Acta Universitatis Carolinae. Mathematica et Physica

A. Jančařík; Tomáš Kepka; Milan Vítek
Multiplication groups of quasigroups and loops IV.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 46 (2005), No. 1, 77--100

Persistent URL: http://dml.cz/dmlcz/142746

2005 ACTA UNIVERSITATIS CAROLINAE – MATHEMATICA ET PHYSICA VOL. 46, NO. 1

Multiplication Groups of Quasigroups and Loops IV.

ANTONÍN JANČAŘÍK, TOMÁŠ KEPKA AND MILAN VÍTEK

Praha

Received 7. October 2004

Quasigroups with prime number of inner permutations are studied.
Studují se kvazigrupy s prvočíselným počtem vnitřních permutací.

1. Auxiliary results (A)

1.1. Throughout this section, let G be a group such that $G = AB = \{ab; a \in A, b \in B\}$ where A and B are (possible non-abelian) subgroups of G. Notice, that then we also have $G = BA$ (if $x \in G$ and $x^{-1} = ab$, $a \in A$, $b \in B$, then $x = b^{-1}a^{-1} \in \in BA$).

We put $C = A \cap B$ and we denote by S (resp. T) the set of left (right) cosets modulo C in A (resp. B); that is $S = \{aC; a \in A\}$ and $T = \{Cb; b \in B\}$. The coset aC will be denoted by $\bar{a}$.

The following two lemmas are obvious:

1.2 Lemma. *The following conditions are equivalent:*
(i) A (B) *is a left transversal to* B (A) *in* G.
(ii) A (B) *is a right transversal to* B (A) *in* G.
(iii) A (B) *is a two-sided transversal to* B (A) *in* G.
(iv) A (B) *is stable transversal to* B (A) *in* G.
(v) $C = 1$.

1.3 Lemma. *A is a selfconnected transversal to B in G iff $C = 1$ and A is abelian.*

Department of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic

Faculty of Education, Charles University, M. D. Rettigové 4, 116 39 Praha 1, Czech Republic

The work is a part of the research project MSM0021620839 financed by MSMT and partly supported by the Grant Agency of the Czech Republic, Grant # 201/02/0594 and Grant # 406/05/P561.

1.4. Let $a \in A$ and $b \in B$. Then $ba = a_1b_1$ for some $a_1 \in A$, $b_1 \in B$ and, if $ba = a_2b_2$, then $a_1C = a_2C \in S$. Furthermore, if $a_3 = ac$, $c \in C$, then $ba_3 = a_1b_1c$, $b_1c \in B$. Now, we see that the element b determines a transformation q_b of the set S given by $q_b(\bar{a}) = \bar{a}_1$, since $a_4^{-1}ba \in B$ for all $a_4 \in \bar{a}_1$.

1.5 Lemma. *(i) q_b is a permutation of S for every $b \in B$ and $q_b = id_S$ iff $b \in \in \mathbb{L}_G(B)$.*
(ii) $q_{b_1}q_{b_2} = q_{b_1b_2}$ for all $b_1, b_2 \in B$.

Proof. (i) First, let $q(\overline{a_1}) = q(\overline{a_2})$, $q = q_b$. Then $ba_1 = a_3b_1$, $ba_2 = a_3b_2$, $ba_1b_1^{-1} = a_3 = ba_2b_2^{-1}$, $a_2^{-1}a_1 = b_2^{-1}b_1 \in C$ and $\overline{a_1} = \overline{a_2}$ and $a_3 \in q(\bar{a})$. Then q is a permutation of S. For the rest note that $\mathbb{L}_G(B) = \{b; a^{-1}ba \in B$ for every $a \in A\}$.
(ii) We have $b_2a = a_1b_3$, $a_1 \in q_{b_2}(\bar{a})$, $b_1a_1 = a_2b_4$, $a_2 \in q_{b_1}(\overline{a_1}) = q_{b_1}q_{b_2}(\bar{a})$. Now, $b_1b_2a = b_1a_1b_3 = a_2b_4b_3$ and $a_2 \in q_{b_1b_2}(\bar{a})$. ▲

1.6 Corollary. *The mapping $\varphi : B \to S!$, $\varphi(b) = q_b$, is a homomorphism of the group B into the symmetric group $S!$ of permutations of S and* $\mathrm{Ker}(\varphi) = \mathbb{L}_G(B)$.

1.7 Corollary. *(i) If $k = [A : C]$ is finite, then $[B : \mathbb{L}_G(B)] \leq k!$.*
(ii) If A is finite and B infinite, then $\mathbb{L}_G(B) \neq 1$.

1.8 Corollary. *If $m =$* card(A) *and $n =$* card(B) *are finite and if $k =$* card(C) *and $L=$* card$(\mathbb{L}_G(B))$*, then $l \geq n/(m/k)!$.*

1.9. For $a \in A$, let l_a denote the permutation of S defined by $l_a(\overline{a_1}) = \overline{aa_1} = aa_1C$. Now, let $a_2b_2 = a_3b_3$. Then $l_{a_2}q_{b_2}(\bar{a}) = \overline{a_2a_4}$, $b_2a = a_4b_4$, $l_{a_3}q_{b_3}(\bar{a}) = \overline{a_3a_5}$, $b_3a = a_5b_5$, $a_2a_4b_4 = a_2b_2a = a_3b_3a = a_3a_5b_5$ and $\overline{a_2a_4} = \overline{a_3a_5}$. Thus we can define a mapping $\Phi : G \to S!$ by $\Phi(ab) = l_aq_b$.

1.10 Proposition. *(i) Φ is a homomorphism of G into $S!$ and* $\mathrm{Ker}(\Phi) = C\mathbb{L}_G(B)$.
(ii) $\Phi \restriction A$ is injective and $\Phi(a) = l_a$ for every $a \in A$.
(iii) $\Phi \restriction B = \varphi$ (1.6) and $\Phi(b) = q_b$ for every $b \in B$.

Proof. (i) Let $b_1a_2 = a_3b_3$ and $a_1b_1a_2b_2 = a_4b_4$. Now, $\alpha = \Phi(a_1b_1)\Phi(a_2b_2) = l_{a_1}q_{b_1}l_{a_2}q_{b_2}$, $b_1a_2a = a_3b_3a$ and $q_{b_1}l_{a_2} = l_{a_3}q_{b_3}$. Hence $\alpha = l_{a_1}l_{a_3}q_{b_3}q_{b_2} = l_{a_1a_3}q_{b_3b_2}$. On the other hand, $\beta = \Phi(a_1b_1a_2b_2) = l_{a_4}q_{b_4}$ and $a_1b_1a_2b_3 = a_1a_3b_1b_2$. Now, we can choose $a_4 = a_1a_3$, $b_4 = b_3b_2$ and we see $\alpha = \beta$.
If $\Phi(ab) = \mathrm{id}_S$, then $l_aq_b(\bar{1}) = \bar{1}$ and consequently $\bar{a} = \bar{1}$, $a \in C$, $l_a = \mathrm{id}_S$, $q_b = \mathrm{id}_S$ and $b \in \mathbb{L}_G(B)$.
(ii) and (iii) Easy. ▲

1.11 Corollary. *If $m =$* card(A) and $n =$ card(B) are finite and if $k =$ card(C) and $t =$ card$(C\mathbb{L}_G(B))$, then $t \geq n/((m-k)/k!)$. In particular, if $C = 1$, then $t =$ card$(\mathbb{L}_G(B))$ and $t \geq n/(m-1)!$ (cf. 1.8.).

1.12 Remark. (i) Proceeding as in 1.4, we define a permutation p_a of T, $a \in A$, by $bab_4^{-1} \in B$ for every $b_4 \in Cb_1 = p_a(Cb)$, $ba = a_1b_1$. Now, $\psi : A \to T!$, $\psi(a) =$

$= p_a$, is a homomorphism into the opposite group $(T!)^{op}$ (then $a \to p_{a^{-1}}$ is a homomorphism of A into $T!$) and $\mathrm{Ker}(\psi) = \mathbb{L}_G(A)$.

(ii) Proceeding similarly as in 1.9, we get a homomorphism $\Psi : G \to (T!)^{op}$ such that $\mathrm{Ker}(\Psi) = C\mathbb{L}_G(A)$.

1.13 Lemma. *Let H be a subgroup of G such that $A \cap H = 1$. Then* $\mathrm{card}(H) \leq \mathrm{card}(B)$. Moreover, if $C = 1$ and $G = AH$, then $\mathrm{card}(H) = \mathrm{card}(B)$.

Proof. Suppose, on the contrary, that $\mathrm{card}(B) < \mathrm{card}(H)$. There are mappings $f : H \to A$ and $g : H \to B$ such that $x = f(x)g(x)$ for every $x \in H$. Clearly, g is not injective, and so $g(x) = g(y)$ for some x, $y H$, $x \neq y$. Now, $xy^{-1} = f(x)f(y)^{-1} \in A \cap H = 1$ and $x = y$, a contradiction. ▲

1.14 Lemma. *Suppose that A is abelian. Then:*

(i) $C \subseteq \mathbb{L}_G(B)$.

(ii) If $\mathbb{L}_G(B) = 1$, then $C = 1$ and $\mathbb{Z}(G) \subseteq A$.

(iii) If $\mathbb{L}_G(A) = 1 = \mathbb{L}_G(B)$, then $\mathbb{Z}(G) = 1$.

Proof. (i) Obvious.

(ii) Let $z \in \mathbb{Z}(G)$, $z = ab$. Then, for every $a_1 \in A$, $aba_1 = za_1 = a_1z = a_1ab = aa_1b$ and so, $b^{a_1} = b$ and it is clear that $b \in \mathbb{L}_G(B) = 1$. Thus $z = a \in A$.

(iii) Use (ii). ▲

1.15 Proposition. *Suppose that A is abelian and let N be normal subgroup of G such that $N/\mathbb{L}_G(B) = \mathbb{Z}(G/\mathbb{L}_G(B))$. Then $\mathbb{N}_G(B) = NB$.*

Proof. We can assume that $\mathbb{L}_G(B) = 1$. Then $\mathbb{Z}(G) \cap B = 1$, $\mathbb{Z}(G) \subseteq A$ and $C = 1$.

For every $x \in \mathbb{N}_G(B)$, define a transformation t_x of A by $a^x \in t_x(a)B$ for every $a \in A$. First, we show that $t_x \in A!$. To that purpose, let $x = cd$, $c \in A$, $d \in B$. If $t_x(a_1) = t_x(a_2)$, then $(a_2^{-1}a_1)^x \in B$, $a_2^{-1}a_1 = c^{-1}a_2^{-1}a_1c \in C = 1$, $a_1 = a_2$. Further, if $a_3 \in A$, then $da_3 = a_4e$, $a_4 \in A$, $e \in B$ and we have $a_4^x = a_4^d = (a_4ee^{-1})^d = a_3e^{-1}d$, and so $t_x(a_4) = a_3$.

Now, let x, $y \in \mathbb{N}_G(B)$ and $a \in A$. We have $a^x = t_x(a)b_1$, $b_1 \in B$, $t_x(a)^y = t_y(t_x(a))b_3$, where $b_3 = b_2b_1^y \in B$. On the other hand, $a^{xy} \in t_{xy}y(a)B$, and hence $t_{xy}(a) = t_y(t_x(a))$.

We have proven that the mapping $\tau : x \to t_{x^{-1}}$ is a homomorphism of $\mathbb{N}_G(B)$ into $A!$. Clearly, $K = A \cap \mathbb{N}_G(B) \subseteq \mathrm{Ker}(\tau)$ and $\mathrm{Ker}(\tau) \cap B \subseteq \mathbb{L}_G(B) = 1$. On the other hand, since $B \subseteq \mathbb{N}_G(B)$, we have $\mathbb{N}_G(B) = KB$. Thus $K = \mathrm{Ker}(\tau)$ and both B and K are normal subgroups of $N_G(B)$. Since $K \cap B = 1$, we have $\mathbb{N}_G(B) = K \times B$ and $K \subseteq \mathbb{C}_G(B)$. Of course, $K \subseteq \mathbb{C}_G(A)$, and so $K \subseteq \mathbb{Z}(G)$. On the other hand, $\mathbb{Z}(G) \subseteq A \cap \mathbb{N}_G(B) = K$ trivially. ▲

1.16 Corollary. *Suppose that A is abelian and $\mathbb{L}_G(B) = 1$. Then:*

(i) $C = 1$, $\mathbb{Z}(G) \subseteq A$ and $\mathbb{N}_G(B) = \mathbb{Z}(G) \times B$.

(ii) If $\mathbb{Z}(G) = 1$*, then* $\mathbb{N}_G(B) = B$.
(iii) If $\mathbb{L}_G(A) = 1$*, then* $\mathbb{Z}(G) = 1$ *and* $\mathbb{N}_G(B) = B$.

2. Auxilliary results (B)

2.1. In this section, let G be a group such that $G = AB$, where A nd B are abelian subgroup of G.

2.2 Proposition. G *is metabelian and* $G' = \langle [A, B] \rangle$ *is abelian.*

2.3 Proposition. *(i)* $\mathbb{M}_G(A) = AG'$ *and* $\mathbb{M}_G(B) = BG'$.

(ii) If $A \neq B$ *and at least one of the subgroups* A, B *is finite, then either* $\mathbb{M}_G(A) \neq G$ *or* $\mathbb{M}_G(B) \neq G$.

Proof. See [2] ▲

2.4 Lemma. *Let* C *be a subgroup of* G *such that* $A \subseteq C$. *Then:*

(i) $C = A(C \cap B)$.
(ii) $\mathbb{Z}(C) = (\mathbb{Z}(C) \cap A)(\mathbb{Z}(C) \cap B)$.
(iii) $\mathbb{Z}(C) \cap B \subseteq \mathbb{Z}(G)$.
(iv) If $\mathbb{Z}(G) \cap B = 1$*, then* $\mathbb{Z}(C) \subseteq A$.
(v) If $C \trianglelefteq G$*, then* $\mathbb{Z}(C) \trianglelefteq G$ *and* $AG' \subseteq C$.

Proof. (i) and (v) are obvious and (iv) follows from (ii), (iii).

(ii) Let $a \in A$ and $b \in B \cap C$ be such that $ab \in \mathbb{Z}(C)$. Then $ab = ba$ and, for every $c \in B \cap C$, $abc = cab = cba = bca$. Thus $ax = xa$ for every $x \in B \cap C$, and so $a \in \mathbb{Z}(C)$ by (i). Since $ab \in \mathbb{Z}(C)$, we also have $b \in \mathbb{Z}(C)$.

