Şcoala Normală Superioară Bucureşti

Aplicaţii ale omologiei şi coomologiei grupurilor

Student:
Chirvăsitu Alexandru

Coordonator:
Prof. Dr. Daniel Matei

Bucureşti, 2009

Cuprins

Introducere

Omologia şi coomologia grupurilor îşi are originea în studiul unor probleme de topologie algebrică. În [Hu], Hurewicz a introdus ceea ce astăzi se numesc spaţiile $K(G, 1)$ (un tip de spaţii Eilenberg-MacLane) pentru un grup G, anume CW complexe cu grup fundamental G şi toate celelalte grupuri de omotopie triviale (tot Hurewicz a introdus grupurile de omotopie $\pi_n,\ n \geq 2$). Se pune astfel în mod natural problema studiului omologiei şi coomologiei singulare a spaţiilor $K(G, 1)$. Aceasta se poate lua ca definiţia omologiei şi coomologiei grupului G, odată rezolvate două probleme: existenţa spaţiilor $K(G, 1)$ pentru fiecare G, şi unicitatea grupurilor de (co)omologie definite astfel (cu alte cuvinte, faptul că ele nu depind de alegerea spaţiului $K(G, 1)$).

Existenţa spaţiilor $K(G, 1)$ se demonstrează simplu, pornind cu un graf şi adăugând celule în dimensiuni superioare pentru a obţine în final un CW-complex cu grup fundamental G şi grupuri de omotopie superioare nule. Cât despre problema unicităţii, ea a fost atacată chiar de Hurewicz în articolul menţionat: a demonstrat că toate spaţiile $K(G, 1)$ sunt omotop echivalente. Putem deci vorbi despre un spaţiu Eilenberg-MacLane $K(G, 1)$, acesta fiind unic până la omotopie. Avem astfel o definiţie pur topologică pentru omologia şi coomologia unui grup G, care ar putea fi folosită în locul celei algebrice date mai jos (Definiţia 1.1.1). Desigur, discuţia de până acum defineşte omologia şi coomologia cu coeficienţi în $\mathbb{Z}$, dar se poate acoperi cazul cel mai general al unui G-modul lucrând cu (co)omologie singulară în raport cu un sistem local de coeficienţi.

Următorul pas spre o definiţie algebrică a omologiei a fost făcut de Hopf, care a dat în [Ho] o definiţie pentru $H_2(G, \mathbb{Z})$ care foloseşte o prezentare prin generatori şi relaţii a lui G (în sensul că $G = F/R$, unde F este un grup liber, şi $R \trianglelefteq F$ este un grup normal care dă “relaţiile” ce definesc G). A urmat apoi dezvoltarea teoriei omologice a grupurilor, şi până la mijlocul anilor ’40 se obţinuse o definiţie pur algebrică pentru omologia şi coomologia grupurilor itnrodusă ca mai sus, în context topologic. S-a făcut legătura astfel cu subiecte studiate în algebră. Câteva exemple elocvente sunt problema extensiilor de grupuri unde grupurile de coomologie H^2 au o importanţă fundamentală, “derivările” sau morfismele încrucişate care apar în problema determinării relaţiei dintre diverse complemente ale unui subgrup normal al unui grup (aici este important H^1), şi punerea noţiunii de transfer introdusă iniţial de Schur ([Sch]) într-un cadru mai general, acela al corestricţiei în coomologie şi al restricţiei în omologie, morfisme definite în sens invers celui uzual pentru subgrupuri $H \leq G$ de indice finit ([Eck]).

De-a lungul timpului, pentru tehnicile omologice în teoria grupurilor s-au găsit multe aplicaţii, unele surprinzătoare. Menţionăm de exemplu construcţia unui corp de numere algebrice cu şir infinit de corpuri Hilbert datorată lui Golod şi Šafarevič ([GS]), care foloseşte coomologia p-grupurilor finite, şi demonstraţia faptului că p-grupurile finite care nu sunt simple au un automorfism exterior de ordin p, datorată lui Gaschütz ([Ga1, Ga2]). Coomologia grupurilor finite şi generalizarea la grupurile profinite se foloseşte astăzi din plin în multe domenii: în teoria algebrică a numerelor (în [CFr, Cap. VII] sunt enunţate rezultatele fundamentale ale teoriei corpului claselor în limbaj coomologic), în geometria algebrică, în probleme de “descent” (micşorarea corpului constantelor pentru varietăţi algebrice; se poate consulta [Se2, Cap. X] sau [Se3, Cap. III]), studiul inelului de reprezentare al unui grup finit cu ajutorul claselor caracteristice ([Th]), etc.

Această lucrare este organizată astfel:

În prima parte se face o trecere în revistă a proprietăţilor de bază ale omologiei şi coomologiei grupurilor. Urmează apoi în partea a doua câteva aplicaţii: rolul grupurilor de coomologie în dimensiuni mici în studiul extensiilor de grupuri, calcule de (co)omologie singulară pentru un spaţiu cu ajutorul coomologiei grupului fundamental al spaţiului, diverse rezultate de teoria grupurilor care folosesc în demonstraţie noţiunea de transfer, o demonstraţie pentru teorema Artin-Schreier asupra corpurilor real închise ce foloseşte coomologia grupului Galois absolut al corpului studiat, şi în sfârşit, studiul câtorva situaţii în care devine importantă noţiunea de multiplicator Schur: extensii centrale, reprezentări proiective, problema reprezentabilităţii functorilor $H^*(G,-)$, etc. În această ultimă secţiune apare şi o aplicaţie (sub forma unui rezultat negativ) la problema determinării grupurilor de ordin n^2 pentru care $A \otimes M_n(\mathbb{C})$ este produs crossed al lui A prin G, unde A este o algebră C^*.

Aplicaţiile prezentate nu sunt poate cele mai interesante, dar scopul a fost numai de a da câteva exemple, unele poate mai rar întâlnite în lucrările în domeniu.

1. Definiţii şi construcţii de bază

1.1. **Omologie şi coomologie ca functori derivaţi.** Vom da aici definiţia omologiei şi coomologiei de grupuri folosind noţiuni de algebră omologică: δ-functori, functori derivaţi ai unui functor exact la stânga/dreapta între categorii abeliene, în particular functorii Tor_i şi Ext^i, etc. Pentru aceste noţiuni facem referire la texte ca [Ro1, We, CE].

Fie G un grup. În general, cu Λ vom nota inelul grupal $\mathbb{Z}[G]$; atunci când va trebui să specificăm şi grupul G, folosim notaţia Λ_G. Foarte importantă pentru noi va fi categoria grupurilor abeliene înzestrate cu o acţiune a lui G prin automorfisme; un asemenea grup îl vom numi şi *G-modul*. Morfismele în această categorie sunt morfismele de grupuri abeliene care comută cu acţiunile lui G pe cele două grupuri. E uşor de văzut că această categorie este echivalentă cu ${}_\Lambda\mathcal{M}$, categoria modulelor stângi peste Λ. Vom mai nota această categorie cu $\mathcal{A}b^G$, pentru că ea este chiar categoria de functori de la G, privit ca şi categorie cu un obiect, la $\mathcal{A}b$, categoria grupurilor abeliene. Analog, notăm cu $\mathcal{A}b_G$ categoria grupurilor abeliene înzestrate cu o G-acţiune la dreapta, care poate fi privită ca fiind categoria Λ-modulelor drepte. Le vom numi pe acestea şi *G-module drepte*.

Avem o scufundare (functor deplin fidel) $\mathcal{A}b \to \mathcal{A}b^G$ (resp. $\mathcal{A}b_G$), care trimite fiecare grup abelian în acel grup abelian înzestrat cu acţiunea trivială a lui G. În acest context, dacă A este grup abelian pe care nu am dat apriori o acţiune a lui G, el va fi privit şi ca Λ-bimodul, fără a mai menţiona în mod explicit acest lucru. De exemplu, în definiţia de mai jos, prin $\mathbb{Z}$ înţelegem grupul aditiv $\mathbb{Z}$ pe care G acţionează trivial la stânga în prima parte, şi la dreapta în partea a doua.

Definiţia 1.1.1. Fie $A \in \mathcal{A}b^G$ un grup cu o acţiune a lui G. Numim *grupul de coomologie* de rang i al lui G în raport cu A (sau cu valori în A) şi notăm cu $H^i(G, A)$ grupul $\mathrm{Ext}^i_\Lambda(\mathbb{Z}, A)$.

În mod analog, numim *grupul de omologie* de rang i al lui G în raport cu A şi notăm cu $H_i(G, A)$ grupul $\mathrm{Tor}^\Lambda_i(\mathbb{Z}, A)$.

Când vrem să ne referim colectiv la grupurile de coomologie (omologie) vom folosi notaţia $H^*(G, A)$ (respectiv $H_*(G, A)$). Pentru $A = \mathbb{Z}$ (pe care G acţionează trivial) scriem simplu $H^*(G)$ şi respectiv $H_*(G)$.

Observaţia 1.1.2. A da un morfism de G-module de la $\mathbb{Z}$ la A este acelaşi lucru cu a da un element din A fixat de acţiunea lui G. Dacă notăm cu A^G subgrupul lui A format de elementele fixate de G, atunci $A \mapsto A^G$ este în mod evident un functor de la $\mathcal{A}b^G$ la $\mathcal{A}b$ izomorf natural cu ${}_\Lambda\mathrm{Hom}(\mathbb{Z}, -)$. Rezultă deci că H^i pot fi priviţi ca functorii derivaţi la dreapta ai acestui functor $A \mapsto A^G$.

În mod analog, functorul $Z \otimes_\Lambda -$ este izomorf natural cu $A \mapsto A_G = A/I_G A$, unde $I_G \leq \Lambda$ este idealul "de augmentare", generat de $s - 1,\ s \in G$, şi deci $I_G A \leq A$ este subgrupul generat de $sa - a,\ s \in G,\ a \in A$. A_G este cel mai mare cât al lui A pe care G acţionează trivial, şi H_i pot fi priviţi ca functorii derivaţi la stânga ai lui $A \mapsto A_G$.

Observaţia 1.1.3. Putem da definiţii analoage lucrând nu peste inelul $\mathbb{Z}$, ci peste un inel arbitrar R. Vom considera atunci cateogria ${}_R\mathcal{M}$ a R-modulelor stângi, categoria ${}_R\mathcal{M}^G$ a R modulelor stângi pe care G acţionează prin izomorfisme de module, ce poate fi identificată cu categoria modulelor stângi peste inelul grupal $R[G]$, etc.

Din Definiţia 1.1.1 şi din proprietăţile binecunoscute ale functorilor derivaţi se pot deduce proprietăţi ale omologiei şi coomologiei de grupuri. Doar vom enunţa rezultatele; pentru demonstraţii se pot consulta de exemplu [We, Cap. 2], [CE, Cap. V], şi de asemenea [Ha, Cap. III, §1] pentru o foarte rapidă trecere în revistă a proprietăţilor de bază ale functorilor derivaţi (inclusiv terminologia legată de δ-functori, ce se poate găsi şi în [We, §2.1]).

Teorema 1.1.4. *În ipotezele din Definiţia 1.1.1 au loc următoarele:*

(a) *$H^*(G,-)$ este un δ-functor coomologic universal definit pe categoria $\mathcal{A}b^G$.*

(a′) *$H_*(G,-)$ este un δ-functor omologic universal definit pe categoria $\mathcal{A}b^G$.*

(b) *$H^i(G,I)=0,\ \forall i\geq 1$ pentru orice obiect injectiv $I\in\mathcal{A}b^G$.*

(b′) *$H_i(G,P)=0,\ \forall i\geq 1$ pentru orice obiect proiectiv $P\in\mathcal{A}b^G$.*

(c) *Pentru orice rezoluţie*

$$0\longrightarrow A\longrightarrow I_0\longrightarrow I_1\longrightarrow\dots$$

în $\mathcal{A}b^G$ în care I_j sunt obiecte coomologic aciclice (adică $H^i(G,I_j)=0$ pentru toţi j şi toţi $i\geq 1$), $H^i(G,A)$ se poate calcula ca fiind coomologia complexului

$$0\longrightarrow I_0^G\longrightarrow I_1^G\longrightarrow\dots.$$

(c′) *Pentru orice rezoluţie*

$$\dots\longrightarrow P^1\longrightarrow P^0\longrightarrow A\longrightarrow 0$$

în $\mathcal{A}b^G$ în care P^j sunt obiecte omologic aciclice ($H_i(G,P^j)=0$ pentru $i\geq 1$), $H_i(G,A)$ se calculează ca omologia complexului

$$\dots\longrightarrow P^1_G\longrightarrow P^0_G\longrightarrow 0.$$

Fiind functori derivaţi, coomologia (omologia) se anulează pe obiecte injective (respectiv proiective) din categoria abeliană $\mathcal{A}b^G$. O observaţie utilă este aceea că functorii se anulează pe obiecte cu care este în general mai uşor de lucrat: cele coinduse (respectiv induse). Definim aici clasele respective de obiecte şi demonstrăm afirmaţia făcută.

Fie X un grup abelian, şi considerăm grupul abelian $\mathrm{Hom}(\Lambda,X)$ (Hom peste $\mathbb{Z}$). G are o acţiune naturală pe $\bar{X}=\mathrm{Hom}(\Lambda X)$, anume cea definită prin

$$(sf)(g)=f(gs),\ \forall f\in\bar{X},\ \forall s,g\in G.$$

"Dual", putem considera G-modulul $\tilde{X}=\Lambda\otimes X$ (tensor peste $\mathbb{Z}$), unde acţiunea lui G este dată de înmulţirea la stânga pe Λ.

Definiţia 1.1.5. Un G-modul se numeşte *coindus* dacă este izomorf cu unul de forma $\bar{X}=\mathrm{Hom}(\Lambda,X)$, cu acţiunea lui G descrisă mai sus.

Un G-modul se numeşte *indus* dacă este izomorf cu unul de forma $\tilde{X}=\Lambda\otimes X$, cu acţiunea naturală a lui G.

Fie acum X un grup abelian, şi

$$0\longrightarrow X\longrightarrow I_0\longrightarrow I_1\longrightarrow\dots \tag{1.1.1}$$

o rezoluţie injectivă a lui X în $\mathcal{A}b$. Pentru că Λ este un grup abelian liber, după ce aplicăm functorul $\mathrm{Hom}(\Lambda, -)$ şirului (1.1.1) obţinem tot un şir exact:

$$0 \longrightarrow \bar{X} \longrightarrow \bar{I_0} \longrightarrow \bar{I_1} \longrightarrow \dots . \tag{1.1.2}$$

Cum I_j sunt grupuri abeliene injective şi deci divizibile, obiectele $\bar{I_j}$ sunt toate injective în $\mathcal{A}b^G$ ([Ro1, Teorema 3.26]). (1.1.2) este aşadar o rezoluţie injectivă a lui $\bar{X}$, şi coomologia $H^*(G, \bar{X})$ este chiar coomologia complexului

$$0 \longrightarrow \bar{I_0}^G \longrightarrow \bar{I_1}^G \longrightarrow \dots . \tag{1.1.3}$$

Se vede însă imediat din definiţii că în general, pentru un grup abelian Y, avem un izomorfism natural $\bar{Y}^G \cong Y$. Şirul (1.1.3) se reduce deci la şirul (1.1.1), din care s-a omis primul termen X. Cum (1.1.1) este rezoluţie, coomologia H^i calculată astfel va fi nulă pentru $i \geq 1$. Am demonstrat astfel prima parte a rezultatului următor (a doua parte demonstrându-se analog):

Propoziţia 1.1.6. *Orice obiect coindus din $\mathcal{A}b^G$ este coomologic aciclic; orice obiect indus este omologic aciclic.*

Încheiem cu observaţia că orice G-modul se poate scufunda într-unul coindus: avem un morfism canonic injectiv de G-module de la A la $\bar{A}$ care trimite $a \in A$ în morfismul de grupuri $\Lambda \to A$ definit prin $s \mapsto sa,\ \forall s \in G$. În mod analog, avem un morfism canonic surjectiv de G-module $\tilde{A} \to A$, care trimite $s \otimes a \in \Lambda \in A,\ s \in G$ în sa.

1.2. **(Co)cicli standard.** Din Definiţia 1.1.1 se vede că omologia şi coomologia unui grup G în raport cu un G-modul A se pot calcula astfel: se consideră o rezoluţie proiectivă

$$P_\bullet = \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

a lui $\mathbb{Z}$ în $\mathcal{A}b^G$ ($\mathcal{A}b_G$), şi $H^*(G, A)$ (resp. $H_*(G, A)$) este coomologia (resp. omologia) complexului ${}_\Lambda\mathrm{Hom}(P_\bullet, A)$ (resp. $P_\bullet \otimes_\Lambda A$).

Pentru a putea face calcule concrete, se alege o anume rezoluţie $P_\bullet$ (de Λ-bimodule, deci funcţionează atât pentru coomologie, cât şi pentru omologie) după cum urmează:

Pentru orice număr natural n, P_n este inelul grupal $\mathbb{Z}[G^{n+1}]$ (produsul a $n+1$ copii ale grupului G), pe care G acţionează la stânga şi la dreapta prin înmulţire la stânga şi respectiv dreapta, G fiind privit ca subgrup în G^{n+1} prin scufundarea diagonală

$$s \mapsto (s, s, \dots, s).$$

P_n este aşadar un $\mathbb{Z}$-modul liber cu baza $(s_0, s_1, \dots, s_n) \in G^{n+1}$. Pentru a putea trata simultan şi termenul $\mathbb{Z}$ din rezoluţia căutată $P_\bullet$, vom conveni ca G^0 să desemneze grupul trivial, şi deci vom pune $P_{-1} = \mathbb{Z}[G^0] = \mathbb{Z}$. Pentru $n \geq 0$, P_n este liber atât la stânga cât şi la dreapta ca Λ-modul.

Pentru orice $n \in \mathbb{N}$ şi orice $i \in \overline{0, n}$, fie $\pi_i : G^{n+1} \to G^n$ proiecţia pe componentele diferite de i. Cu alte cuvinte,

$$\pi_i(s_0, s_1, \dots, s_n) = (s_0, s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n).$$

Când $n = 0$ apare un mic abuz de notaţie: morfismul π_0 va fi atunci pur şi simplu unicul morfism de la G la grupul trivial. Aceste morfisme induc aplicaţii de G-bimodule (tot

π_i) d la P_n la P_{n-1}. Diferenţiala $d_n : P_n \to P_{n-1}$ a complexului $P_\bullet$ pe care vrem să-l construim se defineşte acum ca

$$d_n = \sum_{i=0}^{n} (-1)^i \pi_i.$$

Nu e greu de văzut că acesta este un complex ($d^2 = 0$), şi că el este aciclic, deci obţinem într-adevăr o rezoluţie proiectivă (liberă chiar) a lui $\mathbb{Z}$ atât în $\mathcal{A}b^G$ cât şi în $\mathcal{A}b_G$. O vom numi *rezoluţia standard* a lui $\mathbb{Z}$, dar cociclii cu care vom lucra vor fi uşor modificaţi, după cum explicăm în cele ce urmează.

