

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

FEDERICO MENEGAZZO

Dual-Dedekind subgroups in finite groups

Rendiconti del Seminario Matematico della Università di Padova,
tome 45 (1971), p. 99-111

[<http://www.numdam.org/item?id=RSMUP_1971__45__99_0>](http://www.numdam.org/item?id=RSMUP_1971__45__99_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1971, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*
<http://www.numdam.org/>

DUAL-DEDEKIND SUBGROUPS IN FINITE GROUPS

FEDERICO MENEGAZZO *)

If G is a group and H is a subgroup of G , H is dual-Dedekind in G , or a $\tilde{\mathfrak{D}}$ -subgroup of G (written $H\tilde{\mathfrak{D}}G$) if the following conditions are fulfilled:

$$\text{i) } X \supseteq Y \Rightarrow (Y \cup H) \cap X = Y \cup (H \cap X)$$

$$\text{ii) } H \supseteq Y \Rightarrow (Y \cup X) \cap H = Y \cup (X \cap H)$$

for every pair X, Y of subgroups of G (for the dual notion, namely that of Dedekind subgroups, there called « modular subgroups », see [4]). In this paper we are particularly concerned with the properties of « minimum » $\tilde{\mathfrak{D}}$ -subgroups (i.e. minimal in the set of non identity dual-Dedekind subgroups of a given group G); we establish some necessary conditions in order that a finite group G has non-trivial (i.e. different from 1, G) $\tilde{\mathfrak{D}}$ -subgroups. From these it will follow that a finite group having non-trivial $\tilde{\mathfrak{D}}$ -subgroups cannot be simple (Theorem 3.3) — a similar result for Dedekind subgroups is proved in [2]; it is perhaps worth noting that the converse is false: G non-simple is not a sufficient condition for G to have a non-trivial $\tilde{\mathfrak{D}}$ -subgroup. The proposition « if $N \trianglelefteq G$, then $N\tilde{\mathfrak{D}}G$ » for arbitrary G is false; in the second half of the paper we determine all finite soluble groups where such a condition holds. The main result in this section is (Theorem 4.6): G is soluble and every

*) Indirizzo dell'A.: Seminario Matematico dell'Università di Padova.

Lavoro eseguito nell'ambito dei gruppi di ricerca matematici del C.N.R.

normal subgroup of G is dual-Dedekind in G iff $G = H_1 \times H_2 \times \dots \times H_t$ with each H_i a Hall subgroup of G and either

i) H_i is a modular p -group; or

ii) $H_i = (P_{i1} \times \dots \times P_{is_i})Q_i$ with P_{ij} , Q_i Sylow subgroups of G for different primes, P_{ij} abelian of odd order ($j=1, \dots, s_i$), $Q_i = \langle b_i \rangle$ with b_i inducing a non-identity power automorphism on each P_{ij} .

1. Let L be a lattice. An element $a \in L$ is a dual-Dedekind element of L (a $\mathfrak{D}$ -element of L , $a\mathfrak{D}L$) if

$$\text{i) } x \geq y \Rightarrow (y \cup a) \cap x = y \cup (a \cap x);$$

$$\text{ii) } a \geq y \Rightarrow (y \cup x) \cap a = y \cup (x \cap a)$$

hold for every pair (x, y) of elements in L . Notice that $a\mathfrak{D}L$ if and only if a is a Dedekind element in $\tilde{L}$ (the dual lattice of L); hence properties of $\mathfrak{D}$ -elements of L are properties of Dedekind elements of $\tilde{L}$. We shall use mostly (see [4]):

I) $a\mathfrak{D}L$ iff for every $b \in L$ the maps

$$\varphi^b : x \rightarrow x \cup b \quad \varphi^b : [a/a \cap b] \rightarrow [a \cup b/b]$$

$$\varphi_a : y \rightarrow y \cap a \quad \varphi_a : [a \cup b/b] \rightarrow [a/a \cap b]$$

are inverse lattice-isomorphisms.

II) if $a\mathfrak{D}L$ and $b \in L$, then $a \cap b\mathfrak{D}(b)$.

III) if $a_1\mathfrak{D}L$ and $a_2\mathfrak{D}L$, then $a_1 \cap a_2\mathfrak{D}L$.

IV) if $a_1\mathfrak{D}L$ and $a_2\mathfrak{D}(a_1)$, then $a_2\mathfrak{D}L$.

V) whenever φ is a surjective lattice isomorphism of L onto L' , we have $a\varphi\mathfrak{D}L'$ iff $a\mathfrak{D}L$.

A subgroup H of a group G is dual-Dedekind in G (H is a $\mathfrak{D}$ -subgroup of G , $H\mathfrak{D}G$) if H is a $\mathfrak{D}$ -element of the lattice $\mathfrak{L}(G)$ of all subgroups of G . Normal subgroups are usually not $\mathfrak{D}$ -subgroups; the following are

dual-Dedekind subgroups in any group G :

a) G and the identity subgroup 1 of G (they will be referred to as the « trivial » $\mathfrak{D}$ -subgroups);

b) the subgroups of the centre $Z(G)$;

c) all normal cyclic subgroups;

d) the subgroups of the so-called « kernel »

$$K(G) = \cap \{ \mathfrak{D} \zeta_G(X) \mid X \in \mathfrak{L}(G) \}.$$

All definitions and notations will be standard; throughout this paper « group » means « finite group ».

