Faithful Representations of $p$ Groups at Characteristic $p$, II

G. J. Janusz

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Communicated by W. Feit

Received June 22, 1971

INTRODUCTION

In this paper we continue to study representations of $p$ groups over fields of characteristic $p$ as begun in [7]. Different questions will be considered here and the results in [7] are needed only in Section 2.

This work is motivated in part by two results in the literature. The first is the theorem of D. G. Higman [4] which says that a $p$ group must be cyclic if it has only a finite number of indecomposable representations at characteristic $p$. The second is the determination of all the indecomposable representations of the noncyclic group of order four by Bashev [1], Conlon [2], and also Heller and Reiner [5]. Of particular interest is the result that there exist just two inequivalent representations of this group in any odd dimension greater than or equal to three over any field of characteristic two. This result is also proved by Johnson [9]. The main result of section one shows these groups are distinguished among abelian groups by these properties. In particular, we show that a noncyclic abelian $p$ group of order not equal to four has infinitely many indecomposable representations in each dimension $d$ if $d \geq 2$ and if the ground field is infinite. Moreover, if $p(d - 1)$ is greater than or equal to the exponent of $G$ there exist infinitely many indecomposable representations in dimension $d$ which represent the group faithfully.

In Section 2 we consider a non-abelian $p$ group $G$ and an infinite field $K$. We show there exist infinitely many inequivalent indecomposable $K(G)$-modules $M$ with the property that $M$ represents $G$ faithfully but no proper submodule or proper homomorphic image of $M$ is faithful for $G$. This may be somewhat unexpected in view of the results in [7] which show that such modules are isomorphic to principal left ideals in $K(G)$. It would be possible to use modules constructed in this section along with the sort of construction appearing in section one to show that $G$ has infinitely many indecomposable representations in infinitely many different dimensions.
This sort of result is far less satisfying than that obtained in the abelian case in section one and so we shall not carry out this project here. We turn our attention, instead, to the possibility that $G$ has only a finite number of faithful indecomposable representations in dimension $d$ for some particular $d$. If $G$ is abelian, then it is cyclic or has order four. In case $G$ is non-abelian our results are incomplete. Such groups exist, however. In section four the dihedral group and generalized quaternion group of order $2^{n+2}$ are shown to have exactly two inequivalent faithful representations in dimension $1 + 2^n$ over any field $K$ of characteristic 2. We do require $GF(4) \subseteq K$ in the case of the quaternion group of order eight.

We suspect that groups with this property are very scarce. To support this feeling the main result in section three says (among other things) that for a given prime $p$ and a given dimension $d$, there are only finitely many $p$ groups which have only a finite number of fundamental representations in dimension $d$ over an infinite field. Of course, there are infinitely many $p$-groups having fundamental representations in dimension $d$; for example, the $d \times d$ unit triangular group over the field of $p^m$ elements gives an infinite family of such groups as $m$ takes on different values.

At the end of section three we classify all $p$ groups which have only a finite number of faithful representations of degree three over an infinite field of characteristic $p$.

**Notation.** $G$ always denotes a finite $p$ group and $K$ an infinite field of characteristic $p$. Some results will be valid even if $K$ is finite.

### 1. ABELIAN GROUPS

We state the main results of this section at once.

**Theorem 1.** Let $G$ be an abelian $p$ group which is neither cyclic nor of order four and let $K$ be an infinite field of characteristic $p$. If $G$ has exponent $p^a$ and $d$ is any integer $\geq 1 + p^{a-1}$, then $G$ has infinitely many inequivalent, indecomposable, faithful $K$ representations of dimension $d$.

**Corollary.** If $G$ and $K$ are as in the theorem and if $d$ is any integer $\geq 2$ then $G$ has infinitely many inequivalent, indecomposable $K$ representations of dimension $d$.

The general idea of the proof is to construct a $K$-algebra $A$ and imbed $G$ into the units of $A$. Then we construct $A$-modules upon which $G$ acts by way of the imbedding into $A$. An essential step is the following.
Lemma 1.1. Let $A$ be a $K$-algebra and $T$ a homomorphism of $G$ into the units of $A$ such that $T(G)$ generates $A$ as a $K$-algebra. Let $M$ and $N$ be two $A$-modules which give rise to equivalent representations of $G$ when $G$ acts upon $M$ and $N$ by way of $T(G)$. Then $M$ and $N$ are isomorphic as $A$-modules.

Proof. There is assumed to be a $K$-linear transformation $P$ from $M$ onto $N$ such that $T(g) Pm = PT(g)m$ for all $m$ in $M$ and $g$ in $G$. Since the elements $T(g)$ generate $A$, it follows that $P$ is an $A$-isomorphism.

We begin to discuss various constructions. Let $e, f$ be integers $\geq 2$ and let $A_{e,f}$ (or just $A$) denote the algebra $K[ X, Y ]$ on two commuting generators $X$ and $Y$ which satisfy

$$xe = 0 \neq x^{-1}, \quad Yf = 0 \neq Y^{-1}.$$ 

Lemma 1.2. Let $d$ be any integer in the interval $e + f - 2 < d < ef - 2$. For each element $\lambda \neq 0$ in $K$, there is an ideal $I_{\lambda}$ such that

(i) $X^{e-1}, Y^{f-1}$ are not in $I_{\lambda}$,

(ii) $K$-dimension of $A/I_{\lambda}$ equals $d$,

(iii) $A/I_{\lambda} \cong A/I_{\gamma}$ if and only if $\lambda = \gamma$,

(iv) $A/I_{\lambda}$ is an indecomposable $A$-module.

Proof. We begin with two sequences of integers

\begin{align*}
1 & \leq a_1 < a_2 < \cdots < a_t < e - 1, \\
1 & \leq b_t < b_{t-1} < \cdots < b_1 < f - 1.
\end{align*}  

(1.3)

Let $\lambda$ be any nonzero element in $K$ and $I_{\lambda}$ the ideal generated by the elements

$$x(\lambda) = X^{a_1-1}Y^{f-1} + \lambda X^{e-1}Y^{b_t-1}, \quad X^{a_i}Y^{b_i}$$

for all $i = 1, 2, \ldots, t$. The dimension of $I_{\lambda}$ and $A/I_{\lambda}$ can be easily computed by thinking geometrically. Identify the element $X^aY^b$ with the point $(a, b)$ in the plane. Draw a "staircase" path in the first quadrant starting at $(0, f)$ ending at $(e, 0)$ and having corners at $(a_1, f)$, $(a_1, b_1)$, $(a_2, b_1)$, $(a_2, b_2)$, $\ldots$, $(a_{i+1}, b_i)$, $(a_{i+1}, b_{i+1})$, $\ldots$, $(a_t, b_t)$, $(e, b_t)$. The dimension of $A/I_{\lambda}$ is one less than the number of lattice points in the first quadrant (including the $x$ and $y$ axes) which are below the stairs. It is easily checked that for any given $d$ on the interval $e + f - 2 \leq d \leq ef - 2$ there is at least one "staircase" (and hence one pair of sequences (1.3)) with exactly $d + 1$ lattice points below it. Furthermore, our choice of $I_{\lambda}$ makes it clear that (i) holds. Since $A$ is a $K$-algebra with a unique maximal ideal, it follows $A/I_{\lambda}$ is indecomposable. Now suppose $A/I_{\lambda} \cong A/I_{\gamma}$. Then there is a unit $u$ in $A$ such that $I_{\lambda} = I_{\gamma} u$. (This follows because $A$ is a self-injective ring.)
Thus \( I_\lambda = I_\nu \). Since the distinct elements \( X^i Y^j \) give a basis for \( A \), it follows that \( \lambda = \nu \).

