RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ANDREA LUCCHINI

On p-groups whose L-automorphism group is transitive on the atoms

Rendiconti del Seminario Matematico della Università di Padova, tome 80 (1988), p. 45-53

<http://www.numdam.org/item?id=RSMUP_1988__80__45_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 80 (1988)

On p-Groups whose L-Automorphism Group is Transitive on the Atoms.

ANDREA LUCCHINI (*)

Introduction.

An isomorphic mapping of the subgroup lattice $L(G)$ of a group G onto the subgroup lattice $L(H)$ of a group H is called an L-isomorphism, or a projectivity, of G onto H.

The study of finite groups whose L-automorphism group is transitive on the atoms of their subgroup lattice is introduced in [2]. In that paper the groups satisfying this property and whose order is divisible by two different prime numbers at least, are completely characterized.

For what concerns p-groups in view of the well known results by Shult (see [3]) on groups G such that Aut G is transitive on the minimal subgroups of G, it is a natural question whether, in the case $p \neq 2$, a p-group whose group of autoprojectivities is transitive on the atoms is modular. An affermative answer to this question was given [2] by assuming the more restrictive hypothesis that a cyclic subgroup of the L-automorphism group acts transitively on the atoms of the subgroup lattice.

The aim of the present work is to prove that such a result can be generalized assuming that the transitive subgroup of the L-automorphism group satisfies weaker properties rather than being cyclic. In particular the following results will be proved:

THEOREM A. *A finite p-group, $p \neq 2$, whose L-automorphism group contains a subgroup that is transitive on the atoms of the subgroup lattice and that has its order not divisible by p, is modular.*

(*) Indirizzo dell'A.: Dipartimento di Matematica pura ed applicata, Via Belzoni 7, 35131 Padova (Italy).

THEOREM B. *A finite p-group, $p \neq 2$, whose L-automorphism group contains a soluble subgroup that is transitive on the atoms of the subgroup lattice is modular.*

Notations.

We will indicate with G a finite p-group, $p \neq 2$, of exponent p^m and with Π a subgroup of the L-automorphism group of G that acts transitively on the minimal subgroups of G. In [2] it is proved that it is not restrictive to assume $G' \leqq \Omega_1(G) \leqq Z(G)$ and that the mapping π from $G/\Omega_{m-1}(G)$ into $\Omega_1(G)$ defined by the formula $(a\Omega_{m-1}(G))^\pi = a^{p^{m-1}}$ is an isomorphism.

In this situation $\Omega_1(G)$ can be thought of as a $GF(p)$ algebra if we define, for every x and y in $\Omega_1(G)$, $\gamma(x, y) = [a, b]$ where a and b are two elements of G such that $x = (a\Omega_{m-1}(G))^\pi$ and $y = (b\Omega_{m-1}(G))^\pi$. As it is remarked in [2] G will be modular exactly when $\gamma(x, y) \in \langle x, y\rangle$ for every pair of elements x, y in $\Omega_1(G)$.

We will indicate with K the field $GF(p)$.

Let φ be the homomorphism from Π to the L-automorphism group of $\Omega_1(G)$ that maps an L-automorphism σ of G in its restriction to the subgroup lattice of $\Omega_1(G)$: it is $\Pi^\varphi \cong H/Z\big(GL(\Omega_1(G), K)\big)$ where H is a subgroup of $GL(\Omega_1(G), K)$. Obviously H is transitive on the 1-dimensional subspaces of $\Omega_1(G)$ and for every $\alpha \in H$ the L-automorphism induced by α on $\Omega_1(G)$ coincides with the restriction to $\Omega_1(G)$ of a suitable $\sigma \in \Pi$.

Finally we will indicate with n the dimension of $\Omega_1(G)$ as K-vector space: in the next section it will be proved that we can assume without loss of generality $n \geqq 4$.