(iii) $\mathbb{Z}(C) \cap B \subseteq \mathbb{C}_G(A) \cap \mathbb{C}_G(B) \subseteq \mathbb{C}_G(A \cup B) = \mathbb{Z}(G)$. ▲

2.5 Corollary. *(i)* $A \cap B \subseteq \mathbb{Z}(G) \cap \mathbb{L}_G(A) \cap \mathbb{L}_G(B)$.
(ii) $\mathbb{Z}(G) = (\mathbb{Z}(G) \cap A)(\mathbb{Z}(G) \cap B)$.
(iii) If $\mathbb{Z}(G) \cap A = 1$ *(resp.* $\mathbb{Z}(G) \cap B = 1$*), then* $\mathbb{Z}(G) \subseteq B$ *(resp.* $\mathbb{Z}(G) \subseteq A$*).*
(iv) If $\mathbb{L}_G(A) = 1$ (resp. $\mathbb{L}_G(B) = 1$), *then* $A \cap B = 1$ *and* $\mathbb{Z}(G) \subseteq B$ (resp. $\mathbb{Z}(G) \subseteq A$).
(v) If $A \cap B = 1$ *and both* A *and* B *are torsionfree, then* $\mathbb{Z}(G)$ *is torsionfree.*

2.6 Lemma. *Put* $R = A \cap G'$. *Then:*

(i) $\mathbb{M}_G(A) = AG' \subseteq \mathbb{C}_G(R) \trianglelefteq G$.
(ii) $R \subseteq \mathbb{Z}(\mathbb{C}_G(R)) \trianglelefteq G$.
(iii) If $\mathbb{Z}(G) \cap B = 1$*, then* $R \subseteq \mathbb{Z}(\mathbb{C}_G(R)) \subseteq \mathbb{L}_G(A) \subseteq A$.
(iv) If $R \neq 1$*, then either* $\mathbb{Z}(G) \cap B \neq 1$ or $\mathbb{L}_G(A) \neq 1$.

Proof. (i) Since $R \subseteq G'$ and G' is abelian, we have $G' \subseteq \mathbb{C}_G(R) \trianglelefteq G$. Similarly, $A \subseteq \mathbb{C}_G(R)$.

(ii) Since $\mathbb{C}_G(R) \trianglelefteq G$, we have $\mathbb{Z}(\mathbb{C}_G(R)) \trianglelefteq G$ and, since R is abelian, $R \subseteq \mathbb{Z}(\mathbb{C}_G(R))$.

(iii) Combine (ii) and 2.4(iv).

(iv) If $\mathbb{Z}(G) \cap B = 1$, then $\mathbb{L}_G(A) \neq 1$ by (iii). ▲

2.7 Corollary. *Suppose that either $A \cap G' \neq 1$ or $B \cap G' \neq 1$. Then either $\mathbb{L}_G(A) \neq 1$ or $\mathbb{L}_G(B) \neq 1$.*

2.8 Proposition. *Suppose that $G \neq 1$ and that at least one of the subgroups A, B is finite, Then:*

(i) Either $\mathbb{L}_G(A) \neq 1$ or $\mathbb{L}_G(B) \neq 1$.

(ii) If $A \cap G' = 1 = B \cap G'$, then $\mathbb{Z}(G) \neq 1$.

Proof. (i) By 1.7(i) and 2.7, we can assume that $n = \operatorname{card}(G)$ is finite and $A \cap G' = 1 = B \cap G'$. Now, we shall proceed by induction on n.

If $A = B$, then $\mathbb{L}_G(A) = A = G \neq 1$. Hence, let $A \neq B$ and, by 3.3, let $M = \mathbb{M}_G(A) \neq G$. By 2.4(i), $M = AC$, where $C = M \cap B \neq B$. By induction, there is a normal subgroup $N \trianglelefteq M$ such that $N \neq 1$ and either $N \subseteq A$ or $N \subseteq D$. We have $N \cap M' \subseteq N \cap G' \subseteq (A \cap G') \cup (B \cap G') = 1$. Thus $N \cap M' = 1$ and consequently $N \subseteq \mathbb{Z}(M)$ and $\mathbb{Z}(M) \neq 1$. If $\mathbb{Z}(G) \cap B \neq 1$, then $\mathbb{L}_G(B) \neq 1$. If $\mathbb{Z}(G) \cap B = 1$, then $\mathbb{Z}(M) \subseteq A$ by 2.4(iv). However, $M \trianglelefteq G$.

(ii) According to (i), let $L = \mathbb{L}_G(A) \neq 1$. Then $L \cap G' \subseteq A \cap G' = 1$ and $L \subseteq \mathbb{Z}(G)$. ▲

2.9 Lemma. *(i) $\mathbb{L}_G(A)(A \cap G') \subseteq \mathbb{Z}(AG')$ and $\mathbb{L}_G(B)(B \cap G') \subseteq \mathbb{Z}(BG')$.*

(ii) $\mathbb{C}_G(A) = A\mathbb{Z}(G)$ and $\mathbb{C}_G(B) = B\mathbb{Z}(G)$.

(iii) $\mathbb{N}_G(A) = AZ_1$ and $N_G(B) = BZ_2$, where $Z_1/\mathbb{L}_G(A) = \mathbb{Z}(G/\mathbb{L}_G(A))$ and $Z_2/\mathbb{L}_G(B) = \mathbb{Z}(G/\mathbb{L}_G(B))$.

(iv) $\mathbb{N}_G(A)/\mathbb{C}_G(A) \cong Z_1/\mathbb{Z}(G)$ and $\mathbb{N}_G(B)/\mathbb{C}_G(B) \cong Z_2/\mathbb{Z}(G)$.

Proof. (i) The inclusion $A \cap G' \subseteq \mathbb{Z}(AG')$ follows from the fact that both A and G' are abelian. Further, if $a \in \mathbb{L}_G(A)$, then $a \in \bigcap A^x$, $x \in G$, and hence $a \in \mathbb{Z}(\mathbb{M}_G(A))$. But $\mathbb{M}_G(A) = AG'$ by 2.3(i).

(ii) We have $\mathbb{C}_G(A) = AB_1$, where $B_1 = B \cap C_G(A) \subseteq Z(G)$. The rest is clear.

(iii) and (iv). Use 1.15. ▲

2.10 Proposition. *Suppose that $\mathbb{M}_G(A) = G = \mathbb{M}_G(B)$. Then:*

(i) $AG' = G = BG'$.

(ii) If $A \neq B$, then both A and B are infinite.

(iii) If $\mathbb{Z}(G) = 1$, then $A \cap G' = 1 = B \cap G'$ and $\mathbb{L}_G(A) = 1 = \mathbb{L}_G(B)$.

(iv) $\mathbb{Z}(G) = 1$ if and only if $\mathbb{L}_G(A) = 1 = \mathbb{L}_G(B)$.

Proof. Combine 2.3, 2.5, 2.7 and 2.9. ▲

2.11 Lemma. *Suppose that $\mathbb{Z}(G) \cap B = 1$ (e.g., if $\mathbb{L}_G(B) = 1$). Then:*

(i) $A \cap B = 1$ and $\mathbb{Z}(G) \subseteq \mathbb{L}_G(A) \subseteq A$.

(ii) $\mathbb{C}_G(A) = A$ and $\mathbb{Z}(AG') = \mathbb{L}_G(A)$.

(iii) $A \cap G' \subseteq \mathbb{L}_G(A)$ and $A \cap G' \trianglelefteq G$.

Proof. (i) See 2.5(i), (ii).

(ii) $A \subseteq \mathbb{C}(G) = AC$, $C = \mathbb{C}_G(A) \cap B \subseteq \mathbb{Z}(G) \cap B = 1$, and so $\mathbb{C}_G(A) = A$, and $\mathbb{Z}(AG') \subseteq A$. On the other hand, $\mathbb{Z}(AG') \trianglelefteq G$ implies $\mathbb{Z}(AG') \subseteq \mathbb{L}_G(A)$. Now, $\mathbb{Z}(AG') = \mathbb{L}_G(A)$ by 2.9.

(iii) We have $A \cap G' = \mathbb{L}_G(A) \cap G'$, and so $A \cap G' \trianglelefteq G$. The rest is clear from (ii) and 2.9 (see also 2.6(iii)). ▲

2.12 Proposition. *Suppose that $\mathbb{Z}(G) = 1$. Then:*

(i) $A \cap B = 1$.

(ii) $\mathbb{C}_G(A) = A$ and $\mathbb{C}_G(B) = B$.

(iii) $\mathbb{L}_G(A) = \mathbb{Z}(AG')$ and $\mathbb{L}_G(B) = \mathbb{Z}(BG')$.

(iv) $A \cap G' \subseteq \mathbb{L}_G(A)$ and $B \cap G' \subseteq \mathbb{L}_G(B)$.

(v) $A \cap G' \trianglelefteq G$ and $B \cap G' \trianglelefteq G$.

Proof. See 2.11. ▲

2.13 Lemma. *Put $L = \mathbb{L}_G(A)$ and $C = \mathbb{C}_G(L)$. Then:*

(i) $A \subseteq C \trianglelefteq G$ and $C = AB_1$, where $B_1 = B \cap C$.

(ii) $L \subseteq \mathbb{Z}(C) \trianglelefteq G$.

(iii) If $\mathbb{L}_C(B_1) = 1$, then $\mathbb{Z}(C) = L$.

(iv) If $\mathbb{L}_G(B) = 1$, then $\mathbb{L}_C(B_1) = 1$.

(v) If $\mathbb{L}_C(B) = 1$, $A \trianglelefteq C$ and if B_1 is characteristic in LB_1, then $A = C$ and $A \trianglelefteq G$.

Proof. (i) and (ii). Obvious.

(iii) We have $\mathbb{Z}(C) = (\mathbb{Z}(C) \cap A)(\mathbb{Z}(C) \cap B_1))$ and $\mathbb{Z}(C) \cap B_1 \subseteq \mathbb{L}_C(B_1) = 1$. Thus $\mathbb{Z}(C) \subseteq L$.

(iv) If $b \in \mathbb{L}_C(B_1)$, then $b^a \in B$ for every $a \in A$, $b \in \mathbb{L}_G(B) = 1$ and $b = 1$.

(v) First, $A \trianglelefteq C$ implies $C' \subseteq A$. But then $C \trianglelefteq G$ implies $C' \trianglelefteq G$ and $C' \subseteq$ $\subseteq L \subseteq LB_1 \subseteq C$. Consequently, $LB_1 \trianglelefteq C$ and $B_1 \trianglelefteq C$. But $\mathbb{L}_C(B_1) = 1$ implies $B_1 = 1$ and $C = A$. ▲

2.14 Proposition. *Assume that B is finite, $\mathbb{L}_G(B) = 1$ and if p is a prime such that $p \mid \operatorname{card}(B)$, then $\mathbb{L}_G(A)$ does not contain any element of order p. Then $A \trianglelefteq G$.*

Proof. We proceed by induction on $\operatorname{card}(B)$. Assume, on the contrary, that $A \ntrianglelefteq G$. It follows from 2.13(v) that $A \ntrianglelefteq C$ (we have $LB_1 = L \times B_1$). Now, by induction, $B_1 = B$, $C = G$ and $L = \mathbb{Z}(G)$.

Put $N = \mathbb{N}_G(B)$. By 1.15, $N = B\mathbb{Z}(G) = B \times L$. Further, $\mathbb{L}_G(N) = L \times B_2$, $B_2 = N \cap B$. Of course, B_2 is characteristic in $\mathbb{L}_G(N)$, and hence $B_2 \trianglelefteq G$ and $B_2 = 1$. Thus $\mathbb{L}_G(N) = L$. Finally, $\overline{G} = G/L = (A/L)(N/L) = \overline{A} \cdot \overline{B}$, $\mathbb{L}_{\overline{G}}(\overline{A}) =$ $= 1 = \mathbb{L}_{\overline{G}}(\overline{B})$ and $\overline{G} = 1$ by 2.8(i). This means that $L = G$ and $A = G$, a contradiction. ▲

2.15 Remark. Assume that $A \ntrianglelefteq G$, the primary 2-component of the torsion part of A is cyclic (or quasicyclic) and that B is a finite 2-group, with $\mathbb{L}_G(B) = 1$. By

2.14, $L = \mathbb{L}_G(A)$ contains some elements of order 2. However, the 2-socle S of $L$is cyclic, $\mathrm{card}(S) = 2$, and $S \trianglelefteq G$. On the other hand, every normal 2-element subgroup is in the center. Thus $S \subseteq \mathbb{Z}(G)$ and $\mathbb{Z}(G) \neq 1$.

2.16 Proposition. *Assume that B is a finite p-group for a prime p and that $\mathbb{L}_G(B) = 1$. Then either $A \trianglelefteq G$ or $\mathbb{Z}(G) \neq 1$.*

Proof. Assume $A \ntrianglelefteq G$. Let $L = \mathbb{L}_G(A)$. B 2.14, the p-socle P of L is non-trivial and, of course, $P \trianglelefteq G$. Now, take $e \in P$, $e \neq 1$, and put $E = \langle e^b;\ b \in B \rangle$. Then E is a finitely generated p-elementary abelian group and consequently, E is finite. Clearly, $E \trianglelefteq G$ and we put $K = EB$. Then K is finite p-group, and $K \neq B$. Consequently, K is nilpotent and $N = \mathbb{N}_K(B) \neq B$. But $N \subseteq \mathbb{N}_G(B) = B\mathbb{Z}(G)$. Thus $\mathbb{Z}(G) \neq 1$. ▲

3. Auxiliary results (C)

3.1. Throughout this section, let G be a group such that $G = AH$, where A is an abelian subgroup of G and H is a finite cyclic subgroup with $\mathbb{L}_G(H) = 1$ and $\mathrm{card}(H) = n \geq 2$.

Now, $A \cap H = 1$, $L = \mathbb{L}_G(A) \neq 1$ (by 2.8(i)) and $\mathbb{Z}(G) \subseteq L$.

In the sequel, fix a generator $w \in H$. Then there are mappings $\varrho : A \to A$ and $\sigma : A \to \{0, 1, \dots, n-1\}$ such that $wa = \varrho(a) w^{\sigma(a)}$ for every $a \in A$. We put $A_i = \{a \in A;\ \sigma(A) = i\}$ for every $0 \leq i \leq n-1$.

