ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 4, Fall 1989

ON THE MÖBIUS FUNCTION OF A FINITE GROUP

T. HAWKES[1], I.M. ISAACS[2] AND M. ÖZAYDIN

0. Our purpose is to present an elementary, uniform, and self-contained treatment of a growing body of knowledge about the Möbius function μ associated with the subgroup lattice of a finite group G. Our principal result (Theorem 5.1) has as a special case the following recent theorem of Thévenaz (whose preprint [**25**] came to our attention only after we had completed this work in the early months of 1986): *If an integer n divides $|G|$, then it also divides*

$$(*) \qquad \sum_{\substack{X \leq G \\ |X| \text{ divides } n}} \mu(X).$$

This generalizes a result of Brown's [**4**], which covers the case where $n = |G|_p$, the order of a Sylow p-subgroup of G. Another easy consequence of our Theorem 5.1 is and elementary proof of the theorem of Frobenius about the number of solutions of the equation $x^n = 1$ in a group. We have also included a proof of a conjecture of Thévenaz (see 4.2 of [**26**]).

To emphasize the unity of our approach the main exposition is couched in elementary algebraic language and avoids reference to the Burnside ring, to the theory of projective modules, and to topological methods, all of which have been used by Thévenaz and other authors in this context. For the sake of completeness and directness we have included easier proofs of some known results, and to this extent our presentation is partly expository. In a final section we describe some topological connections and interpretations of our results.

1. Historical Introduction. In his 1936 paper on Eulerian functions Philip Hall [**13**] defined the Möbius function on a subset of a

Received by the editors on September 26, 1986
[1] Research partially supported by N.S.F. and S.E.R.C.
[2] Research partially supported by N.S.F.
Hall acknowledges Weisner's priority for generalizing the number-theoretic version of μ to a lattice in [**29**].

power set, partially ordered by inclusion, and used the inversion formula to compute the number $\varphi_S(G)$ of ordered s-tuples of elements which generate a finite group G. He illustrated the method by evaluating $\varphi_S(G)$ when $G \cong \mathrm{PSL}_2(p)$, with p prime, and in the process computed the Möbius value $\mu(G)$ for these groups. In 1959, in the course of calculating $\varphi_S(G)$ for soluble groups, Gaschütz [**10**] implicitly obtained a formula for $\mu(G)$ in terms of the numbers of complements of chief factors (see also §8 of Wall [**18**]). This formula is stated explicitly by Kratzer and Thévenaz [**15**, Théorème 2.6] and is reproved in our Corollary 3.4 below.

The Möbius function associated with a finite, partially-ordered set (poset) $\mathcal{X}$ is a map $\mu_{\mathcal{X}} : \mathcal{X} \times \mathcal{X} \to \mathbf{Z}$ satisfying $\mu_{\mathcal{X}}(a,b) = 0$ unless $a \leq b$, when it is defined recursively by the equations

$$\begin{aligned} &\mu_{\mathcal{X}}(a,a) = 1, \\ &\sum_{a \leq c \leq b} \mu_{\mathcal{X}}(a,c) = 0 \text{ when } a < b. \end{aligned} \tag{1.1}$$

(The definitive reference on Möbius functions is Rota [**20**].)

If $\mathcal{X}$ has a smallest element, 0 say, we shall write $\mu_{\mathcal{X}}(x)$ for $\mu_{\mathcal{X}}(0,x)$. The $\mu(G)$ referred to in our prefatory remarks is in fact $\mu_{\mathcal{L}}(1,G)$, where $\mathcal{L} = \mathcal{L}(G)$, the poset of all subgroups of G. When discussing subposets of $\mathcal{L}(G)$ we shall reserve the unadorned symbol μ for this meaning.

We will now explain the result of Brown's mentioned at the outset. If p is a prime, $\mathcal{L}_p(G) \subseteq \mathcal{I}(G)$ will denote the subposet of all p-subgroups of G. Observe that the Möbius function with respect to $\mathcal{I}_p(G)$ is simply the restriction of the Möbius function on $\mathcal{I}(G)$. With any poset $\mathcal{X}$ there is associated a simplicial complex called the *order complex* of $\mathcal{X}$, whose n-simplices are the chains in $\mathcal{X}$ with exactly n links. Granted a least element 0 in $\mathcal{X}$, it turns out that the Euler characteristic of the order complex of $\mathcal{X}\backslash\{0\}$ is equal to $1 - s$, where

$$s = \sum_{x \in \mathcal{X}} \mu_{\mathcal{X}}(0,x).$$

(We refer the reader to §9 for more details.) In 1975 Brown [**4**] showed that the Euler characteristic of the order complex of $\mathcal{I}_p(G)\backslash\{1\}$ is congruent to 1 modulo $|G|_p$, the order of a Sylow p-subgroup of G,

or, equivalently, that

$$|G|_p \text{ divides } \sum_{X \in \mathcal{I}_p(G)} \mu(X). \tag{1.2}$$

We will refer to this result as Brown's theorem, although in fact Brown proves a more general result about groups satisfying homological finiteness conditions, which is equivalent to (1.2) for finite groups. Subsequently Quillen [**19**] carried out a more detailed investigation of the topological invariants of the order complex of $\mathcal{I}_p(G)\backslash\{1\}$ and gave another topological proof of (1.2).

A purely algebraic proof of Brown's theorem was first given by Gluck [**11**] in 1981; it exploited an earlier theorem of Dress [**7**] about prime ideals and idempotents in the Burnside ring of G over $\mathbf{Z}$. The connection between the idempotents of this ring and the Möbius function on the poset $\mathcal{C}(G)$ of conjugacy classes of subgroups of G had already been noticed by Solomon [**21**] in 1967. Gluck's algebraic proof was discovered independently by Yoshida [**30**]. The problem of evaluating μ for a given group was addressed by Kratzer and Thévenaz in [**15**], where, in particular, they gave a formula for $\mu(H, G)$ when G is soluble and showed that, for any G, the integer $m\mu(G)$ is always divisible by $|G|$, where m is the square-free part of $|G : G'|$. In particular, when G is perfect, $\mu(G)$ is divisible by $|G|$. (See Corollary 4.9 for a refinement of this.)

The paper is organized as follows. In §2 we review some standard facts about posets and their Möbius functions. These are applied to subposets of $\mathcal{I}(G)$ in §3, where a key result about divisibility (Theorem 3.7) is proved. In §4 we exploit the Möbius inversion formula to prove that $|\mathbf{N}_G(H) : H|$ divides $m\mu(H, G)$, where m is a certain factor of $|G : G'|$, and deduce from it the truth of the conjecture of Thévenaz cited above. Our main results, already mentioned in the preface, are contained in §5 and §6.

If $\mathcal{C}$ denotes the poset of conjugacy classes of subgroups of G, we prove in §7 that if G is soluble, then

$$\mu(G) = \mu_{\mathcal{C}}(G)|G'|.$$

On the basis of a few computations with some insoluble groups, there is some evidence that the solubility hypothesis may be redundant

here. It is certainly not redundant, however, in the theorem that $\mu(G)$ involves only primes dividing $|G|$, which follows from Gaschütz's formula for $\mu(G)$ when G is soluble; in §8 we derive a formula for $\mu(G)$ when G is a direct product of simple groups, and this provides easy counterexamples. Finally, in §9, we discuss the earlier results and proofs of this paper from a topological viewpoint.

2. Posets and chains. Let $\mathcal{X} = (\mathcal{X}, \leq)$ be a finite poset. (Throughout we shall use 'poset' to mean '*finite* poset' except possibly in the final §9.)

DEFINITION 2.1. If $x \in \mathcal{X}$, an *x-chain* is a (possibly empty) linearly ordered subset of the poset

$$\mathcal{X}_{>x} = \{y \in \mathcal{X} : y > x\}.$$

If $\emptyset \neq \mathcal{S} \subseteq \mathcal{X}$, we will write $\max \mathcal{S}$ to denote the set of maximal elements of $\mathcal{S}$.

LEMMA 2.2. *If $y > x$, then*

$$\mu_{\mathcal{X}}(x, y) = \sum (-1)^{|\mathcal{C}|},$$

where the sum is over all x-chains $\mathcal{C}$ with $\max \mathcal{C} = \{y\}$.