Cum orice element din ${}_\Lambda\mathrm{Hom}(P_n, A)$ este morfism de G-module, el este unic determinat de valorile sale pe elemente de forma $(1, s_1, \ldots, s_n) \in G^{n+1}$. Reciproc, orice funcţie g de la G^n la A am alege, există un element f din ${}_\Lambda\mathrm{Hom}(P_n, A)$ care evaluat în $(1, s_1, \ldots, s_n)$ dă $g(s_1, \ldots, s_n)$. Funcţia $g : G^n \to A$ corespunzătoare unui n-colanţ f o vom numi *n-colanţ neomogen*, sau *standard*. Lucrând cu colanţuri neomogene, vedem acum că putem calcula coomologia $H^*(G, A)$ şi astfel (nu demonstrez; sunt simple verificări, făcând trecerea de la colanţuri obişnuite la cele neomogene, după cum am descris):

Fie $C^n(G, A)$ (sau $C^n(A)$, sau C^n când nu este pericol de confuzie) grupul abelian al funcţiilor $G^n \to A$ pentru $n \geq 0$ (din nou, G^0 este grupul trivial). Pentru $f \in C^n(A)$ definim $df \in C^{n+1}(A)$ prin

$$df(s_1, \ldots, s_{n+1}) = s_1 f(s_2, \ldots, s_{n+1}) + \sum_{j=1}^{n} (-1)^j f(s_1, \ldots, s_j s_{j+1}, s_{n+1}) + (-1)^{n+1} f(s_1, \ldots, s_n).$$

Atunci $d^2 = 0$, şi $H^*(G, A)$ este coomologia complexului $C^*(G, A)$.

O construcţie analoagă de "deomogenizare" se poate face şi pentru omologie, dar nu vom avea ocazia să o folosim. Se poate consulta de exemplu [Se2, Secţiunea VII §4]. Elementele din $C^n(G, A)$ anulate de d se numesc *n-cocicli neomogeni* sau *standard*, şi analog, elementele din $d(C^{n-1})$ se vor numi *n-coborduri neomogene*, sau *standard*. Cum numai acestea vor fi obiectele folosite pentru calculul coomologiei, noi le vom numi pur şi simplu colanţuri, cocicli, coborduri. Grupul n-cociclilor neomogeni îl notăm cu $Z^n(G, A)$ (sau $Z^n(A)$, sau Z^n), iar pe cel al n-cobordurilor cu $B^n(G, A)$ (sau $B^n(A)$, sau B^n).

1.3. **Functorialitate.** Este clar din definiţia (co)omologiei că $H^*(G, -)$ şi $H_*(G, -)$ sunt functori aditivi covarianţi de la $\mathcal{A}b^G$ la $\mathcal{A}b$. Vom vedea acum ce se întâmplă când schimbăm şi grupul G printr-un morfism de grupuri $H \to G$. În acest scop, introducem noţiunea următoare:

Definiţia 1.3.1. Fie $\varphi : H \to G$ un morfism de grupuri, şi fie $f : A \to B$ un morfism de grupuri abeliene, unde B şi A sunt un H- şi respectiv un G-modul. Vom spune că φ şi f sunt *cocompatibile* (sau că perechea (f, φ) este cocompatibilă) dacă are loc relaţia

$$f(\varphi(t)a) = tf(a), \ \forall a \in A, \ t \in H.$$

Dacă $f : B \to A$ este un morfism de grupuri abeliene, spunem că φ şi f sunt *compatibile* (sau că perechea este compatibilă) dacă are loc

$$f(tb) = \varphi(t)b, \ \forall b \in B, \ t \in H.$$

Observaţia 1.3.2. Definiţia se interpretează simplu astfel: φ, f sunt cocompatibile dacă şi numai dacă f este morfism de H-module, structura de H-modul pe A fiind cea indusă de structura sa de G-modul prin restricţia scalarilor de la Λ_H la Λ_G dată de φ. Analog, compatibilitatea este echivalentă cu faptul că f este morfism de H-module.

Fie acum (f, φ) o pereche cocompatibilă pentru H-modulul B şi G-modulul A (ca în definiţie). Ea va induce atunci un morfism Φ_f^φ de la $H^*(G, A)$ la $H^*(H, B)$ după cum urmează:

Fiind dat un morfism de inele $R \to S$ şi S-module stângi M, N, avem un morfism canonic $\mathrm{Ext}_S^*(M, N) \to \mathrm{Ext}_R^*(M, N)$, structura de R-module pe M, N fiind cea obţinută prin restricţia scalarilor. Aplicând asta pentru morfismul $\Lambda_H \to \Lambda_G$ indus de φ şi $M = \mathbb{Z},\ N = A$, obţinem un morfism de la $H^*(G, A)$ la $H^*(H, A)$. Compunând apoi cu morfismul $H^*(H, A) \to H^*(H, B)$ indus de morfismul de H-module $f : A \to B$, obţinem aplicaţia căutată.

Analog, dacă (f, φ) este pereche compatibilă, avem un morfism indus $H_*(H, B) \to H_*(G, A)$, notat cu Φ_φ^f.

Să observăm că dacă reprezentăm clasele de coomologie prin cocicli neomogeni ca în secţiunea precedentă, atunci morfismul în coomologie indus de o pereche cocompatibilă (f, φ) este cel obţinut după factorizarea prin coborduri din morfismul de la $Z^n(G, A)$ la $Z^n(H, B)$ definit prin

$$\alpha \mapsto f \circ \alpha \circ \varphi^n,\ \forall \alpha \in Z^n(G, A),$$

unde $\varphi^n : H^n \to G^n$ este produsul a n copii ale lui φ.

Câteva exemple importante de morfisme induse de perechi (co)compatibile:

Orice morfism de grupuri $\varphi : H \to G$ este atât cocompatibil cât şi compatibil cu identitatea pe G-modulul A, unde ca până acum, structura de H-modul va fi cea dată de restricţia scalarilor prin morfismul $\Lambda_H \to \Lambda_G$ indus de φ. Morfismul $H^*(G, A) \to H^*(H, A)$ în coomologie ce se obţine astfel se numeşte *restricţie* (în coomologie), iar cel în omologie, care merge de la $H_*(H, A)$ la $H_*(G, A)$, se numeşte *corestricţie* (în omologie). În particular, aceste exemple funcţionează dacă $H \leq G$ şi φ este incluziunea. Pentru restricţie folosim notaţia Res_H^G, sau $\mathrm{Res}_{G/H}$, sau numai Res când este clar la ce morfism de grupuri ne referim, iar pentru corestricţie folosim notaţia Cor_H^G, sau $\mathrm{Cor}_{G/H}$, sau Cor.

Pe de altă parte, fie $H \trianglelefteq G$ un subgrup normal, şi $\varphi : G \to G/H$ proiecţia. Dacă A este un G-modul, G/H acţionează pe A^H. Dacă $f : A^H \to A$ este incluziunea, se vede imediat că (f, φ) este pereche cocompatibilă. Vom avea deci un morfism $H^*(G/H, A^H)$ la $H^*(G, A)$, numit *inflaţie*. Vom nota acest morfism cu Inf_H^G, sau $\mathrm{Inf}_{G/H}$, sau pur şi simplu Inf.

Un alt exemplu interesant ni-l oferă cazul când morfismul φ este un automorfism interior al lui G. Fie $s \in G$ un element, şi $\varphi : G \to G$ conjugarea cu s: $t \mapsto sts^{-1}$. Dacă A este un G-modul, fie $f : A \to A$ automorfismul grupului abelian A definit prin $f(a) = s^{-1}a$ (acţiunea elementului s^{-1} pe A). Că (f, φ) este o pereche cocompatibilă se verifică imediat, deci ea induce un endomorfism Φ_f^φ al lui $H^*(G, A)$. Afirm că acesta e de fapt identitatea. Asta rezultă din faptul că endomorfismele Φ_f^φ constituie de fapt o transformare naturală de δ-functori (comută cu diferenţiala din şirul exact lung de coomologie pentru şiruri exacte scurte de G-module), şi cum pe H^0 este uşor de verificat că Φ este identitatea şi $H^*(G,-)$ este un δ-functor universal (Teorema 1.1.4, (a)), Φ trebuie să fie identic peste tot.

Afirmaţiei de mai sus că Φ este identic i se poate da şi o demonstraţie directă (apare una de exemplu în [Se2, Secţiunea VII §5]), dar tipul de argument de mai sus, ce foloseşte universalitatea δ-functorului, va fi foarte util în cele ce urmează.

Exemplul precedent se poate generaliza. Fie $H \trianglelefteq G$ un subgrup normal, şi $s \in G$ un element. Atunci s acţionează prin conjugare pe H. Această acţiune va fi $\varphi : H \to H$. Pentru un G-modul A avem, ca şi mai sus, $f : A \to A$ definit prin $f(a) = s^{-1}a$. Din nou (f, φ) formează o pereche cocompatibilă, şi obţinem un automorfism al lui $H^*(H, A)$. Variind $s \in G$ se vede că de fapt obţinem o acţiune a lui G pe $H^*(H, A)$. În sfârşit, din exemplul precedent se vede că H acţionează trivial pe $H^*(H, A)$. De aici rezultă că de fapt avem o acţiune a lui G/H pe $H^*(H, A)$. Aceasta este importantă de exemplu în formarea aşa-numitului şir spectral al extensiei de grupuri (sau Hochschild-Serre), după cum vom vedea mai târziu, în Teorema 1.7.4.

Enunţăm acum fără demonstraţie un rezultat ce leagă morfismele de inflaţie şi de restricţie în coomologie pe care le-am introdus mai sus. Este Propoziţia 5 din [Se2, Secţiunea VII §6].

Propoziţia 1.3.3 (Şirul inflaţie-restricţie)**.** *Fie G un grup, $H \triangleleft G$ un subgrup normal, şi A un G-modul. Fie de asemenea $q \geq 1$ un număr natural. Dacă $H^i(H, A) = 0$ pentru $i = \overline{1, q-1}$ (în particular, condiţia este vidă dacă $q = 1$), atunci următorul şir este exact:*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A) \tag{1.3.1}$$

Acum vom schimba uşor contextul. Am introdus mai sus restricţia $H^*(G, A) \to H^*(H, A)$ în coomologie, şi corestricţia $H_*(H, A) \to H_*(G, A)$ în omologie. Când $H \leq G$ este subgrup *de indice finit*, săgeţile pot fi inversate: vom descrie mai jos un morfism de corestricţie $H^*(H, A) \to H^*(G, A)$ în coomologie pentru un G-modul A, şi un morfism de corestricţie $H_*(G, A) \to H_*(H, A)$ în omologie.

Fie deci G un grup şi $H \leq G$ un subgrup de indice finit n. Alegem în G un sistem s_i, $i = \overline{1, n}$ de reprezentanţi la stânga modulo H. Pentru orice G-modul A, vom considera următorul endomorfism de grupuri abeliene:

$$N_{G/H}(a) = \sum_{i=1}^{n} s_i a, \ \forall a \in A. \tag{1.3.2}$$

Ca de obicei, dacă este clar la ce grupuri ne referim, notăm pur şi simplu N. Dacă $a \in A^H$ (cu alte cuvinte a este element fixat de H), atunci se vede imediat că $N(a) \in A^G$. Avem astfel o transformare naturală de la functorul $H^0(H, -)$ (pe $\mathcal{A}b^G$) la $H^0(G, -)$. Am vrea să extindem această transformare la întreg δ-functorul $H^*(H, -)$ (din nou, acesta e considerat aici un δ-functor pe $\mathcal{A}b^G$, bu pe $\mathcal{A}b^H$). Că putem face asta va rezulta din lucruri generale asupra δ-functorilor pe care le reamintim mai jos.

Vom spune că un functor aditiv $F : \mathcal{A} \to \mathcal{B}$ între categorii abeliene este *efasabil* (din fr. effaçable) dacă orice obiect a din $\mathcal{A}$ admite un monomorfism $u : a \mapsto a'$ cu $T(u) = 0$. Analog, spunem că este *coefasabil* (coeffaçable) dacă orice obiect $a \in \mathcal{A}$ admite un epimorfism $u : a' \to a$ cu $T(u) = 0$. Rezultatul care ne interesează este următorul ([Gr, II, 2.2.1]):

Teorema 1.3.4. *Dacă $T = (T^i)_{i\geq 0}$ este un δ-functor cu proprietatea că toţi T^i, $i \geq 1$ sunt efasabili, atunci T este un δ-functor universal.*

Folosind teorema de mai sus, pentru a extinde transformarea $H^0(H, -) \to H^0(G, -)$ dată de "norma" N la o tramsformare de δ-functori de la $H^*(H, -)$ la $H^*(G, -)$ va fi suficient să arătăm că toţi $H^i(H, -)$, $i \geq 1$ sunt efasabili pe $\mathcal{A}b^G$. Asta deoarece atunci teorema spune că $H^*(H, -)$ este universal, şi extinderea se poate face (unic). Că $H^i(H, -)$, $i \geq 1$ sunt efasabili pe $\mathcal{A}b^G$ este însă uşor de arătat: pentru că Λ_G este plat (liber chiar) la dreapta peste Λ_H, modulele injective peste Λ_G sunt injective şi peste Λ_H (structura lor de H-module fiind cea dată de restricţia scalarilor). Cum orice G-modul se poate scufunda într-unul injectiv (rezultat binecunoscut, valabil pentru module peste orice inel; [Ro1, Teorema 3.27], de exemplu), asta ne va da concluzia dorită.

Avem deci o transformare de δ-functori pe $\mathcal{A}b^G$ de la $H^*(H, -)$ la $H^*(G, -)$. Cum spuneam la început, vom numi această transformare corestricţie, şi o vom nota cu Cor_H^G, sau $\mathrm{Cor}_{G/H}$, sau Cor, dacă nu există pericol de confuzie. Un rezultat interesant şi util în aplicaţii este următorul:

Propoziţia 1.3.5. *Fie G un grup şi $H \leq G$ un subgrup de indice n. Atunci* $\mathrm{Cor} \circ \mathrm{Res}$ *pe $H^*(G, -)$ este înmulţirea cu n.*

Demonstraţie. $\mathrm{Cor} \circ \mathrm{Res}$ este prin construcţie o transformare naturală de δ-functori. La fel, înmulţirea cu n este o transformare de δ-functori. Cum $H^*(G, -)$ este universal pe $\mathcal{A}b^G$ (Teorema 1.1.4, (a)), cele două transformări coincid dacă ele coincid pe H^0. Dar asta se constată imediat din definiţiile restricţiei şi corestricţiei. ∎

În mod analog se poate trata şi omologia. Cu aceleaşi notaţii introduse înaintea definiţiei normei (1.3.2), definim aplicaţia

$$N'(a) = \sum_{i=1}^{n} s_i^{-1} a, \ \forall a \in A. \tag{1.3.3}$$

E uşor de văzut că acest endomorfism induce unul de la A_G la A_H, şi un argument analog celui folosit pentru definiţia corestricţiei arată că putem extinde aceasta transformare $H_0(G, -) \to H_0(H, -)$ în mod unic la o transformare de δ-functori pe $\mathcal{A}b^G$ de la $H_*(G, -)$ la $H_*(H, -)$. Vom numi această transformare restricţia în omologie, şi o notăm ca şi până acum cu Res_H^G, sau $\mathrm{Res}_{G/H}$, sau Res. Propoziţia 1.3.5 are de asemenea un analog în omologie.

Aceste construcţii făcute în cazul când indicele lui $H \leq G$ este finit pot fi obţinute după o reformulare şi ca fiind induse de o pereche cocompatibilă (sau compatibilă în cazul omologiei). Dăm mai jos detalii.

Fie $R \to S$ un morfism de inele. Pentru orice S-modul stâng N, ${}_R\mathrm{Hom}(S, N)$ are o structură de S-modul stâng dată de $(sf)(t) = f(ts)$ pentru $s, t \in S$. Are loc următorul rezultat simplu (a cărui demonstraţie o includem, fiind foarte scurtă):

Propoziţia 1.3.6 (Lema lui Shapiro)**.** *Fie M un S-modul stâng. Dacă S este proiectiv ca R-modul stâng, atunci avem un izomorfism canonic de δ-functori pe categoria ${}_R\mathcal{M}$ a R-modulelor stângi*

$$\mathrm{Ext}^*_R(M,-) \cong \mathrm{Ext}^*_S(M,\ {}_R\mathrm{Hom}(S,-)), \tag{1.3.4}$$

unde pentru un S-modul stâng N, ${}_R\mathrm{Hom}(S,N)$ are structura de S-modul stâng dată de $(sf)(t) = f(ts),\ \forall s,t \in S$.

Demonstraţie. Pentru $* = 0$ izomorfismul este binecunoscut, fiind pur şi simplu adjuncţia dintre restricţia scalarilor de la S la R (adjunctul stâng) şi ${}_R\mathrm{Hom}(S,-)$ (adjunctul drept). Pentru că S este proiectiv la stânga peste R, S-modulele stângi proiective sunt proiective şi peste R. Asta înseamnă că cei doi functori pot fi calculaţi dintr-o rezoluţie proiectivă a lui M peste S aplicând termenilor rezoluţiei functorii în prima variabilă ${}_R\mathrm{Hom}(-,-)$ şi ${}_S\mathrm{Hom}(-,\ {}_R\mathrm{Hom}(S,-))$, care am observat deja că sunt izomorfi natural. ■

Aplicând propoziţia în cazul când $R \to S$ este incluziunea $\Lambda_H \to \Lambda_G$ indusă de incluziunea $H \leq G$, obţinem Lema lui Shapiro pentru coomologia grupurilor:

$$H^*(H,A) \cong H^*(G, M_H^G(A)),\ \forall A \in \mathcal{A}b^H, \tag{1.3.5}$$

unde pentru un H-modul A prin $M_H^G(A)$ desemnăm G-modulul ${}_{\Lambda_H}\mathrm{Hom}(\Lambda_G, A)$.

În cazul când $H \leq G$ are indice finit şi A este G-modul, avem o aplicaţie α de la $M_H^G(A)$ la A definită prin

$$f \mapsto \sum_{i=1}^{n} s_i f(s_i^{-1}),$$

unde $s_i \in G$ formează un sistem de reprezentanţi la stânga modulo H. Se vede că α este de fapt morfism de G-module (care de fapt nu depinde de sisyemul (s_i)), deci $(1_G, \alpha)$ este pereche cocompatibilă. Avem aşadar o compunere de morfisme de δ-functori pe $\mathcal{A}b^G$:

$$H^*(H,-) \xrightarrow{\cong} H^*(G, M_H^G(-)) \longrightarrow H^*(G,-).$$

Se verifică imediat faptul că aceasta este chiar corestricţia în coomologie, fiind suficient să facem verificarea pentru H^0.

Din nou, raţionamente analoage se pot face şi pentru omologie. Se foloseşte o altă versiune a Lemei lui Shapiro, în care Tor ia locul lui Ext şi $S \otimes_R -$ ia locul lui ${}_R\mathrm{Hom}(S,-)$.