3.2 Lemma. *(i) ϱ is a permutation of order n of A.*

(ii) $A_0 = \emptyset$ and A is the disjoint union of the sets $A_1, \dots, A_{n-1}$.

(iii) $A_1 = \mathbb{L}_G(A)$, $\varrho(A_1) = A_1$, and $\varrho \restriction A_1$ is an automorphism of A_1.

(iv) $A \cap G' \subseteq A_1$.

(v) $\mathbb{Z}(G) = \{a \in A;\ \varrho(a) = a\} \subseteq A_1$.

(vi) If $A \cap G' = 1$, then $\mathbb{Z}(G) = A_1$ and $\varrho(a) = a$ for every $a \in A_1$.

(vii) $A \trianglelefteq G$ if and only if $\sigma(a) = 1$ for every $a \in A$.

Proof. (i) We have $\varrho = q_w$, where q_w is the permutation defined in 1.4 and 1.5(i).

(ii) Since $A \cap H = 1$, we have $A_0 = \emptyset$ and the rest is clear.

(iii) and (iv) First, $A \cap G' \subseteq L = \mathbb{L}_G(A)$ by 2.11(iii). If $a \in L$, then $\varrho(a) w^{\sigma(a)-1} = waw^{-1} \in A$, and so $w^{\sigma(a)-1} \in A \cap H = 1$, $\sigma(a) = 1$ and $a \in A_1$. Conversely, if $a \in A_1$, then $wa = \varrho(a) w$, and hence $\varrho(a) a^{-1} = waw^{-1}a^{-1} \in$ $\in A \cap G' \subseteq L \subseteq A_1$ and $\varrho(a) \in A_1$. Thus $\varrho(A_1) \subseteq A_1$ and, since ϱ is a permutation of finite order, it follows that $\varrho(A_1) = A_1$ (the fact that $\varrho \restriction A_1$ is in automorphism of A_1 is obvious). Finally, if $1 \leq i$, then $w^i a w^{-i} =$ $= w^{i-1} \varrho(a) w^{1-i} = w^{i-2} \varrho^2(a) w^{2-i} = \dots = \varrho^i(a) \in A_1$. This means that $A_1 \subseteq L$, and so $A_1 = L$.

(v) If $a \in \mathbb{Z}(G)$, then it is clear that $\varrho(a) = a$ and $\sigma(a) = 1$. Conversely, if $a \in A$ and $\varrho(a) = a$, then $a^{-1}wa = a^{-1}aw^{\sigma(a)} = w^{\sigma(a)}$, $a \in \mathbb{N}_G(H) = \mathbb{Z}(G)H$ and $a \in \mathbb{Z}(G)$.

(iv) This is clear from (v) and the proof of (iii).

(vii) This is clear. ▲

3.3 Lemma. *Let a, $b \in A$. Then:*

(i) $\varrho(ab) = \varrho(a)\varrho^{\alpha(a)}(b)$.

(ii) $\sigma(ab) \equiv \sigma\varrho^{\sigma(a)-1}(b) + \sigma\varrho^{\sigma(a)-2}(b) + \dots + \sigma\varrho(b) + \sigma(b)$ *(mod n).*

(iii) $\varrho(a)^{-1} = r^{s(a)}(a^{-1})$.

(iv) If $\sigma(a) = \sigma(b)$, *then* $ab^{-1} \in A_1$ *and* $\varrho(ab^{-1}) = \varrho(a)\varrho(b)^{-1} \in A_1$.

Proof. (i) and (ii). We have $wab = \varrho(a)w^{\sigma(a)}b = \varrho(a)w^{\sigma(a)-1} \cdot \varrho(b) = \dots = \varrho(a)\varrho^{\sigma(a)}(b)w^i$, $i = \sigma\varrho^{\sigma(a)-1}(b) + \dots + \sigma(b)$.

(iii) This follows from (i) for $b = a^{-1}$.

(iv) By (i) and (iii), $\varrho(ab^{-1}) = \varrho(a)\varrho^i(b^{-1}) = \varrho(a)\varrho(b)^{-1}$, $i = \sigma(a)$. Further, $wab^{-1} = \varrho(ab^{-1})w^j$, where $j = \sigma(ab^{-1})$. On the other hand, $wab^{-1} = \varrho(a)w^ib^{-1}$, and so $\varrho(b)^{-1}w^j = w^ib^{-1}$, $w^jb = \varrho(b)\ w^i = wb$, $w^j = w$, $j = 1$. Thus $\sigma(ab^{-1}) = 1$ and $ab^{-1} \in A_1$. ▲

3.4 Lemma. *Let* $1 \leq i\, n - 1$ *be such that* $A_i \neq \emptyset$. *Then:*

(i) $A_i = A_1 b$ *for every* $b \in A_i$.

(ii) $\varrho^{i-1}(a) = a$ *and* $w^{i-1}a = aw^{i-1}$ *for every* $a \in A_1$.

(iii) $\varrho(A_i) = A_j$ *for some* $1 \leq j \leq n - 1$.

Proof. (i) If $a \in A_1$, then $\sigma(ab) = \sigma(b) = i$ by 3.3(ii), and hence $ab \in A_i$. Consequently, if $c \in A_i$, then $cb^{-1} \in A_1$ by 3.3(iv).

(ii) If $b \in A_i$, then $\varrho(b)\varrho^i(a) = \varrho(ba) = \varrho(ab) = \varrho(a)\varrho(b) = \varrho(b)\varrho(a)$ by 1.3(i). Consequently, $a = \varrho^{i-1}(a)$ and $w^{i-1}a = \varrho^{i-1}(a)w^{i-1} = aw^{i-1}$.

(iii) Let a, $b \in A_i$. Then $\varrho(ab^{-1}) = \varrho(a)\varrho(b)^{-1} \in A_1$ by 1.3(iv), and so $\varrho(a)$, $\varrho(b) \in A_j$ for suitable j (see 1.4(i)). We have $\varrho(A_i) \subseteq A_j$ and, since the index $[A : A_1] \leq n - 1$ is finite, in fact $\varrho(A_i) = A_j$. ▲

3.5. $1 \leq i_1 < i_2 < \dots < i_m \leq n - 1$ be all the indices with $A_{i_j} \neq \emptyset$. Then $i_1 = 1$ and, by 1.4(i), $A_{i_1} = A_1, A_{i_2}, \dots, A_{i_m}$ are just all blocks(cosets) modulo A_1 in A, $A/A_1 = \{A_{i_1}, \dots, A_{i_m}\}$ and $[A : A_1] = m$.

Let r_1 denote the smallest number such that $1 \leq r_1 \leq n$ and $\varrho^{r_1}(a) = a$ for every $a \in A_1$. Further, put $r_2 = \gcd(n, i_2 - 1, i_3 - 1, \dots, i_m - 1)$, $r_2 = n$ if $m = 1$ and $H_j = \langle w^{r_j} \rangle$, $G_j = AH_j$, $j = 1, 2$.

3.6 Lemma. *(i)* $r_1 \mid r_2$ *and* $r_1 \mid n$.

(ii) G_1 *and* G_2 *are normal subgroups of* G.

(iii) $G' \subseteq G_2 \subseteq G_1 \subseteq G$.

(iv) $H_2 \subseteq H_1$ *and* $\mathbb{L}_{G_j}(H_j) = 1$, $j = 1, 2$.

(v) $\mathbb{Z}(G_j) = A_1$, $j = 1, 2$.

Proof. (i) Use 3.2(i) and 3.4(ii).

(ii) and (iii). Put $r = r_j$, $1 \le j \le 2$. If $a \in A$, then $w^r a = \varrho^r(a) w^k$, $k = \sigma\varrho^{r-1}(a) + \ldots + \sigma\varrho(a) + \sigma(a) = (\sigma\varrho^{r-1}(a) - 1) + \ldots + (\sigma\varrho(a) - 1) + (\sigma(a) - 1) + r$. Clearly, r divides k, and so $w^k \in H_j$. Consequently, $H_j A \subseteq AH_j$ and $H_j A = AH_j = G_j$ is a subgroup of G. Further, $a^{-1} w^r a = a^{-1}\varrho^r(a) w^k$, so that $a^{-1}w^r a \in G_j$. We see that $x^{-1}H_j x \subseteq G_j$ for every $x \in G$. Similarly, $waw^{-1} = \varrho(a) w^{\sigma(a)-1} \in G_j$ (since r divides $\sigma(a) - 1$) and, again, $x^{-1}Ax \subseteq G_j$. Now, it is clear that $G_j \trianglelefteq G$ and $G' \subseteq G_j$.

(iv) Since $A \subseteq G_j$, we have $\mathbb{L}_{G_j}(H_j) \subseteq \mathbb{L}_G(H) = 1$.

(v) By 2.4(iv), $\mathbb{Z}(G_j) \subseteq A$, so that $\mathbb{Z}(G_j) \subseteq \mathbb{L}_G(A) = A_1$. On the other hand, if $a \in A_1$, then $w^r a = \varrho^r(a) w^r = aw^r$, which shows that $a \in \mathbb{Z}(G_j)$. ▲

3.7. Put $G_3 = AG'$. Then $G_3 = AH_3$, $H_3 = G_3 \cap H$, $H_3 = \langle w^{r_3} \rangle$, where $1 \le r_3 \le n$ and $r_3 \mid n$.

3.8 Lemma. *(i)* $r_2 \mid r_3$.

(ii) $G' \subseteq G_3 \subseteq G_2$ *and* $H_3 \subseteq H_2$.

(iii) $\mathbb{Z}(G_3) = A_1$.

Proof. Easy. ▲

3.9 Lemma. *The following conditions are equivalent:*

(i) $G_1 = G$.

(ii) $H_1 = H$.

(iii) $r_1 = 1$.

(iv) $\varrho(a) = a$ *for every* $a \in A_1$.

(v) $\mathbb{Z}(G) = A_1$.

Proof. Easy. ▲

3.10 Lemma. *The following conditions are equivalent:*

(i) $G_3 = A$.

(ii) $H_3 = 1$.

(iii) $r_3 = n$.

(iv) $G' \subseteq A$.

(v) $A_1 = A$.

(vi) $A \trianglelefteq G$.

Proof. Easy. ▲

3.11. Since $A_1 \subseteq \mathbb{L}_G(A_1H)$, we have $\mathbb{L}_G(A_1H_0)$ for $H_0 = H \cap \mathbb{L}_G(A_1H) = \langle w^{r_0} \rangle$, $1 \le r_0 < n$, $r_0 \mid n$. Further, $G_0 = AH_0$ is a subgroup of G (since $G_0 = A \cdot A_1H_0$) and $A_1H_0 \subseteq \mathbb{L}_G(G_0)$. Clearly, $\mathbb{L}_{G_0}(H_0) = 1$.

3.12 Lemma. *The following conditions are equivalent for* $k \ge 1$:

(i) $r_0 \mid k$.

(ii) $\varrho^k(a)a^{-1} \in A_1$ *for every* $a \in A$.

Proof. If $k = lr_0$, then $w^k \in H_0$ and $a^{-1}w^k a \in A_1H_0$. However, $w^k a = \varrho^k(a)u$ for some $u \in H$, and so $a^{-1}\varrho^k(a) \in A_1$. Conversely, if (ii) is true, then $a^{-1}w^k a \in A_1H$ and so $w^k \in A_1H_0$, $w^k \in H_0$ and $r_0 \mid k$. ▲

3.13 Lemma. *The following conditions are equivalent:*

(i) $A_1H \trianglelefteq G$.
(ii) $G' \subseteq A_1H$.
(iii) $r_0 = 1$.
(iv) $H_0 = H$.
(v) $\varrho(a)a^{-1} \in A_1$ *for every* $a \in A$.
(vi) $\varrho(A_i) = A_i$ *for every* $1 \le i \le n - 1$.

Proof. Easy (use 3.12). ▲

3.14. Denote by φ the natural projection of G onto $\bar{G} = G/A_1H_0$. Then $\bar{G} = \bar{A} \cdot \bar{H}$, where $\bar{A} = \varphi(A) = AH_0/A_1H_0 \cong A/A_1$, $\bar{H} = \varphi(H) = A_1H/A_1H_1 \cong$ $\cong H/H_0$, $\mathbb{L}_G(\bar{H}) = 1$ and $\bar{H}$ is a cyclic group of order r_0.

(i) Assume that $r_0 \ge 2$. Again, there are a permutation $\bar{\varrho}$ of $\bar{A}$ and a mapping $\bar{\sigma} : \bar{A} \to \to \{1, 2, \ldots, r_0 - 1\}$ such that $\varphi(wa) = \varphi(w)\varphi(a) = \bar{\varrho}\varphi(a) \cdot \varphi(w)^{\bar{\sigma}\varphi(a)} =$ $= \bar{\varrho}\varphi(a) \cdot \varphi(w^{\bar{\sigma}\varphi(a)})$ for every $a \in A$. Of course, $\varphi(wa) = \varphi\varrho(a) \cdot \varphi(w^{\sigma(a)})$, and therefore $\bar{\varrho}\varphi(a) = \varphi\varrho(a)$ and r_0 divides $\sigma(a) - \bar{\sigma}\varphi(a)$.

Now, put $B = \{a \in A;\ r_0 \mid (\sigma(a) - 1)\}$ and $C = \varphi^{-1}(\bar{A}_1) = \varphi^{-1}(\mathbb{L}_{\bar{G}}(\bar{A}))$. Then $\bar{A}_1 = \varphi(C)$, $B = C \cap A$ is a subgroup of A and $C = BH_0 = \mathbb{L}(G_0)$. Clearly, $A_1 \subseteq B$ and $C \trianglelefteq G$. Moreover, since $\bar{A}_1 \ne 1$, we have $B \ne A$ and $C \ne A_1H_0$. Finnaly, $B \ntrianglelefteq G$, (otherwise $B = A_1$) and $H_0 \ne 1$. It follows that $r_0 \le n - 1$.

(ii) If $r_0 = 1$, then we put $B = A$ and $C = G$.

