Comment. Math. Helvetici **59** (1984) 425–438 0010–2571/84/030425–14$01.50 + 0.20/0

Fonction de Möbius d'un groupe fini et anneau de Burnside

CHARLES KRATZER et JACQUES THÉVENAZ

Soit G un groupe fini et $S(G)$ le treillis de tous les sous-groupes de G. On se propose d'étudier la fonction de Möbius $\mu(S, T)$ du treillis $S(G)$. A cette fin, on travaille avec l'anneau de Burnside $\Omega(G)$ du groupe G. En effet, une formule due à Gluck [G] exprime chaque idempotent primitif de $\mathbb{Q}\otimes\Omega(G)$ comme combinaison linéaire à coefficients rationnels de la base canonique de $\Omega(G)$ et les coefficients font précisément intervenir la fonction de Möbius de $S(G)$. La structure d'anneau de $\Omega(G)$ donne en conséquence des renseignements sur la fonction μ.

Le premier objectif de cet article est de donner des résultats sur la valeur explicite de la fonction de Möbius, pour un groupe résoluble tout au moins. Une formule due à Crapo exprime la fonction de Möbius d'un treillis quelconque en fonction de tous les compléments d'un point fixé du treillis. Dans le cas du treillis des sous-groupes de G, l'anneau de Burnside fournit une preuve d'un cas particulier de ce résultat. On en déduit des conditions suffisantes pour que $\mu(H, G)$ soit nul. De plus, la formule de Crapo permet un calcul explicite de $\mu(H, G)$ lorsque G est nilpotent, puis résoluble. Dans le cas où G est abélien, on retrouve des résultats dûs à Delsarte [De].

Dans un second volet de cet article, on démontre la propriété de divisibilité suivante: désignons par G' le sous-groupe des commutateurs de G et par $|G:G'|_0$ le produit des facteurs premiers distincts de $|G:G'|$. Alors l'entier $|G:G'|_0 \cdot \mu(S, G)$ est multiple de $|N_G(S):S|$. En particulier, $\mu(1, G)$ est un multiple de $|G|/|G:G'|_0$. Ce résultat est à rapprocher du théorème de Brown [Br] affirmant que la caractéristique d'Euler réduite du complexe simplicial associé à l'ensemble ordonné des p-sous-groupes de G est un multiple de $|G|_p$. En effet, il est bien connu (voir [R, thm 3]) que $\mu(H, G)$ n'est rien d'autre que la caractéristique d'Euler réduite du complexe simplicial associé à l'ensemble ordonné $\{S \in S(G);\ H < S < G\}$. Gluck [G] et Yoshida [Y] ont donné une preuve du théorème de Brown à l'aide des idempotents de l'anneau de Burnside. De même la propriété de divisibilité ci-dessus se démontre à l'aide d'un résultat (en fait équivalent) sur les idempotents de $\mathbb{Q}\otimes\Omega(G)$: si $e(H)$ désigne l'idempotent de $\mathbb{Q}\otimes\Omega(G)$ correspondant au sous-groupe H, alors $|N_G(H):H| \cdot |H:H'|_0$ est le plus petit entier n tel que $n \cdot e(H) \in \Omega(G)$.

Les propriétés homotopiques du complexe simplicial associé à l'ensemble ordonné $\{S \in S(G); H < S < G\}$ seront étudiées dans un prochain article [K–T].

Dans le paragraphe 1, nous rappelons les propriétés élémentaires de l'anneau de Burnside et démontrons quelques faits utiles par la suite. Le paragraphe 2 est consacré au théorème de Crapo et au calcul de la fonction de Möbius des groupes résolubles. Enfin, la propriété d'intégralité de la fonction de Möbius est démontrée au paragraphe 3.

1. Préliminaires sur l'anneau de Burnside

Soit G une groupe fini. Un *G-ensemble* est un ensemble muni d'une action de G. Le groupe de Grothendieck $\Omega(G)$ des G-ensembles finis pour l'opération "réunion disjointe" possède une structure d'anneau, la multiplication étant induite par le produit cartésien de G-ensembles. C'est *l'anneau de Burnside* $\Omega(G)$ du groupe G.

Tout G-ensemble fini est une réunion disjointe de G-ensembles transitifs et un G-ensemble transitif est isomorphe à G/H où H est le stabilisateur d'un point. Deux G-ensembles transitifs G/H et G/K sont isomorphes si et seulement si H et K sont conjugués. Il en résulte que $\Omega(G)$ est $\mathbb{Z}$-libre de base $\{G/H; [H] \in C(G)\}$ où $C(G)$ désigne l'ensemble des classes de conjugaison $[H]$ de sous-groupes H de G.