1. PROPOSITION 1.1. *A finite p-group, $p \neq 2$, generable by at most 3 elements and whose L-automorphism group is transitive on the atoms, is modular.*

PROOF. The case G generable by two elements at most is discussed in [2], section 4. So let $G = \langle a, b, c\rangle$ with a, b, c independent elements of order p^m, the exponent of G: in [2] is proved that G contains at least two independent and with maximal order elements, x and y, such that the subgroup $\langle x, y\rangle$ is modular. Using this fact and changing eventually the operation on G as it is described in [2], Lemma 3.2,

we may suppose $[a, b] = 1$; being the L-automorphism group of G transitive on the atoms, like $\langle a^{p^{m-1}} \rangle$ and $\langle b^{p^{m-1}} \rangle$, $\langle c^{p^{m-1}} \rangle$ also must be contained in a modular subgroup generable by two independent elements of order p^m: so it is not restrictive to assume $[a, c] = (a^{p^{m-1}})^r \cdot (c^{p^{m-1}})^s$; if $s = 0$ $\langle a \rangle$ is normalized by a generator system and so it is in particular a Dedekind subgroup of G: it follows that all cyclic subgroups of G are Dedekind subgroups and so G is modular. If $s \neq 0$ we may assume $[a, c] = c^{p^{m-1}}$; but $[b, c] = (a^{p^{m-1}})^{r_1}(b^{p^{m-1}})^{r_2}(c^{p^{m-1}})^{r_3}$. $\langle a^{p^{m-1}} \rangle$ is contained in at least two different modular subgroups generated by two independent elements of order p^m: the same must be true for every other element of $\Omega_1(G)$, in particular for $(a^{r_3} b^{-1})^{p^{m-1}}$: i.e. there must exists an element $a^r b^s c$ with $[a^{r_3} b^{-1}, a^r b^s c] \in \langle (a^{r_3} \cdot b^{-1})^{p^{m-1}}, (a^r b^s c)^{p^{m-1}} \rangle$: but this is possible if and only if $a^{r_3} b^{-1}$ is normalized by $a^r b^s c$ but then $\langle a^{r_3} b^{-1} \rangle$ is normal in G and again we deduce that G is modular. □

2. Before discussing the general case we need the following result.

LEMMA 2.1. *Let α be an element of H that acts irreducibly on the K-vector space $\Omega_1(G)$ and whose order is not divisible by p: then G is modular or there exists a projectivity from G onto a group G_1 with $G_1' \leqq \leqq \Omega_1(G_1) \leqq Z(G_1)$ and $\Omega_1(G) = \Omega_1(G_1)$ and such that α is an automorphism for the structure of algebra induced by G_1 on $\Omega_1(G_1)$.*

PROOF. Since $p \nmid |\alpha|$ and α acts irreducibly on $\Omega_1(G)$ there exists a K-isomorphism ϱ from $\Omega_1(G)$ into the additive group of a finite extension $K(\lambda)$ of K such that $x^{\alpha\varrho} = \lambda(x^\varrho)$ for every $x \in \Omega_1(G)$ (see [1], 1.7 p. 77); we translate on $K(\lambda)$ the structure of algebra that we have defined on $\Omega_1(G)$ by setting $\beta(l, m) = \gamma(l^{\varrho^{-1}}, m^{\varrho^{-1}})^\varrho$ for every pair (l, m) of elements in $K(\lambda)$. By Lemma 4.1 of [2] it is $\beta(\lambda a, \lambda b) = = k_1(a, b)\lambda\beta(a, b) + k_2(a, b)\lambda a + k_3(a, b)\lambda b$ with $k_i(a, b) \in K$ for every i, $1 \leqq i \leqq 3$. In [2], pp. 286-289, it is proved that if G is not modular then $k_1(a, b)$ is independent of the choice of a and b unless there exists an element $x \in K(\lambda)$ with $\beta(x, y) \in \langle x, y \rangle$ $\forall y \in K(\lambda)$; but we must exclude this last possibility: in fact, since the L-automorphisms act transitively on the atoms, this would imply that for every $z \in K(\lambda)$ it is $\beta(z, y) \in \langle z, y \rangle$ for every $y \in K(\lambda)$ and this is equivalent to saying that G is modular. Therefore the following relation holds:

$$\beta(\lambda a, \lambda b) = k_1 \lambda\beta(a, b) + k_2(a, b)\lambda a + k_3(a, b)\lambda b .$$