3.15 Lemma. $r_0 \le n - 1$ *and* $H_0 \ne 1$.

Proof. See 3.14. ▲

3.16 Lemma. *The following conditions are equivalent:*

(i) $B = A$.
(ii) $r_0 \mid r_2$ *(resp.,* $G_2 \subseteq G_0$ *or* $H_2 \subseteq H_0$*).*
(iii) $r_0 \mid r_3$ *(resp.* $G_3 \subseteq G_0$ *or* $H_3 \subseteq H_0$ *or* $G' \subseteq G_0$*).*
(iv) $G_0 \trianglelefteq G$.
(v) $A_1H_j \trianglelefteq G$ *for at least one* j, $1 \le j \le 3$.
(vi) $A_1H_j \trianglelefteq G$ *for every* j, $2 \le j \le 3$.
(vii) $\varrho^{s(a)-1}(b)b^{-1} \in A_1$ *for all* $a, b \in A$.
(viii) $\varrho^{\sigma(a)-1}(A_i) = A_i$ *for every* $1 \le i \le n - 1$.
(ix) $\varrho^{r_2}(A_i) = A_i$ *for every* $1 \le i \le n - 1$.
(x) $\varrho^{r_3}(A_i) = A_i$ *for every* $1 \le i \le n - 1$.

Proof. First, (i) is equivalent to (ii) by 3.14.; (ii) implies (iii), since $r_2 \mid r_3$; (iii) is equivalent to (iv), since $G_0 \trianglelefteq G$ iff $G' \subseteq G_0$; (ii) and (v) are equivalent by 3.12.

Further, if $G_0 \trianglelefteq G$, then $C = BH_0 = \mathbb{L}_G(G_0) = G_0$, and so $B = A$ (see 3.14). Now, it is clear that the conditions (i), (ii), (iii), (iv) and (vii) are equivalent.

Assume that $A_1H_j \trianglelefteq G$ for some $1 \le j \le 3$ and put $r = r_1$. For $a \in A$, $a^{-1}w^r a \in A_1H_j$. However, $a^{-1}w^r a = a^{-1}\varrho^r(a)u$, $u \in H$, and so $a^{-1}\varrho^r(a) \in A_1$. Now $r_0 \mid r$ by 3.12, and hence $r_0 \mid r_3$. We have shown that (v) implies (iii).

Let $2 \le j \le 3$ be such that r_0 divides $r = r_j$. Then, for every $a \in A$, $a^{-1}w^r a = = a^{-1}\varrho^r(a)u \in AH_j \cap A_1H = A_1H_j$ (use 3.12), and so $a^{-1}H_j a \subseteq A_1H_j$ and $a^{-1}A_1H_j a \subseteq A_1H_j$.

The rest is clear. ▲

3.17. Put $\tilde{G} = G/A_1$, $\tilde{A} = A/A_1$ and $\tilde{H} = HA_1/H_1 \cong H$. Then $\tilde{G} = \tilde{A}\tilde{H}$, $\mathbb{L}_{\tilde{G}}(\tilde{A}) = 1$ and, by 3.4, ϱ indces a permutation $\tilde{\varrho}$ of $\tilde{A}$ and σ induces an injective mapping $\tilde{\sigma} : \tilde{A} \to \{1, 2, \dots, n-1\}$ such that $\psi(w)\psi(a) = \psi(wa) = \psi\varrho(a)(w^{\sigma(a)}) = = \tilde{\varrho}\psi(a) \cdot \psi(w)^{\tilde{\sigma}\psi(a)}$ for all $a \in A$; here, $\psi : G \to \tilde{G}$ is the natural projection. Further, by 3.3, we have $\tilde{\varrho}(\psi(a)\psi(b)) = \tilde{\varrho}\psi(a) \cdot \tilde{\varrho}^{\tilde{\sigma}\psi(a)}(\psi(b))$ for all a, $b \in \tilde{A}$, $\tilde{r}(1) = 1$ and $m = \operatorname{card}(\tilde{A}) = \operatorname{card}(\tilde{\sigma}(\tilde{A}))$. According to 3.12, the order of $\tilde{\varrho}$ s just r_0; notice that $r_0 \le n - 1$. By 3.11, $\mathbb{L}_{\tilde{G}}(\tilde{H}) = \tilde{H}_0 = A_1H_0/A_1 \cong H_0$. Since $A \cap G' \subseteq A_1$, we have $\tilde{A} \cap (\tilde{G})' = 1$.

Now, consider the following three conditions:

(R1) $\tilde{\varrho}$ is an automorphism of $\tilde{A}$;

(R2) $\tilde{\varrho} = \mathrm{id}_{\tilde{A}}$;

(R3) $\tilde{\sigma}$ is a homomorphism of $\tilde{A}$ into $\underline{Z}_n^*$ (the multiplicative group of invertible elements of the ring $\underline{Z} = \underline{Z}/\underline{Z}n$).

3.18 Lemma. *(R1) is true if and only if the equivalent conditions of 3.16 are satisfied.*

Proof. If (R1) is true and if $a \in A$ and $b \in A_i$, then $\varrho(a)b \equiv \varrho(a\varrho^{-1}(b))$ (mod A_1). On the other hand, $\varrho(a\varrho^{-1}(b)) = \varrho(a)\varrho^{\sigma(a)-1}(b)$ by 1.3. This implies that $\varrho^{\sigma(a)-1}b \in A_i$ and $\varrho^{\sigma(a)-1}(b)b^{-1} \in A_i$.

The rest is clear. ▲

3.19 Lemma. *(R2) is true if and only if the equivalent conditions of 3.13 are satisfied.*

Proof. Obvious. ▲

3.20 Lemma. *(R3) is true if and only if $\sigma(ab) \equiv \sigma(a)\sigma(b)$ (mod n) for all $a, b \in A$ (i.e., $\sigma : A \to \underline{Z}_n^*$ is a homomorphism).*

Proof. Obvious. ▲

3.21 Lemma. *(R2) implies (R1) and (R3).*

Proof. If (R2) is true and a, $b \in A$, then $\sigma\varrho^k(b) \equiv \sigma(b)$ for every $k \ge 1$, and hence $\sigma(ab) \equiv \sigma(a)\sigma(b)$ (mod n) by 3.3. ▲

3.22 Lemma. *If (R2) is true, then either $A \trianglelefteq G$ or $\mathbb{Z}(G) \neq 1$.*

Proof. Put $\xi(a, i) = \varrho^i(a)a^{-1} \in A$ (see 3.3(iv)) for all $a \in A$ and $i \geq 0$. Then $\xi(a, 0) = 1$, $\xi(a, 1) = \varrho(a)a^{-1} = b$ and, by induction on i, we check that $\xi(a, i) = b\varrho(b) \dots \varrho^{i-1}(b)$ for every $i \geq 1$. Indeed, $\xi(a, i + 1) = \varrho^{i+1}(a)a^{-1} = \varrho^{i+1}(a)\varrho(a)^{-1}b = \varrho(\varrho^i(a)a^{-1})b = \varrho\xi(a,i)b = \varrho(b\varrho(b) \dots \varrho^{i-1}(b))b = \varrho(b)\varrho^2(b) \dots \varrho^i(b)b$ (use 3.3(iv) and the fact that $\varrho \restriction A_1$ is an automorphism of A_1).

Now, $\varrho\xi(a, r_1) = \varrho(b\varrho(b) \dots \varrho^{r_1-1}(b)) = \varrho(b)\varrho^2(b) \dots \varrho^{r_1}(b) = \varrho(b) \dots \varrho^{r_1-1}(b)b = \xi(a, r_1)$, since $b \in A_1$ and $\varrho^{r_1}(b) = b$. By 3.2(v), $\xi(a, r_1) \in \mathbb{Z}(G)$. In particular, if $\mathbb{Z}(G) = 1$, then $\varrho^{r_1}(a)a^{-1} = \xi(a, r_1) = 1$ and $\varrho^{r_1}(a) = a$ for every $a \in A$. This implies that $r_1 = n$ and $m = 1$ (otherwise r_1 would divide $r_2 - 1$ and then $r_1 = 1$ and $\mathbb{Z}(G) = A_1$) and $A \trianglelefteq G$. ▲

3.23 Lemma. *G' is generated by the elements $\varrho^k(a)a^{-1}w^l$, $l = \sigma(a) + \sigma\varrho(a) + \dots + \sigma\varrho^{k-1}(a) - k$, $1 \leq k \leq n - 1$, $a \in A$.*

Proof. We have $G' = \langle [A, H] \rangle$. ▲

3.24 Lemma. *Assume that $n = p$ is a prime number and that $A \ntrianglelefteq G$ (or $m \geq 2$). Then:*

(i) $p \geq 3$, $m \mid p - 1$ and A/A_1 is cyclic.
(ii) $r_0 = r_1 = r_2 = 1$.
(iii) $\mathbb{Z}(G) = A_1$ and $\varrho(a) = a$ for every $a \in A_1$.
(iv) The condition (R2) is satisfied.
(v) $G' \subseteq A_1H = \mathbb{Z}(G)H = \mathbb{N}_G(H)$.

Proof. Since r_2 divides both $i_2 - 1$ and n, we have $r_2 = 1$ and consequently also $r_1 = 1$. Further, $r_0 = 1$, since $r_0 \mid p$ and $r_0 \leq p - 1$ by 3.14, and so the conditions (R2) and (R2) are satisfied by 3.19 and 3.2.1. In particular, σ is a homomorphism of A into $\underline{Z}_p^* \cong \underline{Z}_{p-1}(+)$, and therefore $m \mid p - 1$. ▲

3.25 Lemma. *Assume that $n = p^2$ for a prime p. Then at least one of the following three cases takes place:*

(i) $r_1 = r_2 = 1$ and $\mathbb{Z}(G) = A_1$.
(ii) $r_0 = 1$ and (R2) is satisfied.
(iii) $A \trianglelefteq G$.

Proof. Assume $A \ntrianglelefteq G$ and $r_2 \neq 1$. Then $m \geq 2$, $r_2 = p$ and p divides $i_j - 1$ for every $1 \leq j \leq m$ (see 3.5). Thus $1 \leq i_j = l_j \cdot p + 1 \leq p^2 - 1$ and $m \leq p$. On the other hand, $\tilde{\varrho}$ is a permutation of $\tilde{A}$, $\mathrm{card}(\tilde{A}) = m$, $\tilde{\varrho}(1) = 1$ and the order of $\tilde{\varrho}$ is r_0. Now, $\tau = \tilde{\varrho} \restriction I$, $I = \tilde{A} \setminus \{1\}$, is a permutation of I, $\mathrm{card}(I) = m - 1 \leq p - 1$ the order of τ is r_0 and $r_0 \mid p$. From this, $r_0 = 1$. ▲

3.26 Lemma. *(i) If $m = [A : A_1]$ is a prime number, then the condition (R1) is satisfied.*

(ii) If $m \leq 2$ then, the condition (R2) is satisfied.

Proof. (i) Since m is prime, A_1 is a maximal subgroup of A. But $A_1 \subseteq N \subseteq A$ and $A_1 \neq B$ (see 3.16). Thus $B = A$ and (R1) is true (3.18, 3.16).

(ii) $\tilde{\varrho}$ is a permutation of $\tilde{A}$ and $\operatorname{card}(\tilde{A}) \leq 2$. Consequqntly $\tilde{\varrho} = id$. ▲

4. Auxiliary results (D)

4.1. This section is a continuation of the preceding one. Moreover, we will asume here that the condition (R2) is satisfied (see 3.17, 3.19, 3.21, 3.22) and that $A \ntrianglelefteq G$. Then $m \geq 2$, $\varrho(A_i) = A_i$ for every $1 \leq i \leq n-1$, $G' \subseteq A_1H$ and σ may be viewed as a homomorphism of A into $\underline{Z}_n^*$. We have $\operatorname{Ker}(\sigma) = A_1$, and so $m = [A : A_1]$ divides $\varphi(n)$, φ being the Euler function.

For $a \in A$ and $i \geq 0$, put $\xi(a, i) = \varrho^i(a)a^{-1}$ (cf. the proof of 3.22). Then $\xi(a, i) \in A_1$, $\xi(a, 0) = 1$, $\lambda(a) = \xi(a, 1) = \varrho(a)a^{-1} = b$ and $\xi(a, i) = b\varrho(b) \ldots \varrho^{i-1}(b)$ for every $i \geq 1$. Finally, $\kappa(a) = \xi(a, r) \in \mathbb{Z}(G)$, $r = r_1$.

4.2 Lemma. *(i) $1 \leq r \leq n-1$, $r \mid n$ and $2 \leq n/r$.*

(ii) $\kappa(a) = \lambda(a)\varrho\lambda(a) \ldots \varrho^{r-1}\lambda(a) \in \mathbb{Z}(G)$ for every $a \in A$.

(iii) $\mathbb{Z}(G) \neq 1$.

(iv) $\xi(a, kr) = \kappa(a)^k$ for all $a \in A$ and $k \geq 0$.

(v) $\kappa(a) = \kappa(b)$ for all $1 \leq i \leq n-1$ and $a, b \in A_i$.

(vi) If $1 \leq i, j \leq n-1$, $a \in A_i$ and $b \in A_j$, then $\xi(\alpha, j-1) = \xi(b, i-1)$.

Proof. (i), (ii) and (iii). See 4.1 and 4.22.

(iv) This is clear from 4.2 and the fact that $\varrho^r \restriction A_1 = \mathrm{id}$.

(v) Since $\varrho(A_i) = A_i$, we have $\varrho^r(ab^{-1}) = \varrho^r(a)\varrho^r(b)^{-1}$ by 3.3(iv). On the other hand, $ab^{-1} \in A_1$, and so $\varrho^r(ab^{-1}) = ab^{-1}$. Now, $\kappa(a) = \varrho^r(a)a^{-1} = \varrho^r(b)b^{-1} = \kappa(b)$.

(vi) $\xi(a, j)\xi(\alpha, 1)^{-1} = \varrho^j(a)\varrho(a)^{-1} = \varrho(\varrho^{j-1}(a)a^{-1}) = \varrho\xi(a, j-1)$ and $\xi(b, i)\xi(b, 1)^{-1} = \varrho\xi(b, i-1)$ by 3.3(iv). On the other hand, $\varrho(a)\xi(b, i)b = \varrho(a)\varrho^i(b) = \varrho(ab) = \varrho(ba) = \varrho(b)\varrho^j(a) = \varrho(b)\xi(a, j)a$. Thus $\xi(a, j)\xi(a, 1)^{-1} = \xi(b, i)\xi(b, 1)^{-1}$ and we see that $\xi(a, j-1) = \xi(b, i-1)$. ▲

4.3 Lemma. *(i) $\lambda\varrho(a) = \varrho\lambda(a)$ for every $a \in A$.*

(ii) $\lambda(ab) = \lambda(a)\lambda(b)$ for all $a \in A_1$, $b \in A$ and $\lambda \restriction A_1$ is an endomorphism of A_1.