PROOF. We use induction on the length of the longest chain from x to y. Denote the maximal element of a non-empty x-chain $\mathcal{C}$ by $m(\mathcal{C})$. Then the map $\mathcal{C} \mapsto \mathcal{D} = \mathcal{C} - \{y\}$ is a bijection from x-chains $\mathcal{C}$ with $m(\mathcal{C}) = y$ to possibly empty x-chains $\mathcal{D}$ satisfying $m(\mathcal{D}) < y$ when $\mathcal{D} \neq \emptyset$. Thus

$$\begin{aligned}
\sum_{m(\mathcal{C})=y} (-1)^{|\mathcal{C}|} &= -\Big(\sum_{\substack{\mathcal{D} \neq \emptyset \\ m(\mathcal{D}) < y}} (-1)^{|\mathcal{D}|} \Big) - 1 \\
&= -\Big(\sum_{x<z<y} \mu_{\mathcal{X}}(x, z) \Big) - \mu_{\mathcal{X}}(x, x) \\
&= \mu_{\mathcal{X}}(x, y),
\end{aligned}$$

where the second equality follows from the inductive hypothesis and the third from the definition of μ.

COROLLARY 2.3. *We have*

$$\sum_{y \in \mathcal{X}} \mu_{\mathcal{X}}(x, y) = \sum_{x-\text{chains } \mathcal{C}} (-1)^{|\mathcal{C}|}.$$

LEMMA 2.4. *Let $\mathcal{X}$ be a poset such that every non-empty subset $\mathcal{S}$ has a greatest lower bound* $\inf \mathcal{S}$. *(Such an $\mathcal{X}$ is called a meet-semilattice.) For $z \in \mathcal{X}$* set $\mathcal{M}(z) = \{m \in \max \mathcal{X} : m \geq z\}$, *and assume that*

$$\inf \mathcal{M}(z) > z.$$

Then $\sum_{x \in \mathcal{X}} \mu_{\mathcal{X}}(z, x) = 0$.

PROOF. By the principle of inclusion-exclusion (See, e.g., Rota [**20**, p. 345]) we have

$$\sum_{x \in \mathcal{X}} \mu_{\mathcal{X}}(z, x) = \sum_{\emptyset \neq \mathcal{S} \subseteq \mathcal{M}(z)} (-1)^{|\mathcal{S}|-1} \Big(\sum_{w \leq \inf \mathcal{S}} \mu_{\mathcal{X}}(z, w) \Big).$$

But $\inf \mathcal{S} \geq \inf \mathcal{M}(z) > z$ for all $\emptyset \neq \mathcal{S} \subseteq \mathcal{M}(z)$, and so each sum $\sum_{w \leq \inf \mathcal{S}} \mu_{\mathcal{X}}(z, w)$ is zero by the definition of $\mu_{\mathcal{X}}$ (see (1.1)). □

Since we occasionally want to work in the dual poset $\mathcal{X}^*$ of a poset $\mathcal{X}$, it is worth observing that

$$\mu^*(y, x) = \mu(x, y), \tag{2.5}$$

where μ^* is the Möbius function of $\mathcal{X}^*$. This is readily seen by noting the bijection

$$\mathcal{C} \mapsto \mathcal{D} = (\mathcal{C} - \{y\}) \cup \{x\}$$

from x-chains $\mathcal{C}$ of $\mathcal{X}$ with $\max \mathcal{C} = \{y\}$ to y-chains $\mathcal{D}$ of $\mathcal{X}^*$ with $\max \mathcal{D} = \{x\}$ and then appealing to Lemma 2.2.

DEFINITION 2.6. We shall call an element a of a poset $\mathcal{X}$ *conjunctive* if the pair $\{a, x\}$ has a least upper bound, written $a \vee x$, for each $x \in \mathcal{X}$.

In particular, if $\mathcal{X}$ is a lattice, then each element of $\mathcal{X}$ is conjunctive.

LEMMA 2.7. *Let $\mathcal{X}$ be a poset with a least element 0, and let $a > 0$ be a conjunctive element of $\mathcal{X}$. Then, for each $b \geq a$, we have*

$$\sum_{a \vee x = b} \mu_{\mathcal{X}}(x) = 0.$$

PROOF. The conclusion certainly holds when $b = a$ by definition of $\mu_{\mathcal{X}}$. Suppose that the result is false and choose a minimal b for which the conclusion fails. Then $0 < b$, and so

$$\begin{aligned} 0 &= \sum_{x \leq b} \mu_{\mathcal{X}}(x) \\ &= \sum_{a \vee x = b} \mu_{\mathcal{X}}(x) + \sum_{a \leq y < b} \Big(\sum_{a \vee x = y} \mu_{\mathcal{X}}(x) \Big). \end{aligned}$$

By the minimality of b, the last sum is zero, and so the conclusion of the lemma holds. This contradiction completes the proof. □

For our applications we need to consider group actions. We say that *a group G acts on a poset $\mathcal{X}$* if $\mathcal{X}$ is a G-set in the usual sense and if additionally $xg \leq yg$ whenever $x \leq y$. In the sequel G will usually act by conjugation on some subposet of $\mathcal{S}(G)$.

If G acts on $\mathcal{X}$ and $g \in G$, we write

$$\mathcal{X}^g = \{x \in \mathcal{X} : xg = x\}$$

for the subposet of fixed points, and we denote the Möbius function on $\mathcal{X}^g$ by μ_g.

LEMMA 2.8. *Let G act on a poset $\mathcal{X}$ fixing the element z of $\mathcal{X}$. For each $g \in G$ define*

$$\pi(g) = \sum_{x \in \mathcal{X}^g} \mu_g(z, x).$$

Then π is a difference of permutation characters of G.

PROOF. Let π_i denote the permutation character of G acting on the z-chains of length i in $\mathcal{X}$. The fixed points of this action are simply the z-chains of length i in $\mathcal{X}^g$, and so

$$\sum_i (-1)^i \pi_i(g) = \sum (-1)^{|\mathcal{C}|}, \text{ over } z-\text{chains } \mathcal{C} \text{ of } \mathcal{X}^g,$$

$$= \sum_{x \in \mathcal{X}^g} \mu_g(z, x) = \pi(g),$$

where the second inequality follows from Corollary 2.3. Thus

$$\pi = \Big(\sum_{i \text{ even}} \pi_i \Big) - \Big(\sum_{i \text{ odd}} \pi_i \Big). \quad \square$$

Finally we need to quote the "lemma that is not Burnside's" (or, rather, the Cauchy-Frobenius lemma - see Neumann [**18**]):

LEMMA 2.9. (a) *If G acts on a set Ω with exactly t orbits, then*

$$\sum_{g \in G} |\Omega^g| = t|G|.$$

(b) *If π is the difference of permutation characters, then the integer $\sum_{g \in G} \pi(g)$ is divisible by $|G|$.*

PROOF. (a) If G is transitive, a count of the set of pairs $S = \{(\omega, g) : \omega \in \Omega, g \in G, \text{ and } \omega g = \omega\}$ in two ways yields

$$|G| = |\Omega| \, |G_\omega| = \sum_{\omega \in \Omega} |G_\omega| = |S| = \sum_{g \in G} |\Omega^g|,$$

where G_ω is the stabilizer of ω. In the general case, apply this to each orbit to give the stated result. Assertion (b) follows at once from (a). $\square$

3. Subgroup posets. Here we are mainly concerned with subposets $\mathcal{X}$ of $\mathcal{S}(G)$, the poset of all subgroups of a finite group, and their Möbius

functions $\mu_{\mathcal{X}}$. The bare μ will always mean $\mu_{\mathcal{S}(G)}$, and $\mu(1, H)$ will be denoted simply by $\mu(H)$ when no confusion can arise. If $L \leq H \leq G$, then $\mu(L, H)$ can be calculated entirely within $\mathcal{S}(H)$ and is independent of the embedding of H in G; in particular, $\mu_{\mathcal{S}(G)}(H)$ $[= \mu_{\mathcal{S}(H)}(H)]$ is an invariant of H.

The following result is a version of a theorem of Crapo [**6**] in this setting. (See also Théorème 2.1 of Kratzer and Thévenaz [**15**].)

LEMMA 3.1. *Let $N \lhd G$ and denote by $\mathcal{K}(G, N)$ the set of all subgroups of G which complement N. Then*

$$\mu(G) = \mu(G/N) \sum_{K \in \mathcal{K}(G,N)} \mu(K, G).$$

PROOF. Since the result is trivial when $N = 1$, assume $N > 1$. By Lemma 2.8 (with $\mathcal{X} = \mathcal{S}(G)$ and N the conjunctive element) we have

$$\begin{aligned} \mu(G) &= -\sum_{\substack{X < G \\ XN = G}} \mu(X) \\ &= -\sum_{X < G} \mu(X/X \cap N) \sum_{K \in \mathcal{K}(X, X \cap N)} \mu(K, X), \end{aligned}$$

where the second equality follows by induction on $|G|$.

