1$ *or* q *is prime.*

We have $|B| = q(q^2-1)/2$ where q is odd. Since $B \trianglelefteq A$ and A acts transitively on $V(X)$, the orbits of B all have the same length, d say (see II. § 1.5 of [10]). Thus d divides $|V(X)|$ and so $d = 2^m$ for some integer m. Now d divides $|B|$ and q is odd, so d divides $(q^2-1)/2$. Furthermore the greatest common divisor of $q-1$ and $q+1$ is two so d divides $q-1$ or $q+1$. In either case $d \leqq q+1$.

Since d is the length of an orbit of B, we see that B must have a subgroup of index d. From II. § 8.28 of [10]), we find that this means that either $q = d = 2$ or $q+1 \leqq d$. The former is impossible, since q is odd. We therefore conclude that $d = q+1$.

Consequently $2^m = q+1$ where q is a prime power and so it follows from Lemma 19.3 of [12] that either $q = 1$ or q is prime.

(g) B *acts on* $V(X)$ *with two orbits of length* $q+1$.

From our arguments in (f) we see that $q+1$ is the largest power of two dividing $|B|$. Hence $|H| = q+1$. Therefore $|G| \leqq 2(q+1)$ and since $|V(X)| \leqq |G|$ and the orbits of

B have length $q+1$ it follows that either B has two orbits of length $q+1$ or else it is transitive and $|V(X)|=q+1$.

Suppose that B acts transitively on $V(X)$. Since q is a prime and q divides $|B|$, B contains elements of order q. As B acts faithfully on $V(X)$ these elements act non-trivially on $V(X)$. Since we have $|V(X)|=q+1$ it follows that B acts 2-transitively on $V(X)$.

This implies that either X is complete or it has no arcs. Accordingly $A=\mathrm{Aut}\,(X)$ is the symmetric group on $l=2^n$ letters. Now G is dihedral so the vertex-stabilizer of its representation on $V(X)$ has order at most two. Thus $|V(X)|=|G|$ or $|G|/2$ and so $l=2^n$ or 2^{n-1}. Since $|G|\geqq 8$ we thus have $l\geqq 4$. If $l>4$ then it is easy to check that G is not a Sylow 2-subgroup of S_l. If $l=4$ then $A=S_4$ and so if $|G|=4$ then $G\leqq A$. Consequently $|G|=8$.

(h) *G is not a Sylow 2-subgroup of A.*

By (g) we know that B has two orbits on $V(X)$, each of length $q+1$. We denote these orbits by Y_1 and Y_2. Let Q be a fixed Sylow q-subgroup of A. Since q is odd, Q is a subgroup of B. As $|V(X)|=2(q+1)$ we see that Q has either one or two non-trivial orbits, each of length q.

Since $B\trianglelefteq A$, the orbits of B are blocks for A. Suppose Q has just one trivial orbit. Then, by II. § 1.13 (c) of [10], $N_A(Q)$ acts transitively on the trivial orbits of Q. It therefore has two orbits, one of length q and the other of length $q+2$. The orbit of length q is an orbit of Q and so lies in Y_1 or Y_2. Hence $N_A(Q)$ fixes the blocks Y_1 and Y_2, which implies that its orbits have length at most $q+1$. We conclude that Q must have two non-trivial orbits.

Thus Q has two orbits of length q and two fixed points. We denote these fixed points by 1 and 2. We may assume without loss that $1\in Y_1$, $2\in Y_2$. Note that since B acts transitively on Y_1 and Y_2 and Q acts transitively on $Y_i\setminus\{i\}$ $(i=1, 2)$, it follows that B acts 2-transitively on Y_i $(i=1, 2)$. Also since $N_A(Q)$ acts transitively on the fixed points of Q, A contains an automorphism α which interchanges 1 and 2.

Since B acts 2-transitively on Y_1, the digraph induced by the vertices in Y_1 is complete or empty (i.e. without arcs). As X and its complement have the same automorphism group we may assume without loss that Y_1 and Y_2 are both empty. Suppose there is a vertex in $Y_2\setminus\{2\}$ such that 1 dominates x i.e. such that $(1, x)$ is an arc in X.