(iii) $\lambda(ab^{-1}) = \lambda(a)\lambda(b)^{-1}$ for all $1 \leq i \leq n-1$ and $a, b \in A_i$.

(iv) $\mathbb{Z}(G) = \{a \in A;\ \lambda(a) = a\}$.

(v) $\kappa\varrho(a) = \varrho\kappa(a) = \kappa(a)$ for every $a \in A$.

(vi) $\kappa(a)^{(\sigma(b)-1)/r} = \kappa(b)^{(\sigma(a)-1)/r}$ for all $a, b \in A$.

(vii) $\lambda(ab) = \lambda(a)\lambda(b)\kappa(b)^{(\sigma(a)-1)/r} = \lambda(a)\lambda(b)\kappa(a)^{(\sigma[b)-1)/r}$ for all $a, b \in A$.

(viii) $\kappa(a)^{n/r} = 1$ for every $a \in A$.

(ix) $\kappa(a) = 1$ *for every* $a \in A_1$.

(x) *If* $1 \leq k \leq (n - r)/r$, *then* $\kappa(a)^k \neq 1$ *for at least one* $a \in A$.

(xi) $\kappa(ab) = \kappa(a)\kappa(b)^{\sigma(a)} = \kappa(a)^{\sigma/b} \cdot \kappa(b)$ *for all* $a, b \in A$.

Proof. (i) $\lambda\varrho(a) = \varrho^2(a)\varrho(a)^{-1} = \varrho(\varrho(a)a^{-1}) = \varrho\lambda(a)$ by 1.3(iv).

(ii) $\lambda(ab) = \varrho(ab)a^{-1}b^{-1} = \varrho(a)a^{-1}\varrho(b)b^{-1} = \lambda(a)\lambda(b)$.

(iii) $\lambda(ab^{-1}) = \varrho(ab^{-1})ba^{-1} = \varrho(a)a^{-1} \cdot \varrho(b^{-1})b = \lambda(a)\lambda(b^{-1})$ by 1.3(iv)

(iv) See 1.2(v).

(v) Since $\kappa(a) \in \mathbb{Z}(G)$, we have $\varrho\kappa(a) = \kappa(a)$. Further, since $\sigma\varrho(a) = \sigma(a)$, we also have $\kappa\varrho(a) = \kappa(a)$.

(vi) $\kappa(a)^{(\sigma(b)-1)/r} = \xi(a, \sigma(b) - 1) = \xi(b, \sigma(a) - 1) = \kappa(b)^{(\sigma(a)-1)/r}$ by 2.3(iv), (vi).

(vii) $\lambda(ab) = \varrho(ab)a^{-1}b^{-1} = \varrho(a)a^{-1} \cdot \varrho^{\sigma(a)}(b)b^{-1} = \lambda(a)\xi(b, \sigma(a)) = \lambda(a)\lambda(b)\varrho\xi(b, \sigma(a) - 1) = \lambda(a)\lambda(b)\varrho(\kappa(b)^{(\sigma(a)-1)/r}) = \lambda(a)\lambda(b)\kappa(b)^{(\sigma(a)-1)/r}$ (use the fact that $\varrho\xi(b, \sigma(a) - 1) = \varrho(\varrho^{\sigma(a)-1}(b)b^{-1}) = \varrho^{\sigma(a)}(b)\varrho(b)^{-1} = \varrho^{\sigma(a)}(b)b^{-1} \cdot \varrho(b)^{-1}b = \xi(b, \sigma(a))\lambda(b)$).

(viii) $\kappa(a)^{n/r} = \xi(a, r)^{n/r} = \xi(a, n) = \varrho^n(a)a^{-1} = 1$.

(ix) This is obvious.

(x) We have $\varrho^{rk} \neq \mathrm{id}_A$, and therefore $\kappa(a)^k = \xi(a, rk) = \varrho^{rk}(a)a^{-1} \neq 1$ for at least one $a \in A$.

(xi) By (vii), $\varrho\lambda(ab) = \varrho\lambda(a)\varrho\lambda(b)\kappa(b)^{(\sigma(a)-1)/r}$, $\varrho^2\lambda(ab) = \varrho^2\lambda(a)\varrho^2\lambda(b)$ $\kappa(b)^{(\sigma(a)-1)/r}, \dots$ Now, $\kappa(ab) = \lambda(ab)\varrho\lambda(ab)\dots\varrho^{r-1}\lambda(ab) = \kappa(a)\kappa(b)\kappa(b)^{\sigma(a)-1} = \kappa(a)\kappa(b)^{\sigma(a)}$ (use 4.2(ii)). ▲

4.4 Lemma. *(i)* $\lambda(a^{-1}) = \lambda(a)^{-1}\kappa(a^{-1})^i = \lambda(a)^{-1}\kappa(a)^j$ *for all* $a \in A$ *and* $i = (1 - \sigma(a))/r$, $j = (1 - \sigma(a^{-1}))/r$.

(ii) $\lambda(ab^{-1}) = \lambda(a)\lambda(b)^{-1} \cdot (\kappa(a)\kappa(b)^{-1})^k$ *for all* $a, b \in A$ *and* $k = (\sigma(b^{-1}) - 1)/r$.

Proof. (i) By 4.3(vii), $1 = \lambda(aa^{-1}) = \lambda(a)\lambda(a^{-1})\kappa(a^{-1})^{-i}$ and $1 = \lambda(aa^{-1}) = \lambda(aa^{-1}) = \lambda(a)\lambda(a^{-1})\kappa(a)^{-j}$.

(ii) By 4.3(vii), $\lambda(ab^{-1}) = \lambda(a)\lambda(b^{-1})\kappa(a)^k$. But, by(i), $\lambda(b^{-1}) = \lambda(b)^{-1}\kappa(b)^{-k}$. ▲

4.5 Lemma. *Let* $a, b \in A$. *Then* $\lambda(a) = \lambda(b)$ *if and only if* $\lambda(ab^{-1}) = 1$ *and also if and only if* $ab^{-1} \in \mathbb{Z}(G)$. *In that case,* $\sigma(a) = \sigma(b)$, *and* $\kappa(a) = \kappa(b)$.

Proof. First, let $\lambda(a) = \lambda(b)$. Then $\kappa(a) = \kappa(b)$ by 4.2(ii), and so $\lambda(ab^{-1}) = 1$ by 4.4(ii). Conversely, if $\lambda(ab^{-1}) = 1$, then $ab^{-1} = \varrho(ab^{-1})$ and $ab^{-1} \in \mathbb{Z}(G)$ (see 4.3(iv)). Finally, if $ab^{-1} \in \mathbb{Z}(G) \subseteq A_1$, then $\sigma(a) = \sigma(b)$ and $\lambda(a) = \lambda(b)$. ▲

4.6 Lemma. *(i)* λ^2 *is a homomorphism of* A *into* A_1.

(ii) $\mathbb{Z}(G) \subseteq \mathrm{Ker}(\lambda^2) = \{a \in A; \lambda(a) \in \mathbb{Z}(G)\} = \{a \in A; \varrho^2(a)\varrho(a)^{-2}a = 1\}$.

(iii) $\lambda^2(a) = \varrho^2(a)\varrho(a)^{-2}$ *for every* $a \in A$.

Proof. Let $a, b \in A$. Then, by 4.3(vii), $\varrho\lambda(ab) = \varrho\lambda(a)\varrho\lambda(b)\kappa(b)^{(\sigma(a)-1)/r}$, and hence $\lambda^2(ab) = \varrho\lambda(ab)\lambda(ab)^{-1} = \varrho\lambda(a)\lambda(a)^{-1}\varrho\lambda(b)\lambda(b)^{-1} = \lambda^2(a)\lambda^2(b)$. Further, $\lambda^2(a) = \varrho\lambda(a)\lambda(a)^{-1} = \varrho(\varrho(a)a^{-1})\varrho(a)^{-1}a = \varrho^2(a)\varrho(a)^{-2}a$. The rest is clear. ▲

4.7 Lemma. *$\mathbb{Z}(G)$ contains at least one element of order n/r (and so* $\operatorname{card}(\mathbb{Z}(G)) \geq n/r$*).*

Proof. For every i, $1 \leq i \leq (n-r)/r$, choose an element $a_i \in A$ such that $\kappa(a_i)^i \neq 1$ (see 4.3(x)) and denote by K the subgroup of $\mathbb{Z}(G)$ generated by all a_i. Then K is finite and $a^{n/r} = 1$ for every $a \in K$. Moreover, it is easy to see that K contains at least one element of order n/r. ▲

4.8 Remark. (i) With regard to 4.3(vii), λ induces a homomorphism of A into $A_1/\mathbb{Z}(G)$. The kernel of this homomorphism is just $\{a \in A;\ \varrho^2(a)\varrho(a)^{-2}a = 1\} = \operatorname{Ker}(\lambda^2)$ (see (4.6)).

(ii) κ induces a mapping $\nu : A/A_1 \to \mathbb{Z}(G)$, $\nu(aA_1) = \kappa(a)$.

(iii) σ induces an injective homomorphism $\mu : A/A_1 \to \underline{Z}_n^*$.

(iv) $\nu(xy) = \nu(x)\nu(y)^{\mu(x)} = \nu(x)^{\mu(y)} \cdot \nu(y)$, $\nu(y)^{(\mu(y)-1)/r} = \nu(y)^{(\mu(x)-1/r}$ and $\nu(x)^{n/r} = 1$ for all $x, y \in A/A_1$.

(v) By 4.5, λ induces an injective mapping v of $A/\mathbb{Z}(G)$ into A_1, $v(a\mathbb{Z}(G)) = \lambda(a)$. In particular, $\operatorname{card}(a/\mathbb{Z}(G)) \leq \operatorname{card}(A_1)$ and $m \leq \operatorname{card}(\mathbb{Z}(G))$.

4.9 Remark. (i) Put $\vartheta(a) = a\varrho(a) \ldots \varrho^{r-1}(a)$ for evey $a \in A_1$. Then $\vartheta : A_1 \to \mathbb{Z}(G)$ is a homomorphism, $\vartheta(a) = a^r$ for every $a \in \mathbb{Z}(G)$ and $\vartheta(b) \neq 1$ for at least one $b \in A_1$.

(ii) $\kappa = \vartheta\lambda$, $\lambda(a)^{n/r} \in \operatorname{Ker}(\vartheta)$ for every $a \in A$. If $b \in A$ and $\lambda(b) \in \mathbb{Z}(G)$ (i.e., if $b \in \operatorname{Ker}(\lambda^2)$), then $\lambda(b)^n = 1$.

4.10 Lemma. $G' \subseteq A_1H_4$.

Proof. We have $G' \subseteq A_1H \cap AH_4 = A_1H_4$. ▲

4.11 Lemma. *Suppose that $r = 1$. Then:*

(i) $\lambda(a) = \kappa(a) = \xi(a, 1) = \varrho(a)a^{-1} \in \mathbb{Z}(G) = A_1$ for every $a \in A$.

(ii) $\xi(a, b) = \lambda(a)^k$ for all $a \in A$ and $k \geq 0$.

(iii) $\lambda(ab) = \lambda(a)\lambda(b)^{\sigma(a)} = \lambda(b)\lambda(a)^{\sigma(b)}$ for all $a, b \in A$.

(iv) $\lambda(a)^n = 1$ for every $a \in A$.

(v) $\mathbb{Z}(G) = A_1$ contains at least one element of order n.

(vi) $\lambda(a) = \lambda(b)$ iff $\sigma(a) = \sigma(b)$.

Proof. Obvious. ▲

4.12 Lemma. *Suppose that $n = p$ is a prime number (see 3.24). Then:*

(i) $m \mid p - 1$, A/A_1 is cyclic, $\mathbb{Z}(G) = A_1$, $r = 1$.

(ii) $\mu : A/A_1 \to \underline{Z}_p^* (\cong \underline{Z}_{p-1}(+))$ is an injective homomorphism.

(iii) $\lambda = \kappa$.

(iv) ν is an injective mapping of A/A_1 into A_1, $\nu(xy) = \nu(x)\nu(y)^{\mu(x)} = \nu(x)^{\mu(y)} \cdot \nu(y)$ and $\nu(x)^p = 1$ for all $x, y \in A/A_1$.

Proof. See 3.24, 4.8 and 4.11. ▲

4.13 Lemma. *Let $= p$ be a prime, $\alpha \in A/A_1$ a generator of A/A_1 (see 4.12) and let $k = \mu(\alpha) \geq 2$. For $1 \leq i$, let $\gamma(i)$ be such that $0 \leq \gamma(i) \leq p - 1$ and $\gamma(i) \equiv (1 + k + \dots + k^{i-1})$ (mod p), $\gamma(0) = 0$. Then:*

(i) $v(\alpha^i) = v(\alpha)^{\gamma(i)}$ for every $i \geq 0$.

(ii) The order of $v(\alpha)$ in A_1 is just p.

(iii) The numbers $0, 1, \gamma(2), \dots, \gamma(m-1)$ are pair-wise different.

(iv) The order of k in $\underline{Z}_p^*$ is just m.

(v) $k^i - 1 \equiv (k-1)\gamma(i)$ (mod p) for every $i \geq 0$.

Proof. (i) The equality is clear for $i = 0$ and we can further proceed by induction; $v(\alpha^{i+1}) = v(\alpha)v(\alpha^i)^k = v(\alpha)(v(\alpha)^{\gamma(i)})^k = v(\alpha)^{\gamma(i)+k+1} = v(\alpha)^{\gamma(i+1)}$ (see 4.12).

(ii) This follows from (i) and 4.3(x).

(iii) We have $A/A_1 = \{1, \alpha, \dots, \alpha^{m-1}\}$ and so $v(A/A_1) = \{1, v(\alpha), v(\alpha)^{\gamma(2)}, \dots, v(\alpha)^{\gamma(m-1)}\}$. Now, take into account that v is injective.

(iv) $k = v(\alpha)$ is of the same order as α.

(v) This is clear from the definition of $\gamma(i)$. ▲

5. Some special cases (A)

5.1. Let G be a group such that $G = AH$, where A is an abelian subgroup of G, $A \ntrianglelefteq G$, $[A : A_1] = 2$, $A_1 = \mathbb{L}_G(A)$, H is a finite cyclic subgroup of order $n \geq 2$ and $\mathbb{L}_G(H) = 1$. Further, let $w \in H$ be generator of H and assume that $waw \in A$ for at least one $a \in A$. Then $m = 2$, $A_{n-1} \neq \emptyset$, $A = A_1 \cup A_{n-1}$, $n \geq 3$, $\sigma(A) = \{1, n-1\}$ and the condition (R2) is satisfied. Moreover, $r = r_1$ divides both n and $n - 2$. Consequently, either $r = 1$ or $r = 2$ and $n \geq 4$ is even.