Each complement for $X \cap N$ in X is a complement for N in G, and, conversely, each complement $K \in \mathcal{K}(G, N)$ also lies in $\mathcal{K}(X, X \cap N)$ for every subgroup X with $K \leq X \leq G$. Since $X/X \cap N \cong G/N$ whenever $XN = G$, we can interchange the order of the above double summation and obtain

$$\mu(G) = -\mu(G/N) \sum_{K \in \mathcal{K}(G,N)} \sum_{K \leq X < G} \mu(K, X).$$

By the definition of μ, the inner sum is equal to $-\mu(K, G)$, and the result follows. □

An alternative formulation of Lemma 3.1 can be obtained from the observation that if $N \lhd G$ and $K \in \mathcal{K}(G, N)$, then the lattice of

subgroups X with $K \leq X \leq G$ is isomorphic to the lattice $\mathcal{J}(N, K)$ of K-invariant subgroups of N. It follows that $\mu(K, G) = \mu_{\mathcal{J}(N,K)}(N)$, and so

$$\mu(G) = \mu(G/N) \sum_{K \in \mathcal{K}(G,N)} \mu_{\mathcal{J}(N,K)}(N).$$

The following corollary shows that $\mu(G) = 0$ whenever G has a Frattini chief factor.

COROLLARY 3.2. *Let G be a group with $\mu(G) \neq 0$. If $N \leq M \lhd G$ with $N \lhd G$, then M/N is complemented in G/N. In particular, $\Phi(G/N) = 1$.*

PROOF. By the previous result $\mu(G/N) \neq 0$, and so we may assume without loss of generality that $N = 1$. Then, by the previous result once more, we have $\mathcal{K}(G, M) \neq \emptyset$. □

If N is an abelian minimal normal subgroup of G with a complement K, then K is a maximal subgroup of G, and so $\mu(K, G) = -1$. We thus have

COROLLARY 3.3. *Let A be an abelian minimal normal subgroup of G and let k denote the number of complements to A in G. Then*

$$\mu(G) = -k\mu(G/A).$$

Applying this inductively, we obtain Gaschütz's formula for the Möbius value of a soluble group.

COROLLARY 3.4. *Let $1 = H_0 < H_1 < \cdots < H_n = G$ be a chief series for the soluble group G, and let k_i denote the number of complements to H_i/H_{i-1} in G/H_{i-1}. Then*

$$\mu(G) = (-1)^n k_1 k_2 \cdots k_n.$$

Corollary 3.3 also yields an easy proof of the following result of P. Hall [**12**].

COROLLARY 3.5. *Let P be a p-group of order p^n. Then $\mu(P) = 0$ unless P is elementary abelian, in which case*

$$\mu(P) = (-1)^n p^{\binom{n}{2}}.$$

PROOF. If $\Phi(P) \neq 1$, then $\mu(P) = 0$ by Corollary 3.2. Otherwise P is elementary abelian, and then we argue by induction on $|P|$. Let $A \leq P$ with $|A| = p$. Then $\mu(P/A) = (-1)^{n-1} p^{\binom{n-1}{2}}$ by induction. Of the $(p^n - 1)/(p-1)$ maximal subgroups of P, a total of $(p^{n-1} - 1)/(p-1)$ contain A. Hence A has $(p^n - p^{n-1})/(p-1) = p^{n-1}$ complements in P, and so Corollary 3.3 gives $\mu(P) = (-1)^n p^{\binom{n-1}{2}+n-1}$, which yields the stated formula. □

DEFINITION 3.6. A subset $\mathcal{X}$ of a poset $\mathcal{P}$ is called *convex* if, whenever $x, y \in \mathcal{X}$ and $x \leq w \leq y$, it follows that $w \in \mathcal{X}$.

The following theorem will play a central part in the proofs of our main results.

THEOREM 3.7. *Let A be a group acting on a poset $\mathcal{P}$. Let $\mathcal{X}$ be an A-invariant, convex subset of $\mathcal{P}$, and assume that $\mathcal{X}$ has a unique minimal element z (necessarily fixed by A). For $a \in A$, set*

$$\mathcal{X}^a = \{x \in \mathcal{X} : xa = x\}.$$

Let B be a normal subgroup of A contained in the kernel of the action of A on $\mathcal{X}$, and assume further that

$$\sum_{x \in \mathcal{X}^a} \mu_a(z, x) = 0 \tag{3.8}$$

for all $a \in A \backslash B$. Then

$$|A : B| \text{ divides } \sum_{x \in \mathcal{X}} \mu_{\mathcal{P}}(z, x).$$

(In applications of this result, we shall take $\mathcal{P} = \mathcal{S}(G)$. The group A will act on G, fixing a convex subset $\mathcal{X}$, and Condition (3.8) will be verified by an appeal to Lemma 2.4.)

PROOF. For each $a \in A$, let μ_a denote the Möbius function for the fixed-point poset $\mathcal{X}^a$. Since $\mathcal{X} = \mathcal{X}^1$ is convex, clearly μ_1 coincides with $\mu_{\mathcal{P}}$ on $\mathcal{X} \times \mathcal{X}$. By Lemma 2.8 the function

$$\pi(a) = \sum_{x \in \mathcal{X}^a} \mu_a(z, x)$$

is a difference of permutation characters of A, and $\pi(a) = 0$ for all $a \in A/B$ by Hypothesis 3.8. Since it is really A/B that acts on $\mathcal{X}$, we can view π as a difference of permutation characters for A/B, and conclude from Lemma 2.9(b) that $|A \backslash B|$ divides

$$\sum_{g \in A/B} \pi(g) = \pi(1) = \sum_{x \in \mathcal{X}} \mu_{\mathcal{P}}(z, x).$$

At this stage we can easily read off some known results. Let G be a group, p a prime, and n an integer which divides $|G|$ and is divisible by $|G|_p$. Let $H \leq G$ have order dividing n and write

$$\mathcal{X} = \{X \leq G : X \geq H \text{ and } |X| \text{ divides } n\}.$$

We see that $\mathcal{X}$ is convex and H is its smallest element. In Theorem 3.7 take $A \in \mathrm{Syl}_p(\mathbf{N}(H))$ and $B = A \cap H$, acting by conjugation on $\mathcal{X}$. If $a \in A \backslash B$ and $M \in \max \mathcal{X}^a$, then $\langle M, a \rangle$ is clearly a-fixed; moreover, since $|\langle M, a \rangle : M|$ divides $|\langle a \rangle|$, a p-number, we have $\langle M, a \rangle \in \mathcal{X}^a$ and hence $\langle M, a \rangle = M$ by the choice of M. Therefore $\langle H, a \rangle \leq \inf \mathcal{M}(H)$, the hypotheses of Lemma 2.4 are satisfied for the poset $\mathcal{X}^a$, and consequently so is its conclusion that

$$\sum_{X \in \mathcal{X}^a} \mu_a(H, X) = 0.$$

In other words, Hypothesis 3.8 is fulfilled. Thus we have

COROLLARY 3.9. *Let G be a finite group whose order is divisible by n, and assume that n in turn is divisible by $|G|_p$, the order of a Sylow p-subgroup of G. If H is a subgroup whose order divides n, then $[\mathbf{N}(H) : H]_p$ divides $\sum \mu(H, X)$, where the sum is over all subgroups X of G with $|X|$ dividing n.*

Of course, when $H = 1$ and $n = |G|_p$, this is exactly Brown's theorem.

By taking for $\mathcal{X}$ the set of all soluble subgroups of G, setting $A = G$, $B = 1$, and verifying Hypothesis 3.8 as before, we similarly obtain

COROLLARY 3.10. *The sum* $\sum \mu(X)$ *over the soluble subgroups* X *of* G *is divisible by* $|G|$.

It is interesting to see how a weaker version of Corollary 3.5 can also be deduced from Theorem 3.7. Let P be an elementary abelian p-group of order p^n, and take $A \in \mathrm{Syl}_p(\mathrm{Aut}(P))$. Then $|A| = |GL(n,p)|_p = p^{\binom{n}{2}}$, and A acts faithfully on P. Let $\mathcal{X}$ be the (convex) set of all *proper* subgroups of P, and observe that each a in A acts trivially on $P/(\cap \max \mathcal{X}^a)$ because $|P : M| = p$ when $M \in \max \mathcal{X}^a$. Thus $\cap \max \mathcal{X}^a > 1$ when $a \neq 1$, and it follows from Lemma 2.4 and Theorem 3.7 that $\mu(P) = -\sum_{x \in \mathcal{X}} \mu(X)$ is divisible by $|A|$. This weaker conclusion of divisibility instead of equality is, in fact, sufficient for our subsequent needs.