We consider in $K(\lambda)$ the element $\mu = k_1^{-1}\lambda$: since $K(\mu) = K(\lambda)$, μ also acts irreducibly and furthermore the following relation holds:

$$[\beta(\mu a, \mu b) - \mu\beta(a, b)]/\mu \in \langle a, b\rangle .$$

The K-bilinear function δ from $K(\mu)\times K(\mu)$ into $K(\mu)$ defined by setting

$$\delta(a, b) = [\beta(\mu a, \mu b) - \mu\beta(a, b)]/\mu$$

satisfies the properties described in [2], Lemma 5.1. By these properties and since, μ acting irreducibly, every $n-1$ dimensional subspace of $K(\mu)$ can be written in the form $\langle \hat{b}\mu^{-1}, \ldots, \hat{b}\mu^{-(n-1)}\rangle$ for a suitable $\hat{b} \in K(\mu)$, we can repeat the construction described in [2] p. 191 in order to get a projectivity from G onto a group G_1 such that for the bilinear function β_1 that represents on $K(\mu)$ the algebra structure induced by G_1, the equality

$$\beta_1(\mu a, \mu b) = \mu\beta_1(a, b)$$

holds for every a and b. □

3. Our purpose is now to prove that for the subgroup H of $GL(\Omega_1(G), K)$ defined above the following result holds.

PROPOSITION 3.1. *If $|H|$ is not divisible by p then G is modular.*

PROOF. The proof proceeds by a series of short steps.

a) It is useful first of all to recall the following result proved by Shult ([3], Th. 3): let G a subgroup of $GL(n, p^s)$, and let $\Phi_n(x)$ denote the cyclotomic polynomial whose roots are the primitive n-th roots of units: if π_0 denotes the set of prime divisors of $\Phi_n(p^s)$ not dividing n and $\pi(G)$ is the set of prime divisors of $|G|$, then one of the following holds:

i) G contains a normal irreducible cyclic subgroup C of index dividing n;

ii) G is a central extension of $LF(2, 2n+1)$ and $\pi = \{2n+1\}$ or $\{n+1, 2n+1\}$;

iii) π contains at most the single prime $n+1$ where $(n+1)^2 \nmid |G|$.

Therefore we need the following remark: if x is an element of prime order p_i, lying in $GL(n, p^s)$, then x acts irreducibly on $V(n, p^s)$ if and only if $p_i \in \pi$.

b) We apply the previous result to the group H: since H is transitive on the 1-dimensional subspace of $\Omega_1(G)$ $(p^n - 1)/(p - 1)$ divides $|H|$, but then $\Phi_n(p)$ also divides $|H|$ and so it is $\pi = \pi_0$; therefore we may suppose $\pi_0 \neq \emptyset$: in fact by [3], Lemma 9, it is $\pi_0 = \emptyset$ if and only if $n = 2$ or $p = 2$. Therefore one of the following holds:

i) H contains a normal irreducible cyclic subgroup C of index dividing n;

ii) $\pi_0 = \{n + 1, 2n + 1\}$ or $\pi_0 = \{2n + 1\}$ and H is a central extension of $LF(2, 2n + 1)$;

iii) $\pi_0 = \{n + 1\}$ and $(n + 1)^2$ does not divide $|H|$.

c) If H contains an irreducible cyclic subgroup $\langle \alpha \rangle$ and we suppose, by absurd, that G is not modular, we may apply Lemma 2: so we may suppose that there exists a projectivity from G onto a group G_1 with $\Omega_1(G) = \Omega_1(G_1)$ and $G_1' \leqq \Omega_1(G_1) \leqq Z(G_1)$ and a K-isomorphism ϱ from $\Omega_1(G)$ onto $K(\lambda)$ such that $x^{\alpha\varrho} = \lambda(x^\varrho)$ for every x in $\Omega_1(G_1)$ and, if we indicate with β_1 the bilinear function induced on $K(\lambda)$ by G_1 as described above, the relation $\beta_1(\lambda a, \lambda b) = \lambda\beta_1(a, b)$ holds for every pair of elements a, b in $K(\lambda)$.