5.1.1 Lemma. *Let $r = 1$. Then:*

(i) $\lambda(a) = \kappa(a) = \varrho(a)a^{-1} \in \mathbb{Z}(G) = A_1$ and $\lambda(a)^n = 1$ for every $a \in A$.

(ii) $\lambda(A_{n-1}) = \{e\}$ is a one-element set end e is an element of order n in A_n.

(iii) $\varrho(a) = a$ for every $a \in A_1$ and $\varrho(b) = be$ for every $b \in A_{n-1} = A \setminus A_1$.

(iv) $G' = \langle ew^{n-2} \rangle$ is a cyclic group of order n.

(v) $G' \cap A = 1 = G' \cap H$ if n is odd.

(vi) $G' \cap A = \langle e^{n/2} \rangle$ is a two-element group and $G' \cap H = 1$ if n is even.

(vii) card $(G'H) = n^2$.

Proof. First, (i) and the equality $\lambda(A_{n-1}) = \{e\}$ follow from 4.11. Further, $\varrho(b) = \lambda(b)b = eb$ and $\varrho^i(b) = e^i b$ for all $i \geq 0$ and $b \in A_{n-1}$. The order of ϱ is n, and hence the same is true for e. The rest is clear from 1.2. ▲

5.1.2 Lemma. *Let $r = 1$. Then:*

(i) If $n \geq 3$ is odd, then $AG' = G \neq HG'$.

(ii) If $n \geq 4$ is even, then $AG' \neq G \neq HG'$.

Proof. Use 5.1.1. ▲

In the remaining part of 5.1, we will assume that $r = 2$; then $n \geq 4$ is even.

5.1.3 Lemma. *(i)* $\kappa(a) = \xi(a, 2) = \varrho^2(a)a^{-1}$ *for every* $a \in A$.
(ii) $\kappa(A_1) = 1$ *and* $\varrho^2(a) = a$ *for every* $a \in A_1$.
(iii) $\kappa(A_{n-1}) = \{e\}$, *where* $e \in \mathbb{Z}(G)$ *and the order of* e *is* $n/2$.

Proof. See 4.1, 4.2 (ii), (v), 4.3(viii), (x). ▲

5.1.4 Lemma. *(i) If* $a, b \in A$ *and either* $a \in A_1$ *or* $b \in A_1$, *then* $\lambda(ab) = \lambda(a)\lambda(b)$.
(ii) $\lambda \restriction A_1$ *is an endomorphism of* A_1.
(iii) If $a, b \in A_{n-1} = A \setminus A_1$, *then* $\lambda(ab) = \lambda(a)\lambda(b)e^{-1}$.
(iv) $\lambda^2(a)\lambda(a)^2 = e$ *for every* $a \in A_{n-1}$.

Proof. (i), (ii) and (iii). See 4.3(ii), (vii) and 5.1.3.
(iv) We have $\varrho^2(a) = a$. But $\varrho^2(a) = \varrho(\lambda(a)a) = \varrho\lambda(a)\varrho(a) = \lambda^2(a)\lambda(a)^2(a)$. Thus $\lambda^2(a)\lambda(a)^2 = 1$.
(v) By (iii), $\lambda(a^2) = \lambda(a)^2 e^{-1}$ and $e = \lambda(a)^2\lambda(a^2)^{-1}$.
Further, $a^2 \in A_1$, and so $\lambda(a^2)^{-1} = \lambda(a^{-2})$ and $e = \lambda(a)^2\lambda(a^{-2})$. Finally, $\lambda^2(a) = \lambda(\varrho(a)a^{-1}) = \varrho(\varrho(a)a^{-1})\varrho(a)^{-1}a = \varrho(a^{-1})\varrho^n(a)\varrho(a)^{-1}a = \varrho(a^{-1})\varrho(a)^{-1}a^2$. But $1 = \varrho(aa^{-1}) = \varrho(a)\varrho^{-1}(a^{-1})$, $\varrho(a^{-1}) = \varrho^{-1}(a^{-1})$, $\varrho(a^{-2}) = \varrho(a^{-1})\varrho^{-1}(a^{-1}) = \varrho(a^{-1})\varrho(a)^{-1}$ and $\lambda^2(a) = \varrho(a^{-1})\varrho(a)^{-1}a^2 = \varrho(a^{-2})a^2 = \lambda(a^{-2})$. ▲

5.1.5 Lemma. *Let* $u \in A_{n-1}$, $v = \lambda(u)$, $z = \lambda(u^{-1})$, $v' = \lambda(u)u^2$ *and* $z' = \lambda(u^{-1})u^2$. *Then:*
(i) $\lambda(v) = \lambda^2(u) = \lambda(u^{-2}) = \lambda(u^2)^{-1} = \lambda(u^2)^{-1} = \lambda(u^{-1})^2e^{-1} = z^2e^{-1}$.
(ii) $\lambda(z) = \lambda^2(u^{-1}) = \lambda(u^2) = \lambda(u^{-2})^{-1} = \lambda(u^2)e^{-1} = v^2e^{-1}$.
(iii) $\lambda(z) = \lambda(v)e$ *and* $v^2 = \lambda(z)e$.
(iv) $vz = e = \varrho(u)\varrho(u^{-1})$.
(v) $z = \lambda(v)v = \varrho(v)$ *and* $v = \lambda(z)z = \varrho(z)$.
(vi) $v' = vu^2$, $z' = zu^{-2}$, $v', z' \in \mathbb{Z}(G)$ *and* $\lambda(v') = \lambda(z') = 1$.
(vii) $vz = v'z' = e$.
(viii) $\varrho(a) = \lambda(u)a$ *and* $\varrho(au) = \lambda(a)avu = \lambda(a)av'u^{-1} = \varrho(a)vu = \varrho(a)v'u^{-1}$ for every $a \in A_1$.

Proof. (i) $\lambda(v) = \lambda^2(u) = \lambda(u^{-2})^{-1}$ by 5.1.4 and its proof. Further, by 5.1.4(iii), $\lambda(u^{-2}) = \lambda(u^{-1})^2e^{-1} = z^2e^{-1}$.
(ii) We can proceed similarly as in (i) (we replace u by u^{-1}).
(iii) Combine (i) and (ii).
(iv) By 5.1.4(iii), $1 = \lambda(uu^{-1}) = \lambda(u)\lambda(u^{-1})e^{-1} = vze^{-1}$, and so $vz = e$. Further, $\varrho(u) = \varrho(u^{-1}) = \lambda(u)u\lambda(u^{-1})u^{-1} = \lambda(u)\lambda(u^{-1}) = e$.
(v) By (iii) and (iv), $z^2 = \lambda(v)e = \lambda(v)vz = \varrho(v)z$, and so $z = \varrho(v)$. Quite similarly, $v = \lambda(z)z = \varrho(z)$.
(vi) Obviously, $v' = vu^2$ and $z' = zu^{-2}$. Further, $v, u^2 \in A_1$, and hence $\lambda(v') = \lambda(v)\lambda(u^2) = \lambda(u^{-2})\lambda(u^2) = \lambda(u^{-2}u^2) = 1$. Similarly, $\lambda(z') = 1$.
(vii) By (vi) and (iv), $v'z' = vu^2zu^{-2} = vz = e$.
(viii) $\varrho(au) = \varrho(a)\varrho(u)$, and the rest is clear. ▲

5.1.6 Lemma. *Consider the situation from 5.1.5 and moreover, assume that* $u^2 = 1$. *Then:*

(i) $v = v'$, $z = z'$ *and* $v, z \in \mathbb{Z}(G)$.

(ii) $v^2 = e = z^2$.

(iii) If $n/2$ *is even, then the order of both* v *and* z *is* n.

(iv) If $n/2$ *is odd, then the order of both* v *and* z *is* $n/2$.

Proof. (i) See 5.1.5.

(ii) By (i) and 5.1.5(iii), $\lambda(v) = \lambda(z) = 1$ and $v^2 = z^2 = e$.

(iii) and (iv). This is clear from (ii) and the fact thhat the order of e is $n/2$. ▲

5.1.7 Remark. If A_1 is finite and of odd order, then $n/2$ is odd and there exists at least one $u \in A_{n-1}$ with $u^2 = 1$.

5.1.8 Lemma. *Let* $u \in A_{n-1}$ *(see 5.1.5). Then:*

(i) $\varrho^i(u) = e^{(i-1)/2} \cdot v'u' = e^{(i-1)/2} \cdot \varrho(u) = e^{(i-1)/2} \cdot vu$ *for every* $i \geq 1$ *odd.*

(ii) $\varrho^i(u) = e^{i/2} \cdot u$ *for every* $i \geq 2$ *even.*

Proof. First, $\varrho(u) = vu = \lambda(u)u = v'u^{-1}$ and $\varrho^2(u) = \varrho(vu) = \varrho(v)\varrho(u) = \varrho(v)vu = zvu = eu$ by 5.1.5(iv), (v). Now, we will proceed by induction on i.

If $i \geq 1$ is odd, then $\varrho^{i+1}(u) = \varrho(e^{(i-1)/2} \cdot vu) = e^{(i-1)/2} \cdot \varrho(vu) = e^{(i+1)/2} \cdot u$.

If $i \geq 2$ is even, then $\varrho^{i+1}(u) = \varrho(e^{i/1} \cdot u) = e^{i/2} \cdot \varrho(u) = e^{i/2} \cdot vu$. ▲

5.1.9 Remark. (i) $\lambda(a) \neq 1$ for every $a \in A_{n-1}$ (if $\lambda(a) = 1$, then $\varrho(a) = a$ and $a \in \mathbb{Z}(G) \subseteq A_1$).

(ii) $a^{-1}waw^{-1} = a^{-1}\varrho(a)ww^{-1} = \lambda(a)$ for every $a \in A_1$.

(iii) $a^{-1}waw^{-1} = a^{-1}\varrho(a)w^{-1}w^{-1} = \lambda(a)w^{-2}$ for every $a \in A_{n-1}$.

(iv) $\lambda(a)^{-1} = \lambda(a^{-1})e^{-1} = \lambda(a^{-1})e^{(n-2)/2}$ for every $a \in A_{n-1}$.

(v) $(e^i\lambda(a)w^j)^{-1} = e^{-i}w^{n-j}\lambda(a^{-1}) = e^{-1}\varrho^{n-j}\lambda(a^{-1})w^{n-j} = e^{-i}\lambda\varrho^{-j}(a^{-1})w^{-j}$ for all $a \in A_1$, $0 \leq i \leq (n-2)/2$, $0 \leq j \leq n-1$.

(vi) $(e^i\lambda(a)w^j)^{-1} = e^{-i-1} \cdot w^{n-j} \cdot \lambda(a^{-1}) = e^{-i-1} \cdot \lambda\varrho^{-j}(a^{-1})w^{-j}$ for all $a \in A_{n-1}$, $0 \leq i \leq (n-2)/2$, $0 \leq j \leq n-1$.

(vii) $e^i\lambda(a)w^k \cdot e^j\lambda(b)w^1 = e^{i+j} \cdot \lambda(a)\varrho^k\lambda(b)w^{k+1} = e^{i+j} \cdot \lambda(a)\lambda(a)\lambda\varrho^k(b)w^{k+1} = e^{i+j} \cdot \lambda(a\varrho^k(b))w^{k+1}$ for all $a, b \in A_1$, $0 \leq i, j \leq (n-2)/2$, $0 \leq k, l \leq n-1$.

(viii) $e^i\lambda(a)w^k \cdot e^j\lambda(b)w^l = e^{i+j} \cdot \lambda(a\varrho^k(b))w^{k+l}$ and $e^j\lambda(b)w^l \cdot e^i\lambda(a)w^k = e^{i+j} \cdot \lambda(\varrho^l(a)b)w^{k-l}$ for all $a \in A_1$, $b \in A_{n-1}$, $0 \leq i$, $j \leq (n-2)/2$, $0 \leq k$, $l \leq n-1$.

(ix) $e^i\lambda(a)w^k \cdot e^j\lambda(b)w^l = e^{i+j+1} \cdot \lambda(a\varrho^k(b))w^{k+l}$ for all a, $b \in A_{n-1}$, $0 \leq i$, $j \leq (n-2)/2$, $0 \leq k$, $l \leq n-1$.

5.1.10 Lemma. $G' = \{e^i\lambda(a)w^{-4i};\ a \in A_1,\ 0 \leq i \leq (n-2)/2\} \cup \{e^i\lambda(a)w^{-4i-2};\ a \in A_{n-1},\ 0 \leq i \leq (n-2)/2\}$.

Proof. Denote by F the set on the right side of the above equality. It follows from 5.1.9 that F is a subgroup of G. Further, $b^{-1}e^i\lambda(a)w^{-4i} \cdot b = e^i\lambda(a)w^{-4i}$

(we have $\varrho^2(b) = b$), $c^{-1}e^i\lambda(a)w^{-4i} \cdot c = e^i\lambda(a)w^{4i}$, $w^{-1}e^i\lambda(a)w^{-4i} \cdot w = e^i\lambda\varrho(a)w^{-4i}$, $b^{-1}e^i\lambda(c)w^{-4i-2} \cdot b = e^i\lambda(a)w^{-4i-2}$, $d^{-1}e^i\lambda(c)w^{-4i-2} \cdot d = e^{-i-1} \cdot \lambda(c)w^{4i+2}$ and $w^{-1}e^i\lambda(c)w^{-4i-2} \cdot w = e^i\lambda\varrho(a)w^{-4i-2}$ for all $a, b \in A_1$, $c, d \in A_{n-1}$. Now, we see that $F \trianglelefteq G$ and, by 5.1.9(ii), (iii), we have $[aF, wF] = 1$ in G/F for every $a \in A$. Since $G/F = \langle aF, wF\rangle$, we conclude that G/F is abelian, i.e., $G' \nsubseteq F$.