4. Möbius inversion. We begin with the well-known Möbius inversion formula. (For instance, see Rota [**20**].)

PROPOSITION 4.1. *Let* f *be a function from a poset* $\mathcal{X}$ *into an additive abelian group. For a fixed* $a \in \mathcal{X}$ *define*

$$F(b) = \sum_{a \leq x \leq b} f(x).$$

Then, for $b \geq a$, *we have*

$$f(b) = \sum_{a \leq x \leq b} \mu_{\mathcal{X}}(x,b) F(x).$$

PROOF. For a fixed element $b \geq a$, we have

$$\begin{aligned} \sum_{a \leq x \leq b} \mu(x,b) F(x) &= \sum_{a \leq x \leq b} \mu(x,b) \Big(\sum_{a \leq y \leq x} f(y) \Big) \\ &= \sum_{a \leq y \leq b} f(y) \Big(\sum_{y \leq x \leq b} \mu(x,b) \Big). \end{aligned}$$

If μ^* denotes the Möbius function for the dual poset $\mathcal{X}^*$, by (2.5) we have $\sum_{y \le x \le b} \mu(x,b) = \sum_{y \le x \le b} \mu^*(b,x) = \delta_{by}$ by definition of μ. Thus the only non-zero term in the final sum above is $f(b)$. □

DEFINITION 4.2. For subgroups L and H of a group G, we define

$$\alpha_L(H,G) = \sum_{X \ge \langle H,L \rangle} \mu(H,X),$$

where the sum runs over all subgroups X of G containing $\langle H,L \rangle$.

Note that $\alpha_G(H,G) = \mu(H,G)$ and that $\alpha_H(H,G) = \delta_{HG}$.

COROLLARY 4.3. *Let $L, H \le G$. Then*

$$\mu(H,G) = \sum \mu(X,G)\alpha_L(H,X),$$

where the sum runs over subgroups X of G containing $\langle H,L \rangle$.

PROOF. In Proposition 4.1, take $\mathcal{P} = \mathcal{S}(G)$, $a = \langle H,L \rangle$, $b = G$ and $f(X) = \mu(H,X)$. Then $F(X) = \alpha_L(H,X)$, and the conclusion of Proposition 4.1 yields the stated equation. □

PROPOSITION 4.4. *Let p be a prime and H a subgroup of G. Set $L = \mathbf{O}^p(G)$. Then $\alpha_L(H,G)$ is divisible by $|\mathbf{N}_G(H) : H|_p$.*

PROOF. Without loss of generality, assume that $H < G$ and let $P \in \mathrm{Syl}_p(\mathbf{N}_G(H))$. Set $\mathcal{X} = \{X \le G : X \ge H, X \not\ge L\}$ and

$$s = \sum_{X \in \mathcal{X}} \mu(H,X).$$

Since $\alpha_L(H,G) + s = 0$ by definition of μ, it is sufficient to show that $|\mathbf{N}_G(H) : H|_p$ divides s. Since $\mathcal{X} = \emptyset$ and $s = 0$ when $H \ge L$, we may suppose that $H \in \mathcal{X}$. Because the subgroup P normalizes H and L, it leaves $\mathcal{X}$ invariant, and $P \cap H$ fixes $\mathcal{X}$ elementwise. Let

$a \in P \backslash (P \cap H)$, and let M be maximal among the a-invariant elements of $\mathcal{X}$. If $M\langle a \rangle \geq L$, then

$$1 < L/(L \cap M) \cong LM/M \leq M\langle a \rangle / M,$$

which is a p-group; but this is impossible because $\mathbf{O}^p(L) = L$. Therefore $M\langle a \rangle \in \mathcal{X}^a$, and hence $a \in M$ by the choice of M. It follows that the intersection of all such M contains $H\langle a \rangle > H$, the least element of $\mathcal{X}$. Hence Hypothesis 3.8 holds by Lemma 2.4, and so by Theorem 3.7 the index $|P : P \cap H|$ divides s, as required.

Our next result is a slightly strengthened form of Théorème 3.1 of Kratzer and Thévenaz [**15**]. To state it, we define the *square-free part* of an integer n to be the product of the distinct prime divisors of n.

THEOREM 4.5. *Let H be a subgroup of G and let m be the square-free part of $|G : G'H|$. Then $|\mathbf{N}_G(H) : H|$ divides $m\mu(H, G)$.*

PROOF. We work one prime at a time. Fix a prime p and let $L = \mathbf{O}^p(G)$. We aim to prove that $|\mathbf{N}_G(H) : H|_p$ divides $m\mu(H, G)$. By Corollary 4.3, we have

$$\mu(H, G) = \sum \alpha_L(H, X)\mu(X, G), \tag{4.6}$$

summed over all subgroups X of G which satisfy

$$LH \leq X \leq G.$$

For such an X we have $L = \mathbf{O}^p(X)$, and we conclude from Proposition 4.4 that

$$|\mathbf{N}_X(H) : H|_p \text{ divides } \alpha_L(H, X). \tag{4.7}$$

In particular, $|\mathbf{N}_G(H) : H|_p$ divides the term in the sum in (4.6) corresponding to $X = G$. It therefore suffices to show

$$|\mathbf{N}_G(H) : H|_p \text{ divides } m\alpha_L(H, X)\mu(X, G) \tag{4.8}$$

whenever $LH \leq X < G$. In particular, we may assume that $LH < G$, whence it follows that $|G : G'H|$ is divisible by p and hence that $m_p = p$.

Now by definition of μ, for a given $X < G$, we have

$$\mu(X,G) = -\sum_{X \leq Y < G} \mu(X,Y),$$

which by Lemma 2.4 equals zero unless X is an intersection of maximal subgroups, which, since they contain L, are necessarily normal of index p. We therefore need consider only subgroups $X \geq H$ for which $X \lhd G$ and G/X is an elementary abelian p-group. In this situation, the final statement of Corollary 3.5 tells us that

$$|G : X| \text{ divides } p\mu(G/X) = p\mu(X,G).$$

Since $X \lhd G$, we see that

$$|\mathbf{N}_G(H) : H| \text{ divides } |G : X|\ |\mathbf{N}_X(H) : H|,$$

and it is clear, since $p|m$, that (4.7) yields (4.8). □

An immediate consequence of Theorem 4.5, obtained by taking $H = 1$, is that, for an arbitrary finite group G,

$$|G| \text{ divides } m\mu(G),$$

where m is the square-free part of $|G : G'|$. We can sharpen this.

COROLLARY 4.9. *Let m be the product of those prime numbers p for which $G/\mathbf{O}^p(G)$ is elementary abelian of order p or p^2. Then*

$$|G| \textit{ divides } m\mu(G).$$

Furthermore, for any prime p,

$$|\mathbf{O}^p(G)|_p \textit{ divides } \sum_K \mu(K,G),$$

where K runs over all complements to $\mathbf{O}^p(G)$ in G.

PROOF. Fix a prime p and write $L = \mathbf{O}^p(G)$. By Lemma 3.1, we have

$$\mu(G) = \mu(G/L) \sum_{K \in \mathcal{K}(G,L)} \mu(K, G),$$

where $\mathcal{K}(G, L)$ is the set of complements to L in G. By Corollary 3.5, we see that $|G : L|$ divides $m\mu(G/L)$ and so, assuming the second assertion for the moment, we see that $|G|_p$ divides $m\mu(G)$, and the first statement follows.

We proceed to prove

$$|L|_p \text{ divides } \sum_{K \in \mathcal{K}(G,L)} \mu(K, G). \tag{4.10}$$

Since $\mu(K_1, G) = \mu(K_2, G)$ whenever K_1 and K_2 are conjugate under the action of L, the part of the sum in (4.10) corresponding to the L-conjugates of some fixed $K \in \mathcal{K}(G, L)$ is equal to $|L : \mathbf{N}_L(K)|\mu(K, G)$, and it suffices to show that this is divisible by $|L|_p$. In particular, it is enough to show

$$|\mathbf{N}_L(K)|_p \text{ divides } \mu(K, G) \tag{4.11}$$

whenever $K \in \mathcal{K}(G, L)$. In this situation, $|\mathbf{N}_L(K)| = |\mathbf{N}_G(K) : K|$, and p does not divide $|G : G'K|$ because $G = \mathbf{O}^p(G)K$; therefore Theorem 4.5 applies and yields 4.11. □

We shall use a somewhat similar argument to prove our next result.

COROLLARY 4.12. *Let n divide $|G|$ and let m be the square-free part of $|G : G'|$. Let*

$$\mathcal{Q} = \{H \leq G : |H| \text{ does not divide } n\}.$$

Then $|G|$ divides $mn \sum_{X \in \mathcal{Q}} \mu(X, G)$.