2. The existence of non-trivial $\mathfrak{D}$ -elements in $\mathfrak{L}(G)$ rather severely restricts the structure of G . The following two lemmas provide examples where, in very simple cases, the structure of G is completely determined.

LEMMA 2.1. Assume $G = \langle a, b \rangle$, $|a| = |b| = p$, p a prime, G non cyclic. Then $\langle a \rangle \mathfrak{D} G$ iff either $|G| = p^2$ or G is a non-abelian group of order pq (q a prime greater than p).

Since in both cases $\mathfrak{L}(G)$ is a modular lattice, the sufficiency of the condition is obvious. The condition is also necessary: the intervals $[\langle a, b \rangle / \langle b \rangle]$ and $[\langle a \rangle / \langle a \rangle \cap \langle b \rangle]$ are isomorphic, hence $\langle b \rangle$ is a maximal subgroup of G and, if G is a p -group, then $|G| = p^2$. Assume that G is not a p -group; then $\langle b \rangle$ is a cyclic p -Sylow subgroup, $\langle b \rangle$ is its own normalizer in G and has a normal complement N . $\langle a \rangle$, as a conjugate of $\langle b \rangle$, is maximal in G and $\langle a \rangle \cap N = 1$; for a $c \in N$ of prime order q one has $N = (\langle a \rangle \cup \langle c \rangle) \cap N = \langle c \rangle \cup (\langle a \rangle \cap N) = \langle c \rangle$, and the conclusion follows.

LEMMA 2.2. Assume $G = \langle a, b \rangle$, $|a| = p$, $|b| = q$, p, q different prime numbers. Then $\langle a \rangle \mathfrak{D} G$ iff either $|G| = pq$, or G contains an elementary abelian p -subgroup $N \triangleleft G$ such that $G = N \langle b \rangle$, and $\langle b \rangle$ operates irreducibly on N .

If $\langle a \rangle \mathfrak{D} G$, then $\langle b \rangle$ is a maximal subgroup of G and from $\langle b \rangle \triangleleft G$ follows $|G| = pq$. If $\langle b \rangle$ is not normal, then $\langle b \rangle$ is a q -Sylow subgroup

which is its own normalizer in G , hence $\langle b \rangle$ has a normal complement N . Since any conjugate of $\langle b \rangle$ is maximal in G , no proper non-trivial subgroup of N is normalized by b nor by a conjugate of b . Let S be a p -Sylow subgroup of N containing $\langle a \rangle$; by the Frattini argument $G = N\mathfrak{N}_G(S)$, hence $\mathfrak{N}_G(S)$ contains a conjugate of $\langle b \rangle$, and $S = N$. The Frattini subgroup $\Phi(N) \neq N$, $\Phi(N) \triangleleft G$, so that $\Phi(N) = 1$ and the « only if » part is proved. Conversely, neglecting the case $|G| = pq$ where everything is obvious, we have to prove that if $1 \neq a \in N$ and $X \in \mathcal{L}(G)$ is arbitrary, $a \notin X$ implies that X is maximal in $\langle a, X \rangle$. But $X \subseteq N$ implies that $\langle a, X \rangle$ is abelian, whereas if $X \not\subseteq N$ a conjugate of $\langle b \rangle$, say $\langle c \rangle$, lies in X , hence $X = \langle c \rangle$ is a maximal subgroup of $G = \langle a, c \rangle$.

3. DEFINITION. Let H be a subgroup of the group G . We shall say that H is a minimum $\mathfrak{D}$ -subgroup of G if H is minimal in the set of all non-identity $\mathfrak{D}$ -subgroups of G .

THEOREM 3.1. *Let H be a minimum $\mathfrak{D}$ -subgroup of G . If $|H|$ is not a prime number, then*

- i) H is normal in G ;
- ii) for every prime number p dividing $|H|$, all the elements of G of order p are in H ; and
- iii) $\mathcal{C}_G(H) = \{x \in G \mid (|x|, |H|) = 1\}$.

First of all, notice that the minimality of H and III, V of section 1 imply that for every $g \in G$ either $g^{-1}Hg \cap H = 1$ or $g^{-1}Hg = H$; furthermore, if $1 \neq A \subseteq H$, then $\mathfrak{N}_G(A) \subseteq \mathfrak{N}_G(H)$: thus, if $g^{-1}Ag = A$, then $1 \neq A \subseteq H \cap g^{-1}Hg$, whence $g^{-1}Hg = H$. Choose now an element $a \in H$ of prime order p . For any $b \notin H$ such that $|b| = p$, $\langle a \rangle = \langle a, b \rangle \cap H \mathfrak{D} \langle a, b \rangle$; by lemma 2.1 either $|\langle a, b \rangle| = p^2$, or $\langle a, b \rangle$ is a non-abelian group of order pq (q a prime greater than p). In the first case $[a, b] = 1$, hence $b \in \mathfrak{N}_G(H)$; moreover, for every $x \in H$, $\langle x \rangle = \langle x, b \rangle \cap H \triangleleft \langle x, b \rangle$, i.e. b is in the normalizer of every subgroup of H . Since the same conclusion holds for ab , it would follow that a is in the kernel of H , so that $\langle a \rangle \mathfrak{D} H$; by IV of section 1 this would imply $\langle a \rangle \mathfrak{D} G$ and $H = \langle a \rangle$,