**Lemma 1.3.** Assume \( e, f \geq 3 \). For any integer \( d > ef - 2 \) there exist infinitely many nonisomorphic \( A \)-modules \( M_\lambda \) of dimension \( d \) such that neither \( X^{e-1} \) nor \( Y^{f-1} \) annihilates \( M_\lambda \).

*Proof.* We first construct an \( A \)-module \( V^{(k)} \) with basis \( v_1, \ldots, v_k, u_0, u_1, \ldots, u_k \) as a \( K \) vector space. The action of \( A \) is determined by the rules

\[
Xv_i = u_{i-1}, \quad Yv_i = u_i, \quad 1 \leq i \leq k,
\]

and

\[
Xu_i = Yu_i = 0 \quad \text{for all} \quad j.
\]

Next select a sequence (1.3) with \( t \geq 2 \). This is possible since we have assumed \( e, f \geq 3 \). For any \( \lambda \neq 0 \) in \( K \) select an ideal \( I_\lambda \) corresponding to the selected sequence. We can select sequences (1.3) with \( t \geq 2 \) such that \( A/I_\lambda \) has dimension \( d_0 \) for any \( d_0 \) on the interval \( e + f - 1 < d_0 \leq ef - 3 \).

We now construct the module \( M_\lambda \) having \( V^{(k)} \) as submodule and having one additional generator \( x_{k+1} \) subject to the conditions.

1. \( Av_{k+1} \cong A/I_\lambda \) by the mapping \( a + I_\lambda \rightarrow av_{k+1} \),
2. \( u_k = X^{e-1} Y^{f-1} v_{k+1} \).

Thus \( M_\lambda \) is a homomorphic image of \( V^{(k)} \oplus A/I_\lambda \) with kernel of dimension one. It follows the dimension of \( M_\lambda \) is \( 2k + d_0 \). The appropriate choice of sequence allows at least one odd and one even possibility for \( d_0 \). Thus for some \( k \) we can arrange the dimension of \( M_\lambda \) to be any preassigned number \( \geq e + f + 1 \).

It is also clear that \( X^{e-1} \) and \( Y^{f-1} \) are outside the annihilator of \( M_\lambda \) because they do not annihilate \( A/I_\lambda \).

Now suppose there is an \( A \)-isomorphism from \( M_\lambda \) onto \( M_\nu \) (both constructed from the same sequence (1.3) and with the same \( k \)). We notice the element \( x(\lambda) \) (defined in the proof of Lemma 1.2) belongs to the ideal generated by \( X^2 \) and \( Y^2 \). Thus

\[
x(\lambda) V^{(k)} = 0.
\]

Also \( x(\lambda) \) belongs to \( I_\lambda \); so \( x(\lambda) Av_{k+1} = 0 \). This forces \( x(\lambda) M_\lambda = (0) \) and because of the isomorphism we also have \( x(\lambda) M_\nu = (0) \). This forces \( x(\lambda) A/I_\nu = (0) \); so \( x(\lambda) \) belongs to \( I_\nu \). It follows that \( \lambda = \nu \).

Finally, we show \( M_\lambda \) is indecomposable. Suppose on the contrary that
$M_\lambda = W_1 \oplus W_2$ for nonzero submodules $W_1$, $W_2$. Then the socle of $M_\lambda$, denoted by $S(M_\lambda)$, must also be a direct sum

$$S(M_\lambda) = S(W_1) \oplus S(W_2).$$

The next step is to see that $S(M_\lambda) = S(XM_\lambda)$. We see this as follows. Clearly, $u_0, \ldots, u_{k-1}$ are in $XV^{(k)} \subseteq XM_\lambda$. Further, the defining relation (ii) above shows $u_k$ is in $X\Lambda v_{k+1}$. It remains to see that $S(X\Lambda v_{k+1}) \subseteq XM_\lambda$. It takes just a brief calculation to check that $S(A/I_\lambda)$ is generated by

$$x^{a_1-1}y^{b_1-1}, x^{a_2-1}y^{b_2-1}, x^{a_3-1}y^{b_3-1},$$

modulo $I_\lambda$. Clearly, all these elements belong to $X\Lambda$ except when $a_1 = 1$. In this case, $y^{b_1-1}$ belongs to the socle; however, the element $x(\lambda)$ belongs to $I_\lambda$. So $y^{b_1-1}$ belongs to the same coset of $I_\lambda$ as $x^{a_1-1}y^{b_1-1}$ which is in $X \Lambda$. These facts prove $S(XM_\lambda) = S(M_\lambda)$. It must follow that

$$S(XW_i) = S(W_i) \quad \text{for} \quad i = 1, 2. \quad (1.4)$$

We shall derive a contradiction from this equation. Let the generators of $W_1$ be expressed as linear combinations of the $v_j$ plus elements in $XM_\lambda + YM_\lambda$. Let $q$ be the largest index for which $v_q$ appears with nonzero coefficient in an expression for some generator of $W_1$. Just suppose $q \leq k$. Then $XW_1$ contains only linear combinations of $u_0, \ldots, u_{q-1}$, whereas $YW_1$ contains an element involving $u_q$ with nonzero coefficient. It follows then that $S(XW_1) \neq S(W_1)$, contrary to Eq. (1.4). The alternative is $q = k + 1$. Let $w$ in $W_1$ be a generator involving $v_{k+1}$ with nonzero coefficient. Since $x^{a}v_j = 0$ for $j \leq k$, we find

$$x^{a}Aw = x^{a}A\Lambda v_{k+1}.$$

If we apply the same argument to $W_2$, we obtain

$$x^{a}A\Lambda v_{k+1} \subseteq W_1 \cap W_2 = (0).$$

Since $I_\lambda$ is the annihilator of $v_{k+1}$, we have $X^a$ is in $I_\lambda$. By Lemma 1.2, part (i) we must have $a \leq 2$ which is against our hypothesis in this lemma.

**Corollary 1.4.** The algebra $A_{2,2}$ has indecomposable modules $V^{(k)}$ and $V_0^{(k)}$ with dimensions $2k + 1$ and $2k$, respectively.

**Proof.** In the case $e = f = 2$ the module $V^{(k)}$ constructed above and the quotient module $V_0^{(k)} = V^{(k)}/Ku_0$ have dimensions $2k + 1$ and $2k$, respectively. One proves that these are indecomposable in a manner similar to the case treated in Lemma 1.3. This method of proof uses the idea found in Curtis–Reiner [3].
We are ready to begin the proof of Theorem 1.

First express the group $G$ as a direct product

$$G = \langle x_1 \rangle \times \cdots \times \langle x_s \rangle,$$

where $x_i$ has order $p^{c_i}$ and

$$c_1 \geq c_2 \geq \cdots \geq c_s.$$

The assumptions in the theorem are that $s \geq 2$ and if $p = 2$ and $c_1 = 1$, then $s \geq 3$. Let $d$ be any integer $\geq 1 + p^{c_1-1}$. Suppose first that $d \leq p^{c_1}$.

Consider the $K$-algebra $A = K[X]$, where

$$X^d = 0 \neq X^{d-1}.$$  

The results in [7, Section 3] imply there exist infinitely many ways of imbedding $G$ into the units of $A$ in such a way that in each imbedding $x_1$ is mapped onto $1 + X$. Moreover, each imbedding gives rise to a representation of $G$ acting on $A$. Distinct imbeddings give rise to mutually inequivalent, faithful, indecomposable representations of $G$ in dimension $d$.