Before giving the proof of this result, we shall show that it is, in fact, equivalent to Conjecture 4.2 in Thévenaz [**26**]. Let $\overline{\mathcal{Q}}$ denote the

augmented poset $\mathcal{Q} \cup \{1\}$. Then by (2.5) and the definition of μ we have

$$\begin{aligned}\mu_{\overline{\mathcal{Q}}}(G) = \mu_{\overline{\mathcal{Q}}}(1, G) &= -\sum_{1<X\leq G} \mu_{\overline{\mathcal{Q}}}(X, G) \\ &= -\sum_{1<X\leq G} \mu(X, G)\end{aligned}$$

since if $X \in \mathcal{Q}$ and $X \leq Y \leq G$, then $Y \in \mathcal{Q}$. The conclusion of 4.12 is therefore equivalent to the statement

$$|G|/n \text{ divides } m\mu_{\overline{\mathcal{Q}}}(G).$$

Since primes which divide m but do not divide $|G|/n$ can be ignored, this is equivalent to

$$|G|/n \text{ divides } \overline{m}\mu_{\overline{\mathcal{Q}}}(G)$$

where $\overline{m} = \text{g.c.d. } (m, |G|/n)$. This, in turn, (for instance by (9.1)) is equivalent to Thévenaz's conjecture.

PROOF OF COROLLARY 4.12. Since

$$\begin{aligned}\sum_{X\in\mathcal{Q}} \mu(X, G) &= \sum_{X\in\mathcal{S}(G)} \mu(X, G) - \sum_{|X| \text{ divides } n} \mu(X, G) \\ &= -\sum_{|X| \text{ divides } n} \mu(X, G),\end{aligned}$$

it will suffice to show that

$$|G| \text{ divides } mn \sum \mu(X, G),$$

as X runs through any G-conjugacy class of subgroups of order dividing n. We must show, in other words, that

$$|G| \text{ divides } mn|G : \mathbf{N}_G(X)|\mu(X, G) \tag{4.13}$$

whenever $X \leq G$ with $|X|$ dividing n. To prove (4.13), therefore, we need that

$$|\mathbf{N}_G(X)| \text{ divides } mn\mu(X, G),$$

and this follows from Theorem 4.5 since $|X|$ divides n. □

5. Generalizations of Brown's theorem. Our main theorem is the following.

THEOREM 5.1. *Let H be a subgroup of G, and let n divide $|G|$. Set*

$$\mathcal{X} = \mathcal{X}_H(n) = \{X \leq G : X \geq H \text{ and } |X| \text{ divides } n\}$$

and

$$s = s_H(n) = (|G|/|\mathbf{N}_G(H) : H|) \sum_{X \in \mathcal{X}} \mu(H, X).$$

Then n divides s.

PROOF. Let p be a prime dividing n. We aim to show that the p-part n_p of n divides s.

We have already dealt with the special case $n_p = |G|_p$ in Corollary 3.9. To handle the general case, let $p^e = |G|_p/n_p$, and set $n^* = np^e$, so that $(n^*)_p = |G|_p$. Setting

$$\mathcal{Y} = \mathcal{X}_H(n^*) \backslash \mathcal{X}_H(n),$$

we obtain

$$s_H(n) = s_H(n^*) - (|G|/|\mathbf{N}_G(H) : H|) \sum_{Y \in \mathcal{Y}} \mu(H, Y).$$

Observe that $\mathcal{Y}$ is invariant under conjugation by $\mathbf{N}_G(H)$; also that if $Y \in \mathcal{Y}$, then $|Y|_p \geq pn_p$. Let L denote the normalizer of Y in $\mathbf{N}_G(H)$. Then the contribution of the set of $\mathbf{N}_G(H)$-conjugates of Y to the sum $\sum_{Y \in \mathcal{Y}} \mu(H, Y)$ is

$$t = |\mathbf{N}_G(H) : L| \mu(H, Y).$$

Since, by the special case, $s_H(n^*)$ is divisible by n_p, to prove the theorem it will suffice to show that

$$n_p \text{ divides } t|G|_p/|\mathbf{N}_G(H) : H|_p. \tag{5.2}$$

Now $|\mathbf{N}_G(H) : H| = |\mathbf{N}_G(H) : L|\ |L : \mathbf{N}_Y(H)|\ |\mathbf{N}_Y(H) : H|$ and $\mathbf{N}_Y(H) = L \cap Y$. Since $|\mathbf{N}_Y(H) : H|_p$ divides $p\mu(H, Y)$ by Theorem 4.5, it follows that $|\mathbf{N}_G(H) : H|_p$ divides

$$|\mathbf{N}_G(H) : L|\ |L : L \cap Y| p\mu(H, Y) = pt|L : L \cap Y|.$$

Moreover, since $|LY|_p \leq |G|_p$, we have $|L : L \cap Y|_p = |LY : Y|_p \leq |G|_p/|Y|_p \leq |G|_p/pn_p$ by the choice of $Y \in \mathcal{Y}$. Consequently $|\mathbf{N}_G(H) : H|_p$ also divides $pt(|G|_p/pn_p) = t|G|_p/n_p$; in other words, $t|G|_p/n_p|\mathbf{N}_G(H) : H|_p$ is an integer, whence (5.2) follows. □

COROLLARY 5.3. *Let $H \leq G$ and n divide $|G|$. Then n divides $|H| \sum \mu(J, X)$, where the sum is over distinct ordered pairs (J, X) with J conjugate to $H, J \leq X \leq G$, and $|X|$ dividing n.*

By now taking $H = 1$ in Corollary 5.3, we obtain Thévenaz's generalization of Brown's theorem.

COROLLARY 5.4. *If n divides $|G|$, then n divides $\sum_{|X| \text{divides } n} \mu(X)$.*

6. A theorem of Frobenius. If X is a group, let $\varphi_S(X)$ denote the number of s-tuples $(x_1, \cdots, x_s)$ of group elements x_i such that $X = \langle x_1, \cdots, x_s \rangle$. Then obviously

$$|G|^s = \sum_{X \leq G} \varphi_s(X). \tag{6.1}$$

Set $\mu^*(X) = \mu(X, G)$. In his paper on Eulerian functions [**13**], Hall uses μ for our μ^* and $\overline{\mu}$ for our $\mu_{\mathcal{S}(G)}$. Then μ^* is the Möbius function associated with the dual poset of $\mathcal{S}(G)$ and so $\mu(G) = \mu^*(1)$. Applying the Möbius inversion formula to (6.1), we obtain

LEMMA 6.2. (P. HALL [**13**]). $\varphi_S(G) = \sum_{X \leq G} \mu^*(X)|X|^S$. *In particular, $\varphi_1(G)$ is zero unless G is cyclic, in which case $\varphi_1(G) = \varphi(|G|)$, the usual Euler φ-function of number theory.*

Corollary 5.3 now yields an elementary proof of Frobenius's theorem. For a different, but related, approach, using the Burnside ring, we refer to Thévenaz [**26**], Theorem 3.3.

THEOREM 6.3. (FROBENIUS). *Let n be a divisor of the order of a finite group G. Then the number of solutions to the equation $x^n = 1$ in G is divisible by n.*

PROOF. Let $\mathcal{X} = \{X \leq G : |X| \text{ divides } n\}$, and let $\mathcal{X}_0$ be the set of cyclic subgroups in $\mathcal{X}$. By Lemma 6.2

$$\begin{aligned}|\{x \in G : x^n = 1\}| &= \sum_{X \in \mathcal{X}_0} \varphi_1(X) = \sum_{X \in \mathcal{X}} \varphi_1(X) \\ &= \sum_{X \in \mathcal{X}} \Big(\sum_{H \leq X} \mu(H, X)|H| \Big) \\ &= \sum_{H \in \mathcal{X}} \Big(|H| \sum_{\substack{X \in \mathcal{X} \\ X \geq H}} \mu(H, X) \Big) \\ &= \sum_{[H] \subseteq \mathcal{X}} \Big(|H| \sum_{(J,X)} \mu(J, X) \Big),\end{aligned}$$

where $[H]$ denotes the conjugacy class of H and where the inner sum of this last expression ranges over distinct pairs (J, X) such that $J \in [H]$ and $J \leq X \in \mathcal{X}$. But this is precisely the sum in Corollary 5.3 that is shown to be divisible by n.

7. The poset of conjugacy classes. If $H \leq G$, let $[H] = \{H^g : g \in G\}$, the conjugacy class of H, and let $\mathcal{C}(G)$ denote the set of all conjugacy classes of subgroups of G. We view $\mathcal{C}(G)$ as a poset with partial ordering $\leq$ defined by the rule

$$[H] \leq [L] \text{ if } H \leq L^g \text{ for some } g \in G.$$

In general, the poset $\mathcal{C}(G)$ is neither a meet- nor a join-semilattice, but it naturally admits Möbius function $\mu_{\mathcal{C}(G)}$, which we denote by λ_G for simplicity. By abuse of notation we shall generally write $\lambda_G(G)$ for $\lambda_G([G])$. Because of the fusion of H-conjugacy classes in G, the

functions λ_H and λ_G are not very closely related and this makes inductive proofs difficult to handle.

For the proof of Theorem 7.2 we shall need the following observation.