Soit S un sous-groupe de G et X un G-ensemble. On désigne par $\langle S, X\rangle$ le nombre de points fixes de X sous l'action de S. Alors $\langle S, \rangle : \Omega(G) \to \mathbb{Z}$ est une homomorphisme d'anneaux, qui ne dépend que de la classe de conjugaison [S]. Suivant Burnside [Bu, §181] et Dress [Dr], nous appelons $\langle S, X\rangle$ la *marque* de X en S. Rappelons le résultat essentiel:

PROPOSITION 1.1. *Le produit des homomorphismes marques*

$$\phi : \Omega(G) \to \prod_{[S] \in C(G)} \mathbb{Z}$$

est injectif et son conoyau est fini. En particulier,

$$1 \otimes \phi : \mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G) \to \prod_{[S] \in C(G)} \mathbb{Q}$$

est un isomorphisme. □

Tout ce qui précède est essentiellement dû à Burnside [Bu, § 181], dans des notations différentes. On trouvera dans [tD] un exposé détaillé ainsi que le calcul explicite de Coker (ϕ). On identifiera désormais $\Omega(G)$ et son image par ϕ. En d'autres termes, un G-ensemble est identifié à la collection de ses marques. De

plus, la marque $\langle S, \rangle$ s'étend bien évidemment en la projection de $\prod_{[S]\in C(G)} \mathbb{Z}$ sur le [S]-ième facteur.

Soit $\{e(H); [H]\in C(G)\}$ la base canonique de $\prod_{[H]\in C(G)} \mathbb{Z}$. Donc, $\langle S, e(H)\rangle = 1$ si $[S]=[H]$ et 0 sinon. Par définition, $e(H)$ ne dépend que de la classe de conjugaison $[H]$. Lorsque la référence au groupe G s'impose, on écrira aussi $e_G(H)$ pour $e(H)$.

Soit $S(G)$ le treillis de tous les sous-groupes de G et soit $\mu(S, T)$ la fonction de Möbius de $S(G)$. Rappelons que μ est définie par $\mu(S, S) = 1$, puis récursivement par $\sum_{S\leqq H\leqq T} \mu(S, H) = 0$. On pose aussi par convention $\mu(S, T) = 0$ si $S \not\leqq T$. Pour d'autres détails sur la fonction de Möbius, voir [A].

Le théorème suivant exprime les idempotents primitifs $e(H)$ comme combinaisons linéaires (à coefficients rationnels) de la base canonique de $\Omega(G)$.

THÉORÈME 1.2 (Gluck [G], Yoshida [Y])

$$e(H) = \sum_{1\leqq S\leqq H} \frac{|S|}{|N_G(H)|} \mu(S, H) G/S.$$

En particulier,

$$e(G) = \sum_{[S]\in C(G)} \frac{\mu(S, G)}{|N_G(S):S|} G/S. \quad \square$$

Le théorème de Gluck permet de retrouver explicitement un G-ensemble dont on connaît toutes les marques:

PROPOSITION 1.3. *Soit* $x \in \mathbb{Q}\otimes\Omega(G)$ *donné par ses marques* $\langle H, x\rangle = a_H$. *Alors,*

$$x = \sum_{[S]\in C(G)} \left(\sum_{H\geqq S} a_H \mu(S, H) |N_G(S):S|^{-1} \right) G/S.$$

Preuve.

$$\begin{aligned} x &= \sum_{[H]\in C(G)} a_H e(H) = \sum_{[H]\in C(G)} \sum_{S\leqq H} a_H \mu(S, H) |N_G(H):S|^{-1} G/S \\ &= \sum_{S,H} a_H \mu(S, H) |G:S|^{-1} G/S \\ &= \sum_{[S]\in C(G)} \left(\sum_{H\geqq S} a_H \mu(S, H) |N_G(S):S|^{-1} \right) G/S. \quad \square \end{aligned}$$

On en déduit le critère d'appartenance à $\Omega(G)$ suivant:

COROLLAIRE 1.4. *Soit* $x \in \mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$. *Alors* x *appartient à* $\Omega(G)$ *si et seulement si, pour tout sous-groupe* S *de* G, $\sum_{H \geq S} \langle H, x \rangle \mu(S, H) \in |N_G(S) : S| \mathbb{Z}$. □

Ainsi, si l'on sait que $x \in \Omega(G)$, on peut en déduire des propriétés de divisibilité de la fonction μ. Cette remarque sera exploitée au paragraphe 3. Réciproquement, ce n'est que si l'on dispose d'informations sur la fonction de Möbius qu'on peut utiliser ce corollaire comme critère d'appartenance à $\Omega(G)$. Par contraste, si l'on dispose d'informations sur les normalisateurs de sous-groupes de G, on a le critère suivant [tD, p. 6]:

PROPOSITION 1.5. *Soit* $x \in \mathbb{Q} \otimes \Omega(G)$. *Alors,* x *appartient à* $\Omega(G)$ *si et seulement si, pour tout sous-groupe* S *de* G.

$$\sum_{[H]} n(S, H)\langle H, x \rangle \equiv 0 \bmod |N_G(S) : S|$$

où $n(S, H)$ *sont certains entiers (dépendants des normalisateurs de sous-groupes de* G*) et la somme est prise sur les classes de conjugaison dans* G *de sous-groupes* H *de* $N_G(S)$ *pour lesquels* H/S *est cyclique.* □

Pour terminer ce paragraphe préliminaire, voici deux résultats qui nous seront utiles par la suite:

PROPOSITION 1.6. *Soit* S *et* T *des sous-groupes de* G *tels que* $S \cdot T = G$. *Alors* $G/S \times G/T \cong G/S \cap T$. *De plus,* $S^g \cap T^h$ *est conjugué à* $S \cap T$ *pour tous* $g, h \in G$.

