GLASNIK MATEMATIČKI
Vol. 40(60)(2005), 207 – 233

ALTERNATE PROOFS OF SOME BASIC THEOREMS OF FINITE GROUP THEORY

Yakov Berkovich

University of Haifa, Israel

Dedicated to Moshe Roitman on the occasion of his 60th birthday

Abstract. In this note alternate proofs of some basic results of finite group theory are presented.

These notes contain a few new results. Our aim here is to give alternate and, as a rule, more short proofs of some basic results of finite group theory: theorems of Sylow, Hall, Carter, Kulakoff, Wielandt-Kegel and so on.

Only finite groups are considered. We use the standard notation. $\pi(n)$ is the set of prime divisors of a natural number n and $\pi(G) = \pi(|G|)$, where $|G|$ is the order of a group G; p is a prime. A group G is said to be *p-nilpotent* if it has a normal p-complement. Given $H < G$, let $H_G = \bigcap_{x \in G} H^x$ and H^G be the *core* and *normal closure* of H in G, respectively. If M is a subset of G, then $\mathrm{N}_G(M)$ and $\mathrm{C}_G(M)$ is the *normalizer* and *centralizer* of M in G. Let $\mathrm{s}_k(G)$ ($\mathrm{c}_k(G)$) denote the number of subgroups (cyclic subgroups) of order p^k in G. Next, E_{p^n} is the elementary abelian group of order p^n; C_m is the cyclic group of order m; D_{2^n}, Q_{2^n} and SD_{2^n} are dihedral, generalized quaternion and semidihedral group of order 2^n, respectively. If G is a p-group, then $\Omega_n(G) = \langle x \in G \mid o(x) \leq p^n \rangle$, $\mho_1(G) = \langle x^{p^n} \mid x \in G \rangle$, where $o(x)$ is the order of $x \in G$. Next, G', $\mathrm{Z}(G)$, $\Phi(G)$ is the derived subgroup, the center and the Frattini subgroup of G; $\mathrm{Syl}_p(G)$ and $\mathrm{Hall}_\pi(G)$ are the sets of p-Sylow and π-Hall subgroups of G. We denote $\mathrm{O}_\pi(G)$ the maximal normal π-subgroup of G. Let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G. If $H < G$

2000 *Mathematics Subject Classification.* 20C15.

Key words and phrases. Sylow p-subgroup, solvable group, Hall subgroup, Carter subgroup.

and $\mu \in \mathrm{Irr}(H)$, then μ^G is the induced character and χ_H is the restriction of a character χ of G to H.

Almost all prerequisites are collected in the following

Lemma J.

(a) *(O. Schmidt; see* [Hup, Satz 5.2]*) If G is a minimal nonnilpotent group, then $G = PQ$, where $P \in \mathrm{Syl}_p(G)$ is cyclic and $Q = G' \in \mathrm{Syl}_q(G)$ is either elementary abelian or special. If $q > 2$, then $\exp(Q) = q$. If Q is abelian, then $Q \cap \mathrm{Z}(G) = \{1\}$ and $\exp(Q) = q$. If Q is nonabelian, then $Q \cap \mathrm{Z}(G) = \mathrm{Z}(Q)$.*

(b) *(Frobenius; see* [Isa1, Theorem 9.18] *+ (a)) If G is not p-nilpotent, it has a minimal nonnilpotent subgroup S such that $S' \in \mathrm{Syl}_p(S)$.*

(c) *(Burnside; see* [Isa1, Theorem 9.13]*) If $P \in \mathrm{Syl}_p(G)$ is contained in $\mathrm{Z}(\mathrm{N}_G(P))$, then G is p-nilpotent.*

(d) *(Tuan; see* [Isa2, Lemma 12.12]*) If a nonabelian p-group G possesses an abelian subgroup of index p, then $|G| = p|G'||\mathrm{Z}(G)|$.*

(e) *(Gaschütz; see* [Hup, Hauptsatz 1.17.4(a)]*) If P, an abelian normal p-subgroup of G, is complemented in a Sylow p-subgroup of G, then P is complemented in G.*

(f) *(see* [Suz, Theorem 4.4.1]*) If a nonabelian p-group G has a cyclic subgroup of index p, then either $G = \langle a, b \mid a^{p^n} = b^p = 1, a^b = a^{1+p^{n-1}} \rangle$ with $n > 2$ for $p = 2$, or $p = 2$ and G is dihedral, semidihedral or generalized quaternion.*

(g) *(see* [Isa2, Lemma 2.27]*) If a group G has a faithful irreducible character, then its center is cyclic.*

(h) *(Ito; see* [Isa2, Theorem 6.15]*) The degree of an irreducible character of a group G divides the index of its abelian normal subgroup.*

(i) *(Chunikhin) If $G = AB$, A_0 is normal in A and $A_0 \le B$, then $A_0 \le B_G$.*

(j) [Ber5, Proposition 19] *If B is a nonabelian subgroup of order p^3 of a p-group G such that $C_G(B) < B$, then G is of maximal class. In particular (Suzuki), if G has a subgroup U of order p^2 such that $C_G(U) = U$, then U is of maximal class.*

(k) *(Blackburn; see* [Ber6, Theorem 9.6] *If $H \le G$, where G is a p-group of maximal class, then $|H/\mho_1(H)| \le p^p$.*

1. Theorems of Sylow, Hall, Carter and so on

We prove Sylow's Theorem in the following form:

Theorem 1.1. *All maximal p-subgroups of a group G are conjugate and their number is $\equiv 1 \pmod p$ so, if P is a maximal p-subgroup of G, then p does not divide $|G : P|$.*

LEMMA 1.2 (Cauchy). *If $p \in \pi(G)$, then G has a subgroup of order p. In particular, a maximal p-subgroup of G is $> \{1\}$.*

PROOF. Suppose that G is a counterexample of minimal order. Then G has no proper subgroup C of order divisible by p and $|G| \neq p$. If G has only one maximal subgroup, say M, it is cyclic. Indeed, if $x \in G - M$, then $\langle x \rangle$ is not contained in M so $\langle x \rangle = G$. Then $\langle x^{o(x)/p} \rangle < G$ is of order p, a contradiction. If G is abelian and $A \neq B$ are maximal subgroups of G, then $G = AB$ so $|G| = \frac{|A||B|}{|A \cap B|}$, and p does not divide $|G|$, a contradiction. If G is nonabelian, then $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} h_i$, where $h_1, \dots, h_k$ are sizes of noncentral G-classes. Since h_i's are indices of proper subgroups in G, p divides h_i for all i. Then p divides $|\mathrm{Z}(G)|$, a final contradiction. □

The set $\mathbf{S} = \{A_i\}_{i=1}^{n}$ of subgroups of a group G is said to be **invariant** if $A_i^x \in \mathbf{S}$ for all $i \leq n$ and $x \in G$. All members of the set $\mathbf{S}$ are conjugate if and only if it has no nonempty proper invariant subset.

LEMMA 1.3. *Let $\mathbf{S} \neq \emptyset$ be an invariant set of subgroups of a group G. Suppose that whenever $\mathbf{N} \neq \emptyset$ is an invariant subset of $\mathbf{S}$, then $|\mathbf{N}| \equiv 1 \pmod{p}$. Then all members of the set $\mathbf{S}$ are conjugate in G.*

PROOF. Assume that $\mathbf{S}$ has a proper invariant subset $\mathbf{N} \neq \emptyset$. Then $\mathbf{S} - \mathbf{N} \neq \emptyset$ is invariant so $|\mathbf{S}| = |\mathbf{N}| + |\mathbf{S} - \mathbf{N}| \equiv 1 + 1 \not\equiv 1 \pmod{p}$, a contradiction. Thus, all members of $\mathbf{S}$ are conjugate in G. □

Let P be a maximal p-subgroup of a group G and P_1 a p-subgroup of G. If $PP_1 \leq G$, then PP_1 is a p-subgroup so $P_1 \leq P$. If P_1 is also maximal p-subgroup of G, then $\mathrm{N}_P(P_1) = P \cap P_1$.

PROOF OF THEOREM 1.1. One may assume that p divides $|G|$. Let $\mathbf{S}_0 = \{P = P_0, P_1, \dots, P_r\}$ be an invariant set of maximal p-subgroups of G; then $P_i > \{1\}$ for all i (Lemma 1.2). Let $r > 0$ and let P act on the set $\mathbf{S}_0 - \{P\}$ via conjugation. Then the size of every P-orbit on the set $\mathbf{S}_0 - \{P\}$ is a power of p greater than 1 since the stabilizer of a 'point' P_i equals $P \cap P_i < P$. Thus, p divides r so $|\mathbf{S}_0| = r + 1 \equiv 1 \pmod{p}$, and the first assertion follows (Lemma 1.3). Then p does not divide $|G : \mathrm{N}_G(P)|$. Since P is a maximal p-subgroup of $\mathrm{N}_G(P) = N$, the prime p does not divide $|N/P|$ (Lemma 1.2) whence p does not divide $|G : N||N : P| = |G : P|$. □

REMARK 1.1 (Frobenius). Let P be a p-subgroup of a group G and let $\mathbf{M} = \{P_1, \dots, P_r\} \subset \mathrm{Syl}_p(G) - \{P\}$ be P-invariant and P is not contained in P_i for all i. Then $|\mathbf{M}| \equiv 0 \pmod{p}$ (let us P act on $\mathbf{M}$ via conjugation) so, by Theorem 1.1, the number of Sylow p-subgroups of G, containing P, is $\equiv 1 \pmod{p}$. Similarly, if $P \in \mathrm{Syl}_p(G)$, then the number of p-subgroups of G of given order that are not contained in P, is divisible by p (P acts on the set of the above p-subgroups!).

Remark 1.2 (Frobenius). Let $\mathbf{M} = \{M_1, \dots, M_s\}$ be the set of all subgroups of order p^k in a group G of order p^m, $k < m$. We claim that $|\mathbf{M}| \equiv 1 \pmod p$. Let $\Gamma_1 = \{G_1, \dots, G_r\}$ be the set of all maximal subgroups of G. Since the number of subgroups of index p in the elementary abelian p-group $G/\Phi(G)$ of order, say p^d, equals $\frac{p^d-1}{p-1} = 1+p+\cdots+p^{d-1} \equiv 1 \pmod p$, we get $|\Gamma_1| \equiv 1 \pmod p$, so we may assume that $k < m-1$. Let α_i be the number of members of the set $\mathbf{M}$ contained in G_i and β_j be the number of members of the set Γ_1 containing M_j, all i, j. Then, by double counting,

$$\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s,$$

By the above, $r \equiv 1 \pmod p$. By induction, $\alpha_i \equiv 1 \pmod p$, all i. Next, β_j is the number of maximal subgroups in $G/M_j\Phi(G)$ so $\beta_j \equiv 1 \pmod p$, all j. By the displayed formula, $|\mathbf{M}| = s \equiv r \equiv 1 \pmod p$.

Remark 1.3 (Frobenius; see also [Bur, Theorem 9.II]). It follows from Remarks 1.1 and 1.2 that the number of p-subgroups of order p^k in a group G of order $p^k m$ is $\equiv 1 \pmod p$.

Remark 1.4. Suppose that $\mathbf{S}_1, \mathbf{S}_2 \subset \mathrm{Syl}_p(G)$ are nonempty and disjoint. Let $P_i \in \mathbf{S}_i$ be such that the set $\mathbf{S}_i$ is P_i-invariant, $i = 1, 2$; then $|\mathbf{S}_i| \equiv 1 \pmod p$, $i = 1, 2$ (see the proof of Theorem 1.1). It follows that $\mathbf{S}_2$ is not P_1-invariant (otherwise, considering the action of P_1 on $\mathbf{S}_2$ via conjugation, we get $|\mathbf{S}_2| \equiv 0 \pmod p$ since $P_1 \notin \mathbf{S}_2$).

Remark 1.5 (Burnside). Let G be a non p-closed group (i.e., $\mathrm{O}_p(G) \notin \mathrm{Syl}_p(G)$) and $P \in \mathrm{Syl}_p(G)$. Suppose that $Q \in \mathrm{Syl}_p(G) - \{P\}$ is such that the intersection $D = P \cap Q$ is a maximal, by inclusion, intersection of Sylow p-subgroups of G. We claim that $N = \mathrm{N}_G(D)$ is not p-closed. Assume that this is false. Then $P_1 \in \mathrm{Syl}_p(N)$ is normal in N. It follows from properties of p-groups that $P \cap P_1 > D$ and $Q \cap P_1 > D$ so P_1 is not contained in P. Therefore, if $P_1 \le U \in \mathrm{Syl}_p(G)$, then $U \ne P$. However, $P \cap Q = D < P \cap P_1 \le P \cap U$, a contradiction.

The following assertion is obvious. If R is an abelian minimal normal subgroup of G and $G = HR$, where $H < G$, then H is maximal in G and $H \cap R = \{1\}$.

Theorem 1.4 (P. Hall [Hal1]). *If π is a set of primes, then all maximal π-subgroups of a solvable group G are conjugate.*

By Theorems 1.1 and 1.4, a maximal π-subgroup of a solvable group G is its π-Hall subgroup, and this gives the standard form of Hall's Theorem.