By [1], Lemma 1.8, n^2 elements ζ_{ij} $(i, j = 1, \ldots, n)$ in $K(\lambda)$ are uniquely determined with $\zeta_{ii} = \zeta_{ij} + \zeta_{ji}$ for every i and j and such that $\beta_1(a, b) = \sum_{i,j=1}^{n} \zeta_{ij} a^{p^{i-1}} b^{p^{j-1}}$ for every pair (a, b) of elements in $K(\lambda)$.

Since $\beta_1(\lambda a, \lambda b) = \lambda\beta_1(a, b)$ we have $\zeta_{ij}\lambda^{p^{i-1}+p^{j-1}} = \zeta_{ij}\lambda$ (see [1] p. 86). But then either $\zeta_{ij} = 0$ for every i, j or there exist two integers i and j with $1 \leqq i < j \leqq n$ such that $\lambda^{p^{i-1}+p^{j-1}} = \lambda$ i.e. $p^{i-1} + p^{j-1} \equiv 1 \bmod |\lambda|$. If $\xi_{ij} = 0$ for every i, j then G_1 is abelian and so G is modular since there exists a projectivity of G onto G_1.

So we can conclude that if G is not modular but H contains a normal irreducible cyclic subgroup C then there exist two integers r and s with $0 \leqq r < s \leqq n - 1$ and $p^r + p^s \equiv 1 \bmod |C|$, furthermore it must be $r > 0$ since $p \nmid |C|$.

d) n is not a prime number: in fact by [3], p. 646, this happens if and only if H is a cyclic group, while in [1] it is proved that a finite p-group with a cyclic subgroup of the L-automorphism group transitive on the atoms is modular.

e) Cases (ii) and (iii) of step (*b*) don't hold. The proof that (ii) does not hold is the same as the one in [3], p. 649, step (*n*). For what concerns (iii), in [3] p. 650 step (*o*) it is shown that it can hold only in three cases:

1) $n = 4,\ p = 3;$

2) $n = 6,\ p = 3;$

3) $n = 6,\ p = 5.$

It is furthermore proved that in all these cases H contains an irreducible cyclic subgroup whose order is divisible by 20 in the first case, by 91 in the second, by 217 in the third. By step (*c*) (1) holds if and only if there exist two integers r and s with $1 \leqq r < s \leqq 3$ and such that $3^r + 3^s \equiv 1 \bmod 20$ while (2) and (3) imply that there exist r and s with $1 \leqq r < s \leqq 5$ and $3^r + 3^s \equiv 1 \bmod 91$ or $5^r + 5^s \equiv 1 \bmod 217$ respectively. It is easy to verify that all these congruences are impossible.

f) We need now an auxiliary numerical result:

LEMMA. *For every prime number p, $p \neq 2$, and every integer number m with $m \geqq 12$, the following inequality holds:*

$$2p^{2/3m} \leqq \left[\frac{p^m - 1}{p - 1}\right] \frac{1}{m}.$$

PROOF. It is $2m \leqq 3^{m/3-1}$ for every natural number $m \geqq 12$: the same inequality obviously holds if we substitute 3 with any other prime number p different from 2: so it is $2m \leqq p^{m/3-1}$, from which we deduce $2mp^{2/3} \leqq p^{m-1} \leqq (p^m - 1)/(p - 1)$.

g) Let us suppose that case (i) of step (*b*) holds, i.e. that H contains a normal irreducible subgroup C of index dividing n; since $|H|$ is divisible by $(p^n - 1)/(p - 1)$ the inequality $(1/n)(p^n - 1)/(p - 1) \leqq |C|$ holds.