Preuve. Les projections modulo S et modulo T définissent un homomorphisme de G-ensembles $\phi : G/S \cap T \to G/S \times G/T$, qui est injectif car, si $(gS, gT) = (hS, hT)$, alors $h^{-1}g \in S \cap T$, et donc $g(S \cap T) = h(S \cap T)$. De plus, sous l'hypothèse $G = S \cdot T$, ϕ est surjectif. En effet, soit $(gS, hT) \in G/S \times G/T$. On écrit $g^{-1}h = st$ avec $s \in S$ et $t \in T$. Alors, $hT = gstT = gsT$ et $gS = gsS$. Par conséquent, $(gS, hT) = \phi(gs(S \cap T))$. La dernière assertion se démontre de manière analogue. □

PROPOSITION 1.7. *Soit* N *le plus petit sous-groupe normal de* G *à quotient nilpotent et soit* S *un sous-groupe de* G *ne contenant pas* N. *Alors il existe* $a \in \Omega(G)$ *tel que* $\langle S, a \rangle = 0$ *et* $\langle G, a \rangle = 1$.

Preuve. Soit p_S le noyau de la marque $\langle S, \ \rangle : \Omega(G) \to \mathbb{Z}$. Dress [Dr] démontre

que p_S et p_T sont contenus dans un même idéal maximal de $\Omega(G)$ si et seulement s'il existe un nombre premier q pour lequel $0^q(S)$ est conjugué à $0^q(T)$ (où $0^q(S)$ désigne le plus petit sous-groupe normal de S tel que $S/0^q(S)$ soit un q-groupe). Donc, si p_S et p_G sont contenus dans un même idéal maximal, alors il existe q avec $S \geqq 0^q(S) = 0^q(G)$, et comme $0^q(G) \geqq N$ par définition de N, on en déduit $S \geqq N$ contrairement à l'hypothèse. Par conséquent, $p_S + p_G = \Omega(G)$ et il existe $a \in p_S$ et $b \in p_G$ tels que $a + b = 1$. La proposition en résulte. □

2. Calcul de la fonction de Möbius

Ce paragraphe est consacré à divers résultats sur la fonction de Möbius du treillis $S(G)$ de tous les sous-groupes d'un fini G. Il est utile de noter qu'à partir des valeurs explicites des marques de $\Omega(G)$, il est facile de calculer les idempotents $e(H)$, donc aussi la fonction de Möbius en vertu du théorème 1.2.

Soit $S(G/H)$ le treillis de tous les sous-groupes de G contenant H et soit $L \in S(G/H)$. Un *complément* de L est un sous-groupe $C \in S(G/H)$ tel que $C \cap L = H$ et $\langle C, L\rangle = G$ (où $\langle C, L\rangle$ désigne le sous-groupe engendré par C et L).

Une formule due à Crapo [A, thm 4.33] exprime la fonction de Möbius d'un treillis quelconque en fonction de tous les compléments d'un point fixé X du treillis. Dans le cas de $S(G/H)$, l'anneau de Burnside fournit une preuve de ce résultat pour un choix de X garantissant que deux compléments ne sont jamais comparables:

THÉORÈME 2.1. (Crapo). *Soit H un sous-groupe de G. Soit N un sous-groupe normal de G et $X = N \cdot H$. Soit $X^\perp$ l'ensemble de tous les compléments de X dans $S(G/H)$. Alors:*

a) *Les treillis $S(G/X)$ et $S(C/H)$ sont isomorphes pour tout $C \in X^\perp$. En particulier $\mu(H, C) = \mu(X, G)$.*

b) $\mu(H, G) = \sum_{C \in X^\perp} \mu(H, C) \cdot \mu(C, G) = \mu(X, G) \sum_{C \in X^\perp} \mu(C, G)$.

LEMME 2.2. *Soit $\rho : G \to L$ un homomorphisme de groupes et soit X un L-ensemble. On désigne par $\rho^*(X)$ l'ensemble X considéré comme G-ensemble via ρ. Alors pour tout sous-groupe S de G, on a $\langle S, \rho^*(X)\rangle_G = \langle \rho(S), X\rangle_L$.*

Preuve.

$$\langle S, \rho^*(X)\rangle_G = \text{Card}\,\{x \in X;\ sx = x \text{ pour tout } s \in S\}$$
$$= \text{Card}\,\{x \in X;\ \rho(s)x = x \text{ pour tout } s \in S\} = \langle \rho(S), X\rangle_L. \quad \square$$