Next we take care of the interval

$$(p^{c_1} + p^{c_s})/p \leq d \leq p^{c_1+c_s} - 2.$$  

The construction of Lemma 1.2 will be used here. Select integers $e$ and $f$ which satisfy

$$1 + p^{c_1-1} \leq e \leq p^{c_1}, \quad 1 + p^{c_{s-1}} \leq f \leq p^{c_s},$$

and

$$e + f - 2 \leq d \leq ef - 2.$$  

There is a monomorphism $\alpha$ imbedding $G$ into the units of $A_{e,f}$ such that

(i) $\alpha(x_1) = 1 + X,$

(ii) $\alpha(x_i)$ is in $K[X]$ for $i < s,$

(iii) $\alpha(x_s) = 1 + Y.$ (1.5)

The image of $\alpha$ generates $A_{e,f}$ so by Lemma 1.1, nonisomorphic $A_{e,f}$ modules give rise to inequivalent representations of $G$.

The modules $A_{e,f}/I_{\lambda}$ constructed in Lemma 1.2 give infinitely many nonisomorphic representations of $G$ having dimension $d$. The next step is to show these are faithful representations of $G$. Suppose $g$ is in $G$ and $\alpha(g)$ acts trivially upon $A_{e,f}/I_{\lambda}$. Then $\alpha(g) - 1$ is in $I_{\lambda}$. We may write $g = xw^r$, where $x$ is in $\langle x_1, \ldots, x_{s-1} \rangle$. Let $\alpha(x) = 1 + WX$, $W \in K[X].$
Then \( \alpha(g) = (1 + XW)(1 + Y)^r \) and this is congruent to 1 modulo \( I_\lambda \).

When this product is expanded by the binomial theorem we find

\[
rY + \cdots + Y^r + XW(1 + Y)^r \text{ is in } I_\lambda.
\]

(1.6)

There is a basis for \( I_\lambda \) consisting of elements \( X^iY^j \) with \( i, j \neq 0 \) and one further element \( x(\lambda) \) defined in the proof of Lemma (1.2). The only way a power of \( Y \) appears with nonzero coefficient in some expression for an element of \( I_\lambda \) is for that power to be \( f - 1 \). It follows that \( r \geq f - 1 \) and

\[
rY + \cdots + Y^r \equiv \gamma Y^{f-1} \text{ modulo } I_\lambda
\]

for some \( \gamma \) in \( K \). Now (1.6) reads as

\[
\gamma Y^{f-1} + \gamma XW + \gamma XWY^{f-1} \text{ is in } I_\lambda.
\]

(1.7)

If \( \gamma = 0 \), then \( (1 + Y)^r = 1 \) in \( A_{e,f} \), so that \( \alpha(x^r) = 1 \) and \( x^r = 1 \) because \( \alpha \) is one-to-one. Then \( \alpha(x) \equiv 1 \) modulo \( I_\lambda \) forces \( \alpha(x) = 1 \) into \( K[X] \cap I_\lambda = (0) \). Thus \( x = 1 \) and so \( g = 1 \), as required.

If \( \gamma \neq 0 \), then (1.7) can be expressed in terms of basis elements of \( I_\lambda \) and the element \( x(\lambda) \) must appear with coefficient \( \gamma \lambda \). It follows that the element (1.7) contains a term \( X^{e-1}Y^{p^f-1} \) with coefficient \( \gamma \lambda \). Since \( W \) is in \( K[X] \), we must have \( h_s = f \) which is against (1.3). Thus \( A_{e,f}/I_\lambda \) is a faithful \( G \) module.

Next we turn to the case where \( d \) is greater than or equal to \( p^{\nu_1} + p^{\nu_s} - 1 \). We want to use Lemma (1.3), so we shall first require \( e, f \geq 3 \) in addition to the requirements already assumed in consideration of the previous case. So it will be necessary to have \( p^{\nu_1} > 2 \) here. The case \( p^{\nu_1} = 2 \) is treated below. We still assume an imbedding \( \alpha \) of \( G \) into the units of \( A_{e,f} \). Then the modules \( M_\lambda \) constructed in Lemma (1.3) can be arranged to have dimension \( d \) and we obtain infinitely many inequivalent indecomposable representations of \( G \) in this way. These are again faithful because the submodule \( A_{e,f}/I_\lambda \) is already faithful.

Now suppose \( p^{\nu_1} = 2 \). So \( G \) is elementary abelian and our assumption now is that \( s \geq 3 \) so \( |G| \geq 8 \). By Corollary (1.4), we know \( A_{2,2} \) has at least one indecomposable module \( V \) of dimension \( d \) for any \( d \geq 2 \) and the annihilator of \( V \) is the one-dimensional ideal \( K \cdot XY \). We imbed \( G \) into the units of \( A_{2,2} \) by a mapping \( \alpha \) in the following way. Let \( \gamma_1, \gamma_2, ..., \gamma_{s-1} \) be elements of \( K \) which are linearly independent over \( GF(2) \). We shall assume \( 1 = \gamma_1 \). Since \( s - 1 \geq 2 \), there exist infinitely many choices for \( \gamma_2, ..., \gamma_{s-1} \). Let \( \alpha(x_i) = 1 + \gamma_i X \) for \( i \leq s - 1 \) and \( \alpha(x_s) = 1 + Y \). This \( \alpha \) is a monomorphism and there exist infinitely many choices of \( \alpha \). Each \( \alpha \) gives an action of \( G \) on \( V \) and in fact gives a faithful indecomposable representation
of \( G \) acting on \( V \). If two imbeddings \( \alpha, \alpha' \) give equivalent representations, then there is a nonsingular linear transformation \( P \) of \( V \) onto \( V \) such that

\[
\alpha(g) P v = P \alpha'(g) v
\]

for all \( g \) in \( G \) and \( v \) in \( V \). If we take \( g = x_1, x_\ast \), we find \( P \) is an \( A_{2,2} \) homomorphism. Thus \( \alpha(g) - \alpha'(g) \) is in \( K \cdot XV \), the annihilator of \( V \). This forces \( \alpha(g) = \alpha'(g) \) for all \( g \) in \( G \). So we have covered all cases and the proof of Theorem 1 is complete.

**Proof of the corollary to Theorem 1.** Let \( d \) be any integer \( \geq 2 \) and \( G \) as described above. It is only necessary to be concerned with cases where \( d \leq p^{a-1} \). It is always possible to map \( G \) onto a group \( \tilde{G} \) of exponent \( p^a \), where \( 1 + p^{a-1} \leq d \leq p^a \). We may also arrange that \( G \) and \( \tilde{G} \) both have \( s \) cyclic direct factors. If \( s \geq 3 \) or if \( s = 2 \), but \( p^a \geq 4 \), then the theorem applies to give infinitely many inequivalent indecomposable representations of \( G \) (and so of \( \tilde{G} \)) having dimension \( d \). In case \( p^a = 2 \) and \( s = 2 \), then \( d = 2 \) and \( \tilde{G} \) has order 4. \( G \) is isomorphic to the group \( \langle 1 + X, 1 + Y \rangle \) in \( A_{2,2} \) and \( A_{2,2} \) has infinitely many nonisomorphic quotients \( A_{2,2}/I_4 \) of dimension two. Namely, take \( I_4 \) to be a principal ideal generated by \( X + \lambda Y \).

## 2. Non-Abelian Groups

One cannot hope to prove Theorem 1 for non-abelian groups. We will see in Section 4, e.g., that a group might have only a finite number of faithful indecomposable representations in a given dimension.

We shall take up a slightly different question. As before, \( K \) is assumed infinite.

**Definition.** A \( K(G) \)-module \( M \) is called minimal faithful if \( G \) acts faithfully on \( M \) but not on any proper submodule.

A \( K(G) \)-module \( M \) is called fundamental if \( M \) is minimal faithful and also \( G \) does not act faithfully on any proper homomorphic image of \( M \).

Minimal faithful modules have been studied in [7] and there we find the following result (for the case of infinite \( K \)).

**Proposition 2.1.** Let \( R \) denote the radical of \( K(G) \) and \( M \) a minimal faithful module. Let \( E \) denote the kernel of the representation of \( G \) on \( RM \). Then \( E \) is elementary abelian and \( M \) is a homomorphic image of \( K(G)/R(E)R \), where \( R(E) \) is the radical of \( K(E) \).