which contradicts our assumption on the order of H . In the second case $\langle b \rangle$ and $\langle a \rangle$ are conjugate in $\langle b \rangle \cup H$; b lies in a conjugate H_1 of H ($H_1 \neq H$) and $\langle b \rangle = (\langle b \rangle \cup H) \cap H_1 \tilde{\mathfrak{D}} \langle b \rangle \cup H$, whence again $\langle a \rangle \tilde{\mathfrak{D}} \langle b \rangle \cup H$, $\langle a \rangle \tilde{\mathfrak{D}} H$ and $H = \langle a \rangle$, thus contradicting our hypothesis on $|H|$. We can now prove that $H \triangleleft G$: let $g \in G$ have order q^n with q a prime number; if $q \mid |H|$, by a previous remark $\langle g^{q^{n-1}} \rangle \subseteq H$ and $g \in \mathfrak{N}_G(H)$; if $q \nmid |H|$, for $a \in H$ of prime order we have $\langle g^{-1}ag \rangle \subseteq \langle a, g \rangle \cap H = \langle a \rangle$, and by the same remark $g \in \mathfrak{N}_G(H)$. Moreover, in the latter case, for every $x \in H$ we get $\langle x \rangle = \langle x, g \rangle \cap H \triangleleft \langle x, g \rangle$ and, assuming $|x|$ to be a prime number, from $[x, g] \neq 1$ it would follow that x too normalizes every subgroup of H , which clearly cannot happen; i.e. g centralizes H . On the other hand in our hypothesis $Z(H) = 1 = H \cap \mathfrak{C}_G(H)$, and if $(|g|, |H|) \neq 1$ then $\langle g \rangle \cap H \neq 1$; all this implies that $\mathfrak{C}_G(H)$ is exactly the set of all the elements of G whose order is prime to $|H|$.

The above theorem does not cover the minimum $\tilde{\mathfrak{D}}$ -subgroups of prime order; they will be dealt with in the following

THEOREM 3.2. *Let $a \in G$ have prime order p . If $\langle a \rangle \tilde{\mathfrak{D}} G$, then either i) $\langle a \rangle^G$ is an elementary abelian p -group, or ii) $G = S(N \times K)$, where $K = \mathfrak{C}_G(\langle a \rangle^G)$ is a Hall subgroup of G , N is an elementary abelian q -group with q a prime greater than p , S is a p -Sylow subgroup of G which is cyclic or generalized quaternion, and $\langle a \rangle^G = \langle a \rangle N$ is a P -group.*

Let us first show that if we can find in G an element b of order p such that $\langle a \rangle \cap \langle b \rangle = 1$ but $[a, b] = 1$, then a permutes with every element of order p in G ; hence it will follow that, if this is the case, $\langle a \rangle^G$ is elementary abelian. Thus, choose if possible $c \in G$ such that $|c| = p$, $[a, c] \neq 1$; by lemma 2.1 $\langle a, c \rangle = \langle a, d \rangle$ where $\langle d \rangle \triangleleft \langle a, c \rangle$ and $|d| = q$ (notice that a and c are conjugate). If $[b, c] = 1$, then $\langle a, b, c \rangle = \langle a, c \rangle \times \langle b \rangle$, $|db| = pq$, whereas $|adb| = p$ and lemma 2.1 imply that no elements of composite order are in $\langle a, adb \rangle$, so that we can assume $[b, c] \neq 1$. $\langle b \rangle$ is then conjugate to $\langle c \rangle$, whence $\langle b \rangle \tilde{\mathfrak{D}} G$. If $b \in \mathfrak{N}_G(\langle d \rangle)$ we get $\langle a, c \rangle \triangleleft \langle a, b, c \rangle = \langle a, c \rangle \times \langle b' \rangle$, where b' is a suitable element of $\langle a \rangle \times \langle b \rangle$, and the above technique leads to a