Preuve du théorème. a) Soit $\phi : S(G/X) \to S(C/H)$; $U \mapsto U \cap C$ et $\psi : S(C/H) \to S(G/X)$; $V \mapsto X \cdot V$. Tout d'abord $X \cdot V$ est bien un sous-groupe car $X \cdot V = N \cdot H \cdot V = N \cdot V$. Comme $X \cdot C = G$, tout élément $u \in U$ s'écrit $u = xc$ $(x \in X, c \in C)$, mais comme $x \in U$, $c \in C \cap U$ et donc $U = X \cdot (U \cap C)$. Ainsi $\psi \circ \phi = id$. Si maintenant $c \in (X \cdot V) \cap C$, alors $c = xv$ $(x \in X, v \in V)$. Comme $v \in C$, $x \in X \cap C = H$ et donc $c \in H \cdot V = V$. Ainsi $(X \cdot V) \cap C = V$ et $\phi \circ \psi = \mathrm{id}$.

b) Soit $x = \sum_{T \cdot N = G} |G : T|^{-1} \cdot \mu(T, G) G/T$ et $z = \sum_{T \cdot N \neq G} |G : T|^{-1} \cdot \mu(T, G) G/T$. Par le théorème 1.2, $x + z = e(G)$. Soit S tel que $S \cdot N = G$ et $S \neq G$. Alors $[S] \not\leqq [T]$ pour tout T tel que $T \cdot N \neq G$, donc $\langle S, G/T \rangle = 0$ et $\langle S, z \rangle = 0$. Il en résulte que

$$\langle S, x \rangle = \langle S, e(G) \rangle = 0 \quad \text{car} \quad S \neq G. \tag{*}$$

Soit maintenant $\rho : G \to G/N$ l'homomorphisme canonique et $y = \rho^*(e_{G/N}(G/N))$. Par le théorème 1.2 appliqué à $e_{G/N}(G/N)$, on a

$$y = \sum_{N \leqq U} |G : U|^{-1} \cdot \mu(U, G) G/U.$$

De plus, par le lemme 2.2:

$$\langle S, y \rangle = \langle S \cdot N/N, e_{G/N}(G/N) \rangle = \begin{cases} 1 & \text{si} \quad S \cdot N = G \\ 0 & \text{si} \quad S \cdot N \neq G \end{cases} \tag{**}$$

Il résulte alors de (*) et (**) que si $S \neq G$, soit $\langle S, x \rangle$, soit $\langle S, y \rangle$ est nul. De plus: $\langle G, x \rangle = \langle G, G/G \rangle = 1$ et $\langle G, y \rangle = \langle G, G/G \rangle = 1$. Par conséquent $xy = e(G)$. Si $T \cdot N = G$ et $U \geqq N$, alors $T \cdot U = G$ et donc $G/T \times G/U = G/T \cap U$ par la proposition 1.6. Par conséquent:

$$e(G) = xy = \sum_{T \cdot N = G} \sum_{U \geqq N} |G : T|^{-1} \cdot |G : U|^{-1} \cdot \mu(T, G) \cdot \mu(U, G) G/T \cap U.$$

Il s'agit maintenant de calculer le coefficient de G/H dans $e(G)$. Si $H = T \cap U$, alors U est entièrement déterminé comme étant $U = N \cdot H$. En effet, tout $u \in U$ s'écrit $u = tn$ (avec $t \in T$ et $n \in N$), mais comme $n \in U$, $t \in T \cap U = H$. Par conséquent, si $H = T \cap U$ (avec $T \cdot N = G$ et $U \geqq N$) alors $U = N \cdot H$ et T est un complément de U dans $S(G/H)$. Le même raisonnement s'applique à tout $\tilde{H} \in [H]$. Notons de plus $\tilde{X} = N \cdot \tilde{H}$ et $\tilde{X}^{\perp}$ l'ensemble de tous les compléments de $\tilde{X}$ dans le treillis $S(G/\tilde{H})$. Si maintenant a_H désigne le coefficient de G/H dans

$e(G)$, on a donc

$$a_H = \sum_{\tilde{H} \in [H]} \sum_{\tilde{C} \in \tilde{X}^\perp} |G : \tilde{C}|^{-1} \cdot |G : \tilde{X}|^{-1} \cdot \mu(\tilde{C}, G) \cdot \mu(\tilde{X}, G).$$

Mais comme les treillis $S(G/H)$ et $S(G/\tilde{H})$ sont isomorphes (par conjugaison), la deuxième somme est constante pour $\tilde{H} \in [H]$, et donc:

$$a_H = |G : N_G(H)| \sum_{C \in X^\perp} |G : H|^{-1} \cdot \mu(C, G) \cdot \mu(X, G),$$

en utilisant de plus $|G : C| \cdot |G : X| = |G : C \cap X| = |G : H|$ (proposition 1.6). Par le théorème 1.2, on a aussi $a_H = |N_G(H) : H|^{-1} \cdot \mu(H, G)$ et il en résulte:

$$\mu(H, G) = \sum_{C \in X^\perp} \mu(C, G) \cdot \mu(X, G).$$

Le deuxième énoncé de b) résulte de a). □

COROLLAIRE 2.3. *Soit H un sous-groupe de G et N un sous-groupe normal de G.*

a) *Si $N \cdot H$ n'a pas de complément dans $S(G/H)$, alors $\mu(H, G) = 0$. En particulier, si N n'a pas de complément, $\mu(H, G) = 0$ pour tout sous-groupe H de N.*

b) *Si $\mu(N \cdot H, G) = 0$, alors $\mu(H, G) = 0$. En particulier si $\mu(1, G/N) = 0$, alors $\mu(H, G) = 0$ pour tout sous-groupe H de N.* □

Désignons par C_p^n le produit de n groupes cycliques d'ordre p (groupe abélien élémentaire).