The proofs of Theorems 1.4, 1.6 and 1.7 are based on the following

Lemma 1.5 ([Ore]). *If maximal subgroups F and H of a solvable group $G > \{1\}$ have equal cores, then they are conjugate.*

PROOF. One may assume that $F_G = \{1\}$; then G is not nilpotent. Let R be a minimal normal, say p-subgroup, of G; then $RF = G = RH$. Let K/R be a minimal normal, say q-subgroup, of G/R, q is a prime. In that case, K is nonnilpotent (otherwise, $\mathrm{N}_G(K \cap F) > F$ so $\{1\} < K \cap F \leq F_G = \{1\}$) hence $q \neq p$. Then $F \cap K$ and $H \cap K$ are nonnormal Sylow q-subgroups of K hence they are conjugate (Theorem 1.1). It follows that then $\mathrm{N}_G(F \cap K) = F$ and $\mathrm{N}_G(H \cap K) = H$ are also conjugate. □

PROOF OF THEOREM 1.4.[1] We use induction on $|G|$. Let F and H be maximal π-subgroups of G and R a minimal normal, say p-subgroup, of G. If $p \in \pi$, then $R \leq F$ and $R \leq H$, by the product formula and F/R, H/R are maximal π-subgroups of G/R so they are conjugate, by induction; then F and R are conjugate. Now assume that $\mathrm{O}_\pi(G) = \{1\}$; then $p \in \pi'$. Let F_1/R, H_1/R be maximal π-subgroups of G/R containing FR/R, HR/R, respectively; then $F_1^x = H_1$ for some $x \in G$ and $F_1/R, H_1/R \in \mathrm{Hall}_\pi(G/R)$, by induction. Assume that $F_1 < G$. Then, by induction, $F \in \mathrm{Hall}_\pi(F_1)$ as a maximal π-subgroup of F_1 so $F_1 = F \cdot R$. Similarly, $H_1 = H \cdot R$. Therefore, $F^x \in \mathrm{Hall}_\pi(H_1)$. Then $H = (F^x)^y = F^{xy}$ for some $y \in H_1$, by induction. Now let $F_1 = G$; then G/R is a π-group. Let K/R be a minimal normal, say q-subgroup, of G/R; then $q \in \pi$. Let $Q \in \mathrm{Syl}_q(K)$; then $K = QR$. By Frattini argument, $G = \mathrm{N}_G(Q)K = \mathrm{N}_G(Q)QR = \mathrm{N}_G(Q)R$ so $\mathrm{N}_G(Q) \in \mathrm{Hall}_\pi(G)$ is maximal in G. Assume that $FR < G$. Then $\mathrm{N}_G(Q) \cap FR$, as a π-Hall subgroup of FR (product formula!), is conjugate with F, contrary to the choice of F. Thus, $FR = HR = G$ and $F_G = \{1\} = H_G$, by assumption. Then F and H are conjugate maximal subgroups of G (Lemma 1.5). □

Let us prove, for completeness, by induction on $|G|$, that a group G is solvable if it has a p'-Hall subgroup for all $p \in \pi(G)$ (Hall–Chunikhin; see [Hal1,Chu]). Let $G_{p'} \in \mathrm{Hall}_{p'}(G)$, where $p' = \pi(G) - \{p\}$, and let $q \in p'$. If $G_{q'} \in \mathrm{Hall}_{q'}(G)$, then $G_{p'} \cap G_{q'} \in \mathrm{Hall}_{q'}(G_{p'})$, by the product formula, so $G_{p'}$ is solvable, by induction. Let R be a minimal normal, say r-subgroup of $G_{p'}$, $r \in p'$. In view of Burnside's two-prime theorem, we may assume that $|\pi(G)| > 2$, so there exists $s \in \pi(G) - \{p, r\}$; let $G_{s'} \in \mathrm{Hall}_{s'}(G)$; then $G = G_{p'}G_{s'}$. By Theorem 1.1, one may assume that $R < G_{s'}$; then $R \leq (G_{s'})_G$ (Lemma J(i)). Next, $(G_{s'})_G$ is solvable as a subgroup of $G_{s'}$. Thus, G has a minimal normal, say r-subgroup, which we denote by R again. If $R \in \mathrm{Syl}_r(G)$, then $G/R \cong G_{r'}$ is solvable so is G. If $R \notin \mathrm{Syl}_r(G)$, then $G_{r'}R/R \in \mathrm{Hall}_{r'}(G/R)$. Let $q \in \pi(G) - \{r\}$; then $R < G_{q'}$ so $G_{q'}/R \in \mathrm{Hall}_{q'}(G/R)$. In that case, by induction, G/R is solvable, and the proof is complete.

A subgroup K is said to be a *Carter subgroup* (= C-subgroup) of G if it is nilpotent and coincides with its normalizer in G.

[1] This proof is independent of the Schur-Zassenhaus Theorem.

Theorem 1.6 (Carter [Car]). *A solvable group G possesses a C-subgroup and all C-subgroups of G are conjugate.*

Proof. We use induction on $|G|$. One may assume that G is not nilpotent. Let R be a minimal normal, say p-subgroup, of G.

Existence. By induction, G/R contains a C-subgroup S/R so $\mathrm{N}_G(S) = S$. Let T be a p'-Hall subgroup of S (Theorem 1.4); then TR is normal in S and $S = TP$, where $P \in \mathrm{Syl}_p(S)$. Set $K = \mathrm{N}_S(T)$; then $K = T \times \mathrm{N}_P(T)$ is nilpotent and $KR = S$ (Theorem 1.4 and the Frattini argument). If $y \in \mathrm{N}_S(K)$, then $y \in \mathrm{N}_S(T) = K$ since T is characteristic in K, and so $\mathrm{N}_S(K) = K$. If $x \in \mathrm{N}_G(K)$, then $x \in \mathrm{N}_G(KR) = \mathrm{N}_G(S) = S$ so $x \in \mathrm{N}_S(K) = K$, and K is a C-subgroup of G.

Conjugacy. Let K, L be C-subgroups of G; then KR/R, LR/R are C-subgroups in G/R so, by induction, $LR = (KR)^x$ for some $x \in G$, and we have $K^x \leq LR$. One may assume that R is not contained in K; then RK is nonnilpotent so R is not contained in L. If $LR < G$, then $(K^x)^y = L$ for $y \in LR$, by induction. Now let $G = LR$; then $G = KR$ so G/R is nilpotent, and this is true for each choice of R. Thus, R is the unique minimal normal subgroup of G so K and L are maximal in G and $K_G = L_G$; then they are conjugate in G (Lemma 1.5). □

Theorem 1.7. *Let a nonnilpotent group $G = N_1 \dots N_k$, where $N_1, \dots, N_k$ are pairwise permutable and nilpotent. Then there exists $i \leq k$ such that $N_i^G < G$.*

Lemma 1.8 ([Ore]). *If $G = AB$, where $A, B < G$, then A and B are not conjugate.*

Proof. Assume that $B = A^g$ for $g \in G$. Then $g = ab$, $a \in A$ and $b \in B$, so $B = A^{ab} = A^b$ and $A = B^{b^{-1}} = B$, $G = A$, a contradiction. □

Proof of Theorem 1.7.[2] Let G be a minimal counterexample. By [Keg], G is solvable. Let $R < G$ be a minimal normal, say p-subgroup; then $G/R = (N_1R/R) \dots (N_kR/R)$, where all N_iR/R are nilpotent. If G/R is not nilpotent, we get $(N_iR)^G < G$ for some i, by induction. Now let G/R be nilpotent. Then, by hypothesis, we get, for all i, $N_iR = G$ so N_i is maximal in G and R is the unique minimal normal subgroup of G, whence $(N_i)_G = \{1\}$ for all i; in that case, $N_1, \dots, N_k$ are conjugate in G (Lemma 1.5). Then $N_rN_s = G$ for some $r, s \leq k$, contrary to Lemma 1.8. □

Supplement 1 to Lemma 1.5. If for arbitrary maximal subgroups F and H of a group G with equal cores, we have $\pi(|G : F|) = \pi(|G : H|)$, then G is solvable.

[2] For $k = 2$, Theorem 1.7 was proved by Janko and Kegel [Keg], independently.

PROOF. Let G be a minimal counterexample. Since the hypothesis inherited by epimorphic images, G has only one minimal normal subgroup R, and R is nonsolvable. Let $p \in \pi(R)$ and $P \in \mathrm{Syl}_p(R)$. Let $\mathrm{N}_G(P) \le F < G$, where F is maximal in G. By Frattini's Lemma, $G = RF$ so $|G : F| = |R : (F \cap R)|$ and $p \notin \pi(|G : F|)$. Let $q \in \pi(|R : (F \cap R|)$. Take $Q \in \mathrm{Syl}_q(R)$ and let $\mathrm{N}_G(Q) \le H < G$, where H is maximal in G. Then $FR = G = HR$ so $F_G = \{1\} = H_G$. However, $q \in \pi(|G : F|)$ and $q \notin \pi(|G : H|)$, a contradiction. □

A group G is said to be *p-solvable*, if every its composition factor is either p- or p'-number.

SUPPLEMENT 2 TO LEMMA 1.5. Let $G > \{1\}$ be a p-solvable group with minimal normal p-subgroup R. Suppose that G possesses a maximal subgroup H with $H_G = \{1\}$. Then all maximal subgroups of G with core $\{1\}$ are conjugate.

PROOF. By hypothesis, $|\pi(G)| > 1$. Let F be another maximal subgroup of G with $F_G = \{1\}$; then $G = FR = HR$ and $F \cap R = \{1\} = H \cap R$. If $R \in \mathrm{Syl}_p(G)$, we are done (Schur-Zassenhaus). Now let $p \in \pi(G/R)$; then G/R is not simple: $p \in \pi(G/R)$. Let K/R be a minimal normal subgroup of G/R. Then, as in the proof of Lemma 1.5, $|\pi(K)| > 1$ so, taking into account that G/R is p-solvable, we conclude that K/R is a p'-subgroup. In that case, $F \cap K$ and $H \cap K$ as p'-Hall subgroups of K, are conjugate (Schur-Zassenhaus) so $H = \mathrm{N}_G(F \cap K)$ and $F = \mathrm{N}_G(H \cap K)$ are also conjugate. □

SUPPLEMENT 3 TO LEMMA 1.5 [Gas]. Let M be a minimal normal subgroup of a solvable group G. Suppose that K^1 and K^2 are complements of M in G such that $K^1 \cap \mathrm{C}_G(M) = K^2 \cap \mathrm{C}_G(M)$. Then K^1 and K^2 are conjugate in G.

PROOF.[3] It follows from $K^iM = G$, that K^i maximal in G, $i = 1, 2$. We have $K^i \cap M = \{1\}$ so $(K^i)_G \le \mathrm{C}_G(M)$, $i = 1, 2$. By the modular law, $\mathrm{C}_G(M) = M \times \mathrm{C}_{K^i}(M)$ so $\mathrm{C}_{K^i}(M) = (K^i)_G$, $i = 1, 2$. Then, by hypothesis, $(K^1)_G = (K^2)_G$ so K^1 and K^2 are conjugate in G, by Lemma 1.5. □

2. GROUPS WITH A CYCLIC SYLOW p-SUBGROUP

Here we prove two results on groups with a cyclic Sylow p-subgroup.

THEOREM 2.1.[4] *Let $P \in \mathrm{Syl}_p(G)$ be cyclic. If H is normal in G and p divides $(|H|, |G : H|)$, then H is p-nilpotent and G is p-solvable*[5].

Suppose that $P \in \mathrm{Syl}_p(G)$ is cyclic.

[3]Compare with [Weh, Theorem 3.7]
[4]Compare with [Wie1]
[5]It is easy to deduce from this that the p-length of G equals 1.

Remark 2.1. Suppose, in addition, that p divides $|\mathrm{Z}(G)|$. Set $N = \mathrm{N}_G(P)$. Since N has no minimal nonnilpotent subgroup S with $S' \in \mathrm{Syl}_p(N)$ (Lemma J(a,b)), it is p-nilpotent so $P \leq \mathrm{Z}(N)$. In that case, G is p-nilpotent (Lemma J(c)).

Remark 2.2. Suppose that G, p, P and H are as in Theorem 2.1 and that $P_1 = P \cap H$ is normal in H so in G. Let $T \in \mathrm{Hall}_{p'}(H)$ (Schur-Zassenhaus); then $H = P_1T$, $G = H\mathrm{N}_G(T) = P_1\mathrm{N}_G(T)$ (Schur-Zassenhaus and Frattini argument). Let $P_2 \in \mathrm{Syl}_p(\mathrm{N}_G(T))$; then $P_1P_2 \in \mathrm{Syl}_p(G)$ is cyclic and $P_2 > \{1\}$ so $P_1 \cap P_2 > \{1\}$. We have $\mathrm{C}_H(P_1 \cap P_2) \geq P_1T = H$ so H is p-nilpotent, by Remark 2.1.