1.4. **Produse cup.** Vom arăta că există o transformare naturală de la bifunctorul $H^p(G,-) \otimes H^q(G,-) \to H^{p+q}(G, - \otimes -)$ (toate produsele tensoriale sunt peste $\mathbb{Z}$) cu proprietăţi analoage produsului cup din coomologia singulară. Imaginea unui element de forma $\xi \otimes \eta \in H^p(G,A) \otimes H^q(G,B)$ în $H^{p+q}(G, A \otimes B)$ se va numi *produsul cup* al claselor de coomologie $\xi \in H^p(G,A)$ şi $\eta \in H^q(G,B)$, şi o vom nota pur şi simplu cu $\xi\eta$.

Pentru a arăta că există o asemenea transformare naturală vom folosi noţiunea de modul coindus, introdusă în Definiţia 1.1.5, şi scufundarea naturală $A \to \bar{A} = \mathrm{Hom}(\Lambda, A)$ din observaţia de la sfârşitul acelei subsecţiuni. Am văzut în Propoziţia 1.1.6 că obiectele coinduse sunt aciclice. Avem atunci, pentru fiecare G-modul A, o rezoluţie canonică aciclică în $\mathcal{A}b^G$

$$C^*(A) = 0 \longrightarrow A \longrightarrow I_0 \longrightarrow I_1 \longrightarrow \dots,$$

Cu $I_0 = \bar{A}$, I_1 este modulul coindus asociat conucleului aplicaţiei naturale $A \to I_0$, etc. Fiind o rezoluţie aciclică, ea poate fi folosită pentru a calcula functorii derivaţi $H^*(G, A)$. De asemenea, se observă că ea este functorială în A: pentru orice morfism de G-module $A \to B$ avem un morfism de complexe de la rezoluţia $C^*(A)$ la $C^*(B)$ compatibil cu morfismul dat.

Să observăm acum că incluziunea canonică $A \to I_0 = \bar{A}$ splitează peste $\mathbb{Z}$. Cu alte cuvinte, A se scufundă ca un sumand direct în grupul abelian $\bar{A}$. Un sumand complementar din $\bar{A} = \mathrm{Hom}(\Lambda, A)$ este, de exemplu, mulţimea tutror acelor morfisme de grupuri abeliene de la Λ la A care se anulează în elementul unitate al grupului. Rezultă de aici că rezoluţia $C^*(A)$ este omotopă cu zero peste $\mathbb{Z}$, şi deci că şi produsul tensorial de complexe $C^*(A) \otimes C^*(B)$ este omotop cu zero. În particular, $C^*(A) \otimes C^*(B)$ este o *rezoluţie* a lui $A \otimes B$. Avem atunci un morfism de complexe de la $C^*(A) \otimes C^*(B)$ la o rezoluţie injectivă în $\mathcal{A}b^G$ a lui $A \otimes B$, unic până la omotopie. Acesta induce atunci un morfism

$$H^*(C^*(A) \otimes C^*(B)) \longrightarrow H^*(G, A \otimes B).$$

Compunând cu morfismele naturale

$$H^p(G, A) \otimes H^q(G, B) \cong H^p(C^*(A)) \otimes H^q(C^*(B)) \longrightarrow H^{p+q}(C^*(A) \otimes C^*(B)),\ p, q \in \mathbb{N},$$

obţinem morfismul căutat

$$H^p(G, A) \otimes H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B), \tag{1.4.1}$$

şi functorialitatea în A şi B rezultă imediat din construcţie. De asemenea, se vede că atunci când în (1.4.1) avem $p = q = 0$, morfismul găsit este cel natural de la $A^G \otimes B^G$ la $(A \otimes B)^G$.

Produsele cup se pot de fini şi concret, la nivel de colanţuri. Vom folosi notaţiile din Secţiunea 1.2. Dacă lucrăm cu rezoluţia standard $P_\bullet$ introdusă acolo, atunci fie f, g cocicli care reprezintă clasele $\xi \in H^p(G, A)$ şi $\eta \in H^q(G, B)$. Atunci $\xi\eta$ este reprezentat de cociclul fg, definit prin

$$(fg)(s_0, s_1, \ldots, s_{p+q}) = f(s_0, \ldots, s_p) \otimes g(s_p, \ldots, s_{p+q}),\ \forall s_i \in G. \tag{1.4.2}$$

Dacă pe de altă parte lucrăm cu cocicli neomogeni şi ca mai sus ξ, η sunt reprezentate de cociclii $f \in C^p(A)$ şi respectiv $g \in C^q(B)$, atunci $\xi\eta$ este reprezentată de $fg \in C^{p+q}(A \otimes B)$, unde

$$(fg)(s_1, \ldots, s_{p+q}) = f(s_1, \ldots, s_p) \otimes s_p g(s_p^{-1} s_{p+1}, \ldots, s_p^{-1} s_{p+q}). \tag{1.4.3}$$

Se poate arăta că cele două definiţii coincid. Pentru construcţia produsului cup pentru aşa-numitele grupuri de coomologie Tate $\hat{H}^n$, $n \in \mathbb{Z}$ facem referire la [CFr, Secţiunea IV §7], sau la [CE, Cap. XII]. În cazul $n \geq 1$ grupurile de coomologie Tate sunt cele obişnuite cu care lucrăm aici, şi se recuperează cea de-a doua definiţie dată mai sus. Enunţăm mai jos câteva proprietăţi ale produsului cup pentru care se poate consulta tot [CE, Cap. XII] (unele dintre acestea se verifică imediat folosind definiţia dată mai sus).

Teorema 1.4.1. *Fie G un grup şi A, B, C trei G-module. a, b sunt elemente din $H^p(G, A)$ şi respectiv $H^q(G, B)$, iar* Cor *şi* Res *desemnează corestricţia şi restricţia în raport cu un subgrup $H \leq G$. Produsul cup are următoarele proprietăţi:*

(a) *Este asociativ, dacă identificăm în mod canonic* $(A \otimes B) \otimes C$ *cu* $A \otimes (B \otimes C)$.
(b) *Este graduat-comutativ:* $ba = (-1)^{pq} ab$ *dacă identificăm* $B \otimes A$ *cu* $A \otimes B$.
(c) $\mathrm{Res}(ab) = \mathrm{Res}(a)\mathrm{Res}(b)$.
(d) $\mathrm{Cor}(a\mathrm{Res}(b)) = \mathrm{Cor}(a)b$.

Încheiem cu observaţia că dacă avem un morfism de G-module de la $A \otimes B$ la C, atunci morfismul (1.4.1) de mai sus se poate compune cu cel natural de la $H^{p+q}(G, A \otimes B)$ la $H^{p+q}(G, C)$, obţinând astfel o generalizare a produsului cup. Dacă A este de pildă un inel pe care acţionează G (prin automorfisme de inele), atunci avem o înmulţire (asociativă) pe $H^*(G, A) = \bigoplus_{i \geq 0} H^i(G, A)$, care este graduat-comutativă dacă A este inel comutativ.

1.5. **Coomologie necomutativă.** Până acum am considerat acţiuni ale unui grup G pe un grup abelian A. Acum vom extinde definiţia grupurilor de coomologie H^0 şi H^1 la cazul când G acţionează prin automorfisme pe un grup nu neaparat comutativ A. H^0 este grup, dar H^1 va fi în general numai o "mulţime punctată", adică o mulţime cu un element distins. Vom vedea apoi că se păstrează parţial proprietatea coomologiei de a fi δ-functor, adică pentru un şir exact scurt de G-module necomutative

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

se păstrează o porţiune iniţială a şirului exact lung de coomologie, dacă dăm o definiţie convenabilă noţiunii de şir exact în categoria mulţimilor punctate.

Fie deci A un G-modul necomutativ, adică un grup pe care G acţionează la stânga prin automorfisme. Vom nota acţiunea cu $G \times A \ni (s, a) \mapsto {}^s a$. $H^0(G, A)$, notat şi A^G, va fi, ca şi în cazul comutativ, mulţimea elementelor fixate de G. Desigur, este un subgrup al lui A.

Vom numi 1-cociclu o aplicaţie $\tilde{a} : G \to A$ notată $s \mapsto a_s$ cu porprietatea

$$a_{st} = a_s {}^s a_t, \ \forall s, t \in G.$$

Vom spune că două cocicluri $\tilde{a}, \tilde{b}$ sunt omoloage dacă există un element $a \in A$ astfel încât

$$b_s = a^{-1} a_s {}^s a, \ \forall s \in G.$$

Se verifică uşor faptul că omologia între cocicluri este o relaţie de echivalenţă pe mulţimea cociclurilor. Mulţimea claselor de echivalenţă de cocicluri modulo omologie se notează cu $H^1(G, A)$, şi se numeşte *prima mulţime de coomologie* a lui G cu valori în A. Ca şi H^0, $H^1(G, A)$ este o mulţime punctată, având ca element distins clasa cociclului constant egal cu elementul unitate al lui A. Când A este comutativ, această mulţime punctată este chiar cea subiacentă grupului clasic de coomologie $H^1(G, A)$, deci cele două noţiuni coincid în cazul comutativ.

Înainte să enunţăm rezultatele analoage şirului exact lung de coomologie anunţate mai sus, avem nevoie de următoarea definiţie:

Definiţia 1.5.1. Un şir $(X, x) \to (Y, y) \to (Z, z)$ de aplicaţii de mulţimi punctate se numeşte *exact în* Y dacă imaginea lui X în Y coincide cu preimaginea lui $z \in Z$.

Un şir de mai multe aplicaţii de mulţimi punctate se numeşte *exact* dacă este exact în fiecare termen (care nu se află într-unul din capetele şirului).

Propoziţiile anunţate sunt următoarele:

Teorema 1.5.2. *Fie*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

un şir exact scurt de G-module, nu neaparat comutative. Avem atunci un şir exact lung de mulţimi punctate:

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C). \tag{1.5.1}$$

Dacă A este subgrup central al lui B în propoziţia precedentă, putem spune mai mult:

Teorema 1.5.3. *Dacă în Teorema 1.5.2 A este subgrup central al lui B, atunci şirul (1.5.1) se poate prelungi la dreapta cu încă un morfism*

$$H^1(G, C) \xrightarrow{\Delta} H^2(G, A), \tag{1.5.2}$$

formând tot un şir exact de mulţimi punctate.

Pentru demonstraţii, care constă într-o serie e verificări simple (odată ce am definit aplicaţiile δ, Δ), facem trimitere la [Se2, Anexa Cap. VII]. Vom defini doar aplicaţiile "cobord" δ şi Δ care apar în (1.5.1) şi respectiv (1.5.2).

Fie deci $c \in C^G$. c este imaginea unui element $b \in B$. Cum c este fixat de G, elementele $b^{-1} \cdot {}^s b \in B$ aparţin de fapt lui $A \leq B$. Definim $\delta(c) = \tilde{a}$, cu cociclul $\tilde{a}$ dat de

$$a_s = b^{-1} \cdot {}^s b, \ \forall s \in G.$$

Verificarea faptului că $\tilde{a}$ este într-adevăr cociclu este imediată (este chiar cobord cu valori în B, adică în B, el este omolog cu cociclul constant egal cu unitatea lui B). b nu este unic, dar alegeri diferite duc la 1-cocicluri omoloage, deci δ este bine definită cu valori în H^1.

Pentru definiţia lui Δ, fixăm o clasă din $H^1(G, C)$ reprezentată de un 1-cociclu $\tilde{c}$ cu valori în C. Construcţia este analoagă celei pentru δ: există elemente $b_s \in B$ care se proiectează peste $c_s \in C$, pentru fiecare $s \in G$. Definim acum cociclul neomogen $f \in C^2(G, A)$ prin

$$f(s,t) b_{st} = b_s {}^s b_t, \ \forall s, t \in G.$$

Pentru că $\tilde{c} = (c_s)_{s \in G}$ este cociclu, în formula de mai sus $f(s,t)$ trebuie într-adevăr să aparţină lui A. Din nou trebuie verificat că f este cociclu, şi că alegeri diferite ale elementelor b_s duc la cocicli ce dau aceeaşi clasă de coomologie. Toate acestea sunt simple verificări.

Are sens şi în cadrul necomutativ noţiunea de pereche cocompatibilă, şi construcţia unui morfism în coomologia H^0 şi H^1 indus de o pereche cocompatibilă. Pentru asta se foloseşte definiţia la nivel de cocicluri neomogene, care a apărut şi în Secţiunea 1.3 într-o observaţie.

Vom avea astfel, pentru orice subgrup $H \leq G$ şi orice G-modul necomutativ A un morfism $\mathrm{Res}_{G/H}$ de la $H^*(G, A)$ la $H^*(H, A)$ cu $* = 0, 1$. De asemenea, avem morfismul de inflaţie $\mathrm{Inf}_{G/H}$ de la $H^*(G/H, A^H)$ la $H^*(G, A)$, şi ca şi în cazul comutativ, conjugarea cu un $s \in G$ pe G şi acţiunea lui s^{-1} pe A formează o pereche cocompatibilă, care induce identitatea în coomologie. Avem deci, pentru orice subgrup normal $H \trianglelefteq G$ şi orice

G-modul necomutativ A, o acţiune naturală a lui G/H pe mulţimile punctate $H^*(H,A)$ (acţiune prin automorfisme de mulţimi punctate, şi de grupuri pentru $*=0$).

1.6. **Coomologie Galois şi grupuri profinite.** Până acum G a fost un grup discret arbitrar. Acum vom explica pe scurt cum se extinde teoria coomologiei grupurilor la cazul când G este grup compact total neconex, sau, ceea ce este echivalent, grup profinit (limită proiectivă de grupuri finite). Pentru rezultate generale asupra grupurilor profinite se poate consulta de exemplu [MZ]. Coomologia grupurilor profinite este tratată în [Se3], şi o introducere rapidă se face în [CFr, Cap. V].

G-modulele pe care le luăm în considerare în acest caz sunt acele G-module A cu proprietatea că acţiunea $G \times A \to A$ este continuă în raport cu topologia profinită a lui G şi topologia discretă a lui A. Echivalent, această proprietate este echivalentă cu condiţia ca A să fie reuniunea subgrupurilor A^U, unde U parcurge mulţimea tuturor subgrupurilor deschise ale lui G. Numim aceste G-module *discrete* sau *continue*, sau pur şi simplu G-module, subînţelegând faptul că atunci când G este profinit, lucrăm numai cu G-module discrete.

Un mod natural de a defini coomologia $H^*(G,A)$ pentru un grup profinit G şi un G-modul discret A ($*=0,1$ când A este necomutativ) este de a imita definiţia uzuală cu cocicluri neomogene, folosind însă numai cocicluri continue $G^n \to A$ în raport cu topologia lui G de grup compact şi topologia discretă a lui A. O altă definiţie posibilă este următoarea:

Am introdus în Secţiunea 1.3 (şi în Secţiunea 1.5 în cazul necomutativ) morfismul de inflaţie $\mathrm{Inf}_H^G : H^*(G/H, A^H) \to H^*(G,A)$. Fie acum $V \le U$ subgrupuri deschise normale ale lui G. Vom avea atunci un morfism de inflaţie

$$\mathrm{Inf} : H^*(G/U, A) \longrightarrow H^*(G/V, A).$$

Din naturalitatea inflaţiei, obţinem un sistem inductiv atunci când grupul normal deschis U dscreşte. Vom pune

$$H^*(G,A) = \varinjlim_U H^*(G/U, A^U). \tag{1.6.1}$$

Că cele două definiţii coincid se vede imediat, observând că mulţimea $C^n(G,A)$ a tuturor funcţiilor continue $G^n \to A$ (ca de obicei, A are topologia discretă) este limita inductivă a mulţimilor $C^n(G/U, A^U)$ când U parcurge mulţimea subgrupurilor deschise normale în G. Asta e valabil şi pentru Z^n, adică submulţimea lui C^n alcătuită din acele funcţii pentru care diferenţiala din Secţiunea 1.2 se anulează (sau mulţimea 1-cociclurilor, aşa cum au fost definite în Secţiunea 1.5 când $n=1$ şi A este necomutativ), etc.

Ca şi în cazul când G era discret, avem restricţie, corestricţie, inflaţie, etc. pentru subgrupuri $H \le G$ *închise* în G. Coomologia este δ-functor pe categoria abeliană a G-modulelor discrete comutative, avem şirul inflaţie-restricţie din Propoziţia 1.3.3, şi avem de asemenea şi porţiunea din şirul exact lung de coomologie dată de Teorema 1.5.2 (şi Teorema 1.5.3) în cazul necomutativ, dacă lucrăm numai cu G-module discrete.

Noţiunea de coomologie a unui grup profinit apare de exemplu în contextul următor:

Fie G un grup algebric peste un corp k. Asta înseamnă că G este o schemă de tip finit peste $\mathrm{Spec}(k)$ (notat de acum încolo cu k, dacă nu există pericol de confuzie) înzestrată cu morfisme de k-scheme $G \otimes_k G \to G,\ G \to G$ şi $k \to G$ care satisfac axiomele produsului, inversului, şi respectiv unităţii într-un grup obişnuit. Cu alte cuvinte, este un grup în categoria k-schemelor de tip finit ([Fr, Cap. II, Ex. C] pentru definiţia unui grup într-o categorie cu produse şi obiect final). Pentru fiecare extindere de corpuri $K \supseteq k$, mulţimea morfismelor de k-scheme de la K la G (sau echivalent, mulţimea morfismelor de K-scheme de la K la $G \times_k K$) are structură de grup. Vom nota această mulţime cu G_K; se numeşte mulţimea punctelor lui G raţionale peste K, sau cu valori în K. Dacă $K \supseteq k$ este o extindere Galois (algebrică, separabilă şi normală, dar posibil infinită), atunci grupul Galois $\mathrm{Gal}(K/k)$ acţionează în mod natural pe G_K.

Orice grup Galois are o structură de grup profinit, pentru că orice extindere Galois este reuniunea subextinderilor sale Galois finite, şi în situaţia din paragraful precedent G_K este un $\mathrm{Gal}(K/k)$-modul discret, după cum se poate vedea cu uşurinţă. Are deci sens să vorbim despre grupurile de coomologie $H^*(\mathrm{Gal}(K,k), G_K)$, pentru $* \in \mathbb{N}$ dacă G este grup algebric comutativ (definiţia este evidentă), şi cu $* = 0, 1$ în general.

Un exemplu ar fi $G = G_a$, schema care ne dă, pentru orice extindere K a lui k, grupul aditiv al lui K. Grupurile de coomologie sunt atunci $H^*(\mathrm{Gal}(K,k), K)$. Se poate arăta că acestea sunt nule pentru $* \geq 1$. Un altul este $G = G_m$, grupul multiplicativ al scalarilor nenuli. Avem atunci grupurile $H^*(\mathrm{Gal}(K/k), K^*)$. Pentru $* = 1$ acest grup este nul (aşa-numita Teoremă 90 a lui Hilbert), iar pentru $* = 2$ vom vedea mai târziu că acest grup joacă un rol foarte important.

Pentru teoria generală a schemelor facem referire la [Ha, Cap. II] sau [Mu]. Pentru o introducere rapidă în teoria grupurilor algebrice se poate consulta [Bo, Cap. AG, I].