Therefore if G is not modular there exist two integers r and s with $0 < r < s < n$ and such that $p^r + p^s \equiv 1 \bmod |C|$: it is obviously also $p^{r+k} + p^{s+k} \equiv p^k \bmod |C|$ for every $k \in \mathbb{Z}$; furthermore being C an irreducible subgroup of H, p has order $n \bmod |C|$ and so the exponents in the last relation may be thought reduced mod n, as we will do from now on.

One side of the congruence $p^{r+k} + p^{s+k} \equiv p^k \bmod |C|$ must represent

an integer exceeding $|C|$; if $n \geqq 12$ by the numerical lemma proved in the previous step it is $|C| \geqq (p^n - 1/p - 1)(1/n) \geqq 2p^{2/3n}$ and, for every $k \in \mathbb{Z}$, one of the two numbers $p^{r+k} + p^{s+k}$ and p^k exceeds $|C|$: it follows that the reduction modulo n of one of the numbers $r + k$, $s + k$, k must be greater than $(2/3)n$: this implies that it is $r = n/3$ and $s = 2n/3$, but then from $p^{n/3} + p^{2n/3} \equiv 1 \mod |C|$ it follows that $p^{n/3} + p^{2n/3} > |C| \geqq p^{2n/3} 2$, a contradiction.

By this last remark and keeping in mind the result contained in step (*d*) the only possibilities for n are $n = 4$, 6, 8, 9 or 10. We must now discuss separately all these cases.

h) Suppose $n = 4$: it must be $p^r + p^s \equiv 1 \mod |C|$ with $1 \leqq \leqq r < s \leqq 3$. We distinguish three possibilities:

1) $r = 1$ $s = 3$: it is $p + p^3 \equiv 1 \mod |C|$; by multiplying this congruence through by p we get $p^2 + 1 \equiv p \mod |C|$: but then it must be $p^2 + 1 > |C|$, an absurdity since $|C| \geqq (1 + p + p^2 + p^3)/4 = = (1 + p)(1 + p^2)/4 \geqq 1 + p^2$.

2) $r = 2$ $s = 3$: multiplying through by p^2 the congruence $p^2 + p^3 \equiv 1 \mod |C|$ we get $1 + p \equiv p^2 \mod |C|$ that is impossible since both $1 + p$ and p^2 are less than $|C|$.

3) $r = 1$ $s = 2$: it is $p + p^2 \equiv 1 \mod |C|$; multiplying through by p and p^2 we get the congruences $p^2 + p^3 \equiv p$ and $1 + p^3 \equiv p^2 \mod |C|$. Subtracting these two congruences the one from the other and comparing with the first we deduce $p^2 - p \equiv p \mod |C|$: again both sides are less than $|C|$ and so also (3) produces a contradiction.

i) Suppose $n = 6$. It is $p^r + p^s \equiv 1 \mod |C|$ with $1 \leqq r < < s \leqq 5$: since $|C| > p^2 + p^3$ it must be $s \geqq 4$. We distinguish between four different possible cases:

1) $r = 1$ $s = 4$: it is $p + p^4 \equiv 1 \mod |C|$; multiplying through by p^2 we get $1 + p^3 \equiv p^2 \mod |C|$, a contradiction.

2) $r = 2$ $s = 4$. $p^2 + p^4 \equiv 1 \mod |C|$ and multiplying through by p^2 we get $1 + p^4 \equiv p^2 \mod |C|$: subtracting the two congruences we deduce $2(p^2 - 1) \equiv 0 \mod |C|$, a contradiction.

3) $r = 3$ $s = 4$. Multiplying through by p^3 the congruence $p^3 + p^4 \equiv 1 \mod |C|$ we get $1 + p \equiv p^3 \mod |C|$ that is impossible since both sides are less than $|C|$.