Remark 2.3. If $\{1\} < H < G$ and $R \leq \Phi(H)$ is normal in G, then $R \leq \Phi(G)$. Indeed, assuming that this is false, we get $G = RM$ for some maximal subgroup M of G. Then, by the modular law, $H = R(H \cap M)$ so $H = H \cap M$. In that case, $R < H \leq M$, a contradiction.

Remark 2.4. If H is normal in G and $G = AH$, where A is as small as possible, then $A \cap H \leq \Phi(A)$. Indeed, if this is false, then $A = B(A \cap H)$, where $B < A$ is maximal. Then $G = AH = B(A \cap H)H = BH$, contrary to the choice of A.

Proof of Theorem 2.1. By the product formula, $P_1 = P \cap H \in \mathrm{Syl}_p(H)$. Set $N = \mathrm{N}_G(P_1)$; then $P \leq N$. Set $N_1 = \mathrm{N}_H(P_1) = N \cap H$. Then, by Remark 2.2 applied to the pair $N_1 < N$, we get $N_1 = P_1 \times T$, where $T \in \mathrm{Hall}_{p'}(N_1)$, and so H is p-nilpotent (Lemma J(c)). By Frattini's Lemma, $G = HN$ so $G/H \cong N/(N \cap H) = N/N_1$; therefore, it remains to prove that N/N_1 is p-solvable. To this end, we may assume that $N = G$; then P_1 is normal in G. In that case, $G/\mathrm{C}_G(P_1)$ as a p'-subgroup of $\mathrm{Aut}(P_1)$, is cyclic of order dividing $p-1$. By Remark 2.1, $\mathrm{C}_G(P_1)$ is p-nilpotent, and we conclude that G is p-solvable[6]. □

Theorem 2.2 ([Hal3, Theorem 4.61]). *If $P \in \mathrm{Syl}_p(G)$ is cyclic of order p^m and $k \leq m$, then $\mathrm{c}_k(G) \equiv 1 \pmod{p^{m-k+1}}$.*

Proof. Let $\mathbf{C} = \{Z_1, \ldots, Z_r\}$ be the set of subgroups of order p^k in G not contained in P. Let P act on $\mathbf{C}$ via conjugation. The P-stabilizer of Z_i equals $P \cap Z_i$ which is of order p^{k-1} at most. It follows that $r = |\mathbf{C}| \equiv 0 \pmod{p^{m-(k-1)}}$. □

3. Groups with a normal Hall subgroup

R. Baer [Bae] has proved that if $P \in \mathrm{Syl}_p(G)$ is normal in G, then $P \cap \Phi(G) = \Phi(P)$.

[6]Since $H \cap P \leq \Phi(G)$, then, by deep Tate's Theorem [Hup, Satz 4.4.7], H is p-nilpotent.

Theorem 3.1. *If H is a normal Hall subgroup of a group G, then $H \cap \Phi(G) = \Phi(H)$.*

Proof. We have $\Phi(H) \leq H \cap \Phi(G)$, by Remark 2.3. To prove the reverse inclusion, it suffices, assuming $\Phi(H) = \{1\}$, to show that $D = H \cap \Phi(G) = \{1\}$. Assume, however, that $D > \{1\}$. Then $D = P \times L$ for some $\{1\} < P \in \mathrm{Syl}_p(D)$. Considering the pair $D/\Phi(P)L < G/\Phi(P)L$, one may assume that $\Phi(P)L = \{1\}$; then $D = P$ is elementary abelian normal subgroup of G. Let $T < H$ be minimal such that $PT = H$. Then $P \cap T \leq \Phi(T)$, by Remark 2.4, and $\mathrm{N}_H(P \cap T) \geq PT = H$ so $P \cap T \leq \Phi(H) = \{1\}$, by Remark 2.3. If $P \leq P_0 \in \mathrm{Syl}_p(H)(= \mathrm{Syl}_p(G))$, then $P_0 = P(P_0 \cap T)$, by the modular law, so P is complemented in P_0. Then, by Lemma J(e), P is complemented in G so P is not contained in $\Phi(G)$, a contradiction. □

4. Subgroup generated by some minimal nonabelian subgroups

Let $p \in \pi(G)$ and let $\mathbf{A}_p(G)$ be the set of all minimal nonabelian subgroups A of G such that A' is a p-subgroup (in that case, A is either a p-group or minimal nonnilpotent). Set $\mathrm{L}_p(G) = \langle H \mid H \in \mathbf{A}_p(G)\rangle$ and $\mathrm{L}(G) = \prod_{p\in\pi(G)} \mathrm{L}_p(G)$. It is known [Ber1] that $\mathrm{L}(G) = G$ if G is a nonabelian p-group and $G' \leq \mathrm{L}(G)$ for arbitrary G.

Theorem 4.1. *Given a group G, the quotient group $G/\mathrm{L}_p(G)$ is p-nilpotent and has an abelian Sylow p-subgroup.*

Proof. Let $P \in \mathrm{Syl}_p(G)$. We may assume that P is not contained in $\mathrm{L}_p(G)$; then P is abelian. Assume that $G/\mathrm{L}_p(G)$ is not p-nilpotent. Then $G/\mathrm{L}_p(G)$ has a minimal nonnilpotent subgroup $H/\mathrm{L}_p(G)$ such that $(H/\mathrm{L}_p(G))'$ is a p-subgroup (Lemma J(b)). Let $T \leq H$ be minimal such that $T\mathrm{L}_p(G) = H$; then $T \cap \mathrm{L}_p(G) \leq \Phi(T)$, by Remark 2.4, and $T/(T \cap \mathrm{L}_p(G)) \cong H/\mathrm{L}_p(G)$. Using properties of Frattini subgroups and Lemma J(a), we get $T = Q \cdot P_0$, where $P_0 = T' \in \mathrm{Syl}_p(T)$, $Q \in \mathrm{Syl}_q(T)$ is cyclic and $|Q : (Q \cap \mathrm{Z}(T))| = q$. Since P_0 is abelian and indices of minimal nonabelian subgroups in T are not multiples of q and Sylow q-subgroups generate T, we get $T = \mathrm{L}_p(T) \leq \mathrm{L}_p(G)$, a contradiction. □

5. Simplicity of A_n, $n > 4$

Here we prove the following classical.

Theorem 5.1 (Galois). *The alternating group $G = \mathrm{A}_n$, $n > 4$, is simple.*

If $n > 4$ and a permutation $x \in \mathrm{S}_n^\#$ is of cycle type $(1^{a_1}, 2^{a_2}, \dots, n^{a_n})$, then $|\mathrm{C}_{\mathrm{S}_n}(x)| = \prod_{i=1}^n (a_i)! i^{a_i} \leq 2(n-2)!$ with equality if and only if x is a transposition.

Let G be a 2-transitive permutation group of degree n, $n > 2$, and let H be a stabilizer of a point in G; then $|G : H| = n$. Assume that $H < M < G$.

If M is transitive, we get $|M : H| = n$ so $M = G$, a contradiction. Then M has an orbit of size $n-1$ since H has so M is a stabilizer of a point in G, a final contradiction. Thus, H is maximal in G so G is primitive. We have $H_G = \{1\}$ since H_G fixes all points.

Proof of Theorem 5.1. We proceed by induction on n. If $n = 5$, G is simple since, by Lagrange, a nontrivial subgroup of G is not a union of G-classes (indeed, sizes of G-classes are $1, 12, 12, 15, 20$). Let $n > 5$ and let H be the stabilizer of a point; then $H \cong \mathrm{A}_{n-1}$ is maximal and nonnormal in G and nonabelian simple, by induction. Then H has no proper subgroup of index $< n-1$ since H is not isomorphic with a subgroup of A_{n-2}. Assume that G has a nontrivial normal subgroup N; then $|N| = n$ since $NH = G$ and $N \cap H = \{1\}$ (H is simple!). Let H act on the set $N^\#$ via conjugation. The H-stabilizer $C = \mathrm{C}_H(x)$ of a 'point' $x \in N^\#$ has index $\leq |N^\#| = n-1$ in H. Assume that $|H : C| < n-1$. Then, by what has just been said, H centralizes x so $|\mathrm{C}_G(x)| \geq |H| \cdot o(x) \geq 2 \cdot \frac{1}{2}(n-1)! > 2(n-2)!$, a contradiction. Thus, $|H : C| = n-1$ so $|C| = \frac{1}{2}(n-2)!$. Then all elements of $N^\#$ are conjugate under H so N is an elementary abelian p-subgroup for some prime p. If $x \in N^\#$, then. since $n \geq 6$, we get $|C_G(x)| \geq |N| \cdot |C| = n \cdot \frac{1}{2}(n-2)! > 2(n-2)!$, a final contradiction. ∎

Let us prove Theorem 5.1 independently of the paragraph preceding its proof. Beginning with the place where N is an elementary abelian p-group of order, say $p^r (= n)$, we get $\mathrm{C}_G(N) = N$ since H is not normal in G. Then H is isomorphic to a subgroup of the group $\mathrm{Aut}(N) \cong \mathrm{GL}(r, p)$, so $|H|$ divides the number

$$(p^r - 1)(p^r - p) \dots (p^r - p^{r-1}) = (n-1)(n-p) \dots (n-p^{r-1}) < \frac{1}{2}(n-1)! = |H|,$$

a contradiction since $r > 1$ and $n > 4$.

Here is the third proof of Theorem 5.1. Let N be a group of order $n > 4$. We claim that $|\mathrm{Aut}(N)| < \frac{1}{2}(n-1)!$. Indeed, let $n_1, \dots, n_r$ be the sizes of $\mathrm{Aut}(N)$-orbits on $N^\#$; then $\mathrm{Aut}(N)$ is isomorphic to a subgroup of $\mathrm{S}_{n_1} \times \dots \times \mathrm{S}_{n_r}$, and the result follows if $r > 1$. If $r = 1$, all elements of $N^\#$ are conjugate under $\mathrm{Aut}(N)$, and we get a contradiction as in the previous paragraph.

Suppose that G, a group of order $n!$, $n > 4$, has a subgroup H of index $\leq n+1$; then G is not simple. Assume that this is false. Then $G \leq \mathrm{A}_{n+1}$ since G is simple. In that case, $|\mathrm{A}_{n+1} : G| \leq \frac{1}{2}(n+1)$, a contradiction since, by Theorem 5.1, A_{n+1} has no proper subgroup of index $< n+1$. (Compare with [Isa1, Example 6.14].)

6. Theorems of Taussky and Kulakoff

The following two theorems have many applications in p-group theory.

THEOREM 6.1 (Taussky). *Let G be a nonabelian 2-group. If $|G : G'| = 4$, then G contains a cyclic subgroup of index* 2 [7].

PROOF. We use induction on m, where $|G| = 2^m$. One may assume that $m > 3$. Let $R \leq G' \cap \mathrm{Z}(G)$ be of order 2. Then G/R has a cyclic subgroup T/R of index 2, by induction. Assume that T is noncyclic. Then $T = R \times Z$, where Z is cyclic of order $2^{m-2} > 2$ so, since $m > 3$ and G/Z_G is isomorphic to a subgroup of D_8, we get $Z_G > \{1\}$. We have $R \times \Omega_1(Z_G) \leq \mathrm{Z}(G)$ so $|\mathrm{Z}(G)| \geq 4$. By Lemma J(d), $|G : G'| = 2|\mathrm{Z}(G)| \geq 2 \cdot 4 = 8$, a contradiction. The last assertion now follows from Lemma J(f). □

Here is another proof of Theorem 6.1. Since $\Phi(G) = \mho_1(G)$, it suffices to prove that $\Phi(G)$ is cyclic. Assume that this is false. Then $\Phi(G)$ has a G-invariant subgroup T such that $\Phi(G)/T$ is abelian of type $(2, 2)$. By [BZ, Lemma 31.8], $\Phi(G/T) \leq \mathrm{Z}(G/T)$ so G/T is minimal nonabelian. In that case, $|(G/T) : (G/T)'| = 8$ (Lemma 16.1, below), a contradiction.

Next we offer the proof of Kulakoff's Theorem [Kul] independent of Hall's enumeration principle, fairly deep combinatorial assertion (Kulakoff considered only the case $p > 2$; our proof also covers the case $p = 2$).

REMARK 6.1. Let H be normal subgroup of a p-group G. If H has no normal abelian subgroup of type (p, p), it is cyclic or a 2-group of maximal class. Indeed, let A be a maximal G-invariant abelian subgroup in H; then A is cyclic. Suppose that $A < H$ and let B/A be a G-invariant subgroup of order p in H/A. Then B has no characteristic abelian subgroup of type (p, p) so, by Lemma J(f), B is a 2-group of maximal class. Assume that $B < H$. Then $|A| > 4$ since $|H| > 8$ and $\mathrm{C}_H(A) = A$. Let $V = \mathrm{C}_H(\Omega_2(A))$; then $|H : V| = 2$ since $\Omega_2(A)$ is not contained in $\mathrm{Z}(H)$. Let $B_1/A \leq V/A$ be G-invariant of order 2. Then B_1 is not of maximal class, contrary to what has just been proved.