Then $(1, y)$ is an arc in X, for each $y\in xQ$. Therefore 1 dominates at least q vertices in Y_2. As B acts transitively on Y_1 it follows that each vertex in Y_1 dominates at least q vertices in Y_2. Further, the automorphism α interchanges 1 and 2 and so it interchanges the blocks Y_1 and Y_2. Consequently each vertex in Y_2 dominates at least q vertices in Y_1.

Suppose 1 does not dominate 2. Then since α interchanges 1 and 2, 1 is not dominated by 2. By our preceding arguments it follows that 1 simultaneously dominates and is dominated by the q vertices in $Y_2\setminus\{2\}$. Accordingly it is now routine to verify that X is isomorphic to the graph $K_{m,m}$ with a 1-factor removed, where $m=q+1$.

If 1 does dominate 2 then it dominates each of the vertices in Y_2 and it follows that $X\cong K_{m,m}$ $(m=q+1)$.

If there is no vertex in $Y_2 \setminus \{2\}$ which is dominated by 1 then, given the existence of α, it is routine to show that either X is empty or isomorphic to $q+1$ copies of K_2.

Thus X is one of four families of graphs. If $q>1$ we claim, but leave the details to the reader, that the Sylow 2-subgroup of Aut (X) is larger than G. If $q=1$ then it is easy to verify that Aut (X) is isomorphic to S_4 or D_8 (the dihedral group of order eight). Since we are assuming that the theorem does not hold for G, we conclude that G is not a Sylow 2-subgroup of $A=\text{Aut}\,(X)$. ∎

Note that D_8 is isomorphic to $\mathbf{Z}_2$ wr $\mathbf{Z}_2$ and that any dihedral 2-group with order at least eight admits a homomorphism onto D_8. Thus Theorem 4.3 shows that our hypothesis in Theorem 3.8 and Corollary 3.9, that G admits no homomorphism onto $\mathbf{Z}_p$ wr $\mathbf{Z}_p$, is not always necessary. This suggests that it might be true that if G is a sufficiently large finite p-group and $\mathscr{C} \subseteq G^*$ such that Aut $(G, \mathscr{C}) = G_1$ then $X(G, \mathscr{C})$ has automorphism group to G. In our opinion this is not the case, but we have no idea how to find the required counterexamples.

References

[1] L. Babai, On a conjecture of M. E. Watkins on graphical regular representations of groups, *Compositio Math.*, **37** (1978), 291—296.

[2] L. Babai, Finite digraphs with given regular automorphism groups, *Periodica Math. Hung.* to appear.

[3] H. Bender, Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt, *J. Algebra*, **17** (1971), 527—554.

[4] H. Bender, The Brauer—Suzuki—Wall theorem, *Ill. J. Math.*, **18** (1974), 229—235.

[5] R. Brauer, M. Suzuki and G. E. Wall, A characterization of the two-dimensional unimodular projective groups over finite fields, *Ill. J. Math.*, **2** (1958), 718—745.

[6] J. K. Doyle, Graphical Frobenius representations of abstract groups, *submitted.*

[7] R. Frucht, A one-regular graph of degree three, *Canadian J. Math.*, **4** (1952), 240—247.

[8] C. D. Godsil, GRR's for non-solvable groups, *Proceedings of the conference on algebraic methods in combinatorics*, Szeged (Hungary) 1978, Bolyai—North-Holland, 221—239.

[9] D. Gorenstein, *Finite groups*, Harper & Row, New York, (1968).

[10] B. Huppert, *Endliche Gruppen I*, Springer Verlag, New York, (1967).

[11] W. Imrich and M. E. Watkins, On automorphism groups of Cayley Graphs, *Per. Math. Hung.*, **7** (1976), 243—258.

[12] D. S. Passman, *Permutation Groups*, W. A. Benjamin, New York, (1968).

[13] G. Sabidussi, Vertex-transitive graphs, *Monat. Math.*, **68** (1964), 426—438.

[14] J. Tate, Nilpotent quotient groups, *Topology*, **3** (1964), 109—111.

[15] M. E. Watkins, On the action of non-abelian groups on graphs, *J. Combinatorial Theory*, **11** (1971), 95—104.

[16] M. E. Watkins, Graphical regular representations of alternating, symmetric and miscellaneous small groups, *Aequat. Math.* **11** (1974), 40—50.

[17] T. Yoshida, Character theoretic transfer, *J. Algebra*, **52** (1978), 1—38.