4) $s = 5$. It is $p^r + p^5 \equiv 1 \mod |C|$, from which it follows $p^{r+1} + 1 \equiv p \mod |C|$: it must be $r \geqq 3$; so it is $p^{5-i} + p^5 \equiv 1 \mod |C|$ with $1 \leqq i \leqq 2$; multiplying through by p^{i+1} we deduce $1 + p^i \equiv p^{i+1} \mod |C|$, a contradiction.

j) Suppose $n = 8$. There exist two integers r and s with $1 \leqq \leqq r < s \leqq 7$ such that $p^r + p^s \equiv 1 \mod |C|$: in particular $p^r + p^s$ must exceed $|C|$: since

$$|C| \geqq (1 + p + \ldots + p^7)/8 > (p^5 + p^6 + p^7)/8 \geqq p^5$$

and $p^3 + p^4 \leqq p^5$ it is $s \geqq 5$. There are the following possible cases:

1) $s = 5$. From $p^r + p^5 \equiv 1 \mod |C|$, multiplying through by p^3, we deduce $p^{r+3} + 1 \equiv p^3 \mod |C|$: it must be $p^{r+3} + 1 > |C|$, from which it follows $r = 5 - i$ with $1 \leqq i \leqq 2$. So the congruence $p^{5-i} + + p^5 \equiv 1 \mod |C|$ holds, and we get $1 + p^i \equiv p^{3+i}$, an impossibility, since both the sides are less than $|C|$.

2) $s \geqq 6$, $p^{r+k} + p^{s+k} \equiv p^k \mod |C|$ holds for every $k \in \mathbb{Z}$: in particular choosing $k = 8 - s$ we deduce $p^{r-s+8} + 1 \equiv p^{8-s} \mod |C|$, that can be verified only if $s - r \leqq 2$: multiplying through by p^{-r} the congruence $p^r + p^s \equiv 1 \mod |C|$ we deduce $1 + p^{s-r} \equiv p^{8-r} \mod |C|$, again a contradiction since both the sides are less than $|C|$.

k) Suppose $n = 9$. Using arguments quite similar to the previous ones and remarking that $|C| \geqq (1 + p + \ldots + p^8)/9 \geqq (1 + p + \ldots + + p^8)/p^2 > p^5 + p^6$ we deduce that, for every $k \in \mathbb{Z}$, one of the numbers $s + k$, $r + k$, k, reduced modulo 9, must be $\geqq 7$. If $k = 2$ it is $0 \leqq \leqq s + 2 \leqq 1$ and so $r + 2 \geqq 7$, i.e. $r \geqq 5$. But then, for $k = 4$, we get $0 \leqq r + 4 \leqq 2$ and $2 \leqq s + 4 \leqq 3$, a contradiction.

l) Suppose $n = 10$. The argument is again the same: since $|c| \geqq (1 + p + \ldots + p^9)/10 > p^6 + p^7$, for every $k \in \mathbb{Z}$ one of the numbers $s + k$, $r + k$, k, reduced modulo 10, is $\geqq 8$: from this fact, choosing $k = 0$ we deduce $8 \leqq s \leqq 9$. Therefore, for $k = 2$, being $0 \leqq s + 2 \leqq 1$, we get $r \geqq 6$ and at last, for $k = 4$, we have a contradiction since $0 \leqq r + 4 \leqq 2$ and $2 \leqq s + 4 \leqq 3$.

This complete the proof of Proposition 3.1. □

Since if $|\Pi|$ is not divisible by p $|H|$ also is not divisible by p, from this proposition we get immediately the proof of Theorem A.

We conclude with the proof of Theorem B: let Π be a soluble subgroup of the L-automorphism group of G that is transitive on the atoms of the subgroup lattice of G and let Π^* be a p'-Hall subgroup of Π: since the set of the atoms has cardinality $(p^n - 1)/(p - 1)$, a number not divisible by p, Π^* also is transitive on the atoms and so we can apply the previous theorem. □

REFERENCES

[1] N. BLACKBURN, *Metodi di Lie nei gruppi*, Quaderni dei gruppi di ricerca matematica del C.N.R. (1973).

[2] A. LUCCHINI, *Sui gruppi il cui gruppo delle autoproiettività è transitivo sugli atomi*, Rend. Sem. Mat. Univ. Padova, **75** (1986), pp. 275-294.

[3] E. SHULT, *On finite automorphic algebras*, Illinois J. Math., **13** (1969), pp. 625-653.

Manoscritto pervenuto in redazione il 12 giugno 1987.