REMARK 6.2. If a p-group G is neither cyclic nor a 2-group of maximal class, then $\mathrm{c}_1(G) \equiv 1 + p \pmod{p^2}$ and $\mathrm{c}_k(G) \equiv 0 \pmod{p}$ if $k > 1$. Indeed, G has a normal abelian subgroup R of type (p, p), by Remark 6.1. If G/R is cyclic, the result follows easily since then $\Omega_1(G) \in \{\mathrm{E}_{p^2}, \mathrm{E}_{p^3}\}$. Now let T/R be normal in G/R such that $G/T \cong \mathrm{E}_{p^2}$ and let $M_1/T, \dots, M_{p+1}/T$ be all subgroups of order p in G/T. It is easy to check that

$$\mathrm{c}_n(G) = \mathrm{c}_n(M_1) + \cdots + \mathrm{c}_n(M_{p+1}) - p\mathrm{c}_n(T). \tag{1}$$

Next we use induction on $|G|$. Let $|G| = p^4$. If $|\mathrm{Z}(G)| = p^2$, then, taking $T = \mathrm{Z}(G)$ in (1), we get what we wanted. Let $|\mathrm{Z}(G)| = p$; then $\mathrm{C}_G(R) = M_1$ is the unique abelian subgroup of index p in G so, using (1), we get the desired

[7] In particular, G is dihedral, generalized quaternion or semidihedral, and these groups exhaust the 2-groups of maximal class.

result. Now we let $|G| > p^4$. Then all M_i are neither cyclic nor of maximal class, and, using induction and (1), we complete the proof.

Remark 6.3. Let G be a p-group and $N \le \Phi(G)$ be G-invariant. Then, if $\mathrm{Z}(N)$ is cyclic so is N. Assume that this is false. Then N has a G-invariant subgroup R of order p^2. Considering $\mathrm{C}_G(R)$, we see that $R \le \mathrm{Z}(\Phi(G))$ so $R \le \mathrm{Z}(N)$ and N is not of maximal class. Now the result follows from Remark 6.1.

Remark 6.4. (P. Hall, 1926, from unpublished dissertation). If all abelian characteristic subgroups of a nonabelian p-group G are of orders $\le p$, then G is extraspecial. Indeed, it follows from Remark 6.3 that $|\Phi(G)| = p = |\mathrm{Z}(G)|$ so $G' = \Phi(G) = \mathrm{Z}(G)$.

Lemma 6.2. *Let G be a noncyclic group of order p^m and R a subgroup of order p in $\mathrm{Z}(G)$ and $k > 1$. Then the number of cyclic subgroups of order p^k containing R, is divisible by p, unless G is a 2-group of maximal class.*

Proof. Let $\mathbf{C}$ be the set of all cyclic subgroups of order p^k in G, let $\mathbf{C}^+$ be the set of all elements of the set $\mathbf{C}$ that contain R and set $\mathbf{C}^- = \mathbf{C} - \mathbf{C}^+$. If $Z \in \mathbf{C}^-$, then $RZ = R \times Z$ has exactly p cyclic subgroups of order p^k not containing R. It follows that p divides $|\mathbf{C}^-|$. By Remark 6.2, p divides $|\mathbf{C}|$. Then p divides $|\mathbf{C}^+| = |\mathbf{C}| - |\mathbf{C}^-|$. ◻

Lemma 6.3. *For a p-group G, $p^3 \le |G| \le p^4$, which is neither cyclic nor a 2-group of maximal class, we have $\mathrm{s}_2(G) \equiv 1 + p \pmod{p^2}$.*

Proof. This is trivial (see Remark 6.2). ◻

Theorem 6.4.[8] *Let G be neither cyclic nor a 2-group of maximal class, $|G| = p^m$ and $1 \le k < m$. Then $\mathrm{s}_k(G) \equiv 1 + p \pmod{p^2}$.*

Proof. We use induction on m. For $k = m - 1$ the result is trivial. For $k = 1$ the result follows from Remark 6.2. Therefore, one may assume that $1 < k < m - 1$ and $m > 4$ (see Lemma 6.3). In view of Lemma J(f), we may assume that G has no cyclic subgroup of index p. Let $\mathbf{M}$ be the set of all subgroups of order p^k in G. Let $R \le \mathrm{Z}(G)$ be of order p. Let $\mathbf{M}^+ = \{H \in \mathbf{M} \mid R < H\}$ and put $\mathbf{M}^- = \mathbf{M} - \mathbf{M}^+$.

Let G/R be a 2-group of maximal class and let Z/R be a cyclic subgroup of index 2 in G/R; then Z is abelian of type $(2^{m-2}, 2)$. Replacing R by the subgroup R_1 of order 2 in $\Phi(Z)$, we see that G/R_1 is not of maximal class. So suppose from the start that G/R is not of maximal class. Then, by induction, $|\mathbf{M}^+| = \mathrm{s}_{k-1}(G/R) \equiv 1 + p \pmod{p^2}$. It remains to prove that $|\mathbf{M}^-| \equiv 0 \pmod{p^2}$ since $|\mathbf{M}| = |\mathbf{M}^+| + |\mathbf{M}^-|$. Let $H/R < G/R$ be of order p^k. If $R < \Phi(H)$, then H has no members of the set $\mathbf{M}^-$. Now let R is not contained in $\Phi(H)$; then $H = R \times A$ with $A \in \mathbf{M}^-$. If A

[8] [Kul] for $p > 2$, [Ber3] for $p = 2$.

is cyclic, H contains exactly p members of the set $\mathbf{M}^-$. Then, by Lemma 6.2 and Remark 6.2, converse images in G of cyclic subgroups of G/R of order p^k contribute in $|\mathbf{M}^-|$ a multiple of p^2. Now let A be noncyclic with $\mathrm{d}(A) = d$; then the number of members of the set $\mathbf{M}^-$ contained in H, equals $(1+p+\cdots+p^d)-(1+p+\cdots+p^{d-1}) = p^d > p$ (here $1+p+\cdots+p^d$ is the number of maximal subgroups of H and $1+p+\cdots+p^{d-1}$ is the number of maximal subgroups of H containing R). Then $|\mathbf{M}^-| \equiv 0 \pmod{p^2}$. □

7. Characterization of p-nilpotent groups

We need the following

Lemma 7.1. *Let a p-subgroup P_0 be normal in a group G. If, for each $x \in P_0$, $|G : \mathrm{C}_G(x)|$ is a power of p, then $P_0 \le \mathrm{H}(G)$, the hypercenter of G (= the last member of the upper central series of G).*

Proof. Let $P_0 \le P \in \mathrm{Syl}_p(G)$ and $x \in (P_0 \cap \mathrm{Z}(P))^\#$; then $x \in \mathrm{Z}(G)$, by hypothesis. Set $X = \langle x \rangle$. Take $yX \in (P_0/X)^\#$ and set $Y = \langle y, X\rangle$. Let $r \in \pi(G) - \{p\}$ and $R \in \mathrm{Syl}_r(\mathrm{C}_G(y))$; then $R \in \mathrm{Syl}_r(G)$, by hypothesis, so R centralizes $Y = \langle y, X\rangle$. It follows that $RX/X \le \mathrm{C}_{G/X}(yX)$, so r does not divide $d = |(G/X) : \mathrm{C}_{G/X}(yX)|$. Since $r \ne p$ is arbitrary, d is a power of p, and the pair $P_0/X \le G/X$ satisfies the hypothesis. Now the result follows by induction on $|G|$. □

Remark 7.1 (Wielandt). Let $x \in G^\#$ be a p-element and $|G : \mathrm{C}_G(x)|$ a power of p. Then $G = \mathrm{C}_G(x)P$, where $x \in P \in \mathrm{Syl}_p(G)$, and so $x \in P_G$ (Lemma J(i)).

Theorem 7.2 ([BK]). A group G is p-nilpotent if and only if for each p-element $x \in G$ of order $\le p^{\mu_p}$, where $\mu_p = 1$ for $p > 2$ and $\mu_2 = 2$, $|G : \mathrm{C}_G(x)|$ is a power of p.

Proof. By Remark 7.1, the subgroup $\mathrm{O}_p(G)$ contains all p-elements of orders $\le p^{\mu_p}$ in G. Assume that G is not p-nilpotent. Then G has a minimal nonnilpotent subgroup S such that $S' \in \mathrm{Syl}_p(S)$ (Lemma J(b)). Let a be a generator of nonnormal, say, q-Sylow subgroup of S. Then $S\mathrm{O}_p(G) = \langle a\rangle \mathrm{O}_p(G)$ since $S' \le \mathrm{O}_p(G)$ (Lemma J(a) and Remark 7.1). Let T be the Thompson critical subgroup of $\mathrm{O}_p(G)$ (see [Suz, page 93, Exercise 1(b)]). Then a induces a nonidentity automorphism on T so $\langle a\rangle T$ possesses a minimal nonnilpotent subgroup (Lemma J(b)) which we denote S again. Set $P_0 = \Omega_{\mu_p}(T)$. It follows from $P_0 \le \mathrm{H}(G)$ (Lemma 7.1) that a centralizes P_0, a contradiction since $S' \le P_0$. □

8. On factorization theorem of Wielandt-Kegel

Wielandt and Kegel [Wie2, Keg] have proved that a group $G = AB$, where A and B are nilpotent, is solvable. Below, using the Odd Order Theorem, we prove the following

Theorem 8.1 ([Ber2]). *Let a group $G = AB$, where $(|A|, |B|) = 1$. Let $A = P \times L$, where $P \in \mathrm{Syl}_2(G)$ and let B be nilpotent. Then G is solvable.*

Recall that a subgroup K of $G = AB$ is said to be *factorized* if $K = (K \cap A)(K \cap B)$. If, in addition, $(|A|, |B|) = 1$ and K is normal in G, then K is factorized always.

Lemma 8.2 ([Wie2]). *Let $G = AB$, $(|A|, |B|) = 1$, A_0 is normal in A and B_0 is normal in B. Then subgroups $H = \langle A_0, B_0 \rangle$ and $\mathrm{N}_G(H)$ are factorized.*

Proof. Let $x = ab^{-1} \in \mathrm{N}_G(H)$ $(a \in A,\ b \in B)$; then $H^a = H^{xb} = H^b$. We have $A_0 = A_0^a \leq H^a$, $B_0 = B_0^b \leq H^b = H^a$ so $H = \langle A_0, B_0 \rangle \leq H^a = H^b$. Then $H^a = H = H^b$, $a \in \mathrm{N}_A(H) = \mathrm{N}_G(H) \cap A$, $b \in \mathrm{N}_B(H) = \mathrm{N}_G(H) \cap B$ hence $\mathrm{N}_G(H) \leq (\mathrm{N}_G(H) \cap A)(\mathrm{N}_G(H) \cap B) \leq \mathrm{N}_G(H)$, and $\mathrm{N}_G(H)$ is factorized. Next, H is normal in $\mathrm{N}_G(H)$ and $(|\mathrm{N}_G(H)| \cap A, |\mathrm{N}_G(H) \cap B|) = 1$ so $H = (H \cap \mathrm{N}_G(H) \cap A)(H \cap \mathrm{N}_G(H) \cap B) = (H \cap A)(H \cap B)$. ◻

If K and L are Hall subgroups of a solvable group X, then $KL^u = L^u K$ for some $u \in X$. Indeed, set $\sigma = \pi(K) \cup \pi(L)$ and let $K \leq H$, where $H \in \mathrm{Hall}_\sigma(X)$ (Theorem 1.4). By Theorem 1.4 again, $L^u \leq H$ for some $u \in X$. Now $KL^u = H$, by the product formula.

Lemma 8.3 ([Wie2]). *Suppose that $A, B < G$ are such that $AB^g = B^g A$ for all $g \in G$. If $G = A^G B = AB^G$, then $G = AB^g$ for some $g \in G$.*

Proof. Let A be not normal in G (otherwise, $G = A^G B = AB$). Then $A \neq A^x$ for some $x = b^g$, where $b \in B$ and $g \in G$. We have $A < A^* = \langle A, A^x \rangle$ and $A^* B^g = B^g A^*$ for all $g \in G$. Working by induction on $|G : A|$, we get $G = A^* B^g$. However, $A^* B^g = \langle A, A^x, B^g \rangle = \langle A, B^g \rangle = AB^g$. ◻

Remark 8.1 ([Keg]). If $A, B < G$ and $AB^g = B^g A < G$ for all $g \in G$, then either $A^G < G$ or $B^G < G$. Indeed, if $A^G = G = B^G$, then $G = AB^g$ for some $g \in G$ (Lemma 8.3), contrary to the hypothesis.