LEMMA 7.1. *Let $N \lhd G = NX$ with $N \cap X = 1$. If $n \in N$, then n centralizes $X \cap X^n$.*

PROOF. Let $x \in X \cap X^n$, so that $x = y^n$ for some $y \in X$. Then X contains $y^{-1}x = [y, n]$, and so $[y, n] \in X \cap N = 1$. It follows that $x = y$ and $[x, n] = 1$. □

THEOREM 7.2. *If G is soluble, then $\mu(G) = \lambda_G(G)|G'|$.*

PROOF. We argue by induction on $|G|$. If $G' = 1$, then $\lambda_G = \mu$ and we are done. Therefore suppose $G' \neq 1$, and let N be a minimal normal subgroup of G contained in G'. Since $[N]$ is conjunctive in $\mathcal{C}(G)$, by Lemma 2.7 we have

$$\lambda_G(G) = -\sum \lambda_G([X]), \tag{7.3}$$

where the sum is over the conjugacy classes $[X]$ of complements X to N in G. (Here we are appealing to the fact that proper supplements to N in G are complements because N is abelian.) We assert that

$$\lambda_G([X]) = \lambda_X(X). \tag{7.4}$$

For suppose that $H, H^g \leq X$. Then $H \leq X \cap X^{g^{-1}}$, and since $G = XN$, we have $g^{-1} = xn$ for some $x \in X$ and $n \in N$. Thus $H \leq X \cap X^n$ and by Lemma 7.1 the element n centralizes H, and consequently $H^g = H^{x^{-1}}$. Therefore a non-empty intersection of $\mathcal{S}(X)$ with a conjugacy class of subgroups of G is a conjugacy class of X. It follows that $\mathcal{C}(X)$ is order-isomorphic with the subposet $\{[H] : H \leq X\}$ of $\mathcal{C}(G)$, and hence (7.4) holds. Since $X \cong G/N$, we conclude from (7.3) that

$$\lambda_G(G) = -c\lambda_{G/N}(G/N), \tag{7.5}$$

where c is the number of conjugacy classes of complements to N in G. If $c = 0$, then $N \leq \Phi(G)$, and so $\lambda_G(G) = 0 = \mu(G)$ by Corollary 3.2.

Therefore suppose that $c > 0$, and note that if X is a complement to N in G, then X is not normal in G because we supposed that $N \leq G'$. Since X is maximal in G, we have $\mathbf{N}_G(X) = X$, and so each conjugacy class of complements to N in G contains $|G : X| = |N|$ elements. Hence by Corollary 3.3 we have

$$\begin{aligned}\mu(G) &= -c|N|\mu(G/N) \\ &= -c|N|\lambda_{G/N}(G/N)|(G/N)'| \quad \text{(by induction)} \\ &= \lambda_G(G)|N|\ |G'/N| \quad \text{(by 7.5)} \\ &= \lambda_G(G)|G'|. \ \square\end{aligned}$$

We have considered the possibility of dropping the hypothesis of solubility from Theorem 7.2, and in every example checked that the formula stood. In this connection we are grateful to Michael C. Slattery for helpful discussions and for running a computer check of A_n and S_n $(n = 6, 7)$ and PSL(3,3) on CAYLEY.

8. The μ-value of some direct products. For a soluble group G, Corollary 3.4 implies that when the integer $\mu(G)$ is non-zero, its prime divisors always divide $|G|$. Our goal in this section is to derive a formula for $\mu(G)$ when G is a direct product of simple groups which will show that, here at least, the hypothesis of solubility is indispensable.

LEMMA 8.1. *The number of complements to $A \times 1$ in $A \times B$ equals* $|\mathrm{Hom}(B, A)|$.

PROOF. Let C be a complement to $A \times 1$ in $A \times B$, and denote the projections of C into the two components by π_A and π_B. Then $\pi_B : C \to B$ is an isomorphism, and $\pi_A\pi_B^{-1}$ therefore belongs to $\mathrm{Hom}(B, A)$. Conversely, given $\theta \in \mathrm{Hom}(B, A)$, it is easy to verify that $C_\theta = \{(\theta(b), b) : b \in B\}$ is a subgroup of $A \times B$ complementing $A \times 1$ and that $\pi_A\pi_B^{-1} = \theta$ when $C = C_\theta$. Thus $\theta \mapsto C_\theta$ is a bijection from $\mathrm{Hom}(B, A)$ to the set of complements to $A \times 1$ in $A \times B$. $\square$

DEFINITION 8.2. We say that a group A has the *N-property* with respect to a group B if $|\mathrm{Hom}(B, N_A(T)/T)| = 1$ for all T with

$1 < T \leq A$. (This holds, for example, when B is a simple group with $|B| \geq |A|$.)

LEMMA 8.3. *Let $G = A \times B$, where A has the N-property with respect to B. Let S be a supplement to $A(= A \times 1)$ in G. Then either*

(a) $S = (S \cap A) \times B$ *with* $S \cap A > 1$, *or*

(b) $S \cap A = 1$.

PROOF. Given a supplement S, set $T = S \cap A$, and assume that S is not of Type (b), i.e., that $T \neq 1$. Let $N = \mathbf{N}_G(T)$, and write $Y = N \cap A$. Then $B \leq N$, and $N = N \cap AB = YB$; hence $N/T \cong (Y/T) \times B$. Since S supplements A, we have $|S/T| = |G : A| = |B|$. But $S \leq N$ and $(S/T) \cap (Y/T) = 1$; therefore S/T complements Y/T in N/T. By Lemma 8.1, the number of such complements is $|\mathrm{Hom}(B, Y/T)|$, which is 1 by hypothesis, and therefore S/T must be the unique complement TB/T. Thus $S = TB$, and S is of Type (a). □

THEOREM 8.4. *If A is nontrivial and has the N-property with respect to B, then*

$$\mu(A \times B) = \mu(B)[\mu(A) - s],$$

where s is the number of epimorphisms from B onto A.

PROOF. Applying Lemma 2.7 to $G = A \times B$ with A as the conjunctive element, we have

$$\begin{aligned} \mu(G) &= -\sum_{\substack{S<G \\ AS=G}} \mu(S) \\ &= -h\mu(B) - \sum_{1<T<A} \mu(T \times B), \end{aligned}$$

where h is the number of homomorphisms from B into A, by Lemma 8.3. Arguing by induction on $|A|$, we have $\mu(T \times B) = \mu(B)(\mu(T) - s(T))$ for $1 < T < A$, where $s(T)$ is the number of epimorphisms from

B onto T. Thus

$$\begin{aligned}\mu(G) &= -h\mu(B) - \mu(B)\sum_{1<T<A}(\mu(T) - s(T)) \\ &= \mu(B)\Big[-h - \sum_{1<T<A}\mu(T) + \sum_{1<T<A}s(T)\Big] \\ &= \mu(B)\Big[-h + (1+\mu(A)) + \sum_{1<T<A}s(T)\Big].\end{aligned}$$

Since $\sum_{1<T<A} s(T) = h - 1 - s$, we get the stated formula. □

COROLLARY 8.5. *If A and B are non-isomorphic simple groups, then $\mu(A \times B) = \mu(A)\mu(B)$.*

PROOF. Without loss of generality, $|B| \geq |A|$. Then A has the N-property with respect to B and $s = 0$. □

Theorem 8.4 also enables us to compute $\mu(G)$ when G is a direct power of a simple group.

COROLLARY 8.6. *Let A be a non-abelian simple group and $G = A \times \cdots \times A$, the direct product of n copies of A. Then $\mu(G) = 0$ if $\mu(A) = 0$, or else*

$$\mu(G) = \mu(A)^n \prod_{r=1}^{n-1}(1 - rt),$$

where $t = |\mathrm{Aut}(A)|/\mu(A)$.

PROOF. We proceed by induction on n, noting that the conclusion holds for $n = 1$. Assume that $n > 1$ and write $G = A \times B$, where B is the direct power of $n - 1$ copies of A. Certainly A has the N-property with respect to B by order considerations, and $s = (n-1)|\mathrm{Aut}(A)|$ because, as is well known, there are precisely $n - 1$ different possible kernels for epimorphisms from $B \to A$ (see, for example, Huppert [**14**;

I, 9.12(b)]). Thus, by Theorem 8.4,

$$\begin{aligned}\mu(G) &= \mu(B)[\mu(A) - (n-1)|\mathrm{Aut}(A)|] \\ &= \mu(A)\mu(B)[1 - (n-1)t].\end{aligned}$$

By induction $\mu(B) = \mu(A)^{n-1}\prod_{r=1}^{n-2}(1-rt)$, which yields the stated formula. □

If $A = A_5$, the alternating group of degree 5, then $|\mathrm{Aut}(A)| = 120$ and $\mu(A) = -60$. Thus

COROLLARY 8.7. *If G is the direct power of n copies of A_5, then*

$$\mu(G) = (-60)^n \cdot 3.5 \cdots (2n-1).$$

In particular, every prime divides $\mu((A_5))^n)$ for some n.