PROPOSITION 2.4. *Soit G un groupe nilpotent et S un sous-groupe de G.*

a) *Si S n'est pas normal dans G, $\mu(S, G) = 0$.*

b) *Si $S \lhd G$ et G/S n'est pas un produit de groupes abéliens élémentaires, alors $\mu(S, G) = 0$.*

c) *Si $S \lhd G$ et $G/S = \prod_{i=1}^r C_{p_i}^{n_i}$ (avec p_i premier), alors $\mu(S, G) = \prod_{i=1}^r (-1)^{n_i} p_i^{\binom{n_i}{2}}$.*

Remarques. 1) Lusztig [L] démontre que le complexe simplicial associé au treillis des sous-espaces d'un $\mathbb{F}_p$-espace vectoriel de dimension n a l'homologie d'un bouquet de $p^{\binom{n}{2}}$ sphères de dimension $n-2$. Il en résulte que la caractéristique d'Euler réduite de ce complexe est $(-1)^n p^{\binom{n}{2}}$, ce qui est un cas particulier du résultat ci-dessus.

2) Cette proposition généralise le résultat de Delsarte [De] qui ne traitait que le cas abélien.

LEMME 2.5. *Soit G et F deux groupes d'ordre premier entre eux, S un sous-groupe de G et T un sous-groupe de F. Alors:* $\mu(S\times T, G\times F) = \mu(S, G)\cdot\mu(T, F)$.

Preuve. On prend $N = G$ et $H = S\times T$ dans le théorème 2.1. Alors $X = G\times T$ et $C = S\times F$ est l'unique complément de X dans $S(G/H)$. En effet, comme $(|G|, |F|) = 1$, tout sous-groupe de $G\times F$ est de la forme $U\times V$ avec $U\leqq G$ et $V\leqq F$. Ainsi $\mu(S\times T, G\times F) = \mu(S\times F, G\times F)\cdot\mu(G\times T, G\times F) = \mu(S, G)\cdot\mu(T, F)$. □

Preuve de la proposition 2.4. a) Soit $\Phi(G/S)$ l'intersection de tous les sous-groupes maximaux de G contenant S. Comme tout sous-groupe maximal est normal, $\Phi(G/S)$ est normal, donc contient S strictement. Comme tout sous-groupe est contenu dans un sous-groupe maximal, $\Phi(G/S)$ n'a pas de complément dans le treillis $S(G/S)$. On conclut à l'aide du corollaire 2.3.

b) Quitte à passer au groupe quotient G/S, on peut supposer $S = 1$. Soit $\Phi(G)$ l'intersection de tous les sous-groupes maximaux de G (sous-groupe de Frattini). Comme G est nilpotent, $G/\Phi(G)$ est un produit de groupes abéliens élémentaires. Donc, $\Phi(G) \neq 1$. On conclut alors comme dans a).

c) On peut supposer $S = 1$. Par le lemme 2.5, il suffit de montrer que si $G = C_p^n$, alors $\mu(1, G) = (-1)^n p^{\binom{n}{2}}$. On procède par récurrence sur n. Si $n = 1$, $\binom{n}{2} = 0$ et clairement $\mu(1, C_p) = -1$. Si $n > 1$, soit $N = C_p^{n-1}$ un sous-groupe d'indice p de G. Soit $N^\perp$ l'ensemble des compléments de N.

$$\begin{aligned}\text{Card}\,(N^\perp) &= \text{Card}\,\{C_p \leqq G\} - \text{Card}\,\{C_p \leqq N\}\\ &= (p^n - 1)/(p-1) - (p^{n-1} - 1)/(p-1) = p^{n-1}.\end{aligned}$$

Par le théorème 2.1: $\mu(1, G) = \mu(N, G)\sum_{C\in N^\perp}\mu(C, G)$, mais comme $G/C \cong C_p^{n-1}$ et $G/N \cong C_p$, on obtient:

$$\mu(1, G) = (-1)\cdot p^{n-1}\cdot(-1)^{n-1}\cdot p^{\binom{n-1}{2}} = (-1)^n p^{\binom{n}{2}}.$$ □

La fonction de Möbius d'un groupe nilpotent étant déterminée, la question suivante est d'étudier celle des groupes résolubles.

Rappelons qu'une suite décroissante de sous-groupes de G est dite *principale* si chaque sous-groupe de la suite est normal dans G et si la suite ne peut pas être

raffinée en une suite ayant la même propriété. Si G est résoluble, tous les quotients successifs d'une suite principale sont abéliens.