Lemma 8.4 (Wielandt). *Let $A = P \times Q$ be a nilpotent Hall subgroup of G, $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$, p and q are distinct primes. Then every $\{p, q\}$-subgroup of G is nilpotent.*

Proof. We use induction on $|G|$. Suppose that H is a nonnilpotent $\{p, q\}$-subgroup of minimal order in G. Then H is minimal nonnilpotent so, say $H = P_1 \cdot Q_1$, where $P_1 \in \mathrm{Syl}_p(H)$, $Q_1 = H' \in \mathrm{Syl}_q(H)$ (Lemma J(a)). We may assume that $Q_1 \leq Q$ and $\mathrm{N}_Q(Q_1) \in \mathrm{Syl}_q(\mathrm{N}_G(Q_1))$ (Theorem

1.1). However, $P < \mathrm{N}_G(Q_1)$ so $N_A(Q_1)$ is a nilpotent $\{p,q\}$-Hall subgroup of $\mathrm{N}_G(Q_1)$, by induction. Since the nonnilpotent $\{p,q\}$-subgroup $H \le \mathrm{N}_G(Q_1)$, we get $\mathrm{N}_G(Q_1) = G$, by induction, and so Q_1 is normal in G hence $\mathrm{C}_G(Q_1)$ is also normal in G. Then p does not divide $|G : \mathrm{C}_G(Q_1)|$, i.e., all p-elements of G centralize Q_1. In that case, H is nilpotent, a contradiction. ◻

Recall that a group, generated by two noncommuting involutions, is dihedral.

Proof of Theorem 8.1. Suppose that G is a counterexample of minimal order. Then $P > \{1\}$, by Odd Order Theorem, and all proper factorized subgroups and epimorphic images of G are solvable. Since all proper normal subgroups and epimorphic images are products of two nilpotent groups of coprime orders so solvable, G must be simple. Then, by Burnside's p^α-Lemma [Isa2, Theorem 3.8], $L \neq \{1\}$ and $|\pi(B)| > 1$.

(i) Assume that, for $A_0 \in \{P, L\}$ and $\{1\} < B_0 \in \mathrm{Syl}(B)$, we have $H = \langle A_0, B_0\rangle < G$. Then, by Lemma 8.2, H is factorized so solvable. By virtue of paragraph, following Lemma 8.2, one may assume that $H = A_0B_0 = B_0A_0$. Let $g = ba \in G$, where $a \in A$ and $b \in B$. We have

$$A_0B_0^g = A_0B_0^{ba} = A_0B_0^a = (A_0B_0)^a = (B_0A_0)^a = B_0^{ba}A_0 = B_0^gA_0. \tag{2}$$

Since $A_0B_0^g < G$, by the product formula, G is not simple, by Remark 8.1, a contradiction. Thus, $H = G$.

(ii) Let $u \in \mathrm{Z}(P)$ be an involution, $r \in \pi(B)$ and $R \in \mathrm{Syl}_r(B)$. Set $H = \langle u, R\rangle$ and assume that $H < G$. By Lemma 8.2, H is factorized so solvable. Let F be a $\{2, r\}$-Hall subgroup of H containing R. Replacing A by its appropriate G-conjugate, one may assume that $u \in P_0 \in \mathrm{Syl}_2(A\cap F)$; then $F = P_0R$. Let M be a minimal normal subgroup of F; then either $M \le P_0$ or $M \le R$. In the first case, $\mathrm{N}_G(M) \ge \langle L, R\rangle = G$, by (i), a contradiction. Now assume that $M \le R$. Then $\mathrm{N}_G(M) \ge T = \langle u, B\rangle$ so $G = AT$. By Lemma J(i), $1 \neq u \in T_G$, a contradiction.

(iii) Let $u \in \mathrm{Z}(P)$ be an involution. We claim that $\mathrm{C}_G(u) = A$. Assume that this is false. By the modular law, $\mathrm{C}_G(u)$ is factorized so solvable, and $\mathrm{C}_B(u)$ contains an element b of prime order, say q. Then $\mathrm{C}_G(b) \ge H = \langle u, R\rangle$, where $R \in \mathrm{Syl}_r(B)$ for some $r \in \pi(B) - \{q\}$. In that case, $H < G$, contrary to (ii).

(iv) Let $u \in \mathrm{Z}(P)$ and $v \in G$ be distinct involutions. Assume that $D = \langle u, v\rangle$ is not a 2-subgroup; then D is dihedral with $|\pi(D)| > 1$ and $u \notin \mathrm{Z}(D)$. Let $\{1\} < T < D$, $|T| = p \in \pi(D) - \{2\}$; then $\langle u\rangle \cdot T$ is dihedral of order $2p$. By Lemma 8.4, $2p$ does not divide $|A|$ so we may assume that $T < B$. Let $\{1\} < Q \in \mathrm{Syl}_q(B)$ with $q \in \pi(B) - \{p\}$. Then $\mathrm{N}_G(T) \ge \langle u, Q\rangle = G$, by (i), a contradiction.

(v) Let u and v be as in (iv). Then, by (iv), there is $g \in G$ such that $\langle u, v\rangle \le P^g < A^g = P^g \times L^g$ so $L^g < \mathrm{C}_G(u) = A$, by (iii). Then $L^g = L$

and $v \in \mathrm{C}_G(L) < G$. Thus, $\mathrm{C}_G(L)$ contains all involutions v of G so G is not simple, a final contradiction[9]. $\square$

THEOREM 8.5 ([Keg]). *If a group G is a product of two nilpotent subgroups, it is solvable.*

PROOF. Suppose that $G = AB$, where A and B are nilpotent, is a minimal counterexample; then some prime $p \in \pi(A) \cap \pi(B)$ (Theorem 8.1). Let $A_0 \in \mathrm{Syl}_p(A)$ and $B_0 \in \mathrm{Syl}_p(B)$. Replacing, if necessary, B by its conjugate, one may assume that $K = \langle A_0, B_0 \rangle \le P \in \mathrm{Syl}_p(G)$. Clearly, $K \cap A = A_0$ and $K \cap B = B_0$ so, since K is factorized (Lemma 8.2), we get $K = A_0B_0$. As in part (i) of the proof of Theorem 8.1, we get $A_0B_0^g = B_0^gA$, all $g \in G$, and this is a proper subgroup of G. By Remark 8.1, one may assume that $A_0^G < G$. By induction, G has no nontrivial solvable normal subgroup. Therefore, since, by the modular law, A_0^GA and A_0^GB are factorized, we get $A_0^GA = G = A_0^GB$. It follows that p does not divide $|G : A_0^G|$ so $P^G = A_0^G$. Let $A_0 \le C_0 < A_0^G$, where C_0 is a maximal p-subgroup of A_0^G permutable with all conjugates of B_0. As above, $P^G = B_0^G$ so $A_0^G = B_0^G$; denote this subgroup by H. It follows that B_0^y does not normalizes C_0 for some $y \in H$ so there exists $x \in B_0^y$ such that $C_0^x \ne C_0$. Set $T = \langle C_0, C_0^x \rangle (> C_0)$. Since $T \le H$ is permutable with all conjugates of B_0, it follows from the choice of C_0 that T is not a p-subgroup. Since $TB_0^y = \langle C_0, C_0^x, B_0^y \rangle = \langle C_0, B_0^y \rangle = C_0B_0^y = B_0^yC_0$ is a p-subgroup, we get a contradiction. $\square$

9. A SOLVABILITY CRITERION

The following nice theorem is known in the case where M is solvable.

THEOREM 9.1. *Let $\{1\} < \mathbf{N}$ be normal in G and let M be a maximal subgroup of G with $M_G = \{1\}$. If $\{1\} < T$ is a minimal normal p-subgroup of M for some prime p and $M \cap \mathbf{N} = \{1\}$, then $\mathbf{N}$ is solvable.*

PROOF.[10] Clearly, $\mathbf{N}$ is a minimal normal subgroup of G. Since $M \le \mathrm{N}_G(T) < G$, we get $\mathrm{N}_G(T) = M$ and so $\mathrm{N}_{T\mathbf{N}}(T) = T$[11]. It follows that $T \in \mathrm{Syl}_p(T\mathbf{N})$ so $\mathbf{N}$ is a p'-subgroup (Theorem 1.1). Let $r \in \pi(\mathbf{N})$. By Theorem 1.1, p does not divide $|\mathrm{Syl}_r(\mathbf{N})|$ so there exists a T-invariant $R \in \mathrm{Syl}_r(\mathbf{N})$.

Assume that there is another T-invariant $R_1 \in \mathrm{Syl}_r(\mathbf{N})$; then $R_1 = R^x$ for some $x \in \mathbf{N}$ (Theorem 1.1). Hence both T and T^x normalize R_1 so $\langle T, T^x \rangle \le \mathrm{N}_{T\mathbf{N}}(R_1)$. Note that $T, T^x \in \mathrm{Syl}_p(T\mathbf{N})$ so $T, T^x \in \mathrm{Syl}_p(\mathrm{N}_{T\mathbf{N}}(R_1))$.

[9]Repeating, word for word, the proof of Theorem 8.1, we get the following result (A.N. Fomin). Let $G = AB$, where $(|A|, |B|) = 1$, $A = P \times L$ with $P \in \mathrm{Syl}_2(G)$ and $B = Q \times M$ with $Q \in \mathrm{Syl}_q(G)$, q is a prime. Then G is q-solvable.

[10]I am indebted to Janko who reported me this proof.

[11]It follows from the classification of finite simple groups, that $\mathbf{N}$ is solvable, and we are done. However, we want to give an elementary proof.

By Theorem 1.1, $T^z = T^x$ for some $z \in \mathrm{N}_{T\mathbf{N}}(R_1)$. By the modular law, $\mathrm{N}_{T\mathbf{N}}(R_1) = T\mathrm{N}_{\mathbf{N}}(R_1)$ so $z = tx_0$ for some $t \in T$ and $x_0 \in \mathrm{N}_{\mathbf{N}}(R_1)$. We have $T^x = T^z = T^{tx_0} = T^{x_0}$, and so $x_0x^{-1} \in \mathrm{N}_{\mathbf{N}}(T) = \{1\}$. Hence $x = x_0$. We get $R_1 = R^x = R^{x_0}$ so $R = R_1^{x_0^{-1}} = R_1$, a contradiction.

Take $y \in M$. Since T normalizes R then $T^y = T$ also normalizes R^y. By the previous paragraph, $R^y = R$, so M normalizes R. Since M is maximal in G, we get $MR = G$ so $R = \mathbf{N}$ and $\mathbf{N}$ is solvable. ∎

EXAMPLE 9.2. Let $G = A \times \mathbf{N}$. where A and $\mathbf{N}$ are isomorphic nonabelian simple groups, and let M be a diagonal subgroup of G. Then $M \cong A$ is maximal in G so $G = M\mathbf{N}$, $M \cap \mathbf{N} = \{1\}$ and $\mathbf{N}$ is nonsolvable. We also have $M_G = \{1\}$.

10. Abelian subgroups of maximal order in the symmetric group S_n

Now we prove the following

THEOREM 10.1.[12] *Let $G \leq \mathrm{S}_n$ be abelian of maximal order, where $n = k + 3m$ with $k \leq 4$. Then $G = A \times Z_1 \times \cdots \times Z_m$, where $A, Z_1, \ldots, Z_m$ are regular of degrees $k, 3, \ldots, 3$ (m times), respectively*[13].

LEMMA 10.2. *Let A be a maximal abelian subgroup of $G = H_1 \times \cdots \times H_r$. Then $A = (A \cap H_1) \times \cdots \times (A \cap H_r)$.*

PROOF. Let A_i be the projection of A into H_i, $i = 1, \ldots, r$. Then $A \leq B = A_1 \times \cdots \times A_r$ so $A = B$ since B is abelian and A is maximal abelian. Since $A_i = A \cap H_i$ for all i, we are done. ∎

PROOF OF THEOREM 10.1. If G is transitive, it is regular of order n since the G-stabilizer of a point equals $\{1\}$. If $n > 4$, S_n has an abelian subgroup of order $2(n-2) > n$, a contradiction. Thus, if G is transitive, then $n \leq 4$.

Let G be intransitive. Then $\{1, \ldots, n\} = \Omega_1 \cup \cdots \cup \Omega_r$ is the partition in G-orbits, $r > 1$, so $G \leq W = \mathrm{S}_{\Omega_1} \times \cdots \times \mathrm{S}_{\Omega_r}$, where S_{Ω_i} is the symmetric group on Ω_i, $i = 1, \ldots, r$. By Lemma 10.2, $G = T_1 \times \cdots \times T_r$, where $T_i = G \cap \mathrm{S}_{\Omega_i}$ is a regular abelian subgroup of S_{Ω_i}. By the previous paragraph, $|T_i| \leq 4$. Assume that $|T_1| = |T_2| = 4$. Then $\mathrm{S}_{\Omega_1 \cup \Omega_2}$ has an abelian subgroup B of order 18 contained in $\mathrm{S}_2 \times \mathrm{S}_3 \times \mathrm{S}_3$, and this is a contradiction since then $|G| < |B \times T_3 \times \cdots \times T_r|$. If $|T_1| = 2$ and $|T_2| = 4$, then $\mathrm{S}_{\Omega_1 \cup \Omega_2}$ has an abelian subgroup B of order 9 contained in $\mathrm{S}_3 \times \mathrm{S}_3$, and this is a contradiction since then $|G| < |B \times T_3 \times \cdots \times T_r|$. Similarly, equalities $|T_1| = |T_2| = |T_3| = 2$ are impossible. ∎

[12] Compare with [BM]

[13] Thus, if not all abelian subgroups of maximal order are conjugate in S_n, then $k = 4$ and S_n contains exactly two classes of such subgroups.

