René Schoof Amsterdam, February 15, 2004

In this note we present a proof of the following result.

Theorem. *(Gaschütz) Let p be a prime number and let G be a finite p-group. Suppose that we have $G \not\cong \mathbf{Z}/p\mathbf{Z}$. Then p divides the order of* $\mathrm{Out}(G)$.

The main tool is the following. Let A be a *normal* and *commutative* subgroup of G. The group G acts on both A and G/A by conjugation. The exact sequence of cohomology sets associated to the exact sequence $0 \longrightarrow A \longrightarrow G \longrightarrow G/A \longrightarrow 0$ is given by

$$0 \longrightarrow A \cap Z(G) \longrightarrow Z(G) \longrightarrow \{g \in G : [g, G] \subset A\}/A \xrightarrow{\delta} H^1(G, A) \xrightarrow{\varepsilon} H^1(G, G).$$

Here δ sends $g \in G$ to the 1-cocycle $G \longrightarrow A$ given by $x \mapsto [g, x]$. The map that sends a 1-cocycle $f \in H^1(G, G)$ to the homomorphism $\varphi : G \to G$ given by $x \mapsto f(x)x$ is a an isomorphism of the cohomology set $H^1(G, G)$ with the pointed set of conjugacy classes of $\mathrm{End}(G)$. Here two endomorphism $\varphi, \varphi' : G \longrightarrow G$ are called conjugate, when there exists $a \in G$ for which $\varphi'(x) = a\varphi(x)a^{-1}$ for all $x \in G$.

The classes of the invertible homomorphisms in $\mathrm{End}(G, G)$ form the group $\mathrm{Out}(G)$ of automorphisms of G modulo inner automorphisms. Since A is commutative, the set $H^1(G, A)$ has a natural group structure. The restriction of the map ε to the subgroup $H^1(G/A, A)$ of $H^1(G, A)$ is a *group homomorphism* $H^1(G/A, A) \longrightarrow \mathrm{Out}(G)$, the image of which is a commutative p-group. Since the cocycles $x \mapsto [g, x]$ are trivial on A if and only if g is contained in the *centralizer* $\mathrm{Cent}(A) = \{g \in G : gx = xg \text{ for all } x \in A\}$ of A, there is an exact sequence of *groups*

$$0 \to A \cap Z(G) \longrightarrow Z(G) \xrightarrow{h} \{g \in \mathrm{Cent}(A) : [g, G] \subset A\}/A \xrightarrow{\delta} H^1(G/A, A) \xrightarrow{\varepsilon} \mathrm{Out}(G).$$

Proposition 1. *Suppose that G is a finite p-group not isomorphic to $\mathbf{Z}/p\mathbf{Z}$, for which $\#\mathrm{Out}(G)$ is not divisible by p. Then we have the following.*

(a) For every subgroup $N \subset G$ of index p we have $Z(N) \not\subset Z(G)$. In particular, G is not abelian.

(b) For every maximal abelian normal subgroup A of G we have $H^1(G/A, A) = 0$.

Proof. (a) Let $N \subset G$ be a subgroup of index p. In the sequence above we take $A = Z(N)$. Suppose that $A \subset Z(G)$. Then $H^1(G/A, A) = \mathrm{Hom}(G/A, A)$ and $\mathrm{Cent}(A) = G$. The map δ in the sequence induces an isomorphism $\{g \in G : [g, G] \subset A\}/Z(G) \longrightarrow \mathrm{Hom}(G/A, A)$. It sends $g \in G$ to the homomorphism $x \mapsto [g, x]$. However, δ is not surjective. For let $f : G/A \longrightarrow A$ be a non-trivial homomorphism with $\ker(f) = N/A$. If $g \in G$ has the property that $f(x) = [g, x]$ for all $x \in G$, then g centralizes N. If $g \in N$, then $g \in Z(N) = A \subset Z(G)$, while if $g \notin N$, the group G is generated by N and g, so that once again $g \in Z(G)$. It follows that f is trivial. Contradiction.