Conversely, $\lambda(A_1) \subseteq G'$ and $\lambda(a)w^{-2} \in G'$ for every $a \in A_{n-1}$. Further, $(\lambda(a)w^{-2})^{-1} = e^{-1}\lambda(a^{-1})w^2 \in G'$ and $(e^{-1}\lambda(a^{-1})w^2)^2 = e^{-1}\lambda(a^{-2})w^4 \in G'$. Since $a^{-2} \in A_1$, we have $\lambda(a^{-2}) \in G'$ and $e^{-1}w^4 \in G'$. on the other hand, $e^iw^{-4i} \cdot \lambda(a)w^{-2} = e^i\lambda(a)w^{-4i-2}$ for $a \in A_{n-1}$ and $e^iw^{-4i} \cdot \lambda(a) = e^i\lambda(a)w^{-4i}$ for $a \in A_1$. Now, it is clear that $F \subseteq G'$. ▲

5.1.11 Lemma. *(i) If $n = 4k$, $k \geq 1$, then $G' \cap A = \lambda(A_1) \cup e^k\lambda(A_1) \neq 1$.*

(ii) If $n = 4k + 2$, $k \geq 1$, then $G' \cap A = \lambda(A_1) \cap e^k\lambda(A_{n-1}) \neq 1$.

(iii) $H_1 = H_2 = H_3 = \langle w^2\rangle$ (see 3.5, 3.6, 3.7) and $G_1 = G_2 = G_3 = AG' = A\langle w^2\rangle \neq G$ (see 3.7).

Proof. Use 5.1.10. ▲

5.2 Construction. (cf. 5.1.1 and 5.1.2) Let A_1be a non-trivial subgroup of index 2 in an abelian group A (denoted multiplicatively) and let $e \in A_1$ be an element of order $n \geq 3$. Define a permutation ϱ of A by $\varrho(a) = a$ and $\varrho(b) = be$ for all $a \in A_1$ and $b \in A \setminus A_1$; the order of ϱ is just n.

Now, put $\mathscr{G} = \langle L_a, \varrho;\ a \in A\rangle \subseteq A!$ (here, $L_a(x) = ax$, a, $x \in A$). Then $\mathscr{G} = \mathscr{A} \cdot \mathscr{H}$, where $\mathscr{A} = \{L_a;\ a \in A\} \cong A$ and $\mathscr{H} = \langle\varrho\rangle$ is a cyclic group of order n; we have $\varrho L_a = L_a\varrho$ and $\varrho L_b = L_{\varrho(b)}\varrho^{-1} = L_{\varrho(b)}\varrho^{n-1}$ for all $a \in A_1$ and $b \in A \setminus A_1$. Clearly, $\mathbb{L}_{\mathscr{G}}(\mathscr{H}) = 1$, $\mathbb{L}_{\mathscr{G}}(\mathscr{A}) = \mathbb{Z}(\mathscr{G}) = \mathscr{A}_1 = \{L_a;\ a \in A_1\} \cong A_1$ and $\mathscr{G}' = \langle L_a\varrho^{n-2}\rangle$ is a cyclic group of order n.

5.3 Remark. Let A_1 be a non-trivial subgroup of index 2 in an abelian group A and $E = A \setminus A_1$. Let ϱ be an endomorphism of A_1 such that $\varrho^2 = \mathrm{id}$. Put $\lambda(a) = \varrho(a)a^{-1}$ for every $a \in A_1$; then $\lambda^2(a) = \lambda(a)^{-2}$.

(i) Let $u \in A$ and $v \in A_1$ be such that $\lambda(v) = \lambda(u^{-2})$. Put $z = \lambda(v)v$. Then $\lambda(z) = \lambda^2(v)\lambda(v) = \lambda(v^{-2})\lambda(v) = \lambda(v^{-1}) = \lambda(u^2)$ and $\lambda(z)z = v$. Further, $\lambda(vz) = \lambda(v)\lambda(z) = \lambda(u^{-2})\lambda(u^2) = 1$ and $vz = \lambda(v)v^2 \cdot \lambda(z)z^2$. If $v' = vu^2$ and $z' = zu^{-2}$, then $v = v'u^{-2}$, $z = z'u^2$, u, $z \in \mathrm{Ker}(\lambda)$ and $vz = \lambda(v)v^2 = \lambda(z)z^2 = (v')^2u^{-4}\lambda(u^{-2}) = (z')^2u^4\lambda(u^2)(= e)$.

(ii) Let e, $v' \in \mathrm{Ker}(\lambda)$, $u \in E$, be such that $(v')^2 = eu^4\lambda(u^2)$. Then, for $v = v'u^2$, we have $\lambda(v) = \lambda(u^{-2})$. $v' = vu^2$ and $e = \lambda(v)v^2$.

(iii) Take $u \in E$ (see (i) and (ii)), $v' = vu^{-2}$, then $\lambda(v) = \lambda(u^{-2})$. If $u^2 = 1$, $v \in A_1$ and $\varrho(v) = v$, then $\lambda(v) = \lambda(u^{-2})(= 1)$.

(iv) Assume that A_1 is of finite odd order. Then there exists $\in E$ with $u^2 = 1$. Finnaly, if $\varrho(a) \neq a^{-1}$ for some $a \in A_1$ and $v = \varrho(a)a$, then $v \neq 1$, $\varrho(v) = v$ and $v^2 \neq 1$.

5.4 Construction. (cf. 5.1.3, ..., 5.1.11). Let A_1 be a non-trivial subgroup of index 2 in an abelian group A. Put $E = A \setminus A_1$ and consider an authomorphism ϱ of A_1 such that $\varrho^2 = \mathrm{id} \neq \varrho$. Let $u \in E$ and $v \in A_1$ be such that $\varrho(vu^2) = vu^2$ and the order of $e = v\varrho(v)$ is $n/2$ for $n \geq 4$ even (see 5.3).

Extend ϱ to a permutation of A by $\varrho(au) = \varrho(a)vu (= \varrho(av^{-1})eu)$ for every $a \in A_1$. Then ϱ becomes a permutation of order n of A, $\varrho(A_1) = A_1$, $\varrho(E) = E$, $\varrho L_a = L_{\varrho(a)}\varrho$ and $\varrho L_b = L_{\varrho}(\beta)\varrho^{n-1}$ for all $a \in A_1$, $b \in E$.

Let $\mathscr{G} = \langle L_a, \varrho, a \in A \rangle \subseteq A!$. Then $\mathscr{G} = \mathscr{A} \cdot \mathscr{H}$, where $\mathscr{A} = \{L_a;\ a \in A\} \cong A$ $\mathscr{H} = \langle \varrho \rangle$ is a cyclic group of order n, $\mathbb{L}_{\mathscr{G}}(\mathscr{H}) = 1$, $\mathbb{L}_{\mathscr{G}}(\mathscr{A}) = \mathscr{A}_1 = \{L_a;\ a \in A_1\} \cong$ $\cong A_1$, $\mathbb{Z}(\mathscr{G}) = \{L_a;\ a \in A_1;\ \varrho(a) = a\}$ (we have $m = r_1 = 2$ and $\mathscr{A}_{n-1} = \{L_a;$ $a \in E \neq \emptyset\}$.

5.5 Example. Let $A = \underline{Z}_{16}(+)$, $A_1 = 2A$, $\varrho(a) = 3a$ for every $a \in A_1$ (A_1 is a cyclic group of order 8), $u = 1 \in E = A \setminus A_1$, $v = 6 \in A_1$. Then $\varrho(v + 2u) =$ $= \varrho(8) = 8 = v + 2u$, $e = v + \varrho(v) = 8$, $n = 4$.

Further, $\lambda(a) = 2a$, $a \in A_1$, and $\varrho(1) = 7$, $\varrho(3) = 13$, $\varrho(5) = 3$, $\varrho(7) = 9$, $\varrho(9) = 15$, $\varrho(11) = 5$, $\varrho(13) = 11$, $\varrho(15) = 1$, $\varrho(1) = 6$, $\lambda(3) = 10$, $\lambda(5) = 14$, $\lambda(7) = 2$, $\lambda(9) = 6$, $\lambda(11) = 10$, $\lambda(13) = 14$, $\lambda(15) = 2$, $\varrho(2) = 6$, $\varrho(4) = 12$, $\varrho(6) = 2$, $\varrho(8) = 8$, $\varrho(10) = 14$, $\varrho(12) = 4$, $\varrho(14) = 10$, $\lambda(2) = 4$, $\lambda(4) = 8$, $\lambda(6) = 12$, $\lambda(8) = 0$, $\lambda(10) = 4$, $\lambda(12) = 8$, $\lambda(14) = 12$. Consequently, $\lambda(A_1) =$ $= \{0, 4, 8, 12\}$, $\lambda(E) = \{2, 6, 10, 14\}$ and $\mathrm{Ker}(\lambda) = \{0, 8\}$.

Now, consider the corresponding group $\mathscr{G} = \mathscr{A} \cdot \mathscr{H}$ (see 5.4). Then $\mathscr{A} \cong A =$ $= \underline{Z}_{16}(+)$, $\mathscr{H} = \langle \varrho \rangle \cong \underline{Z}_4(+)$, $\mathscr{G}' = \langle L_2\varrho^2 \rangle = \{L_a;\ a \in \lambda(A_1)\} \cup \{L_b\varrho^2;\ b \in \lambda(E)\}$ is a cyclic group of order 8, $\mathscr{G}' \cap \mathscr{H} = 1$, $\mathbb{Z}(\mathscr{G}) = \{L_0, L_8\} \cong \underline{Z}_2(+)$, $\mathbb{N}_{\mathscr{G}}(\mathscr{H}) =$ $= \mathbb{Z}(\mathscr{G})\mathscr{H} \cong \underline{Z}_2(+) \times \underline{Z}_4(+)$, $\mathbb{N}_{\mathscr{G}}(\mathscr{H}) \ntrianglelefteq \mathscr{G}$, $\mathbb{N}_{\mathscr{G}}(\mathscr{A}) = \mathscr{A} \cdot \langle \varrho^2 \rangle = \mathscr{G}' \cdot \mathscr{A} \neq$ $\neq \mathscr{G}$, $\mathscr{G}'\mathscr{H} = \mathscr{A}_1\mathscr{H} \neq \mathscr{G}$.

5.6 Example. Let $A = \underline{Z}_{30}(+)$, $A_1 = 2A$, $\varrho(a) = 4a$ for every $a \in A_1$ (A_1 is a cyclic group of order 15), $u = 1 \in E = A \setminus A_1$, $v = 8 \in A_1$. Then $\varrho(v + u) =$ $= \varrho(10) = 10$, $e = v + \varrho(v) = 10$, $n = 6$. Further, $\lambda(a) = 3a$ for every $a \in A_1$ and $\varrho(1) = 9$, $\varrho(3) = 17$, $\varrho(5) = 25$, $\varrho(7) = 3$, $\varrho(9) = 11$, $\varrho(11) = 19$, $\varrho(13) =$ $= 27$, $\varrho(15) = 5$, $\varrho(17) = 13$, $\varrho(19) = 21$, $\varrho(21) = 29$, $\varrho(23) = 7$, $\varrho(23) = 7$, $\varrho(25) = 15$, $\varrho(27) = 23$, $\varrho(29) = 1$, $\lambda(1) = 8$, $\lambda(3) = 14$, $\lambda(5) = 20$, $\lambda(7) = 26$, $\lambda(9) = 2$, $\lambda(11) = 8$, $\lambda(13) = 14$, $\lambda(15) = 20$, $\lambda(17) = 26$, $\lambda(19) = 2$, $\lambda(21) = 8$, $\lambda(23) = 14$, $\lambda(25) = 20$, $\lambda(27) = 26$, $\lambda(29) = 2$, $\varrho(2) = 8$, $\varrho(4) = 16$, $\varrho(6) = 24$, $\varrho(8) = 2$, $\varrho(10) = 10$, $\varrho(12) = 18$, $\varrho(14) = 26$, $\varrho(16) = 4$, $\varrho(18) = 12$, $\varrho(20) =$ $= 20$, $\varrho(22) = 28$, $\varrho(24) = 6$, $\varrho(26) = 14$, $\varrho(28) = 22$, $\lambda(2) = 6$, $\lambda(4) = 12$, $\lambda(6) = 18$, $\lambda(8) = 24$, $\lambda(10) = 0$, $\lambda(12) = 6$, $\lambda(14) = 12$, $\lambda(16) = 18$, $\lambda(18) =$ $= 24$, $\lambda(20) = 0$, $\lambda(22) = 6$, $\lambda(24) = 12$, $\lambda(26) = 18$, $\lambda(28) = 24$. Consequently, $\lambda(A_1) = \{0, 6, 12, 18, 24\}$, $\lambda(E) = \{2, 8, 14, 20, 26\}$ and $\mathrm{Ker}(\lambda) = \{0, 10, 20\}$.

Now, consider the corresponding group $\mathscr{G} = \mathscr{A} \cdot \mathscr{H}$ (see 5.4). Then $\mathscr{A} \cong A = \underline{Z}_{30}(+)$, $\mathscr{H} = \langle \varrho \rangle \cong \underline{Z}_6(+)$, $\mathscr{G}' = \langle L_4\varrho^2 \rangle$ is a cyclic group of order 15, $\mathscr{G}' \cap \mathscr{H} = 1$, $\mathbb{Z}(\mathscr{G}) = \{L_0, L_{10}, L_{20}\} \cong \underline{Z}_3(+)$.

6.1. Let G be a group such that $G = AH$, where A is an abelian subgroup of G, $A \ntrianglelefteq G$ and H is a (finite cyclic) group of order p, $p \geq 2$ being a prime, such that $\mathbb{L}_G(H) = 1$. Now, by 3.24 and 4.12, we have $p \geq 3$, $\mathbb{Z}(G) = A_1 = \mathbb{L}_G(A)$, $m \mid p - 1, m = [A : A_1]$. Further, by 4.7 (see also 4.13), $\mathbb{Z}(G)$ contains at least one element of order p. Let P and R denote the p-primary component of A and the p-socle of A, resp. Clearly, $R \subseteq P \subseteq \mathbb{Z}(G)$.