THÉORÈME 2.6. *Soit* $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ *une suite principale d'un groupe résoluble* G *et soit* H *un sous-groupe de* G. *On considère la suite* $H = G_n \cdot H \leqq G_{n-1} \cdot H \leqq \cdots \leqq G_1 \cdot H \leqq G_0 \cdot H = G$ *dont on ne conserve que les termes distincts:* $H = H_r < H_{r-1} < \cdots < H_1 < H_0 = G$. *Soit* s_i *le nombre de compléments de* H_i *dans le treillis* $S(G/H_{i+1})$. *Alors*

$$\mu(H, G) = (-1)^r s_1 \cdot \cdots \cdot s_{r-1}.$$

En particulier, $\mu(1, G) = (-1)^n m_1 \cdot \cdots \cdot m_{n-1}$ *où* m_i *est le nombre de compléments de* G_i/G_{i+1} *dans* G/G_{i+1}. *(à noter que ce théorème démontre que* $s_1 \cdot \cdots \cdot s_{r-1}$ *est indépendant du choix de la suite principle).*

Preuve. Il existe un entier a tel que $H = H_r = G_a \cdot H$ et $H < H_{r-1} = G_{a-1} \cdot H$. Montrons tout d'abord que tout complément C de H_{r-1} dans $S(G/H)$ est maximal. Comme $C \geqq H$,

$$G_{a-1} \cdot C = G_{a-1} \cdot H \cdot C = H_{r-1} \cdot C = G. \tag{*}$$

Soit maintenant D un sous-groupe tel que $C \leqq D < G$. Alors, $G_a \leqq D \cap G_{a-1} \leqq G_{a-1}$. Or, $D \cap G_{a-1}$ est normal dans D, donc normalisé par C. De plus, $D \cap G_{a-1}$ est normal dans G_{a-1} car G_{a-1}/G_a est abélien. En vertu de (*), $D \cap G_{a-1}$ est normalisé par $G = G_{a-1} \cdot C$, et comme la suite des G_i est principale, $D \cap G_{a-1}$ est égal à G_{a-1} ou G_a. Mais vu que $D < G$, le premier cas est impossible, sinon D contiendrait G_{a-1} et C, donc G en vertu de (*). Ainsi, $D \cap G_{a-1} = G_a$ ce qui implique aussi $C \cap G_{a-1} = G_a$. Ces deux égalités et la relation (*) montrent que C/G_a et D/G_a sont des compléments dans G/G_a du sous-groupe normal G_{a-1}/G_a. Par conséquent $C = D$.

On démontre maintenant le théorème par récurrence sur r. Si $r = 1$, alors $G_a \leqq H$ et $G_{a-1} \cdot H = G$. Le même argument que ci-dessus montre que H est maximal dans G. Par conséquent, $\mu(H, G) = -1$. Si $r > 1$, on a par induction:

$$\mu(H_{r-1}, G) = (-1)^{r-1} s_1 \cdot \cdots \cdot s_{r-2}.$$

Par le théorème 2.1 (avec $N = G_{a-1}$ et $X = G_{a-1} \cdot H = H_{r-1}$), on a de plus:

$$\mu(H, G) = \mu(H_{r-1}, G) \sum_{C \in H_{r-1}^{\perp}} \mu(C, G)$$

où $H_{r-1}^{\perp}$ est l'ensemble des compléments de H_{r-1} dans $S(G/H)$. Par le début de la preuve, tout $C \in H_{r-1}^{\perp}$ est maximal dans G et donc $\mu(C, G) = -1$. Par conséquent

$$\sum_{C \in H_{r-1}^{\perp}} \mu(C, G) = -s_{r-1}$$

et le résultat en découle. □

Soit $\nu(G)$ le plus petit sous-groupe normal de G tel que $G/\nu(G)$ soit nilpotent. Si $\{\gamma_i(G); i \geqq 0\}$ est la suite centrale descendante de G et si $\gamma_r(G) = \gamma_{r+1}(G)$, alors clairement $\nu(G) = \gamma_r(G)$. On définit encore $\nu_0(G) = G$ et inductivement $\nu_{i+1}(G) = \nu(\nu_i(G))$. Ainsi, G est résoluble si et seulement s'il existe un entier s tel que $\nu_s(G) = 1$.

COROLLAIRE 2.7. a) *Soit* $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ *une suite principale d'un groupe résoluble* G. *Les conditions suivantes sont équivalentes:*

(i) G_i/G_{i+1} *admet un complément dans* G/G_{i+1} *pour tout* $1 \leqq i \leqq n-1$.

(ii) $\mu(1, G) \neq 0$.

(ii) *Tout sous-groupe normal de* G *admet un complément.*

b) *Si* $\mu(1, G) \neq 0$, *alors* $\nu_i(G)/\nu_{i+1}(G)$ *est un produit de groupes abéliens élémentaires. En particulier,* $\nu_i(G)$ *est égal au* i*-ème sous-groupe dérivé de* G.

Preuve. a) (i) $\Rightarrow$ (ii) résulte du théorème 2.6.

(ii) $\Rightarrow$ (iii) résulte du corollaire 2.3.