In fact, it is not difficult to deduce from Corollary 8.7 that there exists a group G and a prime p such that p divides $\mu(G)(\neq 0)$ but does not divide $|\mathrm{Aut}(G)|$.

9. And now for some topology. Some of the results in the preceding sections were originally stated and proved within a topological framework. The topological perspective, while less elementary, yields more. In many cases the homotopy type of a complex can be determined, instead of just the Euler characteristic. Also, there is the potential for extending some results to infinite posets. The purpose of this section is to demonstrate some of these topological considerations. Even though we tried to keep the exposition elementary, some familiarity with standard concepts of algebraic topology is assumed (such as can be found in Spanier [**22**]). Since we saw no reason to duplicate the proof of Quillen's Lemma 9.3 below, this section is not strictly self-contained. For the reader interested in topological methods in combinatorics, we recommend the note by Björner [**2**].

The connection between Euler characteristics and Möbius functions associated with a finite lattice was observed by Rota [**20**]. A later

construction of Folkman [8] associates a simplicial complex to a poset $\mathcal{P}$. This is called the *order complex* of $\mathcal{P}$, and its simplices are the finite, nonempty chains in $\mathcal{P}$. Of course, a simplicial complex is itself a poset (via inclusion), and its order complex, when so viewed, is its barycentric subdivision. Order-preserving (and order-reversing) maps of posets induce simplicial maps of their order complexes. The *geometric realization* functor associates to a complex its underlying topological space and to a simplicial map the induced piecewise-linear (hence continuous) map. These constructions enable us to assign topological properties, such as Euler characteristics, homology, and homotopy, to posets and order-preserving maps.

When Δ is a finite simplicial complex, the *reduced* Euler characteristic $\overline{\chi}(\Delta)$ is the alternating sum of the dimensions of its *reduced* homology groups (with coefficients in any field). Thus $\overline{\chi}(\Delta) + 1$ is the usual Euler characteristic, and $\overline{\chi}(\Delta)$ equals the alternating count of all the simplices including the (-1)-dimensional empty simplex. If $a < b$ in a poset $\mathcal{P}$, the *(open) interval* $\mathcal{P}_{(a,b)}$ is the subposet lying strictly between a and b. A poset is *locally finite* if all intervals are finite. The Möbius function μ is defined for a locally finite poset. The alternating count of all chains whose smallest element is strictly greater than a and whose largest element is b, is equal to $-\mu(a, b)$ by Lemma 2.2. Equivalently,

$$\mu(a, b) = \overline{\chi}(\mathcal{P}_{(a,b)}). \tag{9.1}$$

Our main results can thus be expressed as divisibility properties of certain reduced Euler characteristics. These were obtained by considering the permutation representation of a group of symmetries on the chains of a poset $\mathcal{P}$. Some information is lost by passing to the homology representation (i.e., going from the Burnside ring to the representation ring as discussed by Thévenaz [**25**], for instance), but not for our purposes. (Deeper combinatorial applications of homology representations of groups acting on posets are given in Stanley [**23**].) In fact, Lemma 2.9 and Theorem 3.7 can be replaced by

LEMMA 9.2. *Let Γ be a finite group acting on a finite poset $\mathcal{P}$, preserving its order. If $\overline{\chi}(\mathcal{P}^\alpha) = 0$ for all $\alpha \neq 1$ in Γ, then the virtual representation of Γ on the reduced homology $\overline{H}_*(\mathcal{P}; \mathbb{C})$ is a multiple of the regular representation; hence $|\Gamma|$ divides $\overline{\chi}(\mathcal{P})$.*

PROOF. The (homology) character of α is the Lefschetz number of the map induced by α, which equals $\overline{\chi}(\mathcal{P}^\alpha)$ when computed at the level of simplicial chains. □

In all the applications of Lemma 9.2 we actually show that, for $\alpha \neq 1$, the fixed-point poset $\mathcal{P}^\alpha$ is contractible. For this and other homotopy calculations the key result is the following, which we quote without proof.

LEMMA 9.3. (QUILLEN [**19**], p. 103). *If $f, g : \mathcal{P} \to \mathcal{Q}$ are order-preserving maps of posets such that $f(x) \leq g(x)$ for all x in $\mathcal{P}$, then f is homotopic to g.*

An immediate consequence involves the notion of a conjunctive element (Definition 2.6).

COROLLARY 9.4. *A poset $\mathcal{P}$ containing a conjunctive element is contractible.*

PROOF. If a in $\mathcal{P}$ is the conjunctive element, then the identity map is homotopic to $f(x) = x \vee a$ because $x \leq x \vee a$ for all x in $\mathcal{P}$, by Lemma 9.3. Similarly, $x \vee a \geq a$ implies that f (hence the identity) is homotopic to a constant map. □

Combining Lemma 9.2 with Corollary 9.4 we get quick (and slightly different) proofs of Corollary 3.9 and Corollary 3.10. Another application of Lemma 9.3 is a topological interpretation of Rota's *Galois connection* theorem. (In Walker [**27**], a "local" formulation and a different proof is given, using Quillen's poset version of the Vietoris-Begle theorem.)

PROPOSITION 9.5. *If $\varphi : \mathcal{P} \to \mathcal{Q}$ and $\psi : \mathcal{Q} \to \mathcal{P}$ are ordering-reversing maps of posets satisfying $\psi(\varphi(x)) \geq x$ and $\varphi(\psi(y)) \geq y$ for all x in $\mathcal{P}$ and y in $\mathcal{Q}$ (such φ and ψ are said to form a Galois connection), then φ and ψ induce homotopy equivalences.*

PROOF. The identity maps $1_{\mathcal{P}}$ and $1_{\mathcal{Q}}$ are homotopic to $\psi\varphi$ and $\varphi\psi$ respectively by Lemma 9.3. □

If $\mathcal{P}$ is a finite meet-semilattice (as in Lemma 2.4) with smallest element 0, we denote by $\Delta(\mathcal{P})$ the simplicial complex whose simplices are those subsets σ of $\max\mathcal{P}$ with $\inf\sigma > 0$. Perhaps the most frequently exploited fact in the preceding sections is that $\overline{\chi}(\mathcal{P}/\{0\}) = 0$ if $\inf(\max\mathcal{P}) > 0$ (Lemma 2.4). This again follows from the contractibility of $\Delta(\mathcal{P})$ when it is the simplex with vertices $\max\mathcal{P}$, by the result below.

COROLLARY 9.6. *If $\mathcal{P}$ is a finite meet-semilattice, then $\Delta(\mathcal{P})$ is homotopic to $\mathcal{P}\backslash\{0\}$.*

PROOF. Regarding $\Delta(\mathcal{P})$ as a poset, we can define a Galois connection between $\Delta(\mathcal{P})$ and $\mathcal{P}\backslash\{0\}$ by: $\varphi(\sigma) = \inf\sigma$ and $\varphi(x) = \{y \in \max\mathcal{P} : x \leq y\}$. Now, Proposition 9.5 implies that $\mathcal{P}\backslash\{0\}$ and (the barycentric subdivision of) $\Delta(\mathcal{P})$ are homotopic. □

Corollary 9.6 is also a variant of Rota's cross-cut theorem. In [**20**] Rota, Kan, Peterson and Whitehead defined a homology theory via an arbitrary cross-cut $\mathcal{C}$ (a set of mutually incomparable elements intersecting every maximal chain) of a finite lattice, and showed that its Euler characteristic is invariant, i.e., independent of the choice of $\mathcal{C}$. Folkman's construction of the order complex in [**8**] served to prove Rota's conjecture on the invariance of the Betti numbers. A more recent homotopy treatment can be found in Björner [**1**].

To illustrate the relevance of Corollary 9.6, let $\mathcal{P}$ be the poset of proper subgroups of a finite p-group G. If G is not elementary abelian, then the maximal subgroups intersect nontrivially; hence $\Delta(\mathcal{P})$ is contractible and $\mu(G) = 0$. If G is elementary abelian of rank $r > 0$, then $\Delta(\mathcal{P})$ contains the full $(r-2)$-skeleton of the simplex on $\max\mathcal{P}$, and so it is $(r-3)$-connected. Since the order complex of $\mathcal{P}\backslash\{1\}$ is $(r-2)$-dimensional and the reduced Euler characteristic is $(-1)^r p^{\binom{r}{2}}$ by Corollary 3.5, this is a wedge of $p^{\binom{r}{2}}$ spheres of dimension $r-2$, up to homotopy. (Lusztig [**17**] has observed that this is a special case

of the Solomon-Tits theorem. Essentially the same argument works for any finite semimodular lattice, and establishes the stronger *Cohen-Macaulay* property in the sense of Quillen [**19**].) Kratzer and Thévenaz [**16**] extended this to the poset of proper nontrivial subgroups of a finite soluble group G. The rank r and the integer $p^{\binom{r}{2}}$ are replaced by the length of a chief series and the product of relative complements (as in Corollary 3.4) respectively. Moreover, the homotopy spheres can be geometrically realized so that the action of G (by conjugation) permutes them (see Thévenaz [**24**]).