contradiction. Lemma 2.2 now implies $\langle b, d \rangle = N\langle d \rangle$ with N an elementary abelian normal p -subgroup of $\langle b, d \rangle$ which in turn is normal in $\langle a, b, c \rangle$; $a \notin N$, and for every $x \in N$ we have $\langle x \rangle = \langle x, a \rangle \triangleleft \langle x, a \rangle$, i.e. $a \in \mathcal{C}_G(N)$. Hence $\langle a \rangle = \langle a, d \rangle \cap \mathcal{C}_{\langle a, b, c \rangle}(N) \triangleleft \langle a, d \rangle$, thus contradicting an earlier statement. So far we proved that, if $\langle a \rangle^G$ is not an elementary abelian p -group, then $[a, b] \neq 1$ for every $b \in G$ such that $|b| = p$, $\langle a \rangle \cap \langle b \rangle = 1$; as a consequence, all p -Sylow subgroups of G are either cyclic or generalized quaternion. We now proceed to show that for any pair x, y of elements of G such that $|x| = |y| = p$, $\langle x \rangle \cap \langle y \rangle = 1$, the subgroup $\langle x, y \rangle$ is non abelian and $|\langle x, y \rangle| = pq$, q being independent from the choice of x, y ; since there is in G just one class of conjugate subgroups of order p , it is enough if we prove that $|b| = |c| = p$, $\langle a \rangle \cap \langle b \rangle = \langle a \rangle \cap \langle c \rangle = 1$ implies $|\langle a, b \rangle| = |\langle a, c \rangle|$. Let $u \in G$ be such that $\langle a, b \rangle = \langle a, u \rangle$, $|u| = q$, $\langle u \rangle \triangleleft \langle a, b \rangle$; $c \in \mathcal{Z}_G(\langle u \rangle)$ (were this not the case, by lemma 2.2 two independent conjugates of a would permute), hence $\langle u \rangle \triangleleft \langle a, b, c \rangle = \langle u \rangle \langle a, c \rangle$. Looking at $\langle a, c \rangle$, which by lemma 2.1 is also non abelian of order, say, pr , we see that $\langle a, c \rangle = \langle a, v \rangle$ where $|v| = r$, $\langle v \rangle \triangleleft \langle a, c \rangle$ and $\langle v \rangle = \langle a, c \rangle \cap \mathcal{C}_{\langle a, b, c \rangle}(u)$, so that $\langle a, b, c \rangle = (\langle u \rangle \times \langle v \rangle) \langle a \rangle$. The subgroups $\langle au \rangle$, $\langle av \rangle$, being conjugate to $\langle a \rangle$, are dual-Dedekind in G ; by lemma 2.1 no element of composite order lies in $\langle au, av \rangle$, hence $v^{-1}u \in \langle au, av \rangle$ has prime order: but then $q = r$ (notice that we have also proved that every element of order p normalizes every subgroup of order q). By an easy induction argument one can now prove that any set of elements of order p generates a P -group of order pq^n for a suitable n , so that $\langle a \rangle^G$, which is generated by all such elements of G , is a P -group: $\langle a \rangle^G = \langle a \rangle N$, with N an elementary abelian q -subgroup on which a induces a non identity power automorphism. Our next step is to prove that for every pair x, y of elements of G such that $|x| = q^m$, $|y| = p$, one has $\langle x \rangle \triangleleft \langle x, y \rangle$; by an earlier remark we can assume $m > 1$ and use induction. $\langle x^q \rangle$ is then normal in $\langle y, x^q \rangle$; $\langle y, x^q \rangle / \langle x^q \rangle \cong \langle y, x \rangle / \langle x^q \rangle$: if $|\langle y, x \rangle / \langle x^q \rangle| = pq$ we are through. If this is not the case, then $\langle y, x \rangle / \langle x^q \rangle = (\langle x \rangle / \langle x^q \rangle)(N / \langle x^q \rangle)$ with $N / \langle x^q \rangle$ an elementary abelian normal p -subgroup of $\langle y, x \rangle / \langle x^q \rangle$ (lemma 2.2); $\langle x^q \rangle$ is a q -Sylow subgroup of N , whence $N = M\langle x^q \rangle$ for a suitable elementary abelian p -subgroup M containing $\langle y \rangle$. But then $M = \langle y \rangle$ and again $|\langle y, x \rangle / \langle x^q \rangle| = pq$. For a conjugate b of a such that $\langle b \rangle \cap \langle a \rangle = 1$ one has either $\langle x \rangle \cap \langle a, b \rangle \neq 1$, which

implies $[a, x] \neq 1$; or $\langle x \rangle \cap \langle a, b \rangle = 1$, and $\langle x, a, b \rangle = (\langle x \rangle \times \langle u \rangle) \langle a \rangle$, where $\langle u \rangle$ is the q -Sylow subgroup of $\langle a, b \rangle$, and a induces a non identity power automorphism on $\langle x \rangle \times \langle u \rangle$, whence again $[a, x] \neq 1$; but then $\langle x \rangle = \langle [a, x] \rangle \subseteq \langle a \rangle^G$, i.e. N is the (unique) q -Sylow subgroup of G . Now put $K = \mathcal{C}_G(\langle a \rangle^G)$; $K \cap \langle a \rangle^G = 1$ and, since a p -Sylow subgroup is either cyclic or generalized quaternion and its subgroup of order p lies in $\langle a \rangle^G$, $K \subseteq \{g \in G \mid (|g|, pq) = 1\}$. On the other hand, if $(|g|, pq) = 1$, for every $y \in G$ with $|y| = p$ one has $\langle y \rangle = \langle y, g \rangle \cap \langle a \rangle^G \triangleleft \langle y, g \rangle$; therefore g is in the normalizer of every subgroup of order pq in $\langle a \rangle^G$: but this implies $[g, \langle a \rangle^G] = 1$, which concludes the proof of the theorem.

The following result is a trivial corollary to theorems 3.1, 3.2:

THEOREM 3.3. *Let G be a finite group. If G has non-trivial dual-Dedekind subgroups, then G is not simple.*

REMARK. Finite non simple groups with no non-trivial $\tilde{\mathfrak{D}}$ -subgroups do exist: e.g. the symmetric group S_n is such whenever $n > 3$ (it is a simple matter to verify that no normal subgroup of S_n satisfies the theorems 3.1, 3.2); the case $n = 4$ provides an example of a soluble group which has no non-trivial $\tilde{\mathfrak{D}}$ -subgroups.

