PACIFIC JOURNAL OF MATHEMATICS
Vol. 36, No. 3, 1971

QUASI REGULAR GROUPS OF FINITE COMMUTATIVE NILPOTENT ALGEBRAS

N. H. EGGERT

Let J be a finite commutative nilpotent algebra over a field F of characteristic p. J forms an abelian group under the "circle" operation, defined by $a \circ b = a + b + ab$. This group is called the quasi regular group of J.

Our main purpose is to investigate the relationship between the structure of J as an algebra, and the structure of its quasi regular group.

In particular, the structure of the quasi regular group is described in terms of certain subalgebras of J. These subalgebras are, for fixed j, the p^j powers of elements in J. They are denoted by $J^{(j)}$.

It is conjectured that the dimension of $J^{(j)}$ is greater than or equal to p times the dimension of $J^{(j+1)}$. If this is true, then Theorems 1.1 and 2.1 completely describe the possibilities for the quasi regular group of J. Paragraph 2 considers some special cases of the conjecture.

1. The quasi regular group of J. Let J be a finite commutative nilpotent algebra over a field F with p^u elements. Denote by $J^{(j)}$ the set of p^jth powers of elements in J, $j = 0, 1, \cdots$. The $J^{(j)}$ form a descending chain of subalgebras of J. If t is the minimum exponent such that $x^{p^t} = 0$ for all $x \in J$ then $J^{(t-1)} \neq (0)$ and $J^{(t)} = (0)$. The constant t will be called the height of J. Let the dimension of $J^{(j)}$ be r_j and set $s_h = r_{h-1} + r_{h+1} - 2r_h$, $h = 1, \cdots, t$.

We denote by $G(p, u; s_1, \cdots, s_t)$ the group which is the direct sum of us_h, $h = 1, \cdots, t$, copies of the cyclic group of order p^h.

THEOREM 1.1. *The quasi regular group of J is isomorphic to $G(p, u; s_1, \cdots, s_t)$.*

Proof. Since the pth power of $x \in J$ with respect to the operation "o" is x^p, the number of cyclic summands of order greater than p^h is the dimension of the quotient group $J^{(h)}/J^{(h+1)}$ over the integers modulo p, that is $u(r_h - r_{h+1})$ [1, page 27]. Hence the number of cyclic summands of order p^h in the quasi regular group J is $u(r_{h-1} + r_{h+1} - 2r_h)$, $h = 1, \cdots, t$.

2. The possibilities for the quasi regular group of J. Given certain p-groups, finite commutative nilpotent algebras can be constructed with these groups as their quasi regular groups.

THEOREM 2.1. *Let a_i be arbitrary nonnegative integers for $i = 1, \cdots, t$, $a_t \neq 0$. Then there exists a finite commutative nilpotent algebra J over a field F of order p^u where:*

(i) $r_t = 0$ *and* $r_{i-1} = pr_i + a_i$, $i = 1, \cdots, t$.

(ii) *the quasi regular group of J is $G(p, u; s_1, \cdots, s_t)$ where $s_h = r_{h-1} + r_{h+1} - 2r_h$.*

Proof. Let J_j be the Jacobson radical of $F[X]/(X^n)$, where $n = p^{j-1} + 1$. If $x = X + (X^n)$ then a basis for J_j over F is $\{x, x^2, \cdots, x^{n-1}\}$. Thus the dimension of $J_j^{(i)}$ is p^{j-i-1} for $i < j$. Let J be the direct sum of a_j copies of J_j for $j = 1, \cdots, t$. Then $r_i = \dim J^{(i)} = \sum_{j=i+1}^{t} a_j p^{j-i-1}$, $i < t$, $r_t = \dim J^{(t)} = 0$. A simple calculation gives $r_{i-1} - pr_i = a_i$. By using Theorem 1.1, the proof is complete.

The author conjectures that the converse of the above theorem is also true, that is:

(C) If J is a finite commutative nilpotent algebra over F then $\dim J^{(i-1)} - p \dim J^{(i)} = r_{i-1} - pr_i \geqq 0$.

This is immediate for algebras of height one, height two and $\dim J^{(1)} = 1$, and height two and $p = 2$. The following theorem establishes (C) for algebras of height two and $\dim J^{(1)} = 2$.