11. Characterization of simple groups

Let $\delta(G)$ be the minimal degree of a faithful representation of a group G by permutations. If $G \leq \mathrm{S}_{\delta(G)}$, then G has no one-element orbit. Given $G > \{1\}$, let $\mathrm{i}(G) = \min\{|G : H| \mid H < G\}$. For $G = \{1\}$, we set $\mathrm{i}(G) = 1$. Then $\delta(G) \geq \mathrm{i}(G)$ with equality if G is simple. If $H < G$ is normal, then $\mathrm{i}(G/H) \geq \mathrm{i}(G)$; if, in addition, $H \leq \Phi(G)$, then $\mathrm{i}(G/H) = \mathrm{i}(G)$. The size of each non one-element G-orbit is at least $\mathrm{i}(G)$. It follows that $G \leq \mathrm{S}_{\delta(G)}$ is transitive if $\delta(G) < 2\mathrm{i}(G)$; moreover, in that case the G-stabilizer of a point is maximal in G.

Theorem 11.1 ([Ber4]). *A group $G > \{1\}$ is simple if and only if $\delta(G) = \mathrm{i}(G)$*[14].

Proof. If G is simple, then $\mathrm{i}(G) = \delta(G)$. Now assume that $\delta(G) = \mathrm{i}(G)$ but G has a nontrivial normal subgroup N. Let $G \leq \mathrm{S}_{\delta(G)}$ and H the G-stabilizer of a point; then $|G : H| = \delta(G)$, H is maximal in G and G is transitive. We have $HN = G$ since $H_G = \{1\}$. Let $A \leq H$ be minimal such that $G = AN$; then $A > \{1\}$. Let A_1 be the A-stabilizer of a point moved by A; then $A_1 < A$ and $|A : A_1| \leq \delta(H) < \delta(G) = \mathrm{i}(G)$. By the choice of A, we have $A_1N < G$ so $|G : A_1N| \geq \mathrm{i}(G) > |A : A_1|$. On the other hand,

$$\begin{aligned} |G : A_1N| &= |AN : A_1N| = \frac{|A||N||A_1 \cap N|}{|A \cap N||A_1||N|} \\ &= |A : A_1|\frac{|A_1 \cap N|}{|A \cap N|} \leq |A : A_1| < \mathrm{i}(G), \end{aligned}$$

a final contradiction. □

Theorem 11.2 ([Ber4]). *If, for a group G, we have $\delta(G) = \mathrm{i}(G)+1$, then one of the following holds:*

(a) $G \cong \mathrm{S}_3$.
(b) $\delta(G) = 2^n$, $G = S \cdot \mathrm{E}_{2^n}$, *a semidirect product with kernel* E_{2^n}, $n > 1$, S *is a simple group*[15].

Proof. Let $G \leq \mathrm{S}_\Omega$ where $|\Omega| = \delta(G)$.

By Theorem 11.1, G is not simple. Let E be a minimal normal subgroup of G and let S be the G-stabilizer of a point; then $|G : S| = \delta(G) < 2\mathrm{i}(G)$ so G is transitive, S is maximal in G, $S_G = \{1\}$ and $G = SE$.

(i) Suppose that E is solvable. Then $\delta(G) = |E| = p^n$, a power of a prime p. In that case, $S \cap E = \{1\}$, $\mathrm{i}(G) = p^n - 1$ is not a multiple of p so, if H is a subgroup of index $\mathrm{i}(G)$ in G, then $E \leq H$. It follows that $\mathrm{i}(G) = \mathrm{i}(S)$. We

[14] It follows that if $H < G$ has index $\mathrm{i}(G)$ in G, then G/H_G is simple. If, in addition, G is solvable, then H is normal in G.

[15] If $G = \mathrm{AGL}(n, 2)$, $n > 2$, then $\mathrm{i}(G) = 2^n - 1$, $\delta(G) = 2^n$ so $\delta(G) = \mathrm{i}(G) + 1$. The Frobenius group $G = \mathrm{C}_{2^n-1} \cdot \mathrm{E}_{2^n}$ with prime $2^n - 1$ also satisfies $\delta(G) = \mathrm{i}(G) + 1$.

also have $\mathrm{C}_G(E) = E$. Therefore, if $n = 1$, then $\mathrm{i}(S) = p - 1$ is a prime so $p = 3$ and $G \cong \mathrm{S}_3$. Next let $n > 1$.

Assume that S is not simple. Then, by Theorem 11.1, $\delta(S) \geq \mathrm{i}(S) + 1 = p^n = \delta(G)$, a contradiction. Thus, S is simple.

Let S be solvable. In that case, $\mathrm{i}(S) = |S| = p^n - 1$ is a prime number and so $p = 2$ since $n > 1$; then G is a group of part (b).

Now let S be nonabelian simple. Let $L < E$ be of order p. Then $\mathrm{N}_G(L)$ is a proper subgroup of G of index $\leq \mathrm{c}_1(E) = \frac{p^n-1}{p-1}$. It follows that $\frac{p^n-1}{p-1} \geq \mathrm{i}(S) = p^n - 1$ so $p = 2$, and G is a group of part (b).

(ii) Now let E be nonsolvable. Let $A \leq S$ be minimal such that $AE = G$. Then $A \cap E \leq \Phi(A)$, by Remark 2.4, $G/E \cong A/(A \cap E)$ and

$$\delta(A) \geq \mathrm{i}(A) = \mathrm{i}(A/(A \cap E)) = \mathrm{i}(G/E) \geq \mathrm{i}(G) = \delta(G) - 1 \geq \delta(A),$$

so there are equalities throughout. It follows that $\delta(A) = \mathrm{i}(A)$ so A is simple (Theorem 11.1), $\mathrm{i}(A) = \mathrm{i}(G) = \delta(G) - 1$ and $G = A \cdot E$, a semidirect product with kernel E.

Let $p \in \pi(E)$ be odd, $P \in \mathrm{Syl}_p(E)$ and $N = \mathrm{N}_G(P)$; then $G = NE$ (Frattini). Let $B \leq N$ be as small as possible such that $BE = G$; then $B \cap E = \Phi(B)$ since $B/(B \cap E) \cong A$ is simple. It follows that $\mathrm{i}(B) = \mathrm{i}(A)(= \delta(G) - 1 = \mathrm{i}(G))$. Assume that $B \cap E > \{1\}$. Since $\delta(B) \leq \delta(G) < 2\mathrm{i}(G) = 2\mathrm{i}(B)$, B is transitive; moreover, the B-stabilizer of a point is maximal in B so contains $\Phi(B) = B \cap E > \{1\}$, a contradiction. Thus, $B \cap E = \{1\}$. Let $\{1\} < P_0 \leq P$ be a minimal B-invariant subgroup of P. Set $K = B \cdot P_0$.

Assume that $\mathrm{C}_K(P_0) > P_0$; then $K = B \times P_0$ and $|P_0| = p$. In that case, as it easy to see, $\delta(K) = \delta(B) + p > \delta(G)$ (recall that $p > 2$), a contradiction.

Thus, $\mathrm{C}_K(P_0) = P_0$. Set $|P_0| = p^n$. Then, as in (i), $\mathrm{c}_1(P_0) = \frac{p^n-1}{p-1} \geq \mathrm{i}(B)$ so $p^n > 2\mathrm{i}(B) = 2\mathrm{i}(G) > \delta(G)$ since $p > 2$. Let $H < K$ be such that $|K : H| = \mathrm{i}(K)(\leq \mathrm{i}(B))$. By what has just been proved, $H \cap P_0 > \{1\}$. It follows that $HP_0 < K$ so $|K : HP_0| \geq \mathrm{i}(B)$, and we conclude that $\mathrm{i}(K) = \mathrm{i}(B)$ and $P_0 < H$. It follows that there are at least two K-orbits on Ω so $\delta(K) \geq 2\mathrm{i}(K) = 2\mathrm{i}(B) = 2\mathrm{i}(G) > \delta(G)$, a final contradiction. □

12. On a problem of p-group theory

Consider the following

Problem 1. Classify the nonabelian p-groups G possessing a subgroup Z of order p which contained in the unique abelian subgroup E of type (p, p).

Blackburn [Bla] has posed the following problem. Classify the 2-groups G possessing an involution which contained in only one subgroup of G of order 4. This problem, a partial case of Problem 1, was solved in [BoJ]. Problem 1 is essentially more difficult.

Theorem 12.1. *Let Z be a subgroup of order p of a p-group G such that there is in G only one abelian subgroup of type (p, p), say E, that contains*

Z. Let G be not a 2-group of maximal class; then G has a normal abelian subgroup V of type (p,p). Set $T = \mathrm{C}_G(V)$. In that case, G has no normal subgroup of order p^{p+1} and exponent p and one of the following holds:

(a) *Let $E \neq V$. Then $G = Z \cdot T$. We have $C_G(Z) = Z \times Q$, where $Q = \mathrm{C}_T(Z)$ is either cyclic or generalized quaternion.*
(b) *Now let $E = V$. Then $\Omega_1(T) = E$. If $p > 2$, then T is metacyclic. If $t \in G - T$ is an element of order p, then $G = \langle t \rangle \cdot T$ and $C_G(t) = \langle t \rangle \times Q$, where Q is either cyclic or generalized quaternion. Next, G has no subgroup $\cong \mathrm{E}_{p^3}$.*

Proof. If $Z < K \leq G$, then $K \not\cong \mathrm{E}_{p^3}$.

Assume that G has a normal subgroup H of order p^{p+1} and exponent p. By hypothesis, $\mathrm{C}_{HZ}(Z) \cong \mathrm{E}_{p^2}$ so HZ is of maximal class (Lemma J(j)), contrary to Lemma J(k). Then, by Remark 6.1, G has a normal abelian subgroup V of type (p,p). Set $T = \mathrm{C}_G(V)$.

Suppose that Z is not contained in V; then $E \neq V$ and $|G : T| = p$ since Z is not contained in T (otherwise, $ZV = Z \times V \cong \mathrm{E}_{p^3}$). We have $G = Z \cdot T$, a semidirect product, and $\mathrm{C}_G(Z) = Z \times \mathrm{C}_T(Z)$, by the modular law. Next, $\mathrm{C}_T(Z)$ has no abelian subgroup of type (p,p) (otherwise, if that subgroup is R, then $Z \times R \cong \mathrm{E}_{p^3}$). Then, by Remark 6.1, $\mathrm{C}_T(Z)$ is either cyclic or generalized quaternion.

Let $Z < V$ so $E = V$. In that case, $\Omega_1(T) = V$ so, if $p > 2$, then T is metacyclic (Blackburn; see [Ber3, Theorem 6.1]). Assume that $\mathrm{E}_{p^3} \cong U < G$. Considering $U \cap T$, we see that $Z < U$, a contradiction. Thus, G has no subgroup $\cong \mathrm{E}_{p^3}$. If $t \in G - T$ is of order p, then, as above, $\mathrm{C}_G(t) = \langle t \rangle \times \mathrm{C}_T(t)$, where $\mathrm{C}_T(t)$ is cyclic or generalized quaternion. $\square$

The 2-groups G containing an involution t such that $\mathrm{C}_G(t) = \langle t \rangle \times Q$, where Q is either cyclic or generalized quaternion, are classified in [Jan1, Jan2]. The p-groups without normal subgroup $\cong \mathrm{E}_{p^3}$, are classified for $p > 2$ by Blackburn (see [Ber5, Theorem 6.1]) and for $p = 2$ their classification is reduced to Problem 2, below (see [Jan3]).

Thus, Problem 1 is reduced to the following two outstanding problems:

Problem 2. (Old problem) Classify the 2-groups G with exactly three involutions.

Problem 3. (Blackburn) Classify the p-groups G, $p > 2$, containing a subgroup Z of order p such that $\mathrm{C}_G(Z) = Z \times Q$, where Q is cyclic.

Janko [Jan4] obtained a number of deep results concerning Problem 2. He reduced this problem to the case where G has a normal metacyclic subgroup M of index at most 4. It is easy to show that if $|G : M| = 2$ and G is nonmetacyclic, then the set $G - M$ has an element x of order 4 so, in this case, there is a strong hope to obtain complete classification.

13. The order of the automorphism group of an abelian p-group

In this section we find the order of the automorphism group of an abelian p-group.

Let

$$B = \{x_{1,1}, \dots, x_{1,\alpha_1}, x_{2,1}, \dots, x_{2,\alpha_2}, \dots, x_{r,1}, \dots, x_{r,\alpha_r}\},$$
$$B_1 = \{y_{1,1}, \dots, y_{1,\alpha_1}, x_{2,1}, \dots, y_{2,\alpha_2}, \dots, y_{r,1}, \dots, y_{r,\alpha_r}\}$$

be two bases of an abelian p-group G such that

$$o(x_{i,j}) = o(y_{i,j}) = p^{e_i},\ i = 1, \dots, r, j = 1, \dots, \alpha_i.$$

These bases we call *automorphic* since there is *the* $\phi \in \mathrm{Aut}(G)$ such that $x_{i,j}^{\phi} = y_{i,j}$ for all i, j. Conversely, each automorphism of G sends one basis in an automorphic one. The set of bases of G is partitioned in classes of automorphic bases. The group $\mathrm{Aut}(G)$ acts regularly on each class of automorphic bases. Therefore, to find the order of $\mathrm{Aut}(G)$, it suffices to find the cardinality of an arbitrary class of automorphic bases. The number of all bases of G equals $M = (p^d - 1)(p^d - p)\dots(p^d - p^{d-1})|\Phi(G)|^d$, where $d = \mathrm{d}(G)$, so M is a multiple of $|\mathrm{Aut}(G)|$. It is easy to show, and this follows from Theorem 13.1, that $|\mathrm{Aut}(G)| = M$ if and only if G is homocyclic.