(b) In the exact sequence above we take $N = A$ to be a maximal abelian normal subgroup of G. The centralizer $\mathrm{Cent}(A)$ is equal to A and the map h is surjective. Indeed, if $C_0 = \mathrm{Cent}(A)$ were strictly larger than A, consider the decreasing sequence of groups $C_{i+1} = [C_i, A]$ for $i = 0, 1, \ldots$. Let i be the largest index for which $C_i \not\subset A$ and pick $x \in C_i - A$. Then the group $\langle A, x\rangle$ is a normal commutative subgroup that is strictly larger than A. Contradiction.

It follows from the exactness of the sequence that $H^1(G/A, A) = 0$ as required.

Proposition 2. *Suppose that G is a finite p-group not isomorphic to $\mathbf{Z}/p\mathbf{Z}$, for which $\#\mathrm{Out}(G)$ is not divisible by p. Let A be a maximal commutative normal subgroup of G. Then there exists a subgroup $N \subset G$ of index p for which $G = AN$. Moreover, the group N has the property that $Z(N) \not\subset A$).*

Proof. By Prop. 1*(b)* and the cohomological lemma below, we have that $\widehat{H}^q(H, A) = 0$ for every subgroup H of G/A and every $q \in \mathbf{Z}$. In particular the group $H^2(G/A, A)$ vanishes. This means that G is a semi-direct product of L by A, where $L \subset G$ is a subgroup isomorphic to G/A. Let N be a subgroup of G of index p containing L. Then we have $G = AN$. If $Z(N) \subset A$), the group $Z(N)$ centralizes both N and A so that $Z(N) \subset Z(G)$, which by Prop. 1*(a)* is not the case. Therefore $Z(N) \not\subset A$) and the proposition follows.

Proposition 3. *Suppose that G is a finite p-group not isomorphic to $\mathbf{Z}/p\mathbf{Z}$, for which $\#\mathrm{Out}(G)$ is not divisible by p. Then all maximal abelian normal subgroups of G are cyclic.*

Proof. Let A be a maximal abelian normal subgroups of G. Let $N \subset G$ be subgroup of index p as in Proposition 2. We have that $G = AN$. The group $B = A \cap N$ has index p in A. Indeed, since $[G : N] = p$, the index is at most p and it cannot be equal to 1 because then $A \subset N$, which is impossible. This leads to the following exact sequence.

$$0 \longrightarrow B \longrightarrow A \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0.$$

By Proposition 2, there exists $\zeta \in Z(N)$ of order p modulo $Z(N) \cap A$. We let H denote the subgroup of $Z(N)/(Z(N) \cap A)$ generated by ζ. Then H acts on A by conjugation. Its action on both B and $\mathbf{Z}/p\mathbf{Z}$ is trivial. Since all H-cohomology groups of $\mathbf{Z}/p\mathbf{Z}$ have order p and since $\widehat{H}^q(H, A) = 0$ for all $q \in \mathbf{Z}$, we have that $\widehat{H}^0(H, B) = B/B^p$ has order p. This implies that B is a cyclic group, isomorphic to $\mathbf{Z}/p^m\mathbf{Z}$, say.

If A were *not* cyclic, then we have that $A \cong (\mathbf{Z}/p^m\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})$ and ζ acts on A as multiplication by a matrix of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Here the coordinates in the first row are in $\mathbf{Z}/p^m\mathbf{Z}$, while those in the second row are in $\mathbf{Z}/p\mathbf{Z}$. An explicit computation shows that the norm map $A \longrightarrow A$ is multiplication by the matrix

$$\begin{pmatrix} p & \frac{1}{2}p(p-1)x \\ 0 & 0 \end{pmatrix}.$$

It follows that $\widehat{H}^0(H, A) = \mathbf{Z}/p^m\mathbf{Z}$ modulo the subgroup generated by p and $\frac{1}{2}p(p-1)x$. Since $\widehat{H}^0(H, A) = 0$, this implies that $p = 2$ and that x generates $\mathbf{Z}/p^m\mathbf{Z}$. Since ζ has order $p = 2$ modulo A, its square acts as the identity on A and hence $2x$ is trivial modulo p^m. It follows that $\#B \le 2$ and hence that $\#A \le 4$. Since $\mathrm{Cent}(A) = A$, the natural map $G/A \hookrightarrow \mathrm{Aut}(A)$ is injective, and hence we have $\#G \le 8$. However, G cannot have order ≤ 8. Indeed, G is not commutative and both non-commutative groups of order 8 contain an element of order 4. The subgroup A generated by this element is a maximal normal, commutative subgroup. The group G/A acts on it by multiplication by -1. Therefore $\widehat{H}^0(G/A, A) \neq 0$ in both cases, contradicting Prop. 1*(b)*.