Conversely, if \( E \) is elementary abelian and a normal subgroup of \( G \), then \( K(G)/R(E)R \) is a minimal faithful module.
We now easily obtain the following corollary:

**Corollary 2.2.** Let $M$ be a fundamental module and $E$ the kernel of the representation of $G$ on $RM$. Then $M$ is isomorphic to $K(G)/L$, where $L$ is a left ideal containing $R(E)R$ and is maximal with respect to the property $K(G)/L$ affords a faithful representation of $G$.

This shows the dimensions of minimal faithful and fundamental modules are bounded and so they may be considered as "small". In spite of this, fundamental modules abound.

**Theorem 2.3.** A non-abelian $p$ group has infinitely many nonisomorphic fundamental modules over an infinite field.

*Proof.* We let $z$ be an element of order $p$ in the center of $G$. Then $R(z-1) = (z-1)R$ is an ideal of $K(G)$ and by Proposition 2.1 with $E = \langle z \rangle$ it follows that $K(G)/R(z-1)$ is minimal faithful. Our plan is to produce a family $\{L_\alpha\}$ of left ideals which contain $R(z-1)$ and with $K(G)/L_\alpha$ fundamental. The last step is to show these are mutually non-isomorphic.

Let $g_1, \ldots, g_s$ be a set of representatives of the cosets of $\langle z \rangle$ in $G$ and let

$$u = g_1 + \cdots + g_s.$$ 

Let $A$ denote the ring $K(G)/R(z-1)$ and for $x$ in $K(G)$ let $\bar{x}$ denote the corresponding element in $A$.

**Lemma 2.4.** The elements $z-1$ and $u$ are in the left and right socles of $A$. Every $K$-subspace of $K(z-1) + Ku$ is an ideal in $A$.

*Proof.* The radical of $A$ is $\bar{R}$ and the left or right socle of $A$ is the left or right annihilator of $\bar{R}$. Clearly, $z-1$ annihilates $\bar{R}$ on both sides. It takes some computation to prove the same for $u$. We shall make the computations in $K(G)$.

For each $g$ in $G$ we have equations of the sort

$$gg_i = g_i z^{a_i},$$

where $j$ and $a_i$ depend upon $i$ and $g$. It follows that

$$(g-1)u = \sum g_j z^{a_j} - \sum g_i = \sum g_j (z^{a_j} - 1).$$

If we expand $z^a - 1$ in a Taylor series in powers of $(z-1)$ and use the fact that $(z-1)^2$ is in $R(z-1)$, it follows

$$z^a - 1 = a(z-1) \text{ modulo } R(z-1).$$
The previous equation then simplifies to\[(g - 1)u = (z - 1) \sum a_jg_j \text{ modulo } R(z - 1).\]
The next step is to show \(\sum a_jg_j\) is in \(R\). We have observed the \(a_j\) depend upon \(g\). However, a change of representative from a coset will not change the corresponding \(\sum a_j\). It is necessary now to make a "good" choice of representatives.

Let \(p^t\) be the order of \(g\) modulo \(\langle z \rangle\) and let \[g^{pt} = z^r \quad \text{for some } r.\]

Let \(x_1, \ldots, x_k\) be representatives of the cosets of \(\langle g, z \rangle\) in \(G\). We may now select the representatives of the cosets of \(\langle z \rangle\) as \[g_{ij} = g^i x_j \quad 0 \leq i < p^t, \quad 1 \leq j \leq k.\]

Now we have
\[
g g_{i,i} = g_{i+1,i} \quad \text{if } i + 1 < p^t,
= g_{0,i} z^r \quad \text{if } i + 1 = p^t.
\]
Thus
\[
\sum a_j = \sum_{i=1}^k r = r[G : \langle g, z \rangle].
\]

If \(G = \langle g, z \rangle\), then \(G\) is abelian since \(z\) was central. We have assumed \(G\) to be non-abelian; so \(p\) divides \([G : \langle g, z \rangle]\) and thus \(\sum a_j = 0\) in \(K\). This allows us to write\[(g - 1)u = (z - 1) \sum a_jg_j = (z - 1) \sum a_j(g_j - 1) = 0 \text{ modulo } R(z - 1).\]

This holds for an arbitrary \(g\) in \(G\) and so \(Ru \subseteq R(z - 1)\). Thus \(\bar{u}\) is in the left socle of \(A\). By symmetry, we argue \(\bar{u}\) is also in the right socle.

The last statement in the lemma follows from the fact that every element of \(A\) is a scalar plus an element in \(\bar{R}\).

For any non-zero \(\lambda\) in \(K\) let \(v(\lambda)\) be the element \((z - 1) + \lambda u\). Let \(I_\lambda\) be the ideal \(Kv(\lambda) + R(z - 1)\).

**Lemma 2.5.** \(K(G)/I_\lambda\) is a faithful \(G\)-module.

**Proof.** If there is a nonidentity kernel of the action of \(G\) on \(K(G)/I_\lambda\), then there is a nonidentity element \(e\) in the center of \(G\) which acts trivially. For such an element we find\[(e - 1) K(G) = K(G)(e - 1) \subseteq I_\lambda.\]
However, $c - 1$ is not in $R(z - 1)$ because by Proposition 2.1 the module $K(G)/R(z - 1)$ is faithful for $G$. Thus there is a nonzero $\gamma$ in $K$ such that

$$c - 1 = \gamma\tau(\lambda) = \gamma(z - 1) + \gamma\lambda u \mod R(z - 1) \quad (2.6)$$

for some $\gamma$ in $K$.

Certainly, $R(z - 1) \subseteq K(G)(z - 1)$; so Eq. (2.6) is valid as a congruence modulo $K(G)(z - 1)$. Since $K(G)/K(G)(z - 1)$ is isomorphic to $K(G/\langle z \rangle)$ it follows that the coset representatives $\{g_i\}$ of $\langle z \rangle$ are linearly independent modulo $K(G)(z - 1)$. But the congruence (2.6) implies

$$c - 1 = \gamma\lambda \sum g_i \mod K(G)(z - 1).$$

If $\gamma \lambda \neq 0$, then the number of coset representatives on the left must be the same as the number on the right, i.e., 2. But then $[G: \langle z \rangle] = 2$ implies $|G| = 4$ which is against our assumption that $G$ is non-abelian. Hence $\gamma \lambda = 0$ and $\gamma = 0$ because $\lambda \neq 0$. But we have proved above that $\gamma \neq 0$ if $c \neq 1$, so the lemma follows.

This lemma allows the following key step in the proof of Theorem 2.3:

For each nonzero $\lambda$ in $K$, let $L_\lambda$ be a left ideal such that

(a) $I_\lambda \subseteq L_\lambda$,

(b) $K(G)/L_\lambda$ is a faithful $G$-module,

(c) $L_\lambda$ is maximal with respect to (a) and (b).

Since $I_\lambda = L_\lambda$ satisfies (a) and (b), such left ideals exist. By Corollary 2.2 we have at once that $K(G)/L_\lambda$ is a fundamental module.

**Lemma 2.7.** The two $K(G)$-modules $K(G)/L_\lambda$ and $K(G)/L_\gamma$ are isomorphic if and only if $\lambda = \gamma$.

**Proof.** Since $K(G)$ is a quasi-Frobenius algebra, the isomorphism of the two quotients implies there is a unit $w$ in $K(G)$ with $L_\lambda w = L_\gamma$. By construction, $I_\lambda \subseteq L_\lambda$ and Lemma 2.4 imply $I_\lambda$ is a two-sided ideal of $K(G)$. Thus $I_\lambda = I_\lambda w$. It follows that $L_\gamma$ contains $v(\lambda)$ and $v(\gamma)$ and so

$$(\lambda - \gamma)(z - 1) = \lambda v(\gamma) - \gamma v(\lambda)$$

is an element of $L_\gamma$. However, $z - 1$ cannot be in $L_\gamma$ because $K(G)/L_\gamma$ is faithful. Thus $\lambda = \gamma$.