1.7. **Rezultate suplimentare.** Aici enunţăm şi discutăm pe scurt câteva rezultate binecunoscute ca formule Künneth, coeficienţi universali, şiruri spectrale care sunt utile în lucrul cu (co)omologia grupurilor, etc.

Cunoscând omologia unui grup G cu valori în $\mathbb{Z}$ (ca G-modul trivial, ca de obicei), putem deduce (co)omologia sa cu valori în orice modul trivial, prin intermediul formulei coeficienţilor universali. Mai precis, avem ([HSt, Teorema VI 15.1]):

Teorema 1.7.1 (Teorema Coeficienţilor Universali)**.** *Fie G un grup, şi A un grup abelian, considerat ca G-modul trivial. Atunci, pentru orice număr natural $n \geq 0$ avem următoarele şiruri exacte de grupuri abeliene, naturale în A şi G:*

$$0 \longrightarrow H_n(G) \otimes A \longrightarrow H_n(G,A) \longrightarrow \mathrm{Tor}(H_{n-1}(G), A) \longrightarrow 0, \tag{1.7.1}$$

$$0 \longrightarrow \mathrm{Ext}(H_{n-1}(G), C) \longrightarrow H^n(G,C) \longrightarrow \mathrm{Hom}(H_n(G), C) \longrightarrow 0, \tag{1.7.2}$$

unde produsele tensoriale, Hom, Tor *şi* Ext *sunt peste $\mathbb{Z}$. Mai mult, aceste şiruri scindează, dar scindarea nu este naturală în A.*

Această teoremă reduce calculul (co)omologiei lui G cu valori într-un G-modul trivial la acela al omologiei cu valori în $\mathbb{Z}$. Pentru două grupuri G, H, se pune problema de a determina $H_*(G \times H, \mathbb{Z})$ în funcţie de omologia întreagă a lui G şi H. Acesta este contextul în care se enunţă diverse rezultate “de tip Künneth” (o referinţă: [Ro1, Cap. 11]). În cazul de faţă avem ([HSt, Teorema VI 15.2])

Teorema 1.7.2 (Teorema lui Künneth)**.** *Fie G, H două grupuri. Avem atunci pentru orice $n \in \mathbb{N}$ un şir exact de grupuri abeliene natural în G, H*

$$0 \longrightarrow \bigoplus_{p+q=n} H_p(G) \otimes H_q(H) \longrightarrow H_n(G \times H) \longrightarrow \bigoplus_{p+q=n-1} \mathrm{Tor}(H_p(G), H_q(H)). \quad (1.7.3)$$

Mai mult, şirul scindează, dar scindarea nu este naturală.

Vom trece mai departe la studiul următoarei situaţii: avem un grup G şi un subgrup normal $H \trianglelefteq G$. Se pune problema de a obţine informaţii asupra (co)omologiei lui G cunoscând (co)omologia lui H şi a lui G/H (aici coeficienţii variază; nu lucrăm doar peste $\mathbb{Z}$, sau doar cu module triviale). Vom vedea că răspunsul este dat de un şir spectral.

Pentru definiţii şi proprietăţile elementare ale şirurilor spectrale se pot consulta numeroase surse. Câteva exemple: [We, Cap. 5], [Ro1, Cap. 11], sau [McC, Cap. 2,3]. Ne va interesa mai ales conceptul de şir spectral Grothendieck asociat unei compuneri de functori, care este tratat într-o secţiune specială în primele două referinţe. Reamintim pe scurt în ce constă.

Vom considera următoarea situaţie: avem doi functori aditivi exacţi la stânga $F : \mathcal{A} \to \mathcal{B}$ şi $G : \mathcal{B} \to \mathcal{C}$ pentru categorii abeliene $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$. Presupunem cunoscuţi functorii derivaţi la dreapta RF^* şi RG^* ai lui F şi G, şi am vrea ca de aici să obţinem ceva despre functorii derivaţi $R^*(GF)$ ai compunerii $GF : \mathcal{A} \to \mathcal{C}$. Avem atunci următorul rezultat ([Ro1, Teoremele 11.38, 11.39]):

Teorema 1.7.3 (Şirul spectral Grothendieck)**.** *Fie $U : \mathcal{A} \to \mathcal{B}$ şi $V : \mathcal{B} \to \mathcal{C}$ functori aditivi între categoriile abeliene $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$.*

Presupunem că U, V sunt exacţi la stânga, şi că $\mathcal{A}$ şi $\mathcal{B}$ au suficiente obiecte injective, adică orice obiect este subobiect al unuia injectiv. De asemenea, presupunem că U aplică orice obiect injectiv într-unul V-aciclic (adică obiect $B \in \mathcal{B}$ cu proprietatea că $R^pV(B)$ este nul pentru $p \geq 1$). Există atunci un şir spectral de tip coomologic

$$E_2^{p,q} = R^pV(R^qU(A)) \Rightarrow R^{p+q}(VU)(A). \quad (1.7.4)$$

Dual, dacă U, V sunt exacţi la dreapta, $\mathcal{A}$ şi $\mathcal{B}$ au suficiente obiecte proiective (orice obict este un obiect factor al unuia proiectiv), şi U aplică obiectele proiective în obiecte V-aciclice, atunci există un şir spectral de tip omologic

$$E^2_{p,q} = L_pV(L_qU(A)) \Rightarrow L_{p+q}(VU)(A). \quad (1.7.5)$$

Fixăm acum un grup G şi un subgrup normal $H \trianglelefteq G$. Vom aplica teorema de mai sus cu $\mathcal{A} = \mathcal{A}b^G$, $\mathcal{B} = \mathcal{A}b^{G/H}$, şi $\mathcal{C} = \mathcal{A}b$. Desigur, toate aceste cateogrii au suficiente obiecte proiective şi injective, fiind chiar categoriile modulelor stângi peste inelele $\mathbb{Z}[G]$, $\mathbb{Z}[G/H]$, şi respectiv $\mathbb{Z}$. În primul caz, cel coomologic, functorul U va fi $A \mapsto A^H$, iar V va fi $B \mapsto B^{G/H}$. Evident, ei sunt exacţi la stânga, şi compunerea lor VU este $A \mapsto A^G$. În cazul omologic, U este $A \mapsto A_H$ şi V este $B \mapsto B_{G/H}$. Sunt exacţi la dreapta şi compunerea lor este $A \mapsto A_G$. Functorii derivaţi la dreapta (resp. stânga) în cele două situaţii dau exact coomologia (resp. omologia).

Pentru a putea aplica teorema de mai sus, ar mai trebui să verificăm acum că în primul caz, pentru un G-modul injectiv I, I^H este G/H- coomologic aciclic. Analog, trebuie să arătăm că pentru un G-modul proiectiv P, P_H este G/H-omologic aciclic. Pentru a fixa ideile, dăm argumentul în cazul coomologic; demonstraţia duală decurge întru totul analog. Am văzut în remarca de după Propoziţia 1.1.6 că orice G-modul I se scufundă în G-modulul coindus $\bar{I} = \mathrm{Hom}(\Lambda_G, I)$ (definiţiile sunt în Secţiunea 1.1). Dacă I este injectiv, atunci scufundarea în cauză scindează. Functorul $U : A \mapsto A^H$ se calculează separat pe sumanzi când A este sumă directă de G-module, deci pentru a obţine concluzia dorită este suficient să arătăm că orice G-modul coindus $\bar{X} = \mathrm{Hom}(\Lambda_G, X)$ (X un grup abelian) este trimis de U într-unul G/H-aciclic. Dar se vede imediat din definiţii că $U\bar{X}$ este chiar $\mathrm{Hom}(\Lambda_{G/H}, X)$, adică un G/H-modul coindus. Ştim din Propoziţia 1.1.6 că modulele coinduse sunt aciclice, deci am obţinut ce doream. Acum putem enunţa

Teorema 1.7.4 (Lyndon-Hochschild-Serre)**.** *Fie G un grup, $H \trianglelefteq G$ un subgrup normal, şi A un G-modul. Avem atunci următoarele şiruri spectrale, primul de tip coomologic, iar al doilea de tip omologic:*

$$E_2^{p,q} = H^p(G/H, H^q(H, A)) \Rightarrow H^{p+q}(G, A), \tag{1.7.6}$$

$$E_{p,q}^2 = H_p(G/H, H_q(H, A)) \Rightarrow H_{p+q}(G, A). \tag{1.7.7}$$

Observaţia 1.7.5. În teorema de mai sus, acţiunea lui G/H pe $H^*(H, A)$ este cea naturală introdusă în Secţiunea 1.3, în discuţia despre comportamentul (co)omologiei când morificăm grupul G.

O consecinţă imediată este şirul exact cu 5 termeni ("five-term exact sequence") din (co)omologia grupurilor ([Ro1, teoremele 11.42, 11.43]):

Corolarul 1.7.6. *În ipotezele teoremei precedente, avem următoarele şiruri exacte:*

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H} \to H^2(G/H, A^H) \to H^2(G, A) \tag{1.7.8}$$

$$H_2(G, A) \to H_2(G/H, A^H) \to H_1(H, A)_{G/H} \to H_1(G, A) \to H_1(G/H, A_H) \to 0 \tag{1.7.9}$$

Observăm că (1.7.8) dă o formulare mai precisă a şirului inflaţie restricţie ce a apărut în Propoziţia 1.3.3 în cazul $q = 1$. Cazul general se obţine şi el uşor folosind şirul spectral Hochschild-Serre.

2. Aplicaţii

2.1. H^1, H^2 **şi extensii.** Vom da aici câteva aplicaţii ale inei teoreme a lui Schreier, care afirmă că $H^2(G, A)$ clasifică extensiile de grupuri ale lui A prin G. În acest context, elementul trivial al grupului abelian $H^2(G, A)$ îl joacă produsul semidirect al lui A cu G indus de acţiunea lui G pe A dată iniţial. Vom vedea apoi ce rol joacă H^1 în teoria extensiilor de grupuri. Nu demonstrăm aceste rezultate în detaliu. Ca referinţă se poate consulta de pildă [Ro1, Cap. 5, 10, 11].

Ca şi până acum, A va fi un G-modul (întotdeauna abelian, dacă nu precizăm contrariul). Când A este abelian folosim fără nici o restricţie atât notaţia aditivă cât şi cea multiplicativă pentru operaţia lui A. Ne interesează următoarele obiecte:

Definiţia 2.1.1. O *extensie* a lui A prin G este un şir exact de grupuri de forma

$$(E) : 1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1, \tag{2.1.1}$$

astfel încât acţiunea prin conjugare a unui element $e \in E$ pe $A \leq E$ să fie acţiunea dată a lui $p(e) \in G$ pe A.

Acestea sunt obiectele pe care vrem să le clasificăm, fiind dat G-modulul A. Vom introduce pe mulţimea lor o relaţie de echivalenţă, şi clasificarea se va face pentru clasele de echivalenţă.

Definiţia 2.1.2. Două extensii (E) şi (E') ca în definiţia precedentă se numesc *echivalente* dacă există un morfism $\varphi : E \to E'$ care face următoarea diagramă comutativă:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "1_A"] & E \arrow[r] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\
1 \arrow[r] & A \arrow[r] & E' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Observaţia 2.1.3. Se remarcă imediat că un morfism f ca în definiţia aceasta trebuie să fie de fapt izomorfism.

O extensie (E) ca în Definiţia 2.1.1 se va numi *trivială* dacă p este o retracţie, adică există un morfism $x : G \to E$ astfel încât $p \circ x = 1_G$. Cu alte cuvinte, şirul (E) trebuie să scindeze. În acest caz E se mai numeşte şi *produsul semidirect* al lui A prin G, subînţelegându-se aici acţiunea lui G pe A. Desigur, noţiunea de produs semidirect are sens şi dacă G-modulul A este necomutativ.

Vom nota mulţimea claselor de echivalenţă de extensii ale lui A prin G cu $\mathcal{E}xt(G, A)$. Clasa unei extensii triviale o vom nota cu $0 \in \mathcal{E}xt(G, A)$ (toate extensiile triviale sunt echivalente). Enunţăm acum rezultatul de clasificare anunţat:

Teorema 2.1.4 (Schreier)**.** *Există o bijecţie între* $H^2(G, A)$ *şi* $\mathcal{E}xt(G, A)$ *astfel încât* $0 \in H^2(G, A)$ *corespunde lui* $0 \in \mathcal{E}xt(G, A)$.

Vom reaminti pe scurt felul în care se construieşte bijecţia. Vom folosi notaţiile din Secţiunea 1.2 pentru cocicli şi coborduri neomogene, anume $Z^n(G, A)$ şi respectiv $B^n(G, A)$. Pe noi ne interesează aici cazul $n = 2$.

Presupunem dată o extensie (E) ca în (2.1.1). Alegem o secţiune x pentru p. x este o funcţie de la G la E astfel încât $p \circ x = 1_G$, dar nu este neapărat un morfism de grupuri. Vom presupune şi că x este *normalizată*, adică $x(1) = 1$. Din faptul că p este morfism însă (şi din faptul că A este nucleul lui p), deducem existenţă unei funcţii $f : G \times G \to A$ astfel încât

$$x(s)x(t) = f(s, t)x(st),\ \forall s, t \in G.$$

Se verifică imediat faptul că f este 2-cociclu, folosind asociativitatea produsului din G (se calculează $x(stu)$ în două moduri). De asemenea, f este normalizat în sensul că $f(1, s) = f(s, 1) = 0,\ \forall s \in G$. Se arată apoi că extensii echivalente dau naştere unor cocicli omologi (cu aceeaşi clasă de omologie). De asemenea, o extensie trivială dă naştere clasei triviale de coomologie: se alege x morfism de grupuri, şi atunci cociclul asociat f este identic nul. Avem deci o funcţie de la $\mathcal{E}xt(G, A)$ la $H^2(G, A)$.

Reciproc, pornim cu un cociclu f. Orice cociclu este omolog cu unul normalizat: e suficient să adunăm la f cobordul unui colanţ din $C^1(G, A)$ care în $1 \in G$ ia valoarea 0. Putem deci presupune că f este normalizat. Atunci construim următoarea extensie (E) ca în (2.1.1):

Ca mulţime, $E = A \times G$. Produsul este definit prin

$$(a, s)(b, t) = (a + {}^s b + f(s, t), st).$$

Se verifică faptul că înmulţirea este asociativă, şi că avem un element neutru, şi că elementele sunt inversabile. Incluziunea $A \to E$ este $a \mapsto (a, 1)$, şi proiecţia $E \to G$ este $(a, s) \mapsto s$. Acum se arată că doi cocicli normalizaţi omologi dau extensii echivalente, şi obţinem deci o aplicaţie de la $H^2(G, A)$ la $\mathcal{E}xt(G, A)$. Mai mult, se verifică imediat că cele două construcţii făcute sunt inverse una alteia, deci obţinem într-adevăr o bijecţie între cele două mulţimi. Se vede şi că extensia corespunzătoare clasei triviale de coomologie este trivială.

Observaţia 2.1.5. Teorema lui Schreier funcţionează şi în cazul când G este profinit, dacă ne mărginim la G-module discrete *finite*. Asta rezultă din existenţa unei secţiuni continue pentru orice morfism surjectiv de grupuri profinite ([Se3, Secţiunea 1.2, Prop. 1]).

Vom considera acum extensii triviale. Vrem să clasificăm automorfismele $\varphi : E \to E$ ca în Definiţia 2.1.2, care conservă structura extensiei. Le vom numi pe acestea *automorfisme stabilizatoare*, şi notăm mulţimea lor cu $\mathrm{Stab}(E)$. Ea este grup cu compunerea, şi notăm cu $\mathrm{Stab}_0(E)$, grupul automorfismelor interioare care stabilizează extinderea scindată (E).

Grupul E este ca mulţime $A \times G$, cu înmulţirea dată de

$$(a, s)(b, t) = (a + {}^s b, st).$$

Un morfism stabilizator φ trebuie să fie de forma $(a, s) \mapsto (a + h(s), s)$, unde $h : G \to A$ este o funcţie. Pentru ca φ să fie morfism, este necesar şi suficient ca h să fie 1-cociclu (se traduce pur şi simplu asociativitatea lui φ într-o proprietate a lui h, care va fi exact condiţia de 1-cociclu). Pe de altă parte, pentru ca φ să fie automorfism interior, este necesar şi suficient ca h să fie cobord, adică de forma $h(s) = {}^s a_0 - a_0$ pentru un $a_0 \in A$: dacă h este de forma asta atunci φ este conjugarea cu $(-a_0, 1)$, şi reciproc, dacă φ este conjugarea printr-un element (b, t), atunci $h(s) + {}^s b$ este funcţie constantă în s, deci $h(s)$ va fi chiar $-{}^s b + b$. Din definiţia bijecţiei dintre 1-cociclii $Z^1(G, A)$ şi $\mathrm{Stab}(E)$ vedem că ea este de fapt morfism de grupuri. Avem deci:

Teorema 2.1.6. *Fie A un G-modul şi (E) extensia trivială corespunzătoare. Există un izomorfism de grupuri $Z^1(G, A) \cong \mathrm{Stab}(E)$ care aplică subgrupul $B^1(G, A) \leq Z^1(G, A)$ pe grupul $\mathrm{Stab}_0(G)$ al automorfismelor interioare care stabilizează (E). Avem deci un izomorfism între $H^1(G, A)$ şi $\mathrm{Stab}(E)/\mathrm{Stab}_0(E)$.*

Observaţia 2.1.7. De fapt, un izomorfism între grupul automorfismelor care stabilizează o extensie E a lui A prin G şi $Z^1(G, A)$ există chiar dacă extensia nu este trivială. Demonstraţia este foloseşte aceeaşi idee ca discuţia de mai sus, numai că în loc să privim G ca subgrup al lui E, lucrăm cu o secţiune pentru proiecţia $E \to G$.

În particular, se vede că grupul automorfismelor stabilizatoare pentru o extensie a lui A prin G este abelian şi nu depinde decât de acţiunea lui G pe A, şi nu propriu-zis de extensia $E \to G$.

Ca o consecinţă a acestor teoreme de clasificare şi a calculelor asupra restricţiei şi corestricţiei din Secţiunea 1.3 avem următorul rezultat:

Propoziţia 2.1.8 (Lema Schur-Zassenhaus)**.** *Fie G un grup finit, şi A. Dacă ordinele $n = |G|$ şi $m = |A|$ sunt prime între ele, atunci orice extensie E a lui A prin G scindează. Mai mult, complementele lui A în E (adică subgrupurile lui E care se aplică izomorf pe G prin $E \to G$) sunt conjugate.*

Demonstraţie. Teorema 2.1.4 ne spune că prima afirmaţie este echivalentă cu $H^2(G, A) = 0$. Cum G este finit, avem un morfism de corestricţie de la coomologia grupului trivial 1 la cea a lui G; în cele ce urmează $\mathrm{Cor} = \mathrm{Cor}_1^G$, şi la fel pentru restricţie. Din Propoziţia 1.3.5 ştim că avem $\mathrm{Cor} \circ \mathrm{Res}$ pe $H^2(G, A)$ este înmulţirea cu $n = |G|$. Este de asemenea morfismul nul, pentru că factorizează prin $0 = H^2(1, A)$. Pe de altă parte, cum $m = |A|$ este prim cu n, înmulţirea cu n este un izomorfism pe A şi deci şi pe $H^2(G, A)$ (din functorialitate în A). Rezultă de aici că $H^2(G, A)$ este într-adevăr nul, c.c.t.d.