THEOREM 2.2. *Let J be a commutative nilpotent algebra over a perfect field F of characteristic p. Let x, y be elements of J and suppose x^p and y^p are linearly independent over F. Then the dimension of J is greater than or equal to $2p$.*

Proof. Suppose the theorem is false. That is, assume there is a finite commutative nilpotent algebra J over F and:

(i) $x, y \in J$ and x^p, y^p are independent over F,

(ii) $\dim J < 2p$.

We assume J is an algebra of least dimension over F which satisfies (i) and (ii). It then follows that:

(iii) J is generated by x and y, and

(iv) If I is an ideal of J and an algebra over F then $I = (0)$ or for some $a, b \in F$, $0 \neq ax^p + by^p \in I$.

If (iv) were false then J/I would satisfy (i) and (ii) and the dimension of J/I would be less than the dimension of J.

We may assume x^p is in the annihilator of J. This follows since, by (iv), there are elements a, b in F where $ax^p + by^p \neq 0$ is in the annilhilator. By replacing x by $x' = a'x + b'y$, where $a'^p = a$ and $b'^p = b$, conditions (i) through (iv) hold and x'^p is in the annihilator.

Let $\mathscr{C}$ be the cartesian product of the nonnegative integers with themselves less (0, 0). Let the total ordering $\prec$ be defined in $\mathscr{C}$ by: $(s, t) \prec (i, j)$ if $s + t < i + j$ or $s + t = i + j$ and $s < i$.

LEMMA. *If* $x^i y^j \neq 0$ *then* $i + j \leqq p$.

Proof. Let $(n, m(0))$ be the maximum element in $\mathscr{C}$, with respect to $\prec$, such that $x^n y^{m(0)} \neq 0$. Suppose that $n + m(0) > p$.

Since x^p is in the annihilator of J, $n \leqq p$ and $m(0) > 0$, thus if $n > 0$ then $\mathscr{A} = \{(i, j) \in \mathscr{C}: i \leqq n, \text{ and } j \leqq m(0)\}$ has more than $2p$ elements. The monomials $x^i y^j$, $(i, j) \in \mathscr{A}$, are dependent, thus a nontrivial relation.

$$\Sigma a_{ij} x^i y^j = z = 0, (i, j) \in \mathscr{A}$$

exists. Let (s, t) be minimum such that $a_{st} \neq 0$. Consider

$$0 = z x^{n-s} y^{m(0)-t} .$$

For $(s, t) \prec (i, j)$ it follows that $(n, m(0)) \prec (i + n - s, j + m(0) - t)$. By the definition of $(n, m(0))$ we obtain $0 = a_{st} x^n y^{m(0)}$. This is a contradiction; thus $n = 0$.

Now define $m(i)$ to be the maximum integer such that $x^i y^{m(i)} \neq 0$, $i = 0, \cdots, p$. Since $x, \cdots, x^p, y, \cdots, y^p$ are dependent, let

$$z = \sum_{i=h}^{p} a_i x^i + \sum_{i=l}^{p} b_i y^i = 0 , \tag{1}$$

where $a_h \neq 0$ and $b_l \neq 0$. There is at least one nonzero a_j since $y, \cdots, y^p$ are independent. Likewise at least one b_i is nonzero. Thus considering $x^{p-h} z$ and $y^{m(0)-l} z$ we find $x^{p-h} y^l \neq 0$ and $x^h y^{m(0)-l} \neq 0$.

We will now show that, for $k = 0, \cdots, h$, if $i \geqq k$ and $x^i y^j \neq 0$ then $(i, j) \leqq (k, m(k))$. Suppose this has been shown for $0, \cdots, k - 1$. Since $(i + 1, m(i + 1)) \prec (i, m(i))$ for $i < k$, we see that $m(0) \geqq m(i) + 2i$. From $x^h y^{m(0)-l} \neq 0$ and $h < k - 1$ we have