Since $K$ is an infinite field, there exist infinitely many nonisomorphic fundamental modules $K(G)/L_\lambda$ which completes the proof of the theorem.
3. Groups in a Given Degree

In this section we consider the possibility that a $p$ group $G$ has only a finite number of faithful indecomposable representations in a particular dimension $d$. Of course, this is only of interest when the field $K$ is infinite. The result in section one shows this cannot happen for an abelian group $G$ unless $G$ is cyclic or has order four. It can happen for non-abelian $G$ and we shall give examples in section four. One expects this condition to be very restrictive and the feeling is supported by the difficulty in obtaining examples.

The examples given below show that certain groups have only a finite number of faithful indecomposable representations in a certain degree $d$ where it happens that $d$ is the smallest dimension in which any faithful representation could theoretically occur. In particular, the representations are fundamental. The lack of examples leads us to suspect that when a group $G$ has only a finite number of faithful indecomposable representations of degree $d$, then these representations are fundamental. At least it seems that $d$ should be "small" in some sense. Unfortunately, it is not possible at this time to make this idea precise.

The main theorem in this section shows that groups with the above property are scarce. More precisely, once $d$ and $p$ are given there can be only a finite number of $p$ groups $G$ with the property that $G$ has only a finite number of fundamental modules of dimension $d$ over the field $K$.

**Theorem 3.1.** Let $G$ be a non-abelian group and $K$ an infinite field of characteristic $p$. Suppose $G$ has only a finite number ($\neq 0$) of inequivalent fundamental modules over $K$ which have dimension $d$. Then

(i) the number of generators for $G$ is $\leq \frac{1}{2}(d + 1)(d - 2)$,
(ii) $|G| \leq f_p(d)$ for some function $f_p$ depending only on $p$.

The proof will be given in several steps. The first is a general property of fundamental modules.

**Step 1.** A fundamental module is isomorphic to a principal left ideal of $K(G)$.

**Proof.** If $M$ is a fundamental module, then such too is the contragradient module $M^\ast$. The dual of Corollary 2.2 implies that fundamental modules are isomorphic to left ideals and the corollary itself implies they have a single generator.

Now to fix the notation, let $K(G)m_1,...,K(G)m_s$ be a full set of non-isomorphic fundamental left ideals of dimension $d$. Suppose also that $R^N$ is the highest power of the radical of $K(G)$ which is nonzero. It is well
known that $R^N$ has dimension one and is contained in every nonzero left or right ideal of $K(G)$.

The main part of the proof will be to show $R^{N-1}$ is contained in $K(G)m_1K(G)$. After this, some dimension counting will finish the proof.

Take any element $w$ in $R^{N-1}$ with $w$ not in $R^N$. For an element $\lambda$ in $K$ let

$$M_\lambda = K(G)(m_1 + \lambda w).$$

Step 2. For infinitely many $\lambda$, $M_\lambda$ is fundamental of dimension $d$.

We shall prove $M_\lambda$ is faithful except for possibly a finite number of $\lambda$ and then show $M_\lambda$ is fundamental of dimension $d$, whenever it is faithful.

Suppose some nonidentity element acts trivially on $M_\lambda$. Then there is a nonidentity element $z$ in the center of $G$ which acts trivially upon $M_\lambda$. Thus $(z - 1)M_\lambda = (0)$. So, in particular,

$$(z - 1)m_1 = -\lambda(z - 1)w.$$  (3.2)

The module $K(G)m_1$ is faithful; so $(z - 1)K(G)m_1 \neq (0)$. Since $z$ is central, it follows that $(z - 1)m_1 \neq 0$. Thus in Eq. (3.2) we find the scalar $\lambda$ is uniquely determined by $(z - 1)m_1$ and $(z - 1)w$. Since there are only a finite number of possible $z$ in the center of $G$, there are only a finite number of $\lambda$ that can occur with $M_\lambda$ not faithful.

From now on, assume $M_\lambda$ is faithful and $\lambda \neq 0$.

The next objective is to compute the dimension of $M_\lambda$. We observe that $Rw \subseteq R^N \subseteq Rm_1$ since $R^N$ is in every nonzero left ideal. It follows then that

$R(m_1 + \lambda w) \subseteq Rm_1 + Rw \subseteq Rm_1$.

(3.3)

We shall prove that equality holds. The module $K(G)m_1$ must have dimension two and so the left annihilator $S$ of $w$ has codimension 2 in $K(G)$. Thus $R = Ku \oplus S$ (vector space direct sum) with $uw \neq 0$ and in fact $R^N = Kuw$. We now obtain

$$Rm_1 = Ku_m + Sm_1,$$

(3.4)

$$R(m_1 + \lambda w) = Ku(m_1 + \lambda w) + Sm_1.$$  (3.5)

If $Sm_1 \neq 0$, then $R^N \subseteq Sm_1$ and so $uw$ is in $Sm_1$. It follows that the vector spaces on the right side in (3.4) and (3.5) are identical; so equality holds in (3.3). If $Sm_1 = 0$, then $K(G)m_1$ is a homomorphic image of $K(G)/S$ which has dimension two. $K(G)m_1$ is faithful; so $G$ has a faithful two-dimensional representation. This forces $G$ to be abelian which is against our assumption in the theorem. Thus the unique maximal submodules of $M_\lambda$ and $K(G)m_1$ are the same and both must have the same dimension $d$.

It follows at once that $M_\lambda$ is minimal faithful because every proper submodule
of $M_\lambda$ is contained in $RM_\lambda$ which equals $Rm_1$. Since $K(G)m_1$ is minimal faithful, $Rm_1$ does not afford a faithful representation of $G$.

To see that no proper quotient of $M_\lambda$ is faithful, we first select $z \neq 1$ such that $(z - 1)K(G)m_1 \subseteq R^N$. Such a $z$ exists because $K(G)m_1/R^N$ is not faithful. Then it follows $(z - 1)K(G)w$ is also in $R^N$ because $w$ is in $R^{N-1}$. Thus $(z - 1)M_\lambda \subseteq R^N$. Any proper homomorphic image of $M_\lambda$ is also a homomorphic image of $M_\lambda/R^N$ which has $z$ in the kernel. Thus $M_\lambda$ is fundamental and step 2 is completed.

**Step 3.** $R^{N-1} \subseteq Rm_1 + m_1R + Rm_1R$.

The right side contains $R^N$; so we need only show $w$ is in the right side when $w$ is selected as above. The module $M_\lambda$ constructed above must be isomorphic to $K(G)m_i$ for some $i$ and since there are infinitely many $\lambda$ available we must have $M_\lambda$ isomorphic to $M_\gamma$ for some $\lambda \neq \gamma$ in $K$. Since isomorphisms between left ideals are carried out by right multiplication with units of $K(G)$, we may suppose there is a unit $u = 1 + s$, with $s$ in $R$, such that $(m_1 + \lambda w)u$ and $(m_1 + \gamma w)$ generate the same left ideal. Two generators of the same left ideal also differ by a unit multiple (on the left) so there is a $v = \alpha + r$, $0 \neq \alpha$ in $K$, $r$ in $R$ such that

$$(\alpha + r)(m_1 + \lambda w)(1 + s) = m_1 + \gamma w.$$  \hfill (3.6)

Before proceeding further it will be necessary to know $\alpha = 1$. Suppose $m_1$ is in $R^k$ but not in $R^{k+1}$. In step 2 we saw $m_1$ was not in $R^{N-1}$; so $k \leq N - 2$. In particular, $w$ is in $R^{k+1}$. Now read Eq. (3.6) modulo $R^{k+1}$ and see

$$\alpha m_1 = m_1 \neq 0 \text{ modulo } R^{k+1}.$$  

Thus $\alpha = 1$. Use this and multiply out Eq. (3.6) and it turns out that

$$(\gamma - \lambda)w = rm_1 + m_1s + rm_1s + \text{terms in } R^N.$$  

From the facts that $\gamma \neq \lambda$ and $R^N$ is in $Rm_1$ the proof of step 3 is easily completed.