Folosind Teorema 2.1.6, se vede că ultima afirmaţie din enunţ este echivalentă cu a arăta că $H^1(G, A) = 0$. Demonstraţia este perfect analoagă celei de mai sus, pentru H^2. ∎

Observaţia 2.1.9. În afirmaţia lemei se poate renunţa la ipoteza ca A să fie abelian, obţinându-se astfel Teorema Schur-Zassenhaus, dar rezultatul devine considerabil mai dificil.

Introducem acum următorul concept:

Definiţia 2.1.10. *dimensiunea coomologică* a unui grup G, notată $\mathrm{cd}(G)$, este cel mai mare număr natural n pentru care există un G-modul A cu $H^n(G, A) \neq 0$.

Observaţia 2.1.11. În mod analog se poate introduce şi dimensiunea omologică, folosind omologia în locul coomologiei.

Observaţia 2.1.12. Din Lema lui Shapiro (Propoziţia 1.3.6) rezultă imediat că $\mathrm{cd}(H) \leq \mathrm{cd}(G)$ pentru orice subgrup $H \leq G$.

Vom vedea acum că grupurile libere au dimensiune coomologică 1. Se observă că ea este cel puţin 1 pentru un grup liber (netrivial) G, pentru că G admite morfisme nenule în orice grup, iar $H^1(G, A) = \mathrm{Hom}(G, A)$ pentru un G-modul trivial A. Avem mai întâi următorul rezultat simplu:

Lema 2.1.13. *Fie G un grup şi $n \geq 1$ un număr natural. Dacă $H^n(G, A) = 0$ pentru orice G-modul A, atunci* $\mathrm{cd}(G) \leq n - 1$.

Demonstraţie. Trebuie să arăt că $H^m(G, A) = 0$ pentru orice G-modul A şi orice $m \geq n$. Este suficient să arăt pentru $m = n + 1$, pentru că după aceea se foloseşte inducţie. Scudundăm A într-un G-modul aciclic I (un G-modul injectiv de exemplu, sau în G-modulul aciclic $\bar{A}$ folosit în repetate rânduri pnă acum), şi obţinem un şir exact sucrt de G-module

$$0 \longrightarrow A \longrightarrow I \longrightarrow I/A \longrightarrow 0.$$

Aplicând şirul exact lung de coomologie şi folosind faptul că I este aciclic, vom obţine $H^n(G, A/I) \cong H^{n+1}(G, A)$. Concluzia rezultă de aici. ∎

Teorema 2.1.14. *Un grup liber netrivial G are dimensiune coomologică* 1.

Demonstraţie. Am observat deja mai sus că dimensiunea coomologică este cel puţin 1. Din Lema 2.1.13 rezultă că e suficient să arătăm că $H^2(G, A) = 0$ pentru orice G-modul A. Dar din Teorema 2.1.4 ştim că asta eechivalent cu faptul că toate extensiile prin G scindează, ceea ce este evident: o secţiune a unui morfism surjectiv $E \to G$ se defineşte pe o familie liberă de generatori pentru G. ∎

Mult mai dificilă este reciproca acestei teoreme: grupurile de dimensiune coomologică 1 sunt libere. A fost demonstrată în ipoteza că grupul în cauză este finit generat în [St], şi complet în [Sw].

2.2. **Şirul spectral asociat unei acoperiri.** Vom vedea aici cum putem face legătura dintre grupurile de (co)omologie singulară ale unui spaţiu topologic X (cu proprietăţile necesare) şi cele ale acoperirii sale universale $\tilde{X}$. Rezultatul va fi sub forma unui şir spectral în care apare şi (co)omologia grupului fundamental $\pi_1(X)$. Voi avea nevoie de chestiuni de bază despre hiperomologie, pentru care fac trimitere la [We, 5.7].

X va fi un spaţiu topologic conex prin arce, local conex prin arce, şi semilocal simplu conex. Vom desemna acoperirea sa universală prin $\pi : \tilde{X} \to X$. Grupul fundamental $\pi_1(X)$ acţionează pe $\tilde{X}$, deci şi pe complexul $C_*(\tilde{X})$ al lanţurilor singulare ale lui $\tilde{X}$. Mai mult, se vede că pentru feicare $n \in \mathbb{N}$, $C^n(\tilde{X})$ este un G-modul liber. Rezultatul care ne interesează este

Teorema 2.2.1. *Fie A un gru abelian. Atunci au loc următoarele:*

(a) Există un şir spectral de tip omologic

$$E^2_{p,q} = H_p(\pi_1(X), H_q(\tilde{X}, A)) \Rightarrow H_{p+q}(X, A). \tag{2.2.1}$$

(b) Există un şir spectral de tip coomologic

$$E_2^{p,q} = H^p(\pi_1(X), H^q(\tilde{X}, A)) \Rightarrow H^{p+q}(X, A). \tag{2.2.2}$$

Demonstraţie. Demonstrăm (a), (b) fiind analog. Rezultatul este o consecinţă a faptului că există două şiruri spectrale de tip omologic care converg la hiperomologia unui complex mărginit inferior asociată unui functor exact la dreapta ([We, Prop. 5.7.6]).

Functorul exact la dreapta pe care îl folosim este $F : \mathcal{A}b^G \to \mathcal{A}b$ dat de $B \mapsto B_G$ pentru orice G-modul B. Complexul este

$$C_* = \ldots \longrightarrow C_1(\tilde{X}, A) \longrightarrow C_0(\tilde{X}, A) \longrightarrow 0.$$

Cele două şiruri spectrale care converg la hiperomologia $\mathrm{H}_{p+q}(C_*)$ date de [We, Prop. 5.7.6] sunt pe de o parte $H_p(\pi_1(X), H_q(\tilde{X}, A))$, care apare în enunţ, şi pe de altă parte $H_p(H_q(\pi_1(X), C_*))$. Cum însă am observat mai sus că $C_n(\tilde{X})$ sunt G-module libere, G-modulele $C_n(\tilde{X}, A)$ sunt G-module induse, deci omologic aciclice (Propoziţia 1.1.6). Rezultă că termenii celui de-al doilea şir spectral sunt nuli pentru $q > 0$; pentru $q = 0$ se vede că ei dau exact omologia complexului $C_*(X, A)$, deci omologia singulară a lui X. ■

Corolarul 2.2.2. *Dacă acoperirea universală $\tilde{X}$ este spaţiu contractibil, atunci pentru orice grup abelian A avem*

(a) $H_*(X, A) \cong H_*(\pi_1(X), A)$;

(b) $H^*(X, A) \cong H^*(\pi_1(X), A)$.

Observaţia 2.2.3. În acest corolar apare coomologia lui G cu valori într-un G-modul trivial. El se poate generaliza la G-module arbitrare A, caz în care trebuie să folosim coomologia lui X cu valori în *sistemul local* de coeficienţi dat de G-modulul A ([Hat, Anexa 3.H]).

Demonstraţie. Pentru că $\tilde{X}$ este contractibil, ambele şiruri spectrale din teorema precedentă au termeni nuli pntru $q \geq 1$, şi pentru $q = 0$ termenii sunt $H_p(\pi_1(X), A)$ şi respectiv $H^p(\pi_1(X), A)$. ■

Vom vedea acum câteva aplicaţii ale acestor rezultate la probleme de topologie. Pentru asta, voi avea nevoie şi de grupurile de coomologie ale grupurilor ciclice finite. Notez cu $\mathbb{Z}/n$ grupul ciclic d ordin n. Dacă s este un generator al acestuia, ae sens să considerăm pentru fiecare $\mathbb{Z}/n$-modul A înmulţirea cu elementul $D = s - 1 \in \Lambda$, pe care o notăm tot cu D, şi înmulţirea cu $N = \displaystyle\sum_{i=0}^{n-1} s^i$, notată de asemenea cu N. Atunci, rezultatul se enunţă astfel ([Se2, VIII §4]):

Teorema 2.2.4. *Fie $n \in \mathbb{N}^*$ un număr natural nenul, şi $G = \mathbb{Z}/n$ grupul ciclic de ordin n. Atunci, pentru orice G-modul A au loc*

$$H^p(G, A) = \begin{cases} A^G & , p = 0 \\ (\ker N)/DA & , p \geq 1, impar \\ A^G/NA & , p \geq 1, par \end{cases} \tag{2.2.3}$$

Corolarul 2.2.5. *Grupurile cu dimensiune coomologică finită sunt fără torsiune.*

Demonstraţie. Fie G un grup şi $H \leq G$ un subgrup ciclic finit. Avem $\mathrm{cd}(H) \leq \mathrm{cd}(G)$ (Observaţia 2.1.12), dar dacă H este netrivial, Teorema 2.2.4 arată că are dimensiune coomologică infinită. ■

Cu aceste pregătiri, trecem la exemple de aplicaţii. Ca o consecinţă a rezultatului din Corolarul 2.2.2, putem da o interpertare topologică (co)omologiei grupurilor. Reamintim că pentru un număr natural n şi grup netrivial G, un spaţiu $K(G, n)$ este un spaţiu topologic al cărui singur grup de omotopie netrivial este $\pi_n \cong G$. Aceste spaţii se numesc spaţii Eilenberg MacLane, există CW-complexe Eilenberg-MacLane pentru toţi n şi G, singura condiţie fiind cea evident necesară ca G să fie abelian dacă $n \geq 2$, şi sunt unice până la omotopie (dacă sunt CW-complexe). Pentru informaţii suplimentare se poate consulta de exemplu [Hat, Secţiunea 4.2]. În contextul de faţă sunt importante din cauza următorului rezultat.

Teorema 2.2.6. *Fie G un grup, şi X un CW-complex $K(G, 1)$. Atunci (co)omologia lui G cu valori într-un grup abelian A este (co)omologia singulară a lui X cu valori în A.*

Demonstraţie. Acoperirea universală a lui X este CW-complex cu toate grupurile de omotopie nule, deci este contractibilă conform Teoremei lui Whitehead ([Hat, Teorema 4.5]). Se poate aplica acum Corolarul 2.2.2. ■

Observaţia 2.2.7. Acest rezultat se poate formula şi altfel: există un fibrat principal universal cu grup structural G, iar baza sa este un CW-complex $K(G, 1)$ notat de obicei cu BG şi numit *spaţiul clasifiant* al lui G (referinţă: [Hus, 4.11,12,13]). Teorema spune atunci că de fapt (co)omologia grupului G este chiar (co)omologia singulară a spaţiului său clasifiant.

O aplicaţie interesantă a discuţiei de până acum la studiul punctelor fixe ale automorfismelor varietăţilor contractibile:

Propoziţia 2.2.8. *Fie M o varietate netedă contractibilă, şi h un automorfism al lui M (în categoria varietăţilor netede) de ordin prim. Atunci h are un punct fix.*

Demonstraţie. Fie p ordinul lui h. Dacă h nu ar avea un punct fix, atunci câtul $M/\langle h\rangle$ lui M prin acţiunea lui h ar fi o varietate netedă, cu grup fundamental $\mathbb{Z}/p$, şi acoperire universală contractibilă M. Dar atunci, din Corolarul 2.2.2, coomologia lui $M/\langle h\rangle$ cu valori în $\mathbb{Z}$ ar coincide cu $H_*(\mathbb{Z}/p, \mathbb{Z})$. Contradicţia provine din faptul că pe de o parte coomologia unei varietăţi se anulează în dimensiuni mari, dar pe de altă parte, Teorema 2.2.4 spune că există infinit de multe ranguri unde coomologia e nenulă (toate rangurile pare). ■

Folosind rezultatul asupra acoperirilor universale contractibile, putem descoperi proprietăţi pentru grupurile fundamentale ale anumitor varietăţi. Un exemplu:

Propoziţia 2.2.9. *Fie M o varietate Riemann completă şi conexă care are curbura secţională ≤ 0. Atunci grupul fundamental al lui M nu are torsiune.*

Demonstraţie. Un rezultat fundamental asupra varietăţilor Riemann complete, conexe, simplu conexe, şi cu curbură ≤ 0 este Teorema lui Cartan ([Mil, Teorema 19.2]), care afirmă că o astfel de varietate este contractibilă (şi de fapt, difeomorfă cu un spaţiu euclidian de aceeaşi dimensiune).

Rezultă c a varietatea noastră M are acoperire contractibilă, şi putem aplica Corolarul 2.2.2. Dacă $\pi_1(M)$ ar avea un subgrup ciclic finit netrivial, atunci, înlocuind M cu acoperirea corespunzătoare acestui subgrup, putem presupune că $\pi_1(M)$ este ciclic finit şi netrivial. Dar atunci coomologia sa cu valori în $\mathbb{Z}$ este pe de o parte nenulă în toate rangurile pare, şi pe de altă parte, fiind izomorfă cu $H^*(M, \mathbb{Z})$ (Corolarul 2.2.2), este nulă în dimensiuni mai mari decât cea a lui M. Obţinem deci o contradicţie. ■

Mai departe, folosind coomologia grupurilor ciclice finite, teorema lui Künneth în varianta coomologică ((1.7.3)) şi tehnicile din această secţiune, vom deduce un binecunoscut rezultat al lui P.A. Smith ([Sm]) asupra grupurilor finite care acţionează liber pe o sferă $\mathbb{S}^n$. Înainte de asta facem câteva observaţii asupra coomologiei unui produs de două grupuri ciclice finite.

Fie $G = (\mathbb{Z}/m)^2$, produsul direct a două grupuri ciclice de ordin $m \geq 2$. Aplicând Künneth în varianta pentru coomologie, vom avea

$$0 \to \bigoplus_{p+q=n} H^p(\mathbb{Z}/m) \otimes H^q(\mathbb{Z}/m) \to H^n(G) \to \bigoplus_{p+q=n+1} \mathrm{Tor}(H^p(\mathbb{Z}/m), H^q(\mathbb{Z}/m)) \to 0.$$

Din Teorema 2.2.4 ştim cum arată coomologia lui $\mathbb{Z}/m$. Pentru n par, în şirul exact de mai sus termenul din dreapta se anulează, pentru că unul dintre p, q cu $p + q = n + 1$ este impar, şi coomologia (cu valori în $\mathbb{Z}$) în grade impare a lui $\mathbb{Z}/m$ se anulează. Vom avea deci $H^n(G) \cong (\mathbb{Z}/m)^{\frac{n}{2}+1}$ dacă n este par şi nenul. Când n este impar, pe de altă parte, *primul* termen din şirul exact se va anula, şi vom avea $H^n(G) \cong (\mathbb{Z}/m)^{\frac{n-1}{2}}$. Am obţinut deci:

Propoziţia 2.2.10. *Fie $m \geq 2$ un număr natural, şi $G = (\mathbb{Z}/m)^2$. Atunci vom avea*

$$H^n(G) \cong \begin{cases} \mathbb{Z} & , n = 0 \\ (\mathbb{Z}/m)^{\frac{n-1}{2}} & , n \geq 1, impar \\ (\mathbb{Z}/m)^{\frac{n}{2}+1} & , n \geq 1, par \end{cases} \tag{2.2.4}$$

Putem demonstra acum rezultatul lui Smith din [Sm] pe care l-am menţionat mai sus. Prin acţiune liberă a unui grup finit pe o varietate netedă compactă înţelegem acţiune prin automorfisme (în categoria varietăţilor netede) astfel încât nici un element netrivial al grupului nu are puncte fixe. Rezultă atunci (pentru că grupul este finit şi varietatea este compactă) că se poate forma câtul varietăţii prin acţiune, care este tot o varietate, şi că aplicaţia de proiecţie este acoperire normală al cărei grup de transformări de acoperire este chiar grupul cu care am pornit.

Rezultatul anunţat dă informaţii asupra grupurilor abeliene finite care acţionează liber pe o sferă.

Teorema 2.2.11. *Un grup finit abelian care acţionează liber pe o sferă $\mathbb{S}^n$ (pentru un $n \geq 1$) este ciclic.*

Demonstraţie. Putem presupune că G este de forma $(\mathbb{Z}/m)^2$, şi încercăm să găsim o contradicţie. Vom nota cu X câtul $\mathbb{S}^n/G$ prin acţiunea lui G, cu H^* coomologia întreagă a sferei $\mathbb{S}^n$, şi cu $H^*(X)$ cea a lui X. Desigur, nenule sunt numai grupurile H^0, H^n, izomorfe cu $\mathbb{Z}$.

Aplicăm Teorema 2.2.1 în cazul de faţă, acoperirii $\mathbb{S}^n \to X$. Cum şirul spectral coomologic se anulează pe liniile diferite de $0, n$, avem un şir exact lung

$$\ldots \to H^{p+n}(G, H^0) \to H^{p+n}(X) \to H^p(G, H^n) \to H^{p+n+1}(G, H^0) \to H^{p+n+1}(X) \to \ldots$$

Să observăm că o aplicaţie $\mathbb{S}^n \to \mathbb{S}^n$ fără puncte fixe este omotopă cu aplicaţia antipodală. Dacă n este par, atunci aplicaţia antipodală nu conservă orientarea, şi deci singurele grupuri finite care acţionează liber pe sferele pare sune cel trivial şi $\mathbb{Z}/2$. Putem deci să presupunem că n este impar, caz în care aplicaţia antipodală păstrează orientarea. Va rezulta atunci că G conservă orientarea, şi deci acţionează trivial pe H^n. Evident, el acţionează trivial şi pe H^0.

Ne vom uita acum la porţiunea şirului alcătuită din ultimii patru termeni, cu p impar suficient de mare încât termenii din capetele acestei porţiuni să fie nuli. Se poate alege p astfel, pentru că X este varietate de dimensiune n. E suficient să luăm de exemplu $p > 0$. Atunci morfismul de la mijloc, $H^p(G) \to H^{p+n+1}(G)$, va fi izo. Cei doi termeni vor fi $(\mathbb{Z}/m)^{\frac{p-1}{2}}$ şi respectiv $(\mathbb{Z}/m)^{\frac{p+n}{2}}$ (Propoziţia 2.2.10), evident neizomorfi. Avem aşadar o contradicţie, şi demonstraţia este încheiată. ■

Această teoremă se aplică desigur la subgrupurile abeliene ale oricărui grup finit care acţionează liber pe o sferă. Este un fapt binecunoscut că un p-grup ale cărui subgrupuri abeliene sunt ciclice este ciclic dacă p este număr prim impar, şi ciclic sau grup cuaternionic generalizat dacă este 2-grup. Deducem astfel imediat:

Corolarul 2.2.12. *Dacă grupul finit G acţionează liber pe o sferă $\mathbb{S}^n$, atunci subgrupurile sale Sylow de ordin impar sunt ciclice, şi cele de ordin par sunt fie ciclice, fie grupuri cuaternionice generalizate.*

Observaţia 2.2.13. Milnor a arătat în [Mil1] că grupurile finite care acţionează liber pe o sferă au în plus proprietatea că elementele lor involutive (adică de ordin doi) sunt centrale. Se vede că ţinând cont de ce am demonstrat mai sus, asta e echivalent cu a spune că grupurile în cauză au cel mult un element involutiv. În sfârşit, în 1978, Madsen, Thomas şi Wall au arătat în [MTW] că e valabilă şi reciproca acestor rezultate: dacă un grup finit are grupuri Sylow ciclice sau cuaternionice generalizate şi elementele sale involutive sunt centrale, atunci el acţionează liber pe o sferă.