(iii) $\Rightarrow$ (i) Si H est un complément de G_i dans G, alors $H \cdot G_{i+1}/G_{i+1}$ est un complément de G_i/G_{i+1} dans G/G_{i+1}.

b) Si $\nu_i(G)/\nu_{i+1}(G)$ n'est pas un produit de groupes abéliens élémentaires, alors le sous-groupe de Frattini $\Phi = \Phi(\nu_i(G)/\nu_{i+1}(G))$ est non trivial car $\nu_i(G)/\nu_{i+1}(G)$ est nilpotent. De plus Φ n'admet pas de complément dans $\nu_i(G)/\nu_{i+1}(G)$, donc pas non plus dans $G/\nu_{i+1}(G)$. L'image réciproque de Φ dans G est alors sans complément dans G. □

Pour terminer ce paragraphe, voici une dernière relation satisfiaite par la fonction de Möbius:

PROPOSITION 2.8. *Si* G *n'est pas cyclique,* $\sum_{S \in S(G)} |S| \cdot \mu(S, G) = 0$ *et* $\sum_{[S] \in C(G)} |N_G(S) : S|^{-1} \cdot \mu(S, G) = 0$.

Preuve. Soit $R(G)$ l'anneau des caractères de G et $r_G : \mathbb{Q}\otimes\Omega(G) \to \mathbb{Q}\otimes R(G)$ l'homomorphisme d'anneaux qui associe à G/S le caractère $\mathrm{Ind}_S^G(1)$. Maintenant, si H est un sous-groupe propre de G, il est clair que $\mathrm{Res}_H e(G) = 0$. Il en résulte que

$$\mathrm{Res}_H \circ r_G(e(G)) = r_H \circ \mathrm{Res}_H\,(e(G)) = 0$$

pour tout sous-groupe propre H. Par conséquent $r_G(e(G)) = 0$ si G n'est pas cyclique, car il est bien connu que la restriction des caractères au produit de tous les sous-groupes cycliques est injective.

Par le théorème 1.2, $e(G) = \sum_{[S]\in C(G)} |N_G(S):S|^{-1} \cdot \mu(S, G)G/S$ et on obtient donc

$$\sum_{[S]\in C(G)} |N_G(S):S|^{-1} \cdot \mu(S, G)\,\mathrm{Ind}_S^G(1) = 0.$$

Calculons maintenant le coefficient du caractère trivial de G dans cette somme. Comme $(1 \mid \mathrm{Ind}_S^G(1))_G = (1 \mid 1)_S$ par réciprocité de Frobenius, ce coefficient est

$$\sum_{[S]\in C(G)} |N_G(S):S|^{-1} \cdot \mu(S, G) = 0.$$

En sommant maintenant sur tous les sous-groupes de G, on obtient l'autre assertion de la proposition après multiplication par $|G|$. □

Remarque. Le fait que $e(H)$, pour H non cyclique, est dans le noyau de r_G apparaît déjà chez Solomon [S].

3. Propriété de divisibilité de la fonction de Möbius

Si n est un entier positif, on notera n_0 le plus grand diviseur de n sans facteur carré. Par ailleurs G' désigne le sous-groupe des commutateurs de G.

THÉORÈME 3.1. $|G:G'|_0 \cdot \mu(S, G) \in |N_G(S):S|\,\mathbb{Z}$ *pour tout sous-groupe* S *de* G. *En particulier,* $\mu(1, G)$ *est un multiple de* $|G|/|G:G'|_0$.

Ce théorème est en fait équivalent à la proposition suivante qui donne une propriété d'intégralité des idempotents de l'anneau de Burnside $\Omega(G)$.

PROPOSITION 3.2. $|G:G'|_0\, e(G) \in \Omega(G)$.

Comme $e(G) = \sum_{[S] \in C(G)} |N_G(S):S|^{-1} \cdot \mu(S, G) G/S$ en vertu du théorème 1.2, dire que $|G:G'|_0 e(G) \in \Omega(G)$ revient à dire que tous les coefficients $|G:G'|_0 \cdot |N_G(S):S|^{-1} \cdot \mu(S, G)$ sont entiers. Donc 3.2 est équivalent à 3.1.

Cette équivalence permet de démontrer le théorème 3.1 de la manière suivante:

a) On démontre 3.1 lorsque G est nilpotent.

b) On démontre 3.2 dans le cas général.

a) On suppose G nilpotent. Il n'y a rien à montrer si $\mu(S, G) = 0$ et par conséquent, par la proposition 2.4, on peut supposer S normal dans G et $G/S = \prod_{i=1}^{r} C_{p_i}^{n_i}$. Quitte à passer au groupe quotient, on peut supposer $S = 1$. A noter que cette opération remplace $|G:G'|_0$ par $|(G/S):(G/S)'|_0$ qui est un diviseur de $|G:G'|_0$. Comme alors, $G' = 1$, on obtient par la proposition 2.4:

$$|G|^{-1} \cdot |G|_0 \cdot \mu(1, G) = \prod_{i=1}^{r} p_i^{-n_i+1} \prod_{i=1}^{r} (-1)^{n_i} p_i^{\binom{n_i}{2}}$$

qui est entier car $1 + \binom{n}{2} \geqq n$ pour tout $n > 0$.