The next step is concerned with an estimate for the dimension of $K(G)m_1K(G)$ knowing that $K(G)m_1$ has dimension $d$. We make use of the dimension relations (61.3) in Curtis-Reiner [3]. We use $l(t)$ to denote the left annihilator of the element or subset $t$ of $K(G)$.

First we know $K(G)m_1$ is isomorphic to $K(G)/l(m_1)$, so

$$\dim K(G)m_1 = \dim K(G) - \dim l(m_1).$$  \hfill (3.7)

Secondly we obtain from [3]

$$\dim K(G)m_1K(G) = \dim K(G) - \dim l(K(G)m_1K(G)).$$  \hfill (3.8)
Use the equation \( l(K(G) m_1) = l(K(G) m_1 K(G)) \) along with (3.7) and (3.8) to conclude

\[
\dim \left\{ \frac{K(G) m_1 K(G)}{K(G) m_1} \right\} = \dim \left\{ \frac{l(m_1)}{l(K(G) m_1)} \right\}.
\] (3.9)

There is a natural identification of \( K(G)/l(K(G) m_1) \) with the algebra of linear transformations induced upon \( K(G) m_1 \) by the elements in \( K(G) \). If we select a suitable basis with \( m_1 \) as the first basis vector, then \( K(G)/l(K(G) m_1) \) can be identified with a subalgebra of lower triangular matrices of size \( d \times d \) having the same scalar in the diagonal entries of each matrix. Thus \( l(m_1)/l(K(G) m_1) \) is identified with a subalgebra of lower triangular matrices having only zero in the first column and on the diagonal. It follows that

\[
\dim \left\{ \frac{l(m_1)}{l(K(G) m_1)} \right\} \leq \frac{1}{2}(d - 2)(d - 1).
\]

This along with (3.9) and the fact that \( \dim K(G) m_1 = d \) proves

**Step 4.** \( \dim K(G) m_1 K(G) \leq d + \frac{1}{2}(d - 2)(d - 1) \).

**Step 5.** \( \dim(R^{N-1}/R^{N}) \leq \frac{1}{2}(d - 2)(d + 1) \).

This follows at once from step 3 and step 4 if we notice that

\[
K(G) m_1 K(G) \neq Rm_1 \mid m_1 R \mid Rm_1 R
\]

implies

\[
\dim(R^{N-1}/R^{N}) \leq -1 + \dim(Rm_1 + m_1 R + Rm_1 R) \leq -2 + \dim K(G) m_1 K(G).
\]

**Step 6.** The minimal number of generators for \( G \) is equal to

\[
\dim(R^{N-1}/R^{N}).
\]

**Proof.** It is well known that the minimal number of generators for \( G \) is equal to the dimension of \( R/R^2 \). The idea of the proof of this is to show \( g - 1 \) is in \( R^2 \), whenever \( g \) is in the Frattini subgroup \( D(G) \). It is then possible to pass to \( G/D(G) \) without changing the number of generators or the dimension of \( R/R^2 \). For the elementary abelian group \( G/D(G) \) this fact is proved by an easy computation (see [7]). Finally, the results of Jennings [8] have been used by Hill [6] to show \( \ell(R^2) = R^{N-1} \). It follows \( R/R^2 \) and \( R^{N-1}/R^{N} \) have the same dimension.

Now the assertion (i) of the theorem follows from the last two steps.

In order to bound \( |G| \) by a function of \( d \) (and \( p \)) it is only necessary to bound the number of generators, the class, and the exponent of \( G \) in these terms. We have a bound already on the number of generators. Since
$G$ has a faithful representation of degree $d$, it may be viewed as a subgroup of the lower unit triangular group of degree $d$. This triangular group has class number $d - 1$ and exponent $p^a$, where $p^a \leq p(d - 1)$. Hence the class and exponent of $G$ are bounded in terms of $d$ and $p$.

To illustrate the theorem we shall determine all $p$ groups which have only a finite number of faithful three-dimensional representations over an infinite field of characteristic $p$.

If $G$ is such a group and $G$ is abelian, then, by Theorem 1, $G$ is cyclic or has order four. In case $G$ is cyclic of order $p^m$, the smallest degree of a faithful representation is $1 + p^{m-1}$. Thus $|G| = p$ or $4$.

If $G$ is non-abelian, then a representation which is faithful of degree three must be indecomposable since only abelian $p$ groups can act faithfully in degree two. For the same reason, the faithful representation of degree three is fundamental. Thus Theorem 3.1 can be applied to assert that $G$ has at most two generators. Since $G$ is non-abelian, it has exactly two generators. Moreover, by the last paragraph of the proof of Theorem 3.1 we know $G$ has class two and exponent $p$ or $4$. It is not difficult to determine all two generator groups satisfying these conditions. There are three possibilities:

(a) $p$ odd, $G = \langle x, y \mid x^p = y^p = 1, [x, y] \text{ is central of order } p \rangle$

(b) $p = 2$, $G = \langle x, y \mid x^4 = 1, [xy] = x^2, y^2 = 1 \rangle$.

In case (a), consider the representation $T_\alpha$:

\[
\begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
\alpha & 1
\end{pmatrix}.
\]

We leave it to the reader to verify that $T_\alpha$ is a faithful representation of $G$ so long as $\alpha \neq 0$ and $T_\alpha$ is equivalent to $T_\beta$ if and only if $\alpha = \beta$. So when the ground field is infinite, $G$ has infinitely many faithful three-dimensional representations.

We shall prove in section four that the groups in case (b) has only two inequivalent representations provided that $GF(4) \subseteq K$ in the case of the second group of (b). Thus we obtain the following result.

**Theorem 3.10.** Let $G$ be a $p$ group having only a finite number of faithful representations of degree three over an infinite field $K$ of characteristic $p$. Then

(i) $G$ has order $p$,

(ii) $G$ has order four,
(iii) $G$ is a dihedral group of order eight, or
(iv) $G$ is a quaternion group of order eight provided that in this case $GF(4) \subseteq K$.

Conversely, the groups in this list have only a finite number of inequivalent faithful representations of degree three.

4. Dihedral and Generalized Quaternion Groups

In this section we consider the dihedral group $D_n$ and the generalized quaternion group $Q_n$, each of order $2^{n+2}$. We shall use the standard presentation of these groups; namely, we have the group on generators $x$ and $y$ subject to the relations
\[
x^{2^{n+1}} = 1, \quad y^{-1}xy = x^{-1},
\]
\[
y^2 = 1 \text{ for } D_n, \quad y^2 = x^{2^n} \text{ for } Q_n.
\]

If $K$ is a field of characteristic two, these groups cannot have faithful $K$-representation in degrees less than $1 + 2^n$. This is easily seen because it is already true for the cyclic group $\langle x \rangle$. Our object in this section is to prove there exist exactly two inequivalent representations of this degree (provided $GF(4) \subseteq K$ in the case of $Q_1$). The computations are a bit lengthy but, inasmuch as these appear to be the first such examples, we shall present the details.