Rămânând în cadrul acţiunilor de grupuri finite pe sfere, vom folosi Teorema 2.2.1 într-o variantă mai fină pentru a calcula inelul de coomologie al unui spaţiu lenticular (ne interesează deci şi structura multiplicativă a inelului dată de produsul cup în coomologia singulară) cu valori într-un inel de forma $\mathbb{Z}/m$.

Reamintim că fiind date numere naturale $m, n \geq 2$ şi numere naturale $\ell_i,\ i = \overline{1,n}$ prime cu m, spaţiul lenticular $L_m^{2n-1}(\ell_1, \ldots, \ell_n)$ este câtul sferei $\mathbb{S}^{2n-1}$ prin următoarea acţiune (care va fi evident că este liberă) a grupului ciclic $C_m = \mathbb{Z}/m$: se consideră sfera unitate $\mathbb{S}^{2n-1}$ ca fiind scufundată în mod uzual în $\mathbb{C}^n$ ca mulţimea n-uplurilor $(z_1, \ldots, z_n)$ de numere complexe de modul 1, şi un generator al lui C_m acţionează trimiţând $(z_1, \ldots, z_n)$ în $(e^{\frac{2\pi i \ell_1}{m}} z_1, \ldots, e^{\frac{2\pi i \ell_n}{m}} z_n)$ ([Hat, Ex. 2.43]). Spaţiul definit astfel este o varietate netedă de dimensiune $2n-1$, orientabilă (acţiunea lui C_m pe sferă conservă orientarea). Pentru că în calculul inelului de coomologie numerele ℓ_i nu au nici o importanţă, le vom omite şi vom nota pur şi simplu L_m^{n-1} ($2n-1$ este dimensiunea varietăţii, aceeaşi cu a sferei pe care acţionează grupul), sau L_m atunci când nu există pericol de confuzie.

Pentru a putea folosi şirul spectral al acoperirii $\mathbb{S}^{2n-1} \to L_m$ în calculul inelului de coomologie, trebuie să ştim cum se comportă acest şir spectral faţă de produse: produse cup în coomologia singulară, şi ceea ce am numit tot produse cup în coomologia grupurilor, în Secţiunea 1.4. Aici intervine noţiunea de şir spectral de algebre, pentru care se poate consulta [McC, §2.3]. Ce ne interesează aici este faptul că termenii E_2 ai şirului spectral (2.2.2) din Teorema 2.2.1 formează de fapt o algebră bigraduată diferenţială, şi că se poate arăta că şirul spectral converge la coomologia singulară a spaţiului acoperit în sensul şirurilor spectrale de algebre. Nu demonstrăm asta, dar observăm numai că structura de algebră bigraduată apare folosind produsele cup din cele două teorii de coomologie, şi observaţia de după Teorema 1.4.1, care dă produse cup generalizate $H^*(G, A) \otimes H^*(G, B) \to H^*(G, C)$ pentru un morfism de G-module $A \otimes B \to C$. Aici A, B şi C vor fi grupuri de coomologie singulară (cu valori într-un inel comutativ) ale acoperirii $\tilde{X}$, şi morfismul respectiv este chiar produsul cup pe $\tilde{X}$.

Teorema 2.2.4 ne spune cum arată coomologia lui C_m cu valori într-un C_m-modul, dar nu spune nimic despre structura multiplicativă. Se poate arăta că există o clasă de coomologie $u \in H^2(C_m, A)$ astfel încât produsul cup cu u dă izomorfisme $H^*(C_m, A) \to H^{*+2}(C_m, A)$ pentru $* \geq 1$ ([Se2, Cap. VIII, §4], de exemplu). De asemenea, mai observăm că elementele grupului $H^1(C_m, \mathbb{Z}/m) \cong \mathbb{Z}/m$ au pătrat nul în inelul de coomologie $H^*(C_m, \mathbb{Z}/m)$ al grupului ciclic C_m.

Avem acum instrumentele necesare pentru calculul inelului de coomologie al lui L_m. Ne va interesa coomologia cu valori în $\mathbb{Z}/m$ (acelaşi m), şi cea cu valori în $\mathbb{Z}$. În [Hat] inelul de coomologie $H^*(L_m, \mathbb{Z}/m)$ se calculează prin alte câteva metode ([Hat, Ex. 3.41, 3E.2]). Enunţăm rezultatul:

Propoziţia 2.2.14. *$H^*(L_m^{2n-1}, \mathbb{Z})$ este inelul graduat $\mathbb{Z}[\alpha, \beta]/(m\alpha)$ factorizat prin partea de grad $\geq 2n$, unde α şi β au grade 2 şi respectiv $2n-1$.*

$H^*(L_m^{2n-1}, \mathbb{Z}/m)$ este inelul graduat $(\mathbb{Z}/m)[\alpha, \beta]/(\alpha^2)$ factorizat prin partea de grad $\geq 2n$, unde α şi β au grade 1 şi respectiv 2.

Demonstraţie. Pentru că instrumentul de bază în ambele cazuri este şirul exact lung care a apărut şi în demonstraţia pentru Teorema 2.2.11, vom folosi peste tot notaţia H^*

pentru coomologia sferei, care va avea valori fie în $\mathbb{Z}$, fie în $\mathbb{Z}/m$; analog, pentru spaţiul lenticular, scriem $H^*(L_m^{2n-1})$. Şirul exact va fi atunci

$$\begin{aligned} \ldots \to H^p(C_m, H^{2n-1}) \to H^{p+2n}(C_m, H^0) \to H^{p+2n}(L_m^{2n-1}) \to H^{p+1}(C_m, H^{2n-1}) \to \\ \to H^{p+2n+1}(C_m, H^0) \to H^{p+2n+1}(L_m^{2n-1}) \to \ldots \end{aligned}$$

H^0 şi H^{2n-1} sunt ambele egale cu inelul coeficienţilor ($\mathbb{Z}$ sau $\mathbb{Z}/m$) pe care C_m acţionează trivial. În ambele cazuri, pentru $p \in \overline{-2n, -2}$ porţiunea acestui şir alcătuită din primii patru termeni arată că aplicaţia $H^t(C_m, H^0) \to H^t(L_m)$ este izomorfism pentru t între 0 şi $2n-2$ inclusiv. Împreună cu observaţiile asupra inelului de coomologie al grupului ciclic C_m cu valori în $\mathbb{Z}$ şi $\mathbb{Z}/m$ făcute inainte de inceputul acestei demonstraţii, asta arată că inelul de coomologie al spaţiului lenticular cu valori în $\mathbb{Z}$ şi $\mathbb{Z}/m$ este ca în enunţ în grade $\leq 2n-2$. Desigur, este nul în grade $\geq 2n$ pentru că L_m^{2n-1} este varietate $2n-1$-dimensională, deci rămâne să vedem ce se întâmplă în grad $2n-1$.

Ştim deja (din dualitate Poincaré, de exemplu) că $H^{2n-1}(L_m^{2n-1})$ este egal cu inelul de coeficienţi ($\mathbb{Z}$ sau $\mathbb{Z}/m$ în cazul nostru). Dacă lucrăm peste $\mathbb{Z}$, am văzut mai sus că avem coomologie nenulă doar în grade pare. Asta arată imediat că $H^*(L_m^{2n-1}, \mathbb{Z})$ este ca în enunţ. Pentru $\mathbb{Z}/m$ mai examinăm şirul exact de mai sus. Pentru $p = -1$, şirul va fi

$$0 \to H^{2n-1}(C_m, H^0) \to H^{2n-1}(L_m) \to H^0(C_m, H^{2n-1}) \to H^{2n}(C_m, H^0) \to 0.$$

Cum primii doi termeni sunt ambii grupuri ciclice de ordin m (Teorema 2.2.4) şi primul morfism este mono, el trebuie să fie izo. În acest caz rezultă deci că aplicaţia de la $H^t(C_m, H^0)$ la $H^t(L_m)$ din şirul nostru exact (dat de convergenţa şirului spectral la coomologia spaţiului lenticular) este izomorfism pentru toţi t. Observaţiile asupra inelului de coomologie al lui C_m cu valori în $\mathbb{Z}/m$ făcute înaintea demonstraţiei arată acum că $H^*(C_m, \mathbb{Z}/m)$ este ca în enunţ, şi argumentul tocmai încheiat arată că $H^*(L_m, \mathbb{Z}/m)$ este izomorf cu $H^*(C_m, \mathbb{Z}/m)$. ■

2.3. **Morfismul de transfer.** Aici G va fi un grup arbitrar, iar $H \leq G$ va fi un subgrup de indice finit. Transferul este un morfism de grupuri V de la abelianizatul $G_{ab} = G/G'$ la $H_{ab} = H/H'$ (poate fi privit şi ca morfism de la G la H_{ab}, după compunerea cu proiecţia $G \to G_{ab}$); aici, G' este subgrupul derivat $[G, G]$. Vom da două definiţii ale transferului şi câteva aplicaţii.

Transferul a fost introdus de Schur pentru a da o demonstraţie simplă a faptului că orice grup G al cărui centru are indice finit are abelianizat G_{ab} finit ([Ro2, Teorema 7.57]).

Fie deci G un grup, şi $H \leq G$ un subgrup de inice finit $n \in \mathbb{N}^*$. Alegem acum un sistem $\{s_i,\ i = \overline{1,n}\}$ de reprezentanţi la stânga modulo H. Cum G acţionează pe mulţimea G/H a claselor la stânga modulo H prin înmulţire la stânga, pentru un element $s \in G$ vom avea

$$ss_i = s_{\sigma i} h_i,\ h_i \in H, i = \overline{1,n}, \tag{2.3.1}$$

unde σ este o permutare a mulţimii $[n] = \overline{1,n}$.

Definiţia 2.3.1. În situaţia de mai sus, *morfismul de transfer* $V : G_{ab} \to H_{ab}$ este aplicaţia care trimite clasa lui $s \in G$ în G_{ab} în clasa lui $\prod_i h_i \in H$ în H_{ab}.

Din această definiţie nu sunt evidente două lucruri: (a) definiţia lui V nu ar trebui să fie independent de sistemul de reprezentanţi (s_i), şi (b) din moment ce V a fost numit *morfismul* de transfer, am vrea ca el să fie într-adevăr morfism de grupuri. Pentru a demonstra acestea, observăm:

Lema 2.3.2. *Fie $G, H, (s_i)$ şi V ca mai sus. Fie de asemenea χ un caracter al lui H (morfism de la H la $\mathbb{S}^1$). χ este o reprezentare 1-dimensională a lui H, deci induce o reprezentare $n = [G : H]$-dimensională ρ a lui G. Cu $\varepsilon(s)$ notăm semnul permutării induse de $s \in G$ pe G/H prin înmulţire la stânga. Are atunci loc*

$$\chi(V(s)) = \varepsilon(s) \det(\rho(s)), \ \forall s \in G. \tag{2.3.2}$$

Demonstraţie. Reprezentarea indusă ρ se poate descrie astfel: se alege o bază e_i pentru $\mathbb{C}^n$, şi ρ este atunci dat de

$$\rho(s)e_i = \chi(h_i)e_{\sigma i}, \ \forall i.$$

De aici afirmaţia pe care vrem să o demonstrăm rezultă imediat. ∎

Corolarul 2.3.3. *V din Definiţia 2.3.1 este independent de sistemul de reprezentanţi s_i, şi este morfism de grupuri. Mai mult, în Definiţia 2.3.1 putem alege sisteme de reprezentanţi la dreapta, obţinând acelaşi morfism.*

Demonstraţie. Alegerea unui alt sistem de reprezentanţi înseamnă o schimbare de bază în $\mathbb{C}^n$ în lema precedentă. Partea dreaptă din (2.3.2) nu depinde de bază, deci pentru orice caracter χ al lui H_{ab}, $\chi(V(s))$ depinde numai de s. Dar cum caracterele unui grup abelian separă elementele acestuia, $V(s)$ este un element bine definit al lui H_{ab}, care depinde numai de s.

Pennrtu χ fixat, partea dreaptă din (2.3.2) este multiplicativă în s. De aici rezultă că pentru orice χ, $\chi \circ V$ este aplicaţie multiplicativă. Concluzia dorită rezultă acum din aceeaşi observaţie că elementele unui grup abelian sunt separate de caracterele acestuia.

Pentru ultim afirmaţie se observă că în caracterizarea transferului din lema precedentă avem simetrie stânga-dreapta. ∎

Putem sădăm o definiţie omologicp̌entru morfismul de transfer V. Am văzut în Secţiunea 1.3 că atunci când indicele subgrupului $H \leq G$ este finit, avem morfisme de restricţie în omologie, $H_*(G, A) \to H_*(H, A)$, pentru orice G-modul A. Vom vedea că V se descrie ca un astfel de morfism de restricţie.

Să observăm mai întâi că pentru orice grup G, $H_1(G)$ (adică $H_1(G, \mathbb{Z})$ pentru G-modulul trivial $\mathbb{Z}$) este canonic izomorf cu abelianizatul G_{ab}. Vom nota cu $\varepsilon : \Lambda \to \mathbb{Z}$ morfismul de augmentare, care trimite toţi $s \in G$ în $1 \in \mathbb{Z}$, şi cu $I = I_G$ nucleul lui ε. Se vede că pentru orice G-modul A, $H_0(G, A)$ este A/IA. Avem un şir exact scurt de G-module

$$0 \longrightarrow I \longrightarrow \Lambda \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Ne uităm acum la şirul exact lung de omologie asociat. Cum Λ este G-modul indus (Definiţia 1.1.5), el este omologic aciclic (Propoziţia 1.1.6). Şirul de omologie va fi atunci

$$0 \longrightarrow H_1(G) \longrightarrow I/I^2 \longrightarrow \Lambda/I \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Ultimul morfism este chiar izomorfismul $\Lambda/I \to \mathbb{Z}$ indus de ε, deci morfismul $H_1(G) \to I/I^2$ este izo. Dar aplicaţia care trimite $s \in G$ în clasa lui $s-1 \in I$ modulo I^2 factorizează prin G_{ab}, şi este izomorfism de grupuri. Asta ne dă identificarea lui $H_1(G)$ cu G_{ab}.

Observaţia 2.3.4. Că $H_1(G)$ este chiar G_{ab} se poate vedea imediat şi altfel: am spus mai sus (Observaţia 2.2.7) că G este grupul fundamental al spaţiului său clasifiant BG, şi că omologia lui G este omologia singulară a lui BG. Se ştie însă că primul grup de omologie al unui spaţiu este abelianizatul grupului său fundamental, deci $H_1(G) \cong G_{ab}$. Avem totuşi nevoie de identificarea de mai sus dintre H_1 şi G_{ab} pentru calculele care apar în Propoziţia 2.3.5.

Rezultatul următor se demonstrează folosind definiţia restricţiei în omologia de grad zero dată în Secţiunea 1.3 şi faptul că morfismul Res comută cu diferenţiala $\delta : H_1 \overset{\cong}{\to} I/I^2$ din şirul exact lung de omologie. Pentru detalii se poate consulta [Se2, VII §8], unde apare definiţia clasică a transferului folosind sisteme de reprezentanţi la dreapta (ultima afirmaţie din Corolarul 2.3.3).

Propoziţia 2.3.5. *După identificarea lui G_{ab} cu $H_1(G)$ de mai sus, transferul V de la G_{ab} la H_{ab} este chiar restricţia* $\mathrm{Res} : H_1(G) \to H_1(H)$.

În aplicaţiile pe care le vom da morfismului de transfer avem nevoie de faptul că atunci când H este central în Z, transferul are o formă foarte simplă. Avem mai întâi

Propoziţia 2.3.6. *Dacă $n = [G : H]$, $V(s)$ este clasa unui produs de conjuagte ale unor puteri s^{n_j}, $j = \overline{1,t}$ cu $\sum n_j = n$.*

Demonstraţie. Folosim Definiţia 2.3.1, şi descompunem permutarea $\sigma \in S_n$ care apare acolo în cicluri disjuncte. Dacă $(1, 2, \dots, k)$ este un asemenea ciclu, de exemplu, atunci

$$ss_i = s_{i+1}h_i,\ i = \overline{1, k-1},$$
$$ss_k = s_1 h_k.$$

Vom avea deci

$$\prod_{i=1}^{k} h_{k-i+1} = s_1^{-1} s^k s_1$$

(am înmulţit h_i în ordinea descrescătoare a indicilor). Facem asta pentru toate ciclurile, şi rezultă concluzia. ∎

Avem următoarea consecinţă imediată a acestei propoziţii:

Corolarul 2.3.7. *Dacă subgrupul central $H \leq G$ are indice n, atunci transferul este aplicaţia $s \mapsto s^n$.*

Vom vedea acum câteva probleme în rezolvarea cărora morfismul de transfer joacă un rol important. Mai întâi un rezultat care ajută la studiul structurii grupurilor finite:

Propoziţia 2.3.8. *Fie G un grup finit, şi H un subgrup central cu proprietatea că $m = |H|$ şi $n = |G/H|$ sunt prime între ele. Atunci G este produsul dintre H şi un grup K.*

Demonstraţie. Corolarul 2.3.7 ne spune că $x \mapsto x^n$ este un morfism $V : G \to H$. Restricţia lui V la H este un automorfism al lui H, pentru că $(m, n) = 1$. Cum H este central, rezultă de aici că G este produsul dintre H şi nucleul lui V. ∎

Un grup se va numi *cu conjugare finită*, abreviat FC, dacă toate clasele sale de conjugare sunt finite; echivalent, centralizatorii tuturor elementelor trebuie să fie subgrupuri de indice finit. Un fapt care va fi folositor în repetate rânduri în cele ce urmează este următorul:

Propoziţia 2.3.9. *Orice grup FC fără torsiune este abelian.*

Demonstraţie. Fie G un grup FC şi fără torsiune. Putem presupune că este finit generat (e suficient să ne uităm la subgrupurile sale generate de două elemente). Fixăm o mulţime finită S de generatori. Intersecţia tuturor centralizatorilor elementelor din S este chiar centrul lui G. Pentru că toţi aceşti centralizatori au indice finit şi sunt în număr finit, centrul $Z(G)$ are indice finit n. Atunci transferul este $x \mapsto x^n$ (Corolarul 2.3.7), şi este injectiv pentru că G nu are torsiune. Rezultă că putem scufunda G în grupul abelian $Z(G)$, deci G este abelian. ∎

Se ştie că un grup finit generat, fără torsiune, care are un subgrup liber de indice finit este liber (conjectura lui Serre, care apare ca [St, Teorema 5.3]). Vom demonstra aici asta pentru grupuri libere de rang 1, adică grupuri ciclice infinite.