b) On utilise le cas nilpotent pour montrer 3.2 dans le cas général. Soit $N = \nu(G)$ le plus petit sous-groupe normal de G à quotient nilpotent. Par le cas a) et le fait que $G' \geqq N$, on a:

$$x = |G:G'|_0 \, e_{G/N}(G/N) \in \Omega(G/N).$$

Soit alors $y = \rho^*(x)$ où $\rho: G \to G/N$ est la projection canonique. Par le lemme 2.2, les marques de y sont faciles à calculer:

$$\langle S, y \rangle = \langle S \cdot N/N, x \rangle = \begin{cases} |G:G'|_0 & \text{si} \quad S \cdot N = G \\ 0 & \text{si} \quad S \cdot N \neq G \end{cases}$$

Si $S \cdot N = G$ et $S \neq G$, la proposition 1.7 s'applique et il existe donc $a_S \in \Omega(G)$ tel que $\langle S, a_S \rangle = 0$ et $\langle G, a_S \rangle = 1$. Soit alors $a = \prod_S a_S$, le produit étant pris sur tous les S tels que $S \cdot N = G$ et $S \neq G$, et soit $z = ya$.

Il est clair alors que $\langle S, z \rangle = 0$ si $S \neq G$ et $\langle G, z \rangle = |G:G'|_0$. Par conséquent, $|G:G'|_0 \, e(G) = z \in \Omega(G)$. □

Remarques. 1) En induisant à G l'idempotent $e_H(H)$ de $\mathbb{Q} \otimes \Omega(H)$, on voit que le théorème 3.1 est encore équivalent à:

$|N_G(H):H| \cdot |H:H'|_0 \, e(H) \in \Omega(G)$ pour tout sous-groupe H de G.

2) En guise d'alternative, on peut aussi démontrer assez facilement la proposition 3.2 (et donc le théorème 3.1) en utilisant les congruences 1.5.
Finalement, nous allons voir que les résultats 3.1 et 3.2 sont les meilleurs possibles:

PROPOSITION 3.3. $|G:G'|_0$ *est le plus petit entier positif* n *tel que tous les nombres* $n\,|N_G(S):S|^{-1}\cdot\mu(S,G)$ *soient entiers* $(S\in S(G))$.

Preuve. Il suffit en vertu de l'équivalence de 3.1 et 3.2 de montrer que $|G:G'|_0$ divise tout entier n tel que $ne(G)\in\Omega(G)$. Si S est maximal dans G, $\mu(S,G)=-1$, donc le coefficient en G/S de $e(G)$ est $-|N_G(S):S|^{-1}$. Or $|N_G(S):S|$ est soit un diviseur premier de $|G:G'|_0$, soit égal à 1 car S est maximal dans G. □

Remarque. En fait, on peut montrer aussi que $|N_G(H):H|\,|H:H'|_0$ est le plus petit entier positif n tel que $ne(H)\in\Omega(G)$, soit en adaptant la preuve de la proposition 3.3, soit à l'aide des congruences 1.5.

EXEMPLE. Il résulte du théorème 3.1 que $\mu(1,G)$ est un multiple de $|G|$ si G est parfait. Par exemple, $\mu(1,A_5)=60=|A_5|$, $\mu(1,A_6)=720=2\,|A_6|$, mais $\mu(1,PSL_2(\mathbb{F}_7))=0$. Ainsi, contrairement au cas des groupes résolubles, le comportement de la fonction de Möbius des groupes simples semble plus difficile à comprendre.

RÉFERENCES

[A] AIGNER, M. *Combinatorial Theory*. Springer Verlag, Berlin (1979).

[Br] BROWN, K. S. *Euler characteristics of groups: The p-fractional part*. Invent. Math. *29* (1975), 1–5.

[Bu] BURNSIDE, W. *Theory of Groups of Finite Order*. 2nd edition, Cambridge (1911).

[De] DELSARTE, S. *Fonctions de Möbius sur les groupes abéliens finis*. Ann. of Math. *49* (1948), 600–609.

[tD] TOM DIECK, T. *Transformation Groups and Representation Theory*. Springer Lecture Notes in Math. *766* (1979).

[Dr] DRESS, A. *A characterisation of solvable groups*. Math. Z. *110* (1969), 213–217.

[G] GLUCK, D. *Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex*. Ill. J. Math. *25* (1981), 63–67.

[K-T] KRATZER, C. et THÉVENAZ, J. *Type d'homotopie des treillis et treillis des sous-groupes d'un groupe fini*. A paraître.

[L] LUSZTIG, G. *The discrete series of* GL_n *over a finite field*. Ann. of Math. Studies *81* (1974), Princeton Univ. Press.

[R] ROTA, G.-C. *On the Foundations of Combinatorial Theory: I. Theory of Möbius Functions.* Z. für Wahrscheinlich. und Verw. Gebiete *2* (1964), 340–368.

[S] SOLOMON, L. *The Burnside algebra of a finite group.* J. Combin. Theory *2* (1967), 603–615.

[Y] YOSHIDA, T. *Idempotents of Burnside rings and Dress induction theorem.* J. Alg. *80* (1983), 90–105.

Université de Lausanne
Institut de Mathématiques
CH-1015 LAUSANNE

Reçu le 11 juillet 1983/12 janvier 1984