Let $G$ denote either $D_n$ or $Q_n$ for $n \geq 1$. Let $X$ be the matrix of size $1 + 2^n$ having zeros everywhere except for 1's in the positions $(2, 1), (3, 2), \ldots, (1 + 2^n, 2^n)$. Any representation of $G$ in degree $1 + 2^n$ is equivalent to one in which $x$ is mapped onto $I + X$. It is necessary to develop some properties of the algebra $K[X]$.

**Lemma 4.1.** The centralizer of $I + X$ in the full matrix algebra is $K[X]$.

This is well known so we omit the proof.

**Lemma 4.2.** Any $K$-algebra automorphism $\varphi$ of $K[X]$ is induced by conjugation with some matrix $A$ in lower triangular form. For a given $\varphi$ there is a unique such $A$ which has only zeros in the first column except for a 1 in the $(1, 1)$ position. Any other matrix inducing $\varphi$ has the form $BA$ for some unit $B$ in $K[X]$.

**Proof.** Let $\varphi(X) = Xf(X)$, where $f(X)$ is a unit in $K[X]$. We shall describe $A$ by defining its effect upon a basis of the vector space upon which the matrices act.
Let $v_1, v_2, \ldots, v_{1+2^n}$ be the basis such that

$$Xv_i = v_{i+1}, \quad i \leq 2^n,$$

$$Xv_{1+2^n} = 0.$$

Define $A$ to be the matrix such that

$$Av_i = f(X)^{i-1}v_i.$$

Then we find, for $i \leq 2^n$,

$$AXv_i = Av_{i+1} = f(X)^i X v_i = Xf(X) Av_i.$$

The first and last terms are equal also for $i = 1 + 2^n$ and so $AX = Xf(X)A$. Since $f(X)$ is a unit, it follows that $A$ is nonsingular and thus

$$AXA^{-1} = f(X).$$

When $f(X)^{i-1}v_i$ is expressed in terms of the $v_j$, only $v_j$ with $j \geq i$ can have nonzero coefficients. Thus $A$ is lower triangular. Moreover, $Av_1 = v_1$ means the first column of $A$ has only zero entries except for a 1 in the $(1, 1)$ position.

Suppose $A_0$ also induces $\varphi$ upon $K[X]$. Then $A_0 A^{-1}$ centralizes $X$ and so by Lemma 4.1 $A_0 A^{-1} = B$ for some unit $B$ in $K[X]$.

If $B = a_0 + a_1 X + \cdots$, the first column of $A_0$ has $a_{i-1}$ in row $i$. From this we see $A$ is unique.

The main interest is in the special case

$$\varphi(X) = X(I + X + \cdots) = X(I + X)^{-1}.$$

This is equivalent to $\varphi(I + X) = (I + X)^{-1}$.

This automorphism $\varphi$ has order two. Let $A$ be the matrix which induces $\varphi$ on $K[X]$ and which has a 1 in the $(1, 1)$ position and zeros in the rest of the first column. The uniqueness statement applied to $\varphi^2$ and $A^2$ shows $A^2 = I$. We summarize these properties:

(i) $A(I + X)A^{-1} = (I + X)^{-1}$, \hspace{1cm} (4.3)

(ii) $AXA^{-1} = X + X^2 + \cdots + X^{2^n}$,

(iii) $A^2 = I$.

The verification of these properties requires

$$X^{2^n} \neq 0, \quad X^{1+2^n} = 0. \hspace{1cm} (4.4)$$

We shall give now a preliminary description of the representations of $G$. 
It is convenient to introduce some notation here for future use. If $B$ is a unit in $K[X]$, then

(i) $ABA^{-1} = B^A$,
(ii) $N(B) = BB^A$,
(iii) $[B, A] = B^{-1}B^A$.

Remark. $N$ is a multiplicative endomorphism on the units of $K[X]$.

**Lemma 4.5.** Let $T$ be a faithful representation of $D_n$ or $Q_n$ in dimension $1 + 2^n$. Then $T$ is equivalent to a representation $T_B$, for $B$ some unit in $K[X]$, defined as follows. In both cases, $T_B(x) = I + X$.

(a) For $D_n$, $T_B(y) = BA$ with $N(B) = I$.
(b) For $Q_n$ and $n \geq 2$,

$$T_B(y) = B(I + X^{-1+2^n})A, \text{ and } N(B) = I.$$  

(c) For $Q_1$, $T_B(y) = B(I + \alpha X)A$ with $N(B) = 1$, and $\alpha$ is an element of $K$ which satisfies $\alpha^2 + \alpha + 1 = 0$.

**Proof.** An earlier argument insures that $T$ may be transformed so that $T(x) = I + X$. Then in both cases, $T(y)$ is a matrix that inverts $I + X$; so by Lemma 4.2, $T(y) = CA$ for some unit $C$ in $K[X]$. In the case of $D_n$, it is necessary that $T(y^2) = 1$. Thus

$$(CA)^2 = N(C)A^2 = N(C) = I.$$  

Thus $C = B$ is the proper choice for statement (i) of the Lemma.

In the case of $Q_n$, we need

$$T(y)^2 = (I + X)^{2^n} = I + X^{2^n},$$

which forces $N(C) = I + X^{2^n}$. If $n \geq 2$, it is possible to use (4.3) and (4.4) to verify

$$N(C_0) = I + X^{2^n} \quad \text{if } C_0 = I + X^{-1+2^n}.$$  

If $B = CC_0^{-1}$, then $N(B) = N(C)N(C_0^{-1}) = I$ and $T(y) = BC_0A$ as required in (ii).

In case $n = 1$, the element $C_0$ does not work. In its place we use

$$C_1 = I + \alpha X \quad \text{with } \alpha^2 + \alpha + 1 = 0, \quad \alpha \text{ in } K.$$  

Then again $N(C_1) = I + X^2$ and with $B = CC_1^{-1}$ the statement (iii) holds.

The reader may verify for himself that it is necessary to use elements in $GF(4)$ to satisfy this "norm" equation in the case $n = 1$. 


Another observation should be made. If \( N(B) = I \), then \( B \) necessarily is congruent to \( I \) modulo \( X \). We let
\[
U = \{ I + XK[X] \}.
\]
Then \( U \) is a multiplicative group, \( N \) is a homomorphism from \( U \) into itself and all representations of \( D_n \) or \( Q_n \) are obtained by using elements in
\[
U_N = \{ B \in U \mid N(B) = 1 \}.
\]
One more subgroup is needed. Let
\[
U_C = \{ [B, A] \mid B \in U \}.
\]
Since \( U \) is an abelian group, the formula
\[
[C_1, A][C_2, A] = [C_1C_2, A]
\]
is valid, and so \( U_C \) is a subgroup of \( U \). In fact \( U_C \) is a subgroup of \( U_N \).

**Lemma 4.6.** Let \( B, C \) be elements of \( U_N \). The representations \( T_B, T_C \) of \( D_n \) or \( Q_n \) defined in Lemma 4.5 are equivalent if and only if \( C^{-1}B \) is in \( U_C \).

The inequivalent representations of \( D_n \) and \( Q_n \) are in one-to-one correspondence with the elements in the quotient \( U_N/U_C \).

**Proof.** Suppose \( P \) is a matrix such that \( P^{-1}T_B(g)P = T_C(g) \) for all \( g \) in the group. Then with \( g = x \) we see that \( P \) must centralize \( I + X \). Thus \( P \) is in \( K[X] \) by Lemma 4.1. We may multiply \( P \) by a scalar to insure that \( P \) is in \( U \). Now use \( g = y \) and it follows in either case that \( BP^{-1}APA^{-1} = C \), and so
\[
B^{-1}C = [P, A] \in U_C.
\]
Conversely, if \( B^{-1}C \) is in \( U_C \), then \( B^{-1}C = [PA] \) for some \( P \) and the above steps can be reversed.