$$(h, m(0) - l) \prec (k - 1, m(k - 1)) .$$

Therefore $h + m(0) - l < k - 1 + m(k - 1)$ and $l - h \geqq k$. Now let (u, v) be maximum such that $u \geqq k$ and $x^u y^v \neq 0$. Since $x^{p-h} y^l \neq 0$ and $p - h \geqq l - h \geqq k$ it follows that $u + v \geqq p - h + l \geqq p + k$. If $v = 0$ then $u = p$ and $k = 0$. Since for $k = 0$ our result is established, we consider $v > 0$. If $u > k$ then the set $\mathscr{A} = \{(i, j) \in \mathscr{C}: k \leqq i \leqq u, 0 \leqq j \leqq v\}$ contains $(u - k + 1)(v + 1) \geqq 2(u - k + v) \geqq 2p$ elements. Thus there is a nontrivial relation among the $x^i y^j$, $(i, j) \in \mathscr{A}$. As before, let (s, t) be minimum such that the coefficient, a_{st}, of $x^r y^t$ is nonzero. On multiplying the relation by $x^{u-s} y^{v-t}$ we obtain $0 = a_{st} x^u y^v$ which is contradictory. Therefore $u = k$ and $v = m(k)$. By the definition of (u, v), if $i \geqq u = k$ and $x^i y^j \neq 0$ then $(i, j) \prec (k, m(k))$.

We now have the inequality, $m(0) \geqq 2k + m(k)$, for $k = 0, \cdots, h$. Since $x^h y^{m(0)-l} \neq 0$, $m(h) \geqq m(0) - l$. That is $l \geqq 2h$.

Let $bh + c = p$ where $0 \leqq c < h$. Returning to equation (1) we obtain:

$0 \neq a_h^b x^p = x^c(\Sigma_i a_i x^i)^b = x^c(-\Sigma_i b_i y^i)^b = x^c y^{bl} Y$, where Y is a polynominal in y.

Hence $x^c y^{bl} \neq 0$. This implies $m(0) - 2c \geqq m(c) \geqq bl \geqq 2bh$. Therefore $m(0) \geqq 2p$ and $y, \cdots, y^{2p}$ are independent. This is a contradiction and the lemma is established.

Next we show that if $m + n = p$ and $n \neq p$ then $x^m y^n = c_n x^p$ where $c_n \in F$. Suppose this holds for the powers of y being $0, \cdots, n - 1$. If $x^m y^n = 0$ then the result is established. Thus suppose $x^m y^n \neq 0$. There are $(m + 1)(n + 1) \geqq 2p$ monomials of the form x^p or $x^i y^j$, $i \leqq m, j \leqq n$. Thus there is a nontrivial relation

$$\sum a_{ij} x^i y^j + a x^p = 0 .$$

Let (s, t) be minimum such that the coefficient of $x^s y^t$ is nonzero. By multiplying the relation by $x^{m-s} y^{n-t}$ we obtain:

$$\begin{aligned} 0 &= \sum_{i+j=s+t} a_{ij} x^{i+m-s} y^{j+n-t} + a x^{p+m-s} y^{n-t} \\ &= \sum_{\substack{i+j=s+t \\ (i,j)\neq(s,t)}} c_{j+n-t} a_{ij} x^p + a' x^p + a_{st} x^m y^n . \end{aligned}$$

Since x^p is in the annihilator of J, $x^{p+m-s} y^{n-t}$ is x^p or 0. Therefore $x^m y^n = c_n x^p$.

Similarly we obtain: if $m + n = p$ and $m \neq p$, then $x^m y^n = b_m y^p$. Since x^p and y^p are independent, if $m + n = p$, $m \neq 0$, p then $x^m y^n = 0$.

From equation (1) we may obtain, as before, $x^{p-h} y^l \neq 0$ and $x^h y^{p-l} \neq 0$ where $0 < h, l \leqq p$. Assuming, without loss of generality, $h \geqq l$ we have $h + (p - l) \geqq p$ and by the lemma we have equality, that is, $h = l$. Since $x^h y^{p-h} \neq 0$ we have, by the above paragraph, $h = l = p$. Equation (1) becomes $0 = a_p x^p + b_p y^p$ for nonzero a_p and b_p, a contradiction. This completes the proof of Theorem 2.2.

Reference

1. I. Kaplansky, *Infinite Abelian Groups*, Ann Arbor 1954.

Received January 26, 1968. This research was in part supported by the National Science Foundation, grant GP-1923.

Montana State University