This proves the claim.

Proof of the Theorem. Suppose that G is a finite p-group not isomorphic to $\mathbf{Z}/p\mathbf{Z}$, for which $\#\mathrm{Out}(G)$ is *not* divisible by p. We will derive a contradiction.

Let A be any maximal commutative, normal subgroup of G. By Proposition 3 it is cyclic. Since G is not commutative and since the natural homomorphism $G/A \hookrightarrow \mathrm{Aut}(A)$ is injective, we have $\#A > p$ so that A is isomorphic to $\mathbf{Z}/p^{m+1}\mathbf{Z}$ for some $m \geq 1$. Let N be the maximal normal subgroup constructed in the proof of Prop. 2 . Let $\zeta \in Z(N) - A$ be an element of order p modulo A and let H be the subgroup of G/A generated by ζ. By Prop. 1 and the Lemma below, the group $H^2(H, A)$ vanishes. It follows that the group $\langle A, \zeta \rangle$ is a semidirect product of H by A. This means that there exists $\alpha \in A$ so that $\zeta\alpha$ has order p. Since ζ and hence $\zeta\alpha$ act trivially on the index p subgroup $B = A \cap N$ of A, the element $\zeta\alpha$ acts on A as multiplication by $1 + \lambda p^m$ for some $\lambda \in \mathbf{Z}$.

The group $A' = \langle B, \zeta\alpha \rangle$ is therefore commutative. To see that it is normal, we first note that B is a normal subgroup of G. So, it suffices to see that $g(\zeta\alpha)g^{-1} \in A'$ for every $g \in G$. Writing $g = an$ with $n \in N$ and $a \in A$, this is equal to $an\zeta\alpha n^{-1}a^{-1} = a\zeta n\alpha n^{-1}a^{-1}$. Since the action of G on A/B is trivial, the last expression is congruent to $a\zeta\alpha a^{-1} \equiv \zeta\alpha a^{-\lambda p^m} \equiv \zeta a \pmod{B}$. The first congruence follows from the fact that $\zeta^{-1}a\zeta = a^{1-\lambda p^m}$.

However, since B is not trivial, the group A' is not cyclic. This contradicts Proposition 3. This proves the Theorem.

Lemma. *Let p be a prime number and let G be a finite p-group. Let M be a finite G-module of p-power order. Then the Tate cohomology group $\widehat{H}^q(G, M)$ vanishes for some $q \in \mathbf{Z}$ if and only if we have $\widehat{H}^q(H, M) = 0$ for every subgroup H of G and every $q \in \mathbf{Z}$.*

Proof. We proceed by induction. If the order of G is p, the group G is cyclic and its cohomology is periodic with period 2. Since M is finite, its Herbrand quotient is trivial. Therefore all cohomology groups $\widehat{H}^q(G, M)$ vanish. This proves the theorem when $\#G = p$.

If the order of G is larger than p, then we choose a normal subgroup $N \subset G$, that is neither trivial or equal to G. By shifting the dimension, we may assume that $H^1(G, M)$ vanishes. Since the inflation map $H^1(G/N, M^N) \hookrightarrow H^1(G, M)$ is injective, the cohomology group $H^1(G/N, M^N)$ vanishes. By induction we have that $\widehat{H}^q(G/N, M^N) = 0$ for all $q \in \mathbf{Z}$. In particular $H^2(G/N, M^N)$ vanishes and it follows from the execat sequence of lower terms of the Hochschild-Serre spectral sequence, that $H^1(N, M)^{G/N}$ vanishes. It follows that the cohomology group $H^1(N, M)$ itself vanishes. By induction this implies that $\widehat{H}^q(N, M)$ for all $q \in \mathbf{Z}$.

The fact that both the groups $H^q(G/N, M^N) = 0$ and the groups $H^q(N, M)$ vanish for $q \geq 1$, implies that the Hochschild-Serre spectral sequence degenerates. Therefore we have $H^q(G, M) = 0$ for all $q \geq 1$. By dimension shifting, one concludes that $\widehat{H}^q(G, M) = 0$ for all $q \in \mathbf{Z}$ as required.