4. We have already pointed out that, generally speaking, normal subgroups need not be $\tilde{\mathfrak{D}}$ -subgroups; in order to evaluate, in a sense, the gap between these two classes we proceed to study the groups where every normal subgroup is also a $\tilde{\mathfrak{D}}$ -subgroup (in the main result of this section we restrict ourselves to soluble groups).

PROPOSITION 4.1. *Assume that every normal subgroup of the group G is a $\tilde{\mathfrak{D}}$ -subgroup of G . If $N \trianglelefteq G$, then every normal subgroup of G/N is a $\tilde{\mathfrak{D}}$ -subgroup of G/N .*

Thus, $K/N \trianglelefteq G/N$ implies $K \trianglelefteq G$, $K \tilde{\mathfrak{D}} G$, hence $K \tilde{\mathfrak{D}} [G/N]$ and obviously $K/N \tilde{\mathfrak{D}} G/N$.

PROPOSITION 4.2. *Let N be a minimum normal subgroup of G . If every normal subgroup of G is also a $\tilde{\mathfrak{D}}$ -subgroup, then N is simple.*

Assume first that N is abelian; then $|N| = p^\alpha$ with p a prime and $\alpha \geq 1$; the number k of its subgroups of order p is congruent to 1

(mod p). The normal subgroup $P = \cap \{ \mathcal{O} \mathcal{L}_G(H) \mid H \subseteq N, |H| = p \}$ contains every element of G whose order is prime to p : thus, if $(|x|, p) = 1$, then $\langle x \rangle \cap N = 1$ and, for any such an H , $H = (H \cup \langle x \rangle) \cap N \triangleleft H \cup \langle x \rangle$. So G acts as a p -group of permutations on the set of the k subgroups of order p in N , hence it has at least a fixed point, i.e. $|N| = p$. Assume now that N is abelian; let N_1 be a simple direct factor of N . If $N_1 \neq N$ and $x \in G$ is such that $x^{-1}N_1x \neq N_1$, then $N_1 \times x^{-1}N_1x \subseteq (N_1 \cup \langle x \rangle) \cap N = N_1(\langle x \rangle \cap N)$ and $x^{-1}N_1x$ would be isomorphic to a subgroup of $\langle x \rangle$, which is clearly not the case.

COROLLARY 4.3. *Let G be a soluble group. If every normal subgroup of G is a $\mathfrak{D}$ -subgroup of G , then G is supersoluble.*

PROPOSITION 4.4. *Let G be a nilpotent group. If $H \mathfrak{D} G$, then H is quasi-normal in G .*

This is a trivial consequence of a result of Napolitani, [1].

PROPOSITION 4.5. *Let G be a p -group (p a prime). If every normal subgroup of G is a $\mathfrak{D}$ -subgroup, then G is modular.*

For $u \in Z(G)$, with $|u| = p$, $G/\langle u \rangle$ is by induction a modular p -group. Assume that $G/\langle u \rangle$ is either abelian or Hamiltonian: for arbitrary $x \in G$, $\langle x, u \rangle$ is abelian, hence $\langle x \rangle \mathfrak{D} \langle x, u \rangle$; moreover $\langle x, u \rangle \trianglelefteq G$ implies $\langle x, u \rangle \mathfrak{D} G$ and $\langle x \rangle \mathfrak{D} G$; by proposition 4.4 $\langle x \rangle$ is a quasi-normal subgroup of G , i.e. G is modular. We may then assume that $G/\langle u \rangle$ is neither abelian nor Hamiltonian, so that $G = \langle t, A \rangle$ with $u \in A$, $A/\langle u \rangle$ abelian, $t^{-1}at = a^{1+p^s}u^{\alpha(a)}$ for every $a \in A$ and suitable $\alpha(a)$, $s \geq 2$ if $p = 2$ ([3], p. 13). Just as before one sees that every subgroup of A is dual-Dedekind, whence quasi-normal, in G ; it follows that A is a modular group. Moreover $A^p = \{a^p \mid a \in A\}$ is a subgroup of A , any of whose subgroups is normalized by t ; t^p normalizes every subgroup of A , inducing on every cyclic subgroup a power automorphism which is congruent to 1 (mod. p), and congruent to 1 (mod. 4) if $p = 2$. A cannot be a Hamiltonian group: thus, if $A = Q \times B$ with Q a quaternion group of order 8 and $B^2 = 1$, from $u \in Q$ it would follow that $G/\langle u \rangle$ is abelian, whereas, if $u \notin Q$, $G/\langle u \rangle$ would be a modular 2-group containing a quaternion group, and $G/\langle u \rangle$ would be a Hamiltonian group. There are two cases left:

i) A is abelian. By a previous remark, $\langle t^p, A \rangle$ is modular and all its subgroups are quasi-normal in G . Let $y \in G$ be such that $y \notin \langle t^p, A \rangle$, so that $G = A\langle y \rangle$. If $\langle y \rangle \cap A \neq 1$, since $\langle y \rangle \cap A \trianglelefteq G$, then by induction $G/\langle y \rangle \cap A$ is modular, hence $\langle y \rangle$ is quasi-normal in G . Assume now $\langle y \rangle \cap A = 1$: for every $a \in A$ we get $\langle a \rangle = \langle a, y \rangle \cap A \triangleleft \langle a, y \rangle$, i.e. y induces a power automorphism on the abelian group A , which is congruent to 1 (mod. p). If $p \neq 2$ there is nothing more to prove; if $p = 2$ we remark that, if we had $A^4 = 1$, $G/\langle u \rangle$ would be abelian; hence $A^4 \neq 1$, G/A^4 is by induction a modular group, and the power induced by y is congruent to 1 (mod. 4), which implies that G is modular.