6.1.1 Lemma. *$G' \subseteq RH = R \times H \trianglelefteq G$, $G' \nsubseteq A$, G' is a p-elementary abelian group and $G = AG'$.*

Proof. By 3.24(v), $G' \subseteq \mathbb{Z}(G)H = \mathbb{Z}(G) \times H$. Thus $\mathbb{Z}(G)H \trianglelefteq G$ and, since $RH = R \times H$ is characteristic in $\mathbb{Z}(G)H$, we also have $RH \trianglelefteq G$. Finally, since $G' \nsubseteq A$, $[G : A] = p$ is a prime and $A \subseteq AG' \subseteq G$, we conclude easily that $AG' \subseteq G$. ▲

6.1.2 Lemma. $[w, a] = [a, w^{-1}] = [a, w]^{-1}$ *for all $a \in A$ and $w \in H$.*

Proof. We may assume that $w \neq 1$. Then (see 3.1) we have $[a, w^{-1}] = a^{-1}waw^{-1} = a^{-1}\varrho(a)w^{\sigma(a)-1}, a^{-1}\varrho(a) = \varrho(a)a^{-1} \in A_1 = \mathbb{Z}(G)$ (3.13 and 3.14), $w[a, w^{-1}] = a^{-1}\varrho(a)w^{\sigma(a)} = a^{-1}wa$ and $[a, w^{-1}] = w^{-1}a^{-1}wa = [w, a]$. Similarly, $[a, w] = a^{-1}w^{-1}aw = w^{-\sigma(a)}\varrho(a)^{-1}aw = \varrho(a)^{-1}aw^{-\sigma(a)+1}$ and $[a, w]^{-1} = a^{-1}\varrho(a)w^{\sigma(a)-1} = [a, w^{-1}]$. ▲

6.1.3 Lemma. $w[w, a] = [w, a]w$ *for all $a \in A$ and $w \in H$.*

Proof. Use 6.1.2. ▲

6.1.4 Lemma. $[w, a]^{\sigma(a)} = (a^{-1}\varrho(a))^{\sigma(a)} \cdot w^{\sigma(a)(\sigma(a)-1)}$ *for all $a \in A$ and $w \in H$.*

Proof. We have $[w, a] = a^{-1}\varrho(a)w^{\sigma(a)-1}$ and $a^{-1}\varrho(a) \in \mathbb{Z}(G)$. ▲

6.1.5 Lemma. $a^{-1}[w, a]a = [w, a]^{\sigma(a)}$ *for all $a \in A$ ad $w \in H$.*

Proof. We have $[w, a]a = a^{-1}\varrho(a)w^{\sigma(a)-1} \cdot a = a^{-1}\varrho(a)w^{\sigma(a)-2} \cdot wa = a^{-1}\varrho(a)w^{\sigma(a)-2} \cdot \varrho(a)w^{\sigma(a)} = (a^{-1}\varrho(a))^2 \cdot w^{\sigma(a)-2} \cdot aw^{\sigma(a)} = (a^{-1}\varrho(a))^2 \cdot w^{\sigma(a)-3} \cdot wa \cdot w^{\sigma(a)} = (a^{-1}\varrho(a))^2 \cdot w^{\sigma(a)-3} \cdot \varrho(a)w^{2\sigma(a)} = (a^{-1}\varrho(a))^3 \cdot w^{\sigma(a)-3} \cdot aw^{2\sigma(a)} = \dots = (a^{-1}\varrho(a))^{\sigma(a)} \cdot aw^{\sigma(a)(\sigma(a)-1)} = a \cdot (a^{-1}\sigma(a))^{\sigma(a)} \cdot w^{\sigma(a)(\sigma(a)-1)} = a \cdot [w, a]^{\sigma(a)}$ (use 6.1.4). ▲

6.1.6 Proposition. *Let $a \in A$ be such that the finite cyclic group A/A_1 (see 1.24(i)) iss generated by the block aA_1. The $G' = \langle [w, a] \rangle$ for every $w \in H$, $w \neq 1$. In particular, G' is a p-element group, $A \cap G' = 1$ and $G = AG'$. Moreover, $M = \langle a \rangle H$ is a normal metacyclic subgroup of G and $G \cong M \times A/\langle a \rangle$.*

Proof. Put $K = \langle [w, a] \rangle$. Then $K \subseteq G'$, and so K is a cyclic p-group. If $K = 1$, then $a \in \mathbb{N}_G(H) = A_1H$ (3.24(v), $a \in A_1$ and $A_1 = A$, a contradiction with

$A \ntrianglelefteq G$. Thus $\kappa \neq 1$ and consequently, K is a p-element group. Clearly, $A_1 = \mathbb{Z}(G) \subseteq \mathbb{N}_G(K)$ and its follows from 6.1.5 that $a \in \mathbb{N}_G(K)$. Thus $A \subseteq \mathbb{N}_G(K)$ and, in fact $\mathbb{N}_G(K) = G$, since $w \in \mathbb{N}_G(K)$ by 6.1.4. We have proven that $K \trianglelefteq G$. If $K \subseteq A$, then $w^{-1}aw \in A$ and it follows easily that $w \in \mathbb{N}_G(A)$ and $A \trianglelefteq G$, a contradiction. Consequently, $K \nsubseteq A$, $A \cap K = 1$ $A \neq AK$ and $AK = G$. From this, G/K is abelian, and therefore $G' \notin K$. Thus $K = G'$. ▲

6.1.7 Lemma. *$R \cap G' = 1$ and $RH = R \times H = R \times G'$.*

Proof. By 6.1.6, $A \cap G' = 1$ and G' is a p-element group. Thus $G' \notin R$ and $RH = RG' = R \times G'$. ▲

6.1.8 Lemma. *Let K be a p-element subgroup of RH such that $K \nsubseteq R$ and $K \neq G'$. Then $A \cap K = 1$, $\mathbb{L}_G(K) = 1$ and $G = AK$.*

Proof. We have $RH = RK$ and $AK = ARK = ARH = AH = G$. ▲

6.1.9 Lemma. *Let $l \geq 0$ be such that $\mathbb{Z}_l(G) \subseteq A$ and $H\mathbb{Z}_l(G) \ntrianglelefteq G$. Then $\mathbb{Z}_l(G) \neq \mathbb{Z}_{l+1}(G) \subseteq A$.*

Proof. We have $G/\mathbb{Z}_l(G) = \bar{G} = \bar{A} \cdot \bar{H}$, where $\bar{A} = A/\mathbb{Z}_l(G)$ and $\bar{H} = H\mathbb{Z}_l(G)/\mathbb{Z}_l(G)$ $(\cong H)$. Now, $\bar{A} \ntrianglelefteq \bar{G}$ and $\bar{H} \ntrianglelefteq \bar{G}$. Thus $1 \neq \mathbb{Z}(\bar{G}) \subseteq \bar{A}$ (3.24 and 4.12). ▲

6.1.10 Lemma. *There exists $k \geq 1$ such that $\mathbb{Z}_k(G) \subseteq A$, $\mathbb{L}_G(H\mathbb{Z}_l(G)) = \mathbb{Z}_l(G)$ for every $0 \leq l \leq k$ and $H\mathbb{Z}_k(G) \trianglelefteq G$.*

Proof. We have $\mathbb{Z}_1(G) = \mathbb{Z}(G) \subseteq A$ and $\mathbb{L}_G(H\mathbb{Z}_0(G)) = \mathbb{L}_G(H) = 1 = \mathbb{Z}_0(G)$. Further, if $\mathbb{L}_G(H\mathbb{Z}_r(G)) \neq \mathbb{Z}_r(G)$ for some $r \geq 1$, then $H\mathbb{Z}_r(G) \trianglelefteq G$, and hence $H\mathbb{Z}_s(G) \trianglelefteq G$ for every $s \geq r$. The result is now clear from 6.1.9 and the fact that $G/\mathbb{Z}(G)$ is finite. ▲

6.1.11 Lemma. *Let $k \geq 1$ be as in 6.1.10. Then $\mathbb{Z}_t(G) \subseteq A$ and $H\mathbb{Z}_t(G) = G'\mathbb{Z}_t(G) \trianglelefteq G$ for every $t \geq k$.*

Proof. Assume that $\mathbb{Z}_t(G) \subseteq A$ and $H\mathbb{Z}_t(G) \trianglelefteq G$ for some $t \geq k$ (see 6.1.10). Then $G/\mathbb{Z}_t(G) = \bar{G} = \bar{A} \cdot \bar{H}$, where $\bar{A} = A/\mathbb{Z}_t(G)$, $\bar{A} \ntrianglelefteq \bar{G}$ and $\bar{H} = H\mathbb{Z}_t(G)/\mathbb{Z}_t(G) \trianglelefteq \bar{G}$, $\bar{H} \cong H$. Clearly, $\bar{H} = \bar{G}'$, and so $H\mathbb{Z}_t(G) = G'\mathbb{Z}_t(G)$. Further, since $\bar{A} \ntrianglelefteq \bar{G}$, we have $\bar{H} \nsubseteq \mathbb{Z}(\bar{G})$, and so $\bar{H} \cap \mathbb{Z}(\bar{G}) = 1$ and $\mathbb{Z}(\bar{G}) \subseteq \bar{A}$ by 2.5(ii). Thus $\mathbb{Z}_{t+1}(G) \subseteq A$. ▲

6.1.12 Corollary. *$\mathbb{Z}_l(G) \subseteq A$ for every $l \geq 0$.*

6.1.13 Lemma. *Let v be the smallest non-negative integer such that $\mathbb{Z}_v(G) = Z_{v+1}(G)$. Then $v \geq 1$, $\mathbb{Z}_v(G) \subseteq A$, $H\mathbb{Z}_v(G) = G'\mathbb{Z}_v(G) \trianglelefteq G$ and $[G : \mathbb{Z}_v(G)] \mid p(p-1)$.*

Proof. Easy. ▲

6.2 Proposition. *Let G be a group such that $G = AH$, where A is an abelian subgroup of G and H is a (finite cyclic) subgroup of prime order $p \geq 2$. Then exactly one of the following five cases takes places:*

(1) $H \subseteq A = G$ and G is abelian;

(2) $A \cap H = 1$, $A \trianglelefteq G$, and $G = A \times H$ is abelian;

(3) $A \cap H = 1$, $A \trianglelefteq G$, $\mathbb{L}_G(H) = 1$, $G' \subseteq A$, $G \neq AG'$ and G is not abelian;

(4) $A \cap H = 1$, $A \ntrianglelefteq G$, $G' = H(\trianglelefteq G)$, $G = AG'$, $p \geq 3$ and G is not abelian;

(5) $A \cap H = 1$, $A \ntrianglelefteq G$, $\mathbb{L}_G(H) = 1 \neq \mathbb{Z}(G)$, $H \neq G'$, G' is a subgroup of order p, $G = AG'$, $p \geq 3$ and G is not abelian.

Proof. See 6.1. ▲

6.3 Corollary. *Let G be a group such that $G = AH$, where A is an abelian subgroup and H is a subgroup of a prime order p. If $A \ntrianglelefteq G$, then $p \geq 3$, G' is a subgroup of order p and $G = AG'$. If, moreover, $\mathbb{Z}(G) = 1$, then $H = G'$, A is a finite cyclic group, $card(A) \mid p - 1$ and $card(G) \mid p(p - 1)$.*

6.4 Corollary. *Let G be a group such that $G = AH$ where A is a cyclic subgroup of G and H is a subgroup of prime order. Then G is metacyclic.*

6.5 Remark. Let G be a group such that $G = AH$, where A is abelian, $A \ntrianglelefteq G$, H is p-element for a prime $p \geq 2$ and $H \trianglelefteq G$. Then $A \cap H = 1$, $p \geq 3$ and $H = G'$ (see 6.2(4)). Further, the mapping $\phi : A \to \mathrm{Aut}(H)$, $(\phi(a))(x) = axa^{-1}$, is a homomorphism and $\mathrm{Ker}(\phi) = \mathbb{Z}(G) = \mathbb{L}_G(A) = A_1$. The group $\mathrm{Aut}(H)$ is a cyclic group of order $p - 1$, and hence A/A_1 is a non-trivial cyclic group whose order divides $p - 1$. Clearly, $R \subseteq A_1$, where R is a the p-socle of A. Now, there exists a subgroup H_1 of G such that $\mathrm{card}(H_1) = p$, $\mathbb{L}_G(H_1) = 1$ and $G = AH_1$ if and only if $R \neq 1$. In that case, $RH_1 = RG'$.

(i) If $G = AH_1$ for a subgroup H_1 such that $\mathrm{card}(H_1) = p$ and $\mathbb{L}_G(H_1) = 1$, then $R \times H_1 = RH_1 = RG' = R \times G'$, and hence $R = 1$.

(ii) If H_1 is a subgroup of G such that $H_1 \subseteq RG'$ and $\mathrm{card}(H_1) = p$, then $H_1 \trianglelefteq G$ if and only if $H_1 \subseteq R$ or $H_1 = G'$.

(iii) If H_1 is a subgroup of RG' such that $H_1 \nsubseteq R$, $H_1 \neq G'$ and $\mathrm{card}(H_1) = p$ (such a subgroup exists if and only only if $R \neq 1$), then $\mathbb{L}_G(H_1) = 1$, $RH_1 = RG'$ and $G = AH_1$.

Quasigroups whose inner permutation groups are finite of prime order

7.1 Theorem. *Let Q be a quasigroup such that* $\mathrm{card}(I(Q)) = p$ *for a prime $p \geq 2$. Then Q is either medial or stably nilpotent of class 2. Moreover, in the latter case, the following are true:*

(i) $p \geq 3$.

(ii) Q/s_Q is a (non-trivial) cyclic group whose order divides $p - 1$.

(iii) If Z is the block of s_Q such that $e \in Z$ e being the unique idempotent element of Q), then Z is an abelian group containing at least one element of order p.

(iv) If Q is finite, then p divides $\mathrm{card}(Q)$.

Proof. Use 6.1, 6.2 and [1, Part 3]. ▲

7.2 Construction. *Let* $G = AH$ *be a group as in 6.1. For every* $v \in H$, *there exist a permutation* ϱ_v *of* A *and a mapping* $\sigma_v : A \to \{0, 1, \dots, p-1\}$ *such that* $va = \varrho_v(a)v^{\sigma(a)}$ *for every* $a \in A$.

Now, choose $u, v \in H$ *such that* $H = \langle u, v \rangle$ *and define an operation* $*$ *on* A *ny* $a * b = \varrho_u(a)\varrho_v(b)$ *for all* $a, b \in A$. *Then* $Q(*)$ *becomes a quasigroup,* $M(Q(*)) \cong G$ *and* $I(Q(*)) \cong H(\cong \underline{Z}_p(+))$. *Clearly,* $Q(*)$ *is not medial (see 7.1).*

References

[1] Drápal, A., Kepka, T. and Maršálek, P., *Multiplication groups of quasigroups and loops II*, Acta Univ. Carolinae Math. Phys. **35/1** (1994), 9 – 29.

[2] Itô, N., *Über das Produkt von zwei abelschen Gruppen*, Math. Z. **52** (1955), 400 – 401.