For the most general divisibility results, like Theorem 5.1 or Corollary 5.2, the methods mentioned above are not directly applicable. The strategy then is to obtain the poset we want from a poset $\mathcal{P}$ we can handle, by deleting (or adding) vertices and estimating the change in the reduced Euler characteristic. Earlier, this was done via Möbius inversion. Perhaps more straightforward is the following:

LEMMA 9.7. *Let $\mathcal{P}$ be a finite poset, and let $\mathcal{C}$ be a set of mutually incomparable elements. Then*

$$\overline{\chi}(\mathcal{P}) = \overline{\chi}(\mathcal{P}\backslash\mathcal{C}) + \sum_{x\in\mathcal{C}} \overline{\chi}(\mathcal{P}_{<x})\overline{\chi}(\mathcal{P}_{>x}).$$

PROOF. To delete a singleton $\{x\}$, observe that the order complex of $\mathcal{P}$ is the union of the order complex of $\mathcal{P}\backslash\{x\}$ with the *star* of x, the union of all simplices containing x. The intersection of these (the *link* of x) is the join of the order complexes of $\mathcal{P}_{<x}$ and $\mathcal{P}_{>x}$. The star of x is contractible, so it has reduced Euler characteristic 0. The reduced Euler characteristic of a join is skew multiplicative. Therefore the Mayer-Vietoris sequence of reduced homology implies that

$$\overline{\chi}(\mathcal{P}) = \overline{\chi}(\mathcal{P}\backslash\{x\}) + \overline{\chi}(\mathcal{P}_{<x})\overline{\chi}(\mathcal{P}_{>x}).$$

The general case is obtained by repeatedly applying this equation, observing that $\mathcal{P}_{<x}$ and $\mathcal{P}_{>x}$ are not affected by deleting incomparable elements. □

This formula can also be obtained by counting all chains involving x. The homological argument, however, works even when $\mathcal{P}$ is infinite,

provided that $|\mathcal{C}|$ and the relevant reduced Euler characteristics are finite. An alternative, but essentially equivalent, approach is to consider the homology exact sequence of the pair $(\mathcal{P}, \mathcal{P}\backslash\mathcal{C})$, as in Garst [**9**;] Ch. I, or in Lusztig [**17** p. 11], where the boundary maps are also described. The set $\mathcal{C}$ is usually taken to be an orbit of a group Γ in applications; then $\sum_{x\in\mathcal{C}} \overline{\chi}(\mathcal{P}_{<x})\overline{\chi}(\mathcal{P}_{>x})$ equals $[\Gamma : \Gamma_x]\overline{\chi}(\mathcal{P}_{<x})\overline{\chi}(\mathcal{P}_{>x})$.

To conclude our topological discussion, we illustrate this method by giving a direct proof of Corollary 5.4. This, we recall, states that if n divides $|G|$, then n divides $\overline{\chi}(\mathcal{P}(n))$, where $\mathcal{P}(n)$ is the poset of nontrivial subgroups of order dividing n in a finite group G. We need to show that n_p divides $\overline{\chi}(\mathcal{P}(n))$ for all primes p. If $n_p = |G|_p$, we are done by Corollary 3.9. Otherwise, consider the poset $\mathcal{P}(m)$ corresponding to the integer $m = p^k n$, where $m_p = |G|_p$. If H is in $\mathcal{P}(m)\backslash\mathcal{P}(n)$, then $|H|_p > n_p$, and so n_p divides $\overline{\chi}(\mathcal{P}(m)_{<H}) = \mu(H)$, by Corollary 4.9. (The proof of Corollary 4.9 uses Lemma 3.1, a special case of the Crapo complementation theorem; a topological interpretation of the general case is given in Björner and Walker [**3**].) Now Lemma 9.7 comes into play. Starting with the largest orders, we can delete the elements of $\mathcal{P}(m)\backslash\mathcal{P}(n)$ one by one, preserving divisibility by n_p at each stage, until we reach the desired conclusion. In this application we had no need to consider $\overline{\chi}(\mathcal{P}_{>x})$ and the subset $\mathcal{C}$ was a singleton. In contrast, results like Theorem 5.1 and Theorem A of Thévenaz [**26**] seem to need the full force of Lemma 9.7, combined with careful inductive reasoning.

REFERENCES

1. Anders Björner, *Homotopy type of posets and lattice complementation*, J. Combin. Theory Ser. A **30** (1981), 90-100.

2. ———, *Combinatorics and topology*, Notices AMS **32** (1985), 339-345.

3. ——— and James W. Walker , *A homotopy complementation formula for posets*, European J. Combin. **4** (1983), 11-19.

4. Kenneth S. Brown, *Euler characteristics of groups: the p-fractional part*, Invent. Math. **29** (1975), 1-5.

5. ———, *Cohomology of Groups*, Graduate Texts in Mathematics **87** Springer-Verlag-Berlin-Heidelberg-New York, 1982.

6. Henry H. Crapo, *The Möbius function of a lattice*, J. Combin. Theory **1** (1966), 126-131.

7. Andreas Dress, *A characterization of solvable groups*, Math. Z. **110** (1969), 213-217.

8. Jon Folkman, *The homology groups of a lattice*, J. Math. Mech. **15** (1966), 631-636.

9. Peter F. Garst, *Cohen-Macaulay Complexes and group actions*, Ph.D. thesis, University of Wisconsin, Madison, 1979.

10. Wolfgang Gaschütz. *Die Eulersche Funktion endlicher auflösbarer Gruppen*, Illinois J. Math. **3** (1959), 469-476.

11. David Gluck, *Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex*, Illinois J. Math. **25** (1981), 63-67.

12. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) **36** (1933), 29-95.

13. ———, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134-151.

14. B. Huppert, *Endliche Gruppen* I, Springer-Verlag, -Berlin-Heidelberg-New York, 1967.

15. Charles Kratzer and Jacques Thévenaz, *Fonction de Möbius d'un groupe fini et anneau de Burnside*, Comment. Math. Helv. **59** (1984), 425-438.

16. ——— and ———, *Type d'homotopie de treillis et treillis des sous-groupes d'un groupe finit*, Comment. Math. Helv. **60** (1985), 85-106.

17. George Lusztig, *The discrete Series of GL_n over a Finite Field.* Annals of Math. Stud. 81, Princeton Univ. Press, Princeton N.J., 1974.

18. Peter M. Neumann, *A Lemma that is not Burnside's*, Math. Scientist **4** (1979), 133-141.

19. Daniel Quillen, *Homotopy properties of the poset of nontrivial p-subgroups of a group*, Adv. in Math. **28** (1978), 101-128.

20. Gian-Carlo Rota, *On the foundations of Combinatorial theory.* I. *Theory of Möbius functions*, Z. Wahrsch. Verw. Gebiete **2** (1964), 340-368.

21. Louis Solomon, *The Burnside algebra of a finite group*, J. Combin. Theory **2** (1967), 603-615.

22. Edwin H. Spanier, *Algebraic Topology*, McGraw Hill, New York, 1966.

23. Richard P. Stanley, *Some aspects of groups acting on finite posets*, J. Combin. Theory Ser. A **32** (1982), 132-161.

24. Jacques Thévenaz, *The top homology of the lattice of subgroups of a soluble group*, Discrete Math. **55** (1985), 291-303.

25. ———, *Permutation representations arising from simplicial complexes*, Preprint, École Normale Supérieure, Montrouge, 1985.

26. ———, *Generalizations of Sylow and Brown theorems*, Preprint, École Normale Supérieure, Montrouge, 1985.

27. James W. Walker, *Homotopy type and Euler characteristic of posets*, European J. Combin. **2** (1981), 373-384.

28. G.E. Wall, *Some applications of the Eulerian functions of a finite group*, J. Austral. Math. Soc. **2** (1961), 35-59.

29. Louis Weisner, *Abstract theory of inversion of finite series*, Trans. Amer. Math. Soc. **38** (1935), 474-484.

30. Tomoyuki Yoshida, *Idempotents of Burnside rings and Dress induction theorems*, J. Algebra **80** (1983), 90-105.

MATHEMATICS INSTITUTE. UNIVERSITY OF WARWICK. COVENTRY. CV4 7AL. ENGLAND

MATHEMATICS DEPARTMENT. UNIVERSITY OF WISCONSIN. MADISON. WI 53706 U.S.A.

MATHEMATICS DEPARTMENT, UNIVERSITY OF OKLAHOMA, NORMAN, OK 73019