ii) A is neither abelian nor Hamiltonian. We have $A = \langle v, B \rangle$, B abelian, $v^{-1}xv = x^n$ with $n \equiv 1 \pmod{p}$ for every $x \in B$ and n independent from the choice of x ($n \equiv 1 \pmod{4}$ if $p = 2$; we remark here that $B^4 \neq 1$, otherwise A would be abelian). $A^p \subseteq Z(A)$, hence every subgroup of A^p is normal in G ; both of A/A^p and A/B are abelian, so that $\langle u \rangle = A' \subseteq A^p \cap B$; moreover, we can write B as $B = \langle b \rangle \times B_1$ where $u \in \langle b \rangle$, $\exp B_1 < |b|$ and $|b| \geq 8$ if $p = 2$. We will show that $\langle g_1, g_2 \rangle = \langle g_1 \rangle \langle g_2 \rangle$ for every pair g_1, g_2 of elements of G (without loss of generality, we can assume $g_i \notin A$, since every subgroup of A is quasi-normal in G). Write $\langle g_1 \rangle = \langle a_1 t^{p^h} \rangle$, $\langle g_2 \rangle = \langle a_2 t^{p^k} \rangle$; assuming $0 \leq h \leq k$ we get $g_2 \in A\langle g_1 \rangle$, $\langle g_1, g_2 \rangle = \langle g_1, a \rangle$ for suitable $a_1, a_2, a \in A$. Should $\langle g_1 \rangle$ contain a non-identity normal subgroup K of G , since G/K would be a modular group by the induction hypothesis, then $\langle g_1 \rangle$ would be quasi-normal in G ; hence we can assume $\langle g_1 \rangle \cap A^p = 1$, which implies $u \notin \langle g_1 \rangle$. Suppose $\langle g_1 \rangle \cap A = 1$; then $\langle a \rangle = \langle a, g_1 \rangle \cap A \triangleleft \langle a, g_1 \rangle$, and, if $p \neq 2$, $\langle a, g_1 \rangle$ is modular, whence $\langle g_1, g_2 \rangle = \langle g_1 \rangle \langle g_2 \rangle$. Under the same assumptions, but with $p = 2$, g_1 induces a power automorphism on the abelian group B ; G/B^4 being modular, this power is congruent to 1 (mod. 4), so that if $a \in B$ then $\langle a, g_1 \rangle$ is modular. Let now $a \notin B$; $u \in \langle a, g_1 \rangle$ if and only if $u \in \langle a \rangle$, hence if either $u \notin \langle a \rangle$ or $u \in \langle a^4 \rangle$ we again conclude that $\langle a, g_1 \rangle$ is modular; we are left with one more possibility: $u = a^2 = b^{2^t}$; but $[g_1, b^{2^{t-1}}] = 1$ (for $\langle g_1, b \rangle$ is modular), $[g_1, ab^{2^{t-1}}] = 1$ since $|ab^{2^{t-1}}| = 2$, so that $\langle g_1, a \rangle$ is abelian. Assume now $1 = \langle g_1 \rangle \cap A^p \subsetneq \langle g_1 \rangle \cap A = \langle c \rangle$ with $|c| = p$, $u \in \langle a, g_1 \rangle \cap A = \langle a, c \rangle$; if $|a| = p$ then $\langle g_1 \rangle \triangleleft \langle a, g_1 \rangle = \langle g_1, g_2 \rangle = \langle g_1 \rangle \langle g_2 \rangle$; if $|a| > p$ but $u \notin \langle a \rangle$ we should have $c \in \langle a \rangle \times \langle u \rangle$, whence $c \in \langle a^p \rangle \times \langle u \rangle \subseteq A^p$, contradicting an earlier

hypothesis. We have then $|a| > p$, $u \in \langle a \rangle$: so $\langle a \rangle \trianglelefteq G$ and, if either $p \neq 2$ or $p=2$, $u \in \langle a^4 \rangle$, $\langle g_1, a \rangle$ is modular. It follows that we are left with one last case: $p=2$, $u=a^2=b^{2^l}$. Since $\langle b \rangle \triangleleft G$, $u \in \langle b^4 \rangle$ and $G/\langle u \rangle$ is modular, we see that $\langle g_1, b \rangle$ is also modular, whence $[g_1, b^{2^{l-1}}]=1$; if $a \in \langle b \rangle$, $\langle g_1, a \rangle$ is abelian, whereas, if $a \notin \langle b \rangle$, $|a^{-1}b^{2^{l-1}}|=2$, $a^{-1}b^{2^{l-1}} \in \mathcal{N}_G(\langle g_1 \rangle)$ and finally $\langle g_1 \rangle \triangleleft \langle g_1, g_2 \rangle \subseteq \langle g_1, b^{2^{l-1}}, a^{-1}b^{2^{l-1}} \rangle$, which disposes of the case and ends the proof.