Remark 13.1. Let $x_1, \dots, x_d$ be generators of an abelian p-group G of rank d. By the product formula, $\prod_{i=1}^d o(x_i) \geq |G|$. We claim that, if $\prod_{i=1}^d o(x_i) = |G|$, then $G = \langle x_1 \rangle \times \dots \times \langle x_d \rangle$. Indeed, we have $G = \langle x_1 \rangle \dots \langle x_d \rangle$. Using product formula, we get $\langle x_1 \rangle \cap \langle x_2, \dots x_d \rangle = \{1\}$ so that $G = \langle x_1 \rangle \times \langle x_2, \dots x_d \rangle$. Now, by induction, $\langle x_2, \dots, x_d \rangle = \langle x_2 \rangle \times \dots \times \langle x_d \rangle$ since $\prod_{i=2}^d o(x_i) = |G/\langle x_1 \rangle| = |\langle x_2, \dots, x_d \rangle|$.

In what follows, G is an abelian group of order p^m and type $(\alpha_1 \cdot p^{e_1}, \dots, \alpha_r \cdot p^{e_r})$, where all $\alpha_i \geq 0$ and $e_1 > \dots > e_r \geq 1$. That group has exactly α_i invariants p^{e_i}, all i.

Our solution is divided in r steps.

COMPUTATION OF $|\mathrm{Aut}(G)|$

Step 1. First we choose α_1 elements of maximal order p^{e_1}. All of them lie in the set $G - T_1$, where $T_1 = \Omega_{e_1 - 1}(G)$ ($G - T_1$ is the set of elements of order p^{e_1} in G). Set $f_1 = m$ and $|T_1| = p^{t_1}$. We have $f_1 - t_1 = \alpha_1$ so $|G : T_1| = p^{\alpha_1}$.

As $x_{1,1}$ we take any element of the set $G - T_1$ of cardinality $|G| - |T_1|$. As $x_{1,2}$ we take any element in the set $G - \langle x_{1,1}\, T_1 \rangle$ of cardinality $|G| - p|T_1|$. Continuing so, we take an α_1-th element x_{1,α_1} in the set $G - \langle x_{1,1}, \dots, x_{1,\alpha_1 - 1}, T_1 \rangle$ of cardinality $|G| - p^{\alpha_1 - 1}|T_1|$. Thus, α_1 elements $x_{1,1}, \dots, x_{1,\alpha_1}$ of order p^{e_1} one can choose by

$$\begin{aligned} N_1 &= (p^{f_1} - p^{t_1})(p^{f_1} - p^{1+t_1})\dots(p^{f_1} - p^{\alpha_1 - 1 + t_1}) \\ &= (p^{\alpha_1} - 1)\dots(p^{\alpha_1} - p^{\alpha_1 - 1})p^{\alpha_1 t_1} \end{aligned}$$

ways. By the choice, $|\langle x_{1,1},\dots,x_{1,\alpha_1},\Phi(G)\rangle/\Phi(G)|=p^{\alpha_1}$.

Step 2. Now we choose α_2 elements $x_{2,1},\dots,x_{2,\alpha_2}$ of order p^{e_2} in the set $\Omega_{e_2}(G)-T_2$, where $T_2=\Omega_{e_2}(\Phi(G))\Omega_{e_2-1}(G)$ (if an element of order p^{e_2} generates, modulo $\Phi(G)$, together with $\langle x_{1,1},\dots,x_{1,\alpha_1}\rangle$ a subgroup of order p^{α_1+1}, it must lie in the set $\Omega_{e_2}(G)-T_2$). We have $|\Omega_{e_2}(G)|=p^{f_2}$, where $f_2=(\alpha_1+\alpha_2)e_2+\alpha_3e_3+\cdots+\alpha_re_r$ and $|T_2|=p^{t_2}$, where $t_2=\alpha_1e_2+(e_2-1)\alpha_2+\alpha_3e_3+\cdots+\alpha_re_r$ so that $|\Omega_{e_2}(G):T_2|=p^{f_2-t_2}=p^{\alpha_2}$.

As $x_{2,1}$ we take any element of the set $\Omega_{e_2}(G)-T_2$ of cardinality $p^{f_2}-p^{t_2}$. As $x_{2,2}$ we take any element in the set $\Omega_{e_2}(G)-\langle x_{2,1},T_2\rangle$ of cardinality $p^{f_2}-p^{t_2+1}$. Continuing so, we can choose α_2 elements $x_{2,1},\dots,x_{2,\alpha_2}$ of order p^{e_2} by

$$\begin{aligned}N_2 &= (p^{f_2}-p^{t_2})(p^{f_2}-p^{1+t_2})\dots(p^{f_2}-p^{\alpha_2-1+t_2})\\ &= (p^{\alpha_2}-1)\dots(p^{\alpha_2}-p^{\alpha_2-1})p^{\alpha_2t_2}\end{aligned}$$

ways. By the choice, $|\langle x_{1,1},\dots,x_{1,\alpha_1},x_{2,1},\dots,x_{2,\alpha_2},\Phi(G)\rangle/\Phi(G)|=p^{\alpha_1+\alpha_2}$.

Step 3. All wanted elements of order p^{e_3} are contained in the set $\Omega_{e_3}(G)-T_3$, where $T_3=\Omega_{e_3}(\Phi(G))\Omega_{e_3-1}(G)$. We have $|\Omega_{e_3}(G)|=p^{f_3}$, where $f_3=(\alpha_1+\alpha_2+\alpha_3)e_3+\alpha_4e_4+\cdots+\alpha_re_r$, $|T_3|=p^{t_3}$, where $t_3=(\alpha_1+\alpha_2)e_3+(e_3-1)\alpha_3+\alpha_4e_4+\cdots+\alpha_re_r$ so that $|\Omega_{e_3}(G):T_3|=p^{f_3-t_3}=p^{\alpha_3}$. Acting as above, one can choose α_3 elements $x_{3,1},\dots,x_{3,\alpha_3}$ of order p^{e_3} by

$$\begin{aligned}N_3 &= (p^{f_3}-p^{t_3})(p^{f_3}-p^{1+t_3})\dots(p^{f_3}-p^{\alpha_3-1+t_3})\\ &= (p^{\alpha_3}-1)\dots(p^{\alpha_3}-p^{\alpha_3-1})p^{\alpha_3t_3}\end{aligned}$$

ways. So chosen $\alpha_1+\alpha_2+\alpha_3$ elements generate, modulo $\Phi(G)$, the subgroup of order $p^{\alpha_1+\alpha_2+\alpha_3}$.

And so on. Finally,

Step r. At last, we will choose α_r wanted elements $x_{r,1},\dots,x_{r,\alpha_r}$ of order p^{e_r}. All of them lie in the set $\Omega_{e_r}(G)-T_r$, where $T_r=\Omega_{e_r}(\Phi(G))\Omega_{e_r-1}(G)$. As above, these elements may be chosen by

$$N_r=(p^{\alpha_r}-1)(p^{\alpha_r}-p)\dots(p^{\alpha_r}-p^{\alpha_r-1})p^{\alpha_rt_r}$$

ways.

The elements

$x_{1,1},\dots,x_{1,\alpha_1},x_{2,1},\dots,x_{2,\alpha_2},\dots,x_{x,1},\dots,x_{r,\alpha_r}$, in view of their choice, generate G. Since the product of their orders equals $|G|$, it follows, by Remark 13.1, that they form a basis of G. Thus, $|\mathrm{Aut}(G)|=\prod_{i=1}^r N_i$ so we get

THEOREM 13.1. *If G is an abelian p-group of type $(\alpha_1\cdot p^{e_1},\dots,\alpha_r\cdot p^{e_r})$, then*

$$|\mathrm{Aut}(G)|=p^{\sum_{i=1}^r\alpha_it_i}\prod_{i=1}^r(p^{\alpha_i}-1)(p^{\alpha_i}-p)\dots(p^{\alpha_i}-p^{\alpha_i-1}),$$

where $t_i=(\alpha_1+\cdots+\alpha_{i-1})e_i+(e_i-1)\alpha_i+\sum_{j=i+1}^r\alpha_je_j$.

14. A condition for $\Phi(G) \le \mathrm{Z}(G)$, where G is a p-group, $p > 2$

In this section we prove the following

Theorem 14.1. *For a p-group G, $p > 2$, the following conditions are equivalent:*

(a) *All subgroups of $\Phi(G)$ are normal in G.*
(b) $\Phi(G) \le \mathrm{Z}(G)$.

Proof. It suffices to show that (a) $\Rightarrow$ (b). Let G be nonabelian and $|\Phi(G)| > p$.

Let $\Phi(G)$ be cyclic and U a maximal cyclic subgroup of G containing $\Phi(G)$. If $|G : U| = p$, the result follows from Lemma J(f) so let $|G : U| > p$. Let $U < T < G$, where $|T : U| = p$. Then $\Omega_1(T) \cong \mathrm{E}_{p^2}$ centralizes $\Phi(G)$. If $U = \Phi(G)$, then T is abelian. If $|U : \Phi(G)| = p$, then $\Phi(G) = \Phi(T) \le \mathrm{Z}(T)$ (Lemma J(f)), whence $\mathrm{C}_G(\Phi(G)) \ge T$. Since all such T generate G, we get $\Phi(G) \le \mathrm{Z}(G)$.

Now let $\Phi(G)$ be noncyclic; then $\Phi(G)$ is Dedekindian so abelian. Let $\Phi(G) = U_1 \times \cdots \times U_n$, where $U_1, \dots, U_n$ are cyclic. Working by induction on $|G|$, we get $[\Phi(G), G] \le \bigcap_{i=1}^n U_i = \{1\}$, completing the proof. ∎

If $n > 2$, $p > 2$ and $G = \langle a, b \mid a^{p^n} = b^{p^{n-1}} = 1, a^b = a^{1+p} \rangle$, then $G' = \langle a^p \rangle$ is cyclic so all subgroups of G' are normal in G but G' is not contained in $\mathrm{Z}(G)$. Therefore, it is impossible, in Theorem 14.1, to take G' instead of $\Phi(G)$.

Recently Janko [Jan5] classified the p-groups G in which every nonnormal subgroup is contained in a unique maximal subgroup of G. The original proof in the case $p > 2$ is fairly involved. Theorem 14.2 allows us to simplify the proof essentially.

Theorem 14.2 ([Jan5]). *The following conditions for a nonabelian p-group G, $p > 2$, are equivalent:*

(a) *Every nonnormal subgroup is contained in a unique maximal subgroup of G.*
(b) *G is minimal nonabelian (see Lemma 16.1).*

Proof. If H is a nonnormal subgroup of a minimal nonabelian p-group G, then $H\Phi(G)$ is the unique maximal subgroup of G since $\mathrm{d}(G) = 2$ and H is not contained in $\mathrm{Z}(G) = \Phi(G)$. Thus, (b) $\Rightarrow$ (a).

It remains to prove that (a)$\Rightarrow$ (b). The group G has a nonnormal cyclic subgroup, say U. By hypothesis, all subgroups of $\Phi(G)$ are normal in G so $\Phi(G) \le \mathrm{Z}(G)$ (Theorem 14.1). We have $U\Phi(G) < G$ so $U\Phi(G)$ is the unique maximal subgroup of G containing U since $G/\Phi(G)$ is elementary abelian. It follows that $\mathrm{d}(G)=2$. Then $\Phi(G)=\mathrm{Z}(G)$ has index p^2 in G so it is minimal nonabelian[16]. ∎

Theorem 14.1 is not true for $G=\mathrm{D}_{16}$. However, we have the following

SUPPLEMENT TO THEOREM 14.1. Let G be a 2-group such that all subgroups of $\Phi(G)$ are normal in G. Then the following conditions are equivalent:

(a) $\Phi(G)\leq \mathrm{Z}(G)$.

(b) G has no subgroup of maximal class and order 2^4.

To prove, it suffices to repeat, word for word, the proof of Theorem 14.1.

15. p-GROUPS WITH FAITHFUL IRREDUCIBLE CHARACTER OF DEGREE p^n HAS DERIVED LENGTH AT MOST $n+1$

In this section we prove the following

THEOREM 15.1. *If a p-group G has a faithful irreducible character χ of degree p^n, then its derived length* $\mathrm{dl}(G)\leq n+1$, *and this estimate is best possible.*

PROOF. We use induction on n. One may assume that $n>0$.

Let G have no normal abelian subgroup of type (p,p). Then G is a 2-group of maximal class, by Remark 6.1; then $n=1$, by [Isa2, Theorem 6.15], and $\mathrm{dl}(G)=2=n+1$.