Propoziţia 2.3.10. *Fie G un grup fără torsiune care are un subgrup ciclic infinit H de indice finit. Atunci G este ciclic infinit.*

Demonstraţie. Să observăm mai întâi că pentru orice grup G şi orice subgrup de indice finit H, există un subgrup *normal* al lui G de indice finit conţinut în H: se ia pur şi simplu intersecţia conjugatelor lui H prin elementele dintr-o clasă de reprezentanţi la stânga modulo H, şi se vede uşor că acest grup este normal şi de indice finit în G, fiind intersecţia unui număr finit de subgrupuri de indice finit.

Se vede că dacă în plus un grup cu proprietăţile din enunţ este şi abelian, atunci concluzia are loc: aplicaţia $x \mapsto x^n$ pentru n convenabil ales va fi un morfism injectiv al grupului nostru în subgrupul lui ciclic infinit, deci grupul trebuie să fie ciclic infinit.

Conform observaţiei de la începutul demonstraţiei, putem presupune că avem un subgrup ciclic infinit $\langle a \rangle \trianglelefteq G$ normal şi de indice finit. Un element $b \in G$ acţionează prin conjugare pe $\langle a \rangle$, fie prin $bab^{-1} = a$, fie prin $bab^{-1} = a^{-1}$ (singurele automorfisme ale unui grup ciclic infinit generat de a). Să presupunem că avem varianta a doua, şi să lucrăm în grupul $\langle a, b \rangle$ generat de a şi b. În primul rând, se observă că $\langle a, b^2 \rangle$ este comutativ, deci este ciclic infinit, conform paragrfului precedent. Rezultă că $\langle a, b \rangle$ are un subgrup ciclic infinit de indice 2 pe care b acţionează netrivial.

Ne uităm acum la transferul de la $\langle a, b \rangle$ la $\langle a, b^2 \rangle$. Folosind sistemul de reprezentanţi $1, b$, vedem că imaginea lui b este b^2. În particular, transferul nu este trivial. Dar atunci rezultă că el este injectiv: orice subgrup netrivial are indice finit, deci dacă nucleul ar fi $\neq 1$, am avea un morfism netrivial al unui grup finit într-unul ciclic infinit, evident absurd. Deci avem un morfism injectiv V de la grupul presupus neabelian $\langle a, b \rangle$ la grupul ciclic infinit $\langle a, b^2 \rangle$, şi am obţinut o contradicţie. Rezultă deci că de fapt $\langle a \rangle$ este subgrup ciclic *central* al lui G, de indice finit n, să zicem. Dar atunci transferul este $x \mapsto x^n$ (Corolarul 2.3.7), este injectiv pentru că G nu are torsiune, şi avem aşadar o scufundare a lui G într-un grup ciclic infinit, de unde rezultă concluzia. ∎

Avem următoarea aplicaţie a transferului la studiul elementelor de torsiune dintr-un grup:

Propoziţia 2.3.11. *Fie G un grup ale cărui elemente de torsiune formează o mulţime $S \subseteq G$ finită. Atunci ele formează un subgrup.*

Demonstraţie. Putem presupune că G este generat de S. Evident, mulţimea S e fixată de toate conjugările, deci elementele lui G acţionează prin conjugare pe S. Asta ne dă un morfism ϕ al lui G într-un grup simetric finit, şi nucleul comută cu toate elementele din S; cum S generează G, nucleul lui ϕ este subgrup central de indice finit în G.

Corolarul 2.3.7 ne spune acum că pentru $n = |\mathrm{Im}(\phi)|$, $x \mapsto x^n$ este morfismul de transfer. Pentru că toţi x^n sunt centrali, $x \mapsto x^{kn}$ este morfism pentru orice k. Dacă alegem acum k care să fie divizibil cu ordinele tuturor elementelor din S, din faptul că $x \mapsto x^{kn}$ este aplicaţie multiplicativă rezultă că S este mulţime închisă la înmulţire, deci subgrup al lui G. ∎

Tehnici asemănătoare se pot aplica la studiul elementelor cu clasă finită de conjugare dintr-un grup. Pentru un grup G, vom nota cu $\Delta(G)$ mulţimea elementelor a căror clasă de conjugare este finită. Cu $\Delta^+(G)$ notăm mulţimea elementelor de torsiune din $\Delta(G)$. $\Delta(G)$ se mai numeşte *centrul finit conjugat* (sau *centrul fc*) al grupului G, şi este un obiect foarte util în studiul algebrei grupale a lui G peste un corp. Apare, de exemplu, în caracterizarea algebrelor grupale care sunt prime sau semiprime. Pentru o discuţie se poate consulta [Pas, prima expunere, Δ-*methods in group rings*]. Ne interesează numai următoarele lucruri, pentru demonstrarea cărora se va aplica morfismul de transfer:

Propoziţia 2.3.12. *Fie G un grup, şi $\Delta = \Delta(G)$, $\Delta^+ = \Delta^+(G)$. Atunci au loc următoarele:*

(a) Δ şi Δ^+ sunt subgrupuri caracteristice ale lui G;

(b) Δ^+ este reuniunea subgrupurilor normale finite din G;

(c) Δ/Δ^+ este grup abelian fără torsiune.

Demonstraţie. (a) Este clar că mulţimile Δ şi Δ^+ sunt fixate (ca mulţimi, nu punctual) de toate automorfismele lui G, deci partea importantă este să arătăm că sunt grupuri. Pentru Δ asta e clar: orice conjugat al lui ab este un produs de conjugaţi ai elementelor a şi b, deci parcurge numai o mulţime finită dacă $a, b \in \Delta$.

Rămâne acum să arătăm că torsiunea într-un grup FC formează grup. Demonstraţia este practic identică celei pentru Propoziţia 2.3.11: se ia ca mulţime S reuniunea claselor de conjugare a două elemente arbitrare a, b. Acum demonstraţia pentru Propoziţia 2.3.11 se poate copia cuvânt cu cuvânt.

(b) Din definiţia lui Δ^+ se vede că toate subgrupurile normale finite ale lui G sunt conţinute în Δ^+. Reciproc, alegem un element $a \in \Delta^+$, şi considerăm grupul H generat de clasa de conjugare a lui a. Este un subgrup normal al grupului iniţial, şi este FC, de torsiune, şi finit generat. E deci suficient să vedem că un grup H FC, de torsiune, şi finit generat este finit.

Printr-un argument folosit de câteva ori până acum, un grup FC şi finit generat are centru de indice finit. Un subgrup de indice finit într-unul finit generat este tot finit generat (rezultat binecunoscut), deci $Z(H)$ este grup abelian, finit generat, şi de torsiune. Din structura grupurilor abeliene finit generate rezultă că $Z(H)$ este finit. Cum $H/Z(H)$ este finit, H trebuie să fie finit.

(c) Cum Δ^+ conţine toate elementele de torsiune, grupul Δ/Δ^+ este într-adevăr fără torsiune. Dar este şi un grup FC, deci Propoziţia 2.3.9 spune că este abelian. ■

Prezentăm acum un rezultat interesant care dă o condiţie suficientă pentru ca un grup finit să fie rezolubil. Nu cunosc sursa, dar pare să fie binecunoscut. În demonstraţia de mai jos (există şi altele) se va face în mod crucial uz de morfismul de transfer.

Propoziţia 2.3.13. *Fie G un grup finit. Presupunem că G are un subgrup maximal (propriu) M care este abelian. Atunci G este rezolubil.*

Demonstraţie. Demonstraţia se face prin inducţie după ordinul lui G. Dacă G are centru netrivial Z, acesta fie este conţinut în M, fie nu este. În cel de-al doilea caz G este generat de M şi Z şi deci este abelian, iar în primul caz trecem la G/Z care are un subgrup maximal M/Z care este abelian. Din ipoteza de inducţie G/Z va fi atunci rezolubil, deci G este şi el rezolubil. Putem deci presupune mai departe că G are centru trivial.

Dacă M este normalizat de un element $g \in G\backslash M$ atunci din nou, am terminat: M este normal (fiind maximal), iar câtul G/M trebuie să fie ciclic de ordin prim. G va fi aşadar rezolubil. Putem acum presupune că normalizatorul lui M este chiar M. Dar atunci, dacă $g \in G \setminus M$, conjugatul gMg^{-1} este diferit de M şi ambele sunt maximale, deci împreună ele generează G. Cum sunt şi abeliene, intersecţia lor va fi subgrup central în G. Conform presupunerii noastre că centrul $Z(G)$ e trivial, rezultă că $gMg^{-1} \cap M = \{1\}$ pentru toţi g din afara lui M.

Acum studiem transferul V de la G la M. Mai precis, scopul este să arăt că $V|_M$ este identitatea pe M. Fie deci $s \in M$ un element, de ordin m, să zicem. Să observăm că în acţiunea lui s pe mulţimea claselor la stânga modulo M, G/M, prin înmulţire la stânga, singura clasă fixată este M. Într-adevăr, dacă $sgM = gM$, atunci s va fi conţinut în $M \cap gMg^{-1}$, şi din discuţia de mai sus, asta implică faptul că $g \in M$. Acelaşi lucru este valabil pentru puterile netriviale ale lui s, şi deci acţiunea prin permutări a lui s pe G/M se descompune într-un ciclu de lungime 1, şi cicli disjuncţi de lungime m.

Ne reamintim acum din demonstraţia pentru Propoziţia 2.3.6 că transferul $V(s)$ se scrie ca un produs de conjugate de puteri s^k unde k parcurge mulţimea lungimilor ciclilor din permutarea indusă de s pe G/M. În cazul nostru am văzut că ciclii au lungime m, mai puţin unul, care are lungime 1. Cum s are ordin m, se vede imediat de aici că $V(s) = s$. Am demonstrat deci ceea ce doream: restricţia lui V la M este identitatea. Va rezulta atunci că $K = \ker(V)$ este un complement normal al lui M, în sensul că G este produsul semidirect al lui K prin M.

Pentru a încheia demonstraţia mai rămâne să arăt că nucleul $K = \ker(V)$ este rezolubil. Să observăm că acţiunea prin conjugare a lui M pe K este *liberă*, adică elementele netriviale din M nu fixează elemente netriviale din K. Asta din presupunerea noastră că centrul este trivial. Un rezultat al lui Burnside ([Bu]) asupra grupurilor care acţionează liber arată că subgrupurile Sylow ale unui asemenea grup sunt fie ciclice, fie grupuri generalizate de cuaternioni; în particular, dacă grupul este abelian, el este ciclic. Asta arată deci că M este de fapt ciclic.

În sfârşit, se poate arăta că un automorfism fără puncte fixe netriviale al unui grup finit fixează un subgrup Sylow. Aplicând asta automorfismului lui K dat de conjugarea cu un generator al lui M, şi folosind faptul că M era maximal în G, dducem că K este de fapt p-grup pentru un prim p. în particular, este rezolubil, şi demonstraţia este încheiată. ∎

Observaţia 2.3.14. În demonstraţia de mai sus, morfismul de transfer ne-a permis să arătăm existenţa acelui grup normal K, atunci când conjugaţii lui M prin elemente din $G \setminus M$ îl intersectează trivial pe M. Un rezultat general al lui Frobenius afirmă că dac a G este grup finit şi $H \leq G$ subgrup astfel încât $gHg^{-1} \cap H = \{1\}$, $\forall g \in G \setminus H$, mulţimea elementelor neconjugate cu elemente din H împreună cu $\{1\}$ formează un subgrup (evident normal). Am evitat aici folosirea acestei teoreme. Toate demonstraţiile cunoscute ale ei folosesc teoria reprezentărilor liniare ale grupurilor finite.

Observaţia 2.3.15. Din rezultatul lui Burnside invocat mai sus care dă structura grupurilor Sylow ale unui grup de automorfisme libere avem nevoie numaid e faptul că pentru un număr prim p, $(\mathbb{Z}/p\mathbb{Z})^2$ nu poate acţiona liber şi fidel pe un grup finit. Pentru asta există o demonstraţie elementară şi nu foarte lungă, dar nu am inclus-o pentru a nu lungi inutil demonstraţia de mai sus.

Aceeaşi remarcă este valabilă şi pentru faptul că un automorfism liber fixează un subgrup Sylow.

O aplicaţie pentru propoziţia anterioară:

Propoziţia 2.3.16. *Fie p_i numere prime distincte cu proprietatea că pentru $i \neq j$, p_i nu divide $p_j - 1$. Atunci orice grup de ordin $\prod p_i$ este ciclic.*

Demonstraţie. Demonstraţia se face prin inducţie după ordin. Pentru cazul când avem un singur număr prim e clar, şi ipoteza de inducţie ne spune acum că e satisfăcută ipoteza din Propoziţia 2.3.13. Rezultă că grupul este rezolubil. Dacă H este um subgrup normal propriu şi netrivial, atunci este abelian din ipoteza de inducţie, şi din ipoteza asupra numerelor p_i rezultă că de fapt este central. Dar asta înseamnă că grupul nostru este de fapt nilpotent, deci este produsul subgrupurilor sale Sylow. Asta încheie demonstraţia. ∎

Observaţia 2.3.17. Se poate arătă că numerele de forma $\prod p_i$ ca în enunţ sunt singurele numere naturale n cu proprietatea că orice grup de ordin n este ciclic.

Observaţia 2.3.18. Demonstraţia precedentă se poate modifica foarte uşor astfel încât să rezulte faptul că un grup G cu proprietatea că divizorii primi ai lui $|G|$ sunt p_i şi cu grupuri Sylow ciclice este ciclic.

Propoziţia următoare este un caz particular al teoremei lui Frobenius menţionată în Observaţia 2.3.14. Demonstraţia va folosi tehnica din Propoziţia 2.3.13, unde am văzut că în anumite condiţii, transferul $V : G \to H$ într-un subgrup abelian H al unui grup finit G are proprietatea că restricţia $V|_H$ este identitatea.

Propoziţia 2.3.19. *Fie G un grup finit, şi $H \leq G$ un subgrup rezolubil cu următoarea proprietate: pentru orice element $s \in G \setminus H$, conjugatul sHs^{-1} se intersectează trivial cu H. Atunci H are un complement normal (subgrup normal N astfel încât $G = N \rtimes H$).*

Demonstraţie. Demonstrăm afirmaţia pentru H abelian. În acest caz, se arată ca în demonstraţia pentru Propoziţia 2.3.13 că acţiunea oricărui element x din H prin înmulţire la stânga pe mulţimea G/H a claselor de echivalenţă la stânga modulo H se descompune în cicluri de lungime egală cu ordinul lui x, mai puţin un ciclu de lungime 1. Va rezulta atunci că restricţia transferului la H este identitatea. Nucleul transferului va fi acum complementul normal căutat N.

Mai departe, facem inducţie după ordinul lui H. Exact ca mai sus se arată că restricţia transferului $V : G \to H_{ab}$ la H este proiecţia naturală $H \to H_{ab}$. H a fost presupus rezolubil, deci în particular H_{ab} va fi netrivial. Asta înseamnă că subgrupul normal $K = \ker(V)$ este strict mai mic decât G. De asemenea, $H' = K \cap H$ (subgrupul derivat al lui H) este strict mai mic decât H. Este clar acum că perechea de grupuri (K, H') satisface condiţia pe care prin ipoteză o satisface perechea (G, H): dacă un conjugat sHs^{-1}, $s \in K$ intersectează netrivial grupul H', atunci s trebuie să aparţină lui H, din ipoteză. Dar asta înseamnă că $s \in H' = K \cap H$.

Acum aplicăm ipoteza de inducţie perechii (K, H'), şi concluzia este că avem un complement normal N al lui H' în K. Din argumentul (folosit până acum în repetate rânduri) privind acţiunea lui H pe G/H prin înmulţire la stânga se vede că ordinul lui H şi indicele lui în G sunt prime între ele. Asta înseamnă că există o mulţime finită P de numere prime astfel încât N să fie subgrupul lui K generat de elementele de ordin putere a unui prim din P. Asta arată clar că N este de fapt subgrup caracteristic al lui K (adică este fixat de orice automorfism al lui K). Fiind subgrup caracteristic al unui subgrup normal $K \trianglelefteq G$, este normal în G. Asta încheie demonstraţia. ∎

Observaţia 2.3.20. În rezultatul mai tare datorat lui Frobenius (pe care l-am menţionat în Observaţia 2.3.14) nu se pune ipoteza ca H să fie rezolubil; se demonstrează până la urmă că aceasta are loc automat, dar asta se arată folosind teorema lui Frobenius.

Demonstraţia de mai sus ar funcţiona şi pentru rezultatul mai tare dacă am arăta că un subgrup $H \leq G$ ca în enunţ este rezolubil (sau mai general, nu este perfect). Am avea astfel o demonstraţie nouă a teoremei lui Frobenius.

Ne mai propunem acum să folosim în această secţiune rezultate asupra transferului (şi în general asupra morfismelor de cortestricţie în coomologie sau corestricţie în omologie) pentru a determina structura grupurilor cu subgrupuri Sylow ciclice (Teorema 2.3.24). Un asemenea rezultat, pe care îl enunţăm fără demonstraţie, este următoarea descriere a părţii p-primare a (co)omologiei unui grup finit G, datorată lui Swan. Pentru o demonstraţie se poate consulta de exemplu [Th, Lema 3.4]. Vom folosi notaţia $A_{(p)}$ pentru a desemna partea p-primară a unui grup abelian de torsiune (adică elementele al căror ordin este o putere a numărului prim p).

Propoziţia 2.3.21 (Swan)**.** *Fie G un grup finit, G_p un subgrup Sylow abelian al său, şi N_p normalizatorul lui G_p. Atunci pentru orice G-modul A şi $* \geq 1$, $H^*(G, A)_{(p)}$ este izomorf cu $H^*(G_p, A)^{N_p}$, subgrupul lui $H^*(G_p, A)$ alcătuit din elementele fixate de acţiunea lui N_p pe $H^*(G_p, A)$. Analog, pentru $* \geq 1$, $H_*(G, A)_{(p)}$ este izomorf cu $H_*(G_p, A)^{N_p}$.*

Observaţia 2.3.22. [Th, Lema 3.4] este enunţată mai succint, folosind coomologia Tate a unui grup finit, care înglobează atât coomologia cât şi omologia. Cum noi nu am introdus aici coomologia Tate, am adaptat enunţul.

O consecinţă a acestui rezultat este următoarea:

Corolarul 2.3.23 (Teorema complementului normal a lui Burnside)**.** *Fie G un grup finit şi G_p un p-subgrup Sylow al lui G conţinut în centrul normalizatorului său N_p. Atunci G_p are un complement normal în G (un subgrup normal $K \trianglelefteq G$ cu $G = KG_p$, $K \cap G_p = \{1\}$).*

Demonstraţie. Pentru că G_p este abelian (fiind inclus în centrul normalizatorului său), transferul este un morfism $V : G \to G_p$. Pentru a obţine concluzia dorită, este suficient să arătăm că restricţia lui V la G_p este un automorfism al lui G_p. Vom folosi Propoziţia 2.3.21 pentru omologia H_1 (cu valori în G-modulul trivial $\mathbb{Z}$).