THEOREM 4.6. *The group G is soluble and every normal subgroup of G is dual-Dedekind in G if and only if $G=H_1 \times H_2 \times \dots \times H_t$ with H_i a Hall subgroup of G ($i=1, \dots, t$) and either*

- 1) H_i is a modular p -group; or
- 2) $H_i=(P_{i1} \times \dots \times P_{is_i})Q_i$ with P_{ij} , Q_i Sylow subgroups of G for different primes, P_{ij} abelian of odd order ($j=1, \dots, s_i$), $Q_i=\langle b_i \rangle$, and b_i inducing a non identity power automorphism on each P_{ij} .

PROOF OF NECESSITY. Assume S , a p -Sylow subgroup of G for some prime p , is normal in G ; then, unless S is a direct factor of G , $S \subseteq \Gamma_\infty(G)$ where $\Gamma_\infty(G)$ denotes the intersection of all normal subgroups of G whose factor group is nilpotent. Thus $S \bar{\trianglelefteq} G$ and for $a \in S$, $x \in G$ such that $(x|p)=1$ we have $\langle a \rangle = \langle a \rangle \cup (\langle x \rangle \cap S) = \langle a, x \rangle \cap S \triangleleft \langle a, x \rangle$; if S is not a direct factor of G , we can choose a, x such that $[a, x] \neq 1$, but then $\langle [a, x] \rangle = \langle a \rangle$ and a also induces a power automorphism on S . Let now b be arbitrary in S ; if $[b, x] \neq 1$ the above argument shows that b operates on S as a power automorphism, whereas if $[b, x]=1$ we have $[ab, x] \neq 1$ and the same conclusion holds for ab , hence for b . It follows that S is abelian of odd order, $x^{-1}yx=y^r$ with $r \not\equiv 1 \pmod{p}$, r independent from the choice of $y \in S$, $[G, S]=S$ and $S \subseteq \Gamma_\infty(G)$. Choosing for p the maximum prime divisor of $|G|$, by the supersolubility of G the p -Sylow subgroup is certainly normal, so that an easy induction proves that $\Gamma_\infty(G)$ is a Hall subgroup of G . Moreover G has a normal 2-complement whose quotient group is clearly nilpotent, so that $|\Gamma_\infty(G)|$ is odd; again, by the supersolubility of G , $\Gamma_\infty(G)$ is nilpotent, hence it is a direct product of normal Sylow subgroups of G which are all abelian by the preceding remark, and every element of G operates by conjugation on $\Gamma_\infty(G)$ as a power automorphism. $G/\Gamma_\infty(G)$ is a direct

product of modular p -groups for different primes; notice that every Sylow subgroup of G which is a direct factor has trivial intersection with $\Gamma_\infty(G)$, and is modular; therefore, we can factor out all such subgroups, and write $G = T \times G_1$ with T a modular, nilpotent, Hall subgroup of G and G_1 also satisfying all our assumptions; from now on we shall assume $G = G_1$. Let P be a normal Sylow subgroup of G ; we have already seen that $P \subseteq \Gamma_\infty(G)$ and that every element of G operates on P as a power automorphism; we claim that $G/\mathcal{C}_G(P)$ is a (cyclic) group of prime power order. Deny: then there are a q -Sylow subgroup Q and an r -Sylow subgroup R of G such that $[Q, R] = 1$, $Q \cap \Gamma_\infty(G) = R \cap \Gamma_\infty(G) = 1$, $[Q, P] = [R, P] = P$; choose $a \in Q$, $b \in R$, $u \in P$ such that $[a, P] \neq 1$, $[b, P] \neq 1$, $|u| = p$ ($p \nmid |P|$). The Hall subgroup $Q\Gamma_\infty(G)$ is normal, hence dual-Dedekind, in G , which is a contradiction to $\langle au \rangle = \langle au \rangle \cup (\langle b \rangle \cap Q\Gamma_\infty(G)) \neq (\langle au \rangle \cup \langle b \rangle) \cap Q\Gamma_\infty(G)$ (this owing to the fact that the former group has q -power order, whereas the latter contains $\langle u \rangle = \langle [au, b] \rangle$ which has order p). Therefore we get $G = Q\mathcal{C}_G(P)$ for a suitable q -Sylow subgroup Q of G ; we shall now prove, by induction on $q^b = |Q|$, that Q is cyclic. Without loss of generality we can assume $P = \Gamma_\infty(G)$ (were this not the case, we would work on G/C with C the complement of P in $\Gamma_\infty(G)$). If $Q \cap \mathcal{C}_G(P) = 1$, since $G/\mathcal{C}_G(P)$ is cyclic, then Q is also cyclic. Assume then $Q \cap \mathcal{C}_G(P) \neq 1$; $\mathcal{C}_G(P) \cap Z(Q)$ is a non-trivial normal subgroup of G and by the inductive hypothesis $Q/\mathcal{C}_G(P) \cap Z(Q)$ is cyclic; therefore Q is abelian and all subgroups of QP containing P are normal, hence dual-Dedekind subgroups of G . If now Q were not cyclic we could pick a and b in Q in such a way that $a \notin \mathcal{C}_G(P)$, $a^q \in \mathcal{C}_G(P)$, $b \in Q$, $|b| = q$, $[b, P] = 1$, $\langle a \rangle \cap \langle b \rangle = 1$; for $u \in P$ with $|u| = p$ we would have $\langle au \rangle = \langle au \rangle \cup (\langle ab \rangle \cap \langle a \rangle P) = (\langle au \rangle \cup \langle ab \rangle) \cap \langle a \rangle P \supseteq \langle [au, ab] \rangle = \langle [u, a] \rangle = \langle u \rangle$ i.e. $[u, a] = 1$ contrary to our choice of a . Now let Q_1 be a non normal Sylow subgroup of G , and let $P_{11}, P_{12}, \dots, P_{1s_1}$ be those Sylow subgroups of $\Gamma_\infty(G)$ which are not centralized by Q_1 ; $H_1 = (P_{11} \times \dots \times P_{1s_1})Q_1$ is a direct factor of G , and if $G = H_1$ the theorem is proved. Assume $G \neq H_1$; let Q_2 be a normal Sylow subgroup of G , not contained in H_1 , and let $P_{21}, \dots, P_{2s_2}$ be those Sylow subgroups of $\Gamma_\infty(G)$ which are not centralized by Q_2 ; $H_2 = (P_{21} \times \dots \times P_{2s_2})Q_2$ is also a direct factor of G , and $H_1 \cap H_2 = 1$; in this way we clearly get a decomposition of G as a direct product of factors of the prescribed type.