Next we assume that G has a normal abelian subgroup R of type (p,p); then $|G:\mathrm{C}_G(R)|\leq p$ so there exists a maximal subgroup M of G such that $R\leq M\leq \mathrm{C}_G(R)$. By Lemma J(g), the restriction χ_M of χ to M is reducible. By Clifford theory, $\chi_M=\mu_1+\cdots+\mu_p$, where $\mu_1,\dots,\mu_p$ are pairwise distinct irreducible characters of M, all of the same degree p^{n-1}. We also have $\bigcap_{i=1}^p\ker(\mu_i)=\{1\}$ since χ is faithful. Then, by induction, $\mathrm{dl}(M/\ker(\mu_i))\leq(n-1)+1=n$. Since M is isomorphic to a subgroup of the direct product $(M/\ker(\mu_1))\times\cdots\times(M/\ker(\mu_p))$, we get $\mathrm{dl}(M)\leq n$. Since G/M is abelian (of order p), the derived length of G is at most $n+1$.[17]

It remains to show that $G=\Sigma_{n+1}\in\mathrm{Syl}_p(\mathrm{S}_{p^{n+1}})$ has derived length $n+1$ and a faithful irreducible character of degree p^n. The first assertion is well known. We have $G=H\,\mathrm{wr}\,\mathrm{C}_p$, the standard wreath product with 'passive' factor $H\cong\Sigma_n$ and 'active' factor C_p of order p. In that case,

---

[16] Let us prove the following related result. If every minimal nonabelian subgroup is contained in a unique maximal subgroup of a p-group G, then either (i) $\mathrm{d}(G)=2$ and $\Phi(G)$ is abelian, or (ii) $\mathrm{d}(G)=3$ and $\Phi(G)$ is contained in $\mathrm{Z}(G)$. Indeed, groups from (i) and (ii) satisfy the hypothesis. Now let $\mathrm{d}(G)>2$ and G satisfies the hypothesis. Take minimal nonabelian subgroup H in G. Then $H\Phi(G)$ is maximal in G since $\Phi(H)\leq\Phi(G)$, and we conclude that $\mathrm{d}(G)=3$ since $\mathrm{d}(H)=2$. If $\Phi(G)<T<G$ with $|T:\Phi(G)|=p$, then T is abelian since T is contained in $p+1$ maximal subgroups of G so it has no minimal nonabelian subgroup. Since such subgroups T generate G and centralize $\Phi(G)$, it follows that $\Phi(G)$ is contained in $\mathrm{Z}(G)$.

[17] According to the letter of Ito, he also proved this inequality; his proof is the same.

the base $B = H_1 \times \cdots \times H_p$ of our wreath product has index p in G, and $H_i \cong H$. Let $F = H_2 \times \cdots \times H_p$ and let ϕ be a faithful irreducible character of degree p^{n-1} of $B/F \cong H$ existing by induction. Set $\chi = \phi^G$ and prove that χ is irreducible and faithful (of degree p^n), thereby completing the proof. Since $\ker(\chi) = \ker(\phi)_G = F_G = \{1\}$, the character χ is faithful. Assume, however, that χ is reducible. Then, by Clifford theory, $\chi = \tau_1 + \cdots + \tau_p$, where $\tau_i(1) = p^{n-1}$ for $i = 1, \ldots, p$, hence, by reciprocity, $\chi_B = p \cdot \phi$ so $F = \ker(\phi) \leq \ker(\chi) = \{1\}$, a contradiction. □

Definition 15.2. *A group G is said to be an M^*-group if it satisfies the following condition. Whenever H is a subnormal subgroup of G and χ is a nonlinear irreducible character of H, there exists in H a normal subgroup A of prime index such that χ_A is reducible. We consider abelian groups as M^*-groups.*

Obviously, subnormal subgroups and epimorphic images of M*-groups are M*-groups so, by induction, M*-groups are solvable. The p-groups, being M-groups, are also M*-groups. The symmetric group S_4 is an M-group but not an M*-group.

If m is a natural number, then $\lambda(m)$ denotes the number of prime factors of m (multiplicities counted). For example, $\lambda(32) = 5$, $\lambda(96) = 6$.

Supplement to Theorem 15.1.[18] Suppose that an M*-group G has a faithful irreducible character χ. Then $\mathrm{dl}(G) \leq \lambda(\chi(1)) + 1$.

Proof. One may assume that G is nonabelian; then $\lambda(\chi(1)) = n > 0$. We are working by induction on n. Let T be a normal subgroup of prime index, say p, such that χ_T is reducible. Then, by Clifford theory, $\chi_T = \mu_1 + \cdots + \mu_p$, where $\mu_1, \ldots, \mu_p$ are pairwise distinct G-conjugate irreducible characters of M. We have $\mu_i(1) = \chi(1)/p$ so $\lambda(\mu_i(1)) = n - 1$ and $\mathrm{dl}(T/\ker(\mu_i)) \leq (n - 1) + 1 = n$, by induction. It follows that $T^{(n)}$, the n-th derived subgroup of T, is contained in $\bigcap_{i=1}^{p} \ker(\mu_i) = T \cap \ker(\chi) = \{1\}$, so $\mathrm{dl}(T) \leq n$. Since G/T is abelian, we get $\mathrm{dl}(G) \leq \mathrm{dl}(G/T) + 1 \leq n + 1$. □

16. On groups of order p^4

In this section we clear up the subgroup and normal structure of groups of order p^4 using two easy general Lemmas 16.1 and J(j). In particular, we obtain their classification in the case $p = 2$.

Lemma 16.1 (Redei). *Let G be a minimal nonabelian p-group. Then one of the following holds:*

(a) $G = \langle a, b \mid a^{p^m} = b^{p^m} = 1, a^b = a^{1+p^{m-1}} \rangle$, $m > 1$.
(b) $G = \langle a, b, c \mid a^{p^m} = b^{p^n} = c^p = 1, a^b = ac, [a, c] = [b, c] = 1 \rangle$.
(c) $G \cong Q_8$.

[18] The supplement and its proof were inspired by Isaacs' letter at Jan. 29, 2005.

Remark 16.1. It is easy to prove that $A \cong B$, where $A = Q * X$ and $B = D * Y$ are groups of order 2^4 and $Q \cong \mathrm{Q}_8$, $D \cong \mathrm{D}_8$, $X \cong Y \cong \mathrm{C}_4$. Next, for $p > 2$, we have $C \cong D$, where $C = M * U$ and $D = E * V$ of order p^4, where M and E are nonabelian of order p^3 and exponent p^2 and p, respectively (in our case, $\Omega_1(C)$ is of order p^3 and exponent p and $C = \Omega_1(C) * U$ so $\Omega_1(C)$ is nonabelian, and we get $C \cong D$).

Let G be a group of order p^4. Then one of the following holds:

(i) G is abelian of one of the following five types: (p^4), (p^3, p), (p^2, p^2), (p^2, p, p), (p, p, p, p).

(ii) G is minimal nonabelian. According to Lemma 16.1, there are exactly three types of such groups and two of them are metacyclic (namely, groups from Lemma 16.1(a) with $\{m, n\} = \{3, 1\}, \{2, 2\}$ and the nonmetacyclic group of Lemma 16.1(b) with $m = 2$, $n = 1$.

(iii) G is of maximal class (if $p = 2$, there are exactly three types of such groups, by Theorem 6.1).

(iv) $G = M \times C$, where M is nonabelian of order p^3 and $|C| = p$ (two types).

(v) $G = M * \mathrm{C}_{p^2}$, where M is nonabelian of order p^3 and exponent p (one type).

Indeed, suppose that G is not such as in parts (i)–(iii). Then it contains a minimal nonabelian subgroup M of order p^3. By Lemma J(j), $G = M\mathrm{Z}(G)$. If $\mathrm{Z}(G)$ is noncyclic, then $G = M \times \mathrm{C}_p$, and we get two groups from (iv) (there are two types of nonabelian groups of order p^3). Now suppose that $\mathrm{Z}(G)$ is cyclic and M is metacyclic. Then $|G'| = p$ and $\Phi(G) = G' = \mho_1(G)$. For each p, we get one group, by Remark 16.1. Thus, there are $5+3+2+1 = 11$ types of groups of order p^4, which are not of maximal class so there are exactly $11 + 3 = 14$ types of groups of order 2^4 (Theorem 6.1).

Acknowledgements.

I am indebted to Zvonimir Janko. Martin Isaacs and Noboru Ito for useful suggestions and discussion.

References

[Bae] R. Baer, *Supersoluble immersion*, Can. J. Math. **11** (1959), 353–369.

[BM] R. Bercov and L. Moser, *On abelian permutation groups*, Canad. Math. Bull. **8** (1965), 627–630.

[Ber1] Y. Berkovich, *A corollary of Frobenius' normal p-complement theorem*, Proc. Amer. Math. Soc. **127, 9** (1999), 2505–2509.

[Ber2] Y. Berkovich, *A generalization of theorems of Carter and Wielandt*, Soviet Math. Dokl. **7** (1966), 1525–1529.

[Ber3] Y. Berkovich, *On p-groups of finite order*, Siberian Math. Zh. **9** (1968), 1284–1306 (Russian).

[Ber4] Y. Berkovich, A *necessary and sufficient condition for the simplicity of a finite group*, Algebra and number theory, Nal'chik (1979), 17–21 (Russian).

[Ber5] Y. Berkovich, *On abelian subgroups of p-groups*, J. Algebra **199** (1998), 262–280.

[Ber6] Y. Berkovich, *Groups of Prime Power Order, Part I*, in preparation.
[BJ] Y. Berkovich and Z. Janko, *Groups of Prime Power Order, Part III*, in preparation.
[BK] Y. Berkovich and L. Kazarin, *Indices of elements and normal structure of finite groups*, J. Algebra **283** (2005), 564–583.
[Bla] N. Blackburn, *Groups of prime-power order having an abelian centralizer of type* $(r, 1)$, Mh. Math. **99** (1985), 1–18.
[BoJ] Z. Božikov and Z. Janko, *On a question of N. Blackburn about finite* 2*-groups*, Israel J. Math., to appear.
[Bur] W. Burnside, The Theory of Groups of Finite Order, Dover, NY, 1955.
[Car] R. Carter, *Nilpotent self-normalizing subgroups of soluble groups*, Math. Z. **75** (1961), 136–139.
[Chu] S.A. Chunikhin, *On solvable groups*, Izv. NIIMM of Tomsk Univ. **2** (1938), 220–223.
[Gas] W. Gaschütz, Lectures on Subgroups of Sylow Type in Finite Solvable Groups, Australian Nat. Univ., 1979.
[Hal1] P. Hall, *A note on a soluble groups*, J. London Math. Soc. **3** (1928), 98–105.
[Hal2] P. Hall, *A characteristic property of soluble groups*, J. London Math. Soc. **12** (1937), 198–200.
[Hal3] P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. **2, 40** (1936), 468–501.
[Hup] B. Huppert, Endliche Gruppen, Bd. I, Springer, Berlin, 1967.
[Isa1] I.M. Isaacs, Algebra. A Graduate Course, Brooks/Cole, Pacific Grove, 1994.
[Isa2] I.M. Isaacs, Character Theory of Finite Groups, Academic Press, NY, 1976.
[Jan1] Z. Janko, *Finite* 2*-groups with small centralizer of an involution*, J. Algebra **241** (2001), 818–826.
[Jan2] Z. Janko, *Finite* 2*-groups with small centralizer of an involution, 2*, J. Algebra **245** (2001), 413–429.
[Jan3] Z. Janko, *Finite* 2*-groups with no normal elementary abelian subgroups of order* 8, J. Algebra **246** (2001), 951–961.
[Jan4] Z. Janko, *Finite* 2*-groups with three involutions*, J. Algebra, to appear.
[Jan5] Z. Janko, *Finite* p*-groups with uniqueness condition for nonnormal subgroups*, manuscript.
[Keg] O.H. Kegel, *Produkte nilpotenter Gruppen*, Arch. Math. **12** (1961), 90–93.
[Kul] A. Kulakoff, *Über die Anzahl der eigentlichen Untergruppen und die Elemente von gegebener Ordnung in* p*-Gruppen*, Math. Ann. **104** (1931), 779–793.
[Ore] O. Ore, *Contributions to the theory of groups of finite order*, Duke Math. J. **5** (1938), 431–460.
[Suz] M. Suzuki, Group Theory II, Springer, New York, 1986.
[Weh] B.A.F. Wehrfritz, Finite Groups, World Scientific, Singapore, 1999.
[Wie1] H. Wielandt, *Sylowgruppen and Kompositionsstruktur*, Abhandl. Math. Seminar Univ. Hamburg **22** (1958), 215–228.
[Wie2] H. Wielandt, *Über Produkte von nilpotenten Gruppen*, Illinois J. Math. **2** (1958), 611–618.

Y. Berkovich
Department of Mathematics
University of Haifa
Mount Carmel, Haifa 31905
Israel
E-mail: berkov@math.haifa.ac.il

Received: 2.3.2005.
Revised: 2.5.2005 & 20.7.2005.