The main object of this section is to prove \( U_N/U_C \) has order two. We shall proceed by induction on \( n \). It is important to note that this assertion about the group \( U_N/U_C \) is independent of the requirement \( GF(4) \subseteq K \) in case of \( Q_1 \). So the induction can proceed without particular attention to \( K \).

In case \( n = 1 \), a direct calculation yields
\[
U_N = \{ I + \alpha X + \beta X^2 \mid \alpha = 0, 1, \beta \in K \},
\]
\[
U_C = \{ I + \beta X^2 \mid \beta \in K \}.
\]
Thus the quotient \( U_N/U_C \) has order two in this case. For general \( n \), we always have \( I + X \) in \( U_N \) but not in \( U_C \). This is easily seen because elements in \( U_C \) are always congruent to \( I \) modulo \( X^2 \).
Now assume $n \geq 2$.

The squaring map $B \to B^2$ is a homomorphism of $U$ into itself. Let $U^2$ and $U_2$ denote the image and kernel of this map. For convenience, let $Y = X^2$.

We now have the equations

\begin{align*}
(i) & \quad Y^{2^n-1} \neq 0, \quad Y^{1+2^n-1} = 0, \\
(ii) & \quad A(I + Y)A^{-1} = (I + Y)^{-1},
\end{align*}

in place of (4.3)(i) and (4.4). Moreover, the group of units in $K[Y]$ congruent to 1 modulo $Y$ is precisely $U^2$. The inductive hypothesis applies to give the next statement:

**Lemma 4.7.** $U^2 \cap U_N/[U^2, A]$ has order two.

It is necessary to examine this quotient carefully. The equation $[C, A]^2 = [C^2, A]$ implies

$$(U_C)^2 = [U^2, A].$$

Also $(U_N)^2 \subseteq U_N \cap U^2$; so the squaring map induces a homomorphism from $U_N/[U_C]$ into $U^2 \cap U_N/[U^2, A]$. In fact, this induced map is onto because the nontrivial coset of the second group contains $1 + Y$ which is in the image.

In order to postpone for now the difficulties with elements of order two, we include $U_2$ into the two groups $U_N$ and $U_C$ to get the next step.

**Lemma 4.8.** The squaring map induces an isomorphism from $U_N U_2/U_C U_2$ to the group $U_N \cap U^2/[U^2, A]$ of order two.

Just a little more manipulation is necessary to prepare for the final step. A standard isomorphism theorem implies

$$U_N U_2 U_C U_2 \cong U_N/[U_N \cap U_C U_2]. \quad (4.9)$$

Also the inclusion $U_C \subseteq U_N$ implies $U_N \cap U_C U_2 = (U_N \cap U_2) U_C$. Use this along with (4.9) and Lemma 4.8 to obtain the following.

**Lemma 4.10.** $\{U_N/[U_C]\}/\{(U_N \cap U_2) U_C/U_C\}$ has order two.

Our goal was to prove $U_N/U_C$ has order two; so we will be finished if $U_N \cap U_2 \subseteq U_C$. We will prove slightly more than this.

**Lemma 4.11.** $U_N \cap U_2 = [U_2, A] \subseteq U_C$.

The proof of this statement still requires a number of calculations. For simplicity, let $m$ denote $2^{n-1}$. Then

$$X^{2m} \neq 0, \quad X^{2m+1} = 0.$$
One can easily check that

\[ U_2 = \{ I + X^m(\alpha_1 X + \cdots + \alpha_m X^m) \mid \alpha_i \in K \} \]

In particular, every element in \( U_2 \) can be written as \( I + X^m W \) for some \( W \) in \( XK[X] \). One can check without much difficulty that

\[ (I + X^m W)^4 = I + X^m W^4. \] (4.12)

Using this and the definitions, one verifies

\[ U_N \cap U_2 = \{ I + X^m W \mid W \in XK[X], X^m(W + W^4) = 0 \}, \]

\[ [U_2, A] = \{ I + X^m(W + W^4) \mid W \in XK[X] \}. \] (4.13)

We need to show these are equal. In order to simplify calculations, we introduce a new variable \( Z \) which satisfies \( Z^m \neq 0 \) and \( Z^{m+1} = 0 \). We define the action of \( A \) upon \( K[Z] \) by \( (1 + Z)^4 = (1 + Z)^{-1} \).

Now consider the vector space map \( f \) from \( ZK[Z] \) to \( X^mK[X] \) defined by

\[ f : \alpha_1 Z + \cdots + \alpha_m Z^m \mapsto X^m(\alpha_1 X + \cdots + \alpha_m X^m). \]

This is a vector space isomorphism which commutes with the action of \( A \) because of (4.12).

Let \( \text{Tr} \) be the trace map defined on \( K[Z] \) by \( \text{Tr}(a) = a + a^4 \), and finally let \( \mathcal{C} \) be the elements in \( ZK[Z] \) left invariant by \( A \). By (4.13), we see

\[ U_N \cap U_2 = I + f(\mathcal{C}), \]

\[ [U_2, A] = I + f(\text{Tr} ZK[Z]). \]

Because \( f \) is an isomorphism, the proof of the lemma will be accomplished if it can be proved that \( \mathcal{C} = \text{Tr} ZK[Z] \). It is immediate that \( \text{Tr} ZK[Z] \subseteq \mathcal{C} \), so the desired equality will follow if we can show \( \mathcal{C} \) and \( \text{Tr} ZK[Z] \) have the same \( K \)-dimension. So we try to prove this.

Observe that \( \text{Tr} \) is a \( K \)-linear homomorphism from \( ZK[Z] \) to itself and the kernel is precisely \( \mathcal{C} \). Counting dimensions shows us

\[ \dim \mathcal{C} + \dim \text{Tr} ZK[Z] = \dim ZK[Z] = m = 2^n - 1. \]

The equality of \( \mathcal{C} \) and \( \text{Tr} ZK[Z] \) will now follow from the last step in the proof.

**Lemma 4.14.** \( \dim \mathcal{C} = 2^{n-2} \).
Proof. The dimension of $\mathcal{C}$ is one less than the dimension of the space of fixed points under $A$ in the whole algebra $K[Z]$. We can compute this space of fixed points by using a different basis for $K[Z]$. Namely, any $v$ in $K[Z]$ can be uniquely written as

$$v = \alpha_0 + \alpha_1(1 + Z) + \cdots + \alpha_i(1 + Z)^i + \cdots + \alpha_m(1 + Z)^m.$$ 

In terms of this basis one can compute more easily. In particular, we first have

$$(1 + Z)^iA = 1 + (1 + Z)^{m-i} + (1 + Z)^m.$$ 

The equation $v = v^A$ holds if and only if $\alpha_i = \alpha_{m-i}$ for $1 \leq i \leq m - 1$, and $\sum_{i=1}^{m-1}\alpha_i = 0$.

This forces $\alpha_{2n-2} = 0$. Thus $\alpha_i$ is arbitrary if $i = 0, 1, \ldots, 2^{n-2} - 1$ or if $i = m$ and the remaining $\alpha_j$ are determined. Thus there are $1 + 2^{n-2}$ free choices for the $\alpha_i$. This completes the proof of this lemma and also of Lemma 4.11.

We now summarize the results proved in this section.

**Theorem 4.15.** A faithful representation of $D_n$ or $Q_n$ of degree $1 + 2^n$ over a field of characteristic two is equivalent to one of the representations $T_i$ or $T_{i+1}$ defined in Lemma 4.5.

The reader may notice that if $G$ is either $D_n$ or $Q_n$, then $T_i(G) = T_{i+1}(G)$. Thus a somewhat weaker form of the theorem can be stated.

**Corollary.** The general linear group $GL(1 + 2^n, K)$ over a field $K$ of characteristic two has just one conjugacy class of subgroups isomorphic to $D_n$ or $Q_n$ provided $GF(4) \subset K$ in the case of $Q_1$.

**References**