PROOF OF SUFFICIENCY. Since such a decomposition as is described in the theorem is both group- and lattice-theoretical, it will be enough if we prove the theorem for each one of the factors (nothing is to be proved for the modular ones). Without loss of generality, we can assume $G = (P_1 \times \dots \times P_s)Q$ where the P_i 's and Q are Sylow subgroups of G , Q is cyclic, P_i is abelian of odd order ($i=1, \dots, s$) and Q operates on $P_1 \times \dots \times P_s$ as a group of power automorphisms, with $\mathcal{C}_Q(P_i) \neq Q$. Let $H \trianglelefteq G$; we renumber the P_i 's so hat $[H, P_i] = P_i$ for $i=1, \dots, r$ and $[H, P_i] = 1$ for $i=r+1, \dots, s$. We shall prove that $\varphi^K : X \rightarrow X \cup K$ ($\varphi^K : [H/H \cap K] \rightarrow [HK/K]$) and $\varphi_H : Y \rightarrow Y \cap H$ ($\varphi_H : [HK/K] \rightarrow [H/H \cap K]$) are inverse lattice isomorphisms, whenever K is a subgroup of G ; since $H \trianglelefteq G$, we have only to prove that $X\varphi^K\varphi_H = X$ for every $X \in [H/H \cap K]$. Assume first that

$$K \subseteq (P_1 \times \dots \times P_s)H = (H \cap Q)(P_1 \times \dots \times P_r) \times (P_{r+1} \times \dots \times P_s);$$

we have

$$K = (K \cap (H \cap Q)(P_1 \times \dots \times P_r)) \times (K \cap (P_{r+1} \times \dots \times P_s)) = (H \cap K)L$$

with $L = K \cap (P_{r+1} \times \dots \times P_s) \trianglelefteq G$. We have $H \cup K = H \cup (H \cap K) \cup L = H \cup L$ and, for every $X \in [H/H \cap K]$,

$$\begin{aligned} X\varphi^K\varphi_H &= (X \cup K) \cap H = (X \cup (H \cap K) \cup L) \cap H = \\ &= (X \cup L) \cap H = X \cup (L \cap H) = X. \end{aligned}$$

Assume now that $K \not\subseteq (P_1 \times \dots \times P_s)H$; there exists a q -Sylow subgroup T of G with $T \cap K$ q -Sylow in K ; we have $T \cap H \subseteq T \cap K$. If we call $M = H \cap (P_1 \times \dots \times P_s)$, then $H = M(T \cap H) = M(H \cap K)$; notice that, since every subgroup of M is normal in G , $M \trianglelefteq G$. Now for every $X \in [H/H \cap K]$ we get $X = (X \cap M) \cup (H \cap K)$ and

$$\begin{aligned} (X \cup K) \cap H &= X\varphi^K\varphi_H = ((X \cap M) \cup (H \cap K) \cup K) \cap H = \\ &= ((X \cap M) \cup K) \cap H = (X \cap M) \cup (H \cap K) = X, \end{aligned}$$

thus ending our proof.

REFERENCES

- [1] NAPOLITANI, F.: *Proprietà reticolari dell'insieme dei sottogruppi subnormali*, Rend. Sem. Mat. Univ. Padova, 38 (1967).
- [2] SCHMIDT, R.: *Modulare Untergruppen endlicher Gruppen*, Illinois J. of Math., vol. 13, n. 2 (1969).
- [3] SUZUKI, M.: *Structure of a group and the structure of its lattice of subgroups*, Springer (1956).
- [4] ZASSENHAUS, H.: *The theory of groups*, Vandenhoeck and Ruprecht, Göttingen (1958).

Manoscritto pervenuto in redazione il 27 giugno 1970.