Ştim din Propoziţia 1.3.5 că aplicaţia $\mathrm{Cor}^G_{G_p} \circ \mathrm{Res}^G_{G_p} : H_1(G) \to H_1(G)$ este înmulţirea cu numărul $[G : G_p]$. Cum acesta nu se divide cu p, restricţia transferului $V : G_{ab} \to G_p$ la $(G_{ab})_{(p)}$ trebuie să fie injectivă. Dar Propoziţia 2.3.21 pentru H_1 spune că $(G_{ab})_{(p)}$ este izomorf cu $G_p^{N_p} = G_p$ (ultima egalitate având loc pentru că N_p centralizează G_p). Pe de altă parte, să observăm că $(G_{ab})_{(p)}$ este chiar imaginea lui G_p prin $G \to G_{ab}$. Rezultă de aici că într-adevăr, $V|_{G_p} : G_p \to G_p$ este izo, ceea ce doream să demonstrăm. ■

În sfârşit, teorema lui Burnside asupra grupurilor cu subgrupuri Sylow ciclice la care am făcut referire mai sus este:

Teorema 2.3.24 (Burnside)**.** *Fie G un grup finit cu subgrupuri Sylow ciclice. Atunci G este produs semidirect de două grupuri ciclice cu ordine prime între ele.*

Demonstraţie. Fie G un grup finit cu subgrupuri Sylow ciclice. Dacă p este cel mai mic număr prim care divide ordinul lui G, atunci grupul automorfismelor unui subgrup Sylow G_p de ordin p^n, să zicem, este $p^{n-1}(p-1)$. Din minimalitatea lui p rezultă că normalizatorul N_p al lui G_p în G centralizează G_p, deci se poate aplica Corolarul 2.3.23. G_p are deci un complement normal în G. Prin inducţie după numărul de divizori primi ai lui $|G|$ se arată acum că dacă p este cel mai *mare* divizor prim al lui $|G|$, atunci subgrupul Sylow G_p este normal în G.

Vom face acum inducţie după numărul de divizori primi ai lui $|G|$, cazul când G este ciclic fiind trivial. Tot ce ne interesează din argumentul de mai sus este concluzia că G are un subgrup Sylow G_p normal. Fie t un generator al acestui grup (presupus ciclic prin ipoteză). Avem acum două cazuri:

(a) t este central în G.

Aplicând din nou Corolarul 2.3.23 grupului Sylow $G_p = \langle t \rangle$, va rezulta că G este (izomorf cu) produsul direct $G_p \times (G/G_p)$. Subgrupul derivat al lui G coincide atunci cu subgrupul derivat al lui G/G_p, care din ipoteza de inducţie este un subgrup Hall (adică entru care ordinul şi indicele sunt prime între ele) ciclic, şi am terminat.

(b) t nu este central.

Există atunci un element $a \in G$ de ordin prim cu p astfel încât $ata^{-1} = t^k$, unde $p \not| k-1$. Asta înseamnă că t^{k-1} este comutatorul $[a,t] = ata^{-1}t^{-1}$; cum $p \not| k-1$, t^{k-1} generează G_p. Vom avea deci $G_p \leq G'$. Subgrupul derivat al lui G/G_p este G'/G_p, şi va fi ciclic (şi subgrup Hall al lui G/G_p) din ipoteza de inducţie. Cum G_p este un subgrup abelian normal în G, avem o acţiune prin conjugare a lui G/G_p pe G_p. Asta ne dă un morfism $G/G_p \to \mathrm{Aut}(G_p)$. Cum cel de-al doilea grup este abelian, $G'/G_p = (G/G_p)'$ acţionează trivial pe G_p. Asta înseamnă că G' este abelian (deci ciclic pentru că are subgrupuri Sylow ciclice), şi din faptul că G'/G_p este subgrup Hall al lui G/G_p şi G_p este Hall în G rezultă acum că G' este subgrup ciclic Hall al lui G, c.c.t.d. ∎

Dintre multele aplicaţii ale transferului, mai menţionez aici doar faptul că el apare în mod natural în teoria algebrică a numerelor, în studiul corpului claselor şi al reciprocităţii Artin. De exemplu, un rezultat important în acest context este faptul că dacă G este un grup finit generat, atunci transferul de la G/G' la G'/G'' este trivial ([AT]); asta se foloseşte la demonstraţia faptului că idealele prime ale unui corp de numre algebrice devin principale după trecerea la corpul claselor al lui Hilbert asociat corpului iniţial.

2.4. **Teorema Artin-Schreier.** Vom demonstra aici o caracterizare binecunoscută, datorată lui Artin şi Schreier, a corpurilor cu proprietatea că închiderea lor algebrică este o extensie (proprie) finită. Deşi de obicei demonstraţiile care se dau sunt elementare, aici obţinem rezultatul folosind coomologia grupurilor ciclice finite (Teorema 2.2.4).

Reamintim că un corp k se numeşte *real închis* dacă (a) are o structură de corp ordonat astfel încât orice element nenegativ este pătratul unui element, şi (b) orice polinom peste k de grad impar are o rădăcină în k. Să observăm că ordinea de la (a) este unic definită numai de structura algebrică a corpului, elementele nenegative fiind exact pătratele. Acestea sunt corpuri care au proprietăţi foarte asemănătoare cu $\mathbb{R}$, în sensul că pentru ele se poate demonstra un analog al Teoremei Funademntale a Algebrei. Pe noi însă ne interesează aici o reciprocă a acesteia.

În afară de exemplul evident al numerelor reale, un exemplu de corp algebric închis ar fi cel al numerelor algebrice reale. Analog, se pot obţine alte exemple în felul următor: se ia orice corp algebric închis conţinut în $\mathbb{C}$ şi se consideră mulţimea elementelor reale ale sale. Corpul numerelor reale este cel mai mare, iar cel al numerelor reale algebrice cel mai mic corp obţinut aşa. Se poate arăta că toate acestea sunt neizomorfe, deci avem o clasă bogată de exemple.

Am menţionat mai sus că pentru un corp real închis k are loc un analog al Teoremei Fundamentale a Algebrei. Mai precis, avem:

Teorema 2.4.1. *Fie k un corp real închis. Atunci $k(\sqrt{-1})$ este algebric închis.*

Nu vom demonstra asta aici complet. Există demonstraţii ale Teoremei Fundamentale a Algebrei ($\mathbb{C}$ este algebric închis) care funcţionează cuvânt cu cuvânt în acest cadru mai general. Rezultatul de bază al acestei secţiuni este următoarea reciprocă (dar care conţine parţial şi afirmaţia din teorema de mai sus):

Teorema 2.4.2 (Artin-Schreier)**.** *Fie k un corp care nu este algebric închis, dar a cărui închidere algebrică K are grad finit peste k. Atunci k este real închis, şi $K = k(i)$, unde i este o rădăcină pătrată a lui -1.*

Demonstraţie. Începem prin a observa că de fapt extinderea K/k este Galois: este evident normală pentru că K este algebric închis, şi este separabilă pentru că altfel K ar fi pur inseparabil peste un subcorp al său, şi deci aplicaţia $x \mapsto x^{\mathrm{char}(k)}$ nu ar fi surjectivă pe K, ceea ce este absurd. Vom nota cu G grupul Galois al extensiei, dar pe parcursul demonstraţiei corpul k se va mai modifica, fiind înlocuit cu diverse extensii ale sale; de fiecare dată G va desemna grupul Galois al lui K/k. Demonstraţia se face în câţiva paşi.

Pasul 1. Aici demonstrez că ordinul grupului G este prim cu $\mathrm{ep}(k)$, exponentul caracteristic al lui k. Reamintim că acesta este caracteristica lui k dacă $\mathrm{char}(k) \neq 0$, şi 1 dacă $\mathrm{char}(k) = 0$.

Presupunem că nu este aşa. Atunci, înlocuind G cu un subgrup ciclic de ordin $p = \mathrm{ep}(k)$ şi k cu corpul fixat de acest grup ciclic, putem presupune că G este ciclic de ordin $p = \mathrm{ep}(k) = \mathrm{char}(k)$. Dacă $F : K \to K$ reprezintă morfismul aditiv $x \mapsto x^p - x$, vom avea un şir exact scurt de G-module

$$0 \longrightarrow \mathbb{F}_p \longrightarrow K \xrightarrow{F} K \longrightarrow 0, \tag{2.4.1}$$

unde K aici reprezintă G-modulul aditiv K, iar $\mathbb{F}_p$ este corpul prim al lui k. O porţiune a şirului exact lung de coomologie asociat va fi

$$H^1(G, K) \longrightarrow H^2(G, \mathbb{F}_p) \longrightarrow H^2(G, K).$$

Termenii din capete sunt nuli; am făcut observaţia aceasta în Secţiunea 1.6, chiar la sfârşit. Se poate demonstra folosind Teorema Bazei Normale, şi pentru o demonstraţie se poate consulta [Se2, X §1]. Asta înseamnă că şi termenul din mijloc este nul. Dar grupul ciclic de ordin p G acţionează trivial pe $\mathbb{F}_p$, şi atunci Teorema 2.2.4 arată că H^2 este ciclic de ordin p. Am obţinut deci contradicţia căutată.

Pasul 2. Acum vom fixa un număr prim p care divide ordinul lui G, şi vom înlocui G cu un p-subgrup abelian maximal al său, şi k cu corpul fixat de acest grup. Conform pasului 1, k nu are caracteristică p. Scopul pasului 2 este să arătăm că G acţionează fidel pe grupul rădăcinilor unităţii de ordin putere a lui p.

Notăm cu $T : K^* \to K^*$ morfismul $x \mapsto x^p$ de grupuri multiplicative. Dacă μ_p este grupul rădăcinilor unităţii de ordin p din K, avem şirul exact scurt de G-module

$$0 \longrightarrow \mu_p \longrightarrow K^* \xrightarrow{T} K^* \longrightarrow 0. \tag{2.4.2}$$

μ_p este grup de ordin p pentru că $\mathrm{char}(k) \neq p$, şi G acţionează trivial pe μ_p (G este p-grup, şi grupul automorfismelor lui μ_p are ordin $p-1$). O porţiune a şirului lung de coomologie este

$$H^0(G, K^*) \xrightarrow{T} H^0(G, K^*) \longrightarrow H^1(G, \mu_p) \longrightarrow H^1(G, K^*).$$

Ultimul termen este nul (Teorema 90 a lui Hilbert; [Se2, X §1]), iar primul morfism este pur şi simplu ridicarea la puterea p în k^*, adică elementele lui K^* fixate de G. Teorema 2.2.4 arată că $H^1(G, \mu_p)$ este nenul, deci ridicarea la puterea p pe k este nesurjectivă.

Fie $a \in k^* \setminus (k^*)^p$. Dacă întregul grup μ_{p^∞} al rădăcinilor de ordin putere a lui p ar fi conţinut în k, atunci e uşor de văzut că polinomul $X^{p^n} - a$ ar fi ireductibil de grad p^n peste k, contrazicând $[K : k] < \infty$. Rezultă deci că k nu conţine tot μ_{p^∞}. Aplicând acest raţionament şi corpului obţinut prin adjuncţionarea lui μ_{p^∞} la k, tragem concluzia că $K = k(\mu_{p^\infty})$. Cu alte cuvinte, G acţionează fidel pe grupul rădăcinilor unităţii de ordin putere a lui p.

Pasul 3. Aici vom arăta, folosind rezultatul de la pasul 2, că $\mathrm{char}(k) = 0$, că grupul iniţial G era de ordin 2, şi că G nu fixează rădăcinile pătrate ale lui -1 (deci $K = k(\sqrt{-1})$).

Presupunem mai întâi că $\mathrm{char}(k) = q \neq 0$, şi facem raţionamentul de la pasul 2 pentru un număr prim p care divide $|G|$. Atunci rezultă că un p-subgrup abelian maximal se scufundă în grupul Galois absolut al corpului cu p elemente. Dar este binecunoscut că acest grup Galois este izomorf cu $\hat{\mathbb{Z}}$, completarea lui $\mathbb{Z}$ în raport cu topologia definită de toate subgrupurile sale netriviale. În particular, avem o scufundare a unui grup finit de torsiune într-unul fără torsiune, absurd.

În caracteristică nulă pe de altă parte, este uşor de văzut că μ_{p^∞} este izomorf cu $\mathbb{Q}_p/\mathbb{Z}_p$, grupul aditiv al corpului numerelor p-adice factorizat prin grupul întregilor p-adici. Acest grup este dualul Pontrjagin al lui $\mathbb{Z}_p$, şi deci grupul automorfismelor sale este U_p, grupul unităţilor p-adice (elementele inversabile din inelul $\mathbb{Z}_p$). Dacă facem acum raţionamentul de la pasul 2 pentru un p-subgrup abelian maximal G_p al lui G, vedem că acesta este scufundat în U_p. Mai mult, dacă U_p^1 este grupul unităţilor p-adice congruente cu 1 modulo p, atunci U_p/U_p^1 are ordinul $p - 1$. Rezultă că G_p se scufundă în U_p^1. Dar structura grupurilor U_p^1 este binecunoscută (de exemplu [Iw, Prop. 2.7]): U_p^1 este izomorf cu $\mathbb{Z}_p$ dacă $p \neq 2$, şi cu $\mathbb{Z}_2 \times (\mathbb{Z}/2)$ dacă $p = 2$.

Concluzia este că G nu are p-subgrupuri abeliene netriviale pentru $p \neq 2$, şi un 2-subgrup abelian maximal al lui G are ordin 2. De aici rezultă că $|G| = 2$. Mai mult, torsiunea lui U_2^1 constă exact din $\{\pm 1\}$. Din felul în care se realizează U_2^1 ca grup de automorfisme ale lui $\mu_{2^\infty} \cong \mathbb{Q}_2/\mathbb{Z}_2$ se vede că $-1 \in U_2^1$ nu fixează rădăcinile primitive de ordin patru ale unităţii, adică $K = k(\sqrt{-1})$.

Pasul 4. Aici încheiem demonstraţia, arătând că k poate fi ordonat astfel încât toate elementele pozitive să fie pătrate. Din faptul că închiderea algebrică a lui k are grad doi peste k rezultă imediat afirmaţia asupra polinoamelor de grad impar din definiţia corpului real închis.

O ordine este definită dacă spunem cine este conul P elementelor (strict) pozitive. Concluzia la care vrem să ajungem forţează ca acesta să fie mulţimea pătratelor (vom lucra cu nenule). Din porţiunea şirului de coomologie asociat lui (2.4.2) folosită în pasul 2 se vede că indicele lui $(k^*)^2$ în k^* este egal cu ordinul lui $H^1(G, \mu_2)$, adică 2. Cum -1 nu este pătrat în k (pasul 3), avem $P \cup -P = k^*$, şi reuniunea este disjunctă. Tot ce mai trebuie să arătăm este că P este închis la adunare; cu alte cuvinte, că o sumă de pătrate $a^2 + b^2$ este tot pătrat.

$a^2 + b^2$ este norma elementului $a + b\sqrt{-1} \in K$, şi ceea ce dorim se reduce la a arăta că norma $N : K^* \to k^*$ are imaginea $(k^*)^2$. Evident, $N(K^*) \supseteq (k^*)^2$. Cum $|k^*/(k^*)^2| = 2$, incluziunea inversă va rezulta dacă arătăm că $N(K^*)$ este conţinut strict în k^*. O altă porţiune a şirului lung de coomologie pentru (2.4.2) ne dă

$$H^1(G, K^*) \longrightarrow H^2(G, \mu_2) \longrightarrow K^2(G, K^*).$$

Primul termen este nul (Teorema 90 a lui Hilbert), al doilea este ciclic de ordin doi, iar al treilea este chiar $k^*/N(K^*)$, din Teorema 2.2.4. Rezultă deci că într-adevăr $N(K^*) \neq k^*$, şi demonstraţia este încheiată. ■

Câteva consecinţe, utile în studiul grupurilor Galois:

Corolarul 2.4.3. *Fie k un corp, şi K închiderea sa algebrică. Dacă grupul Galois G al lui K peste k are torsiune, atunci k se poate ordona (în particular $\mathrm{char}(k) = 0$), şi subgrupurile finite maximale ale lui G au ordin doi.*

Corolarul 2.4.4. *Normalizatorul (sau echivalent, centralizatorul) unui element a de ordin doi al grupului Galois absolut al lui $\mathbb{Q}$ este grupul generat de a.*

Demonstraţie. Un element care comută cu a acţionează pe corpul K fixat de a. Dar conform teoremei, K este real închis. Am remarcat mai sus că automorfismele corpurilor real închise conservă şi ordinea. Se ştie că un corp ordonat are o "închidere" ordonată, adică un corp real închis şi algebric peste corpul dat, şi această extensie e unică până la izomorfism de extensii.

În cazul nostru, va rezulta că extensia $\mathbb{Q} \subset K$ este izomorfă cu incluziunea lui $\mathbb{Q}$ în corpul numerelor algebrice reale. Asta înseamnă că $\mathbb{Q}$ este dens în K (în raport cu topologia dată de ordine), şi deci K nu are automorfisme netriviale. Am arătat deci că t fixează K punctual, şi t trebuie să fie atunci sau trivial, sau a. ■

Observaţia 2.4.5. Demonstraţia funcţionează de fapt pentru orice corp de numere (extensie finită a lui $\mathbb{Q}$) care are cel puţin o scufundare în $\mathbb{R}$.

Asta implică imediat

Corolarul 2.4.6. *Grupul Galois absolut $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ are centru trivial.*

Observaţia 2.4.7. Demonstraţia pentru acest ultim rezultat este valabilă în cazul mai general când în locul lui $\mathbb{Q}$ avem un corp de numere care are o scufundare în $\mathbb{R}$ (Observaţia 2.4.5). De fapt, acest ultim corolar este valabil pentru *orice* corp de numere, dar demonstraţia rezultatului general este mai complicată.

2.5. **Extensii centrale şi reprezentări proiective.** Vom introduce aici noţiunea de multiplicator Schur, pe care o vom folosi pentru studiul extensiilor centrale de grupuri şi al reprezentărilor proiective, adică al morfismelor unui grup dat la grupul proiectiv liniar. La sfârşitul secţiunii vom vedea nişte aplicaţii ale acestei discuţii.

Ne interesează acum mai ales G-modulele triviale; pentru acestea ne vom aplica teorema de clasificare a lui Schreier (Teorema 2.1.4) şi vom vedea că în anumite condiţii, există o asemenea extensie "universală" pentru grupul dat G.

Definiţia 2.5.1. *Multiplicatorul Schur* al unui grup G, notat şi cu $M(G)$, este grupul $H_2(G, \mathbb{Z})$, unde $\mathbb{Z}$ este G-modul trivial.

Să ne amintim de şirul (1.7.2) ce apare în Teorema Coeficienţilor Universali (Teorema 1.7.1) pentru $n = 2$:

$$0 \longrightarrow \operatorname{Ext}(H_1(G), A) \longrightarrow H^2(G, A) \longrightarrow \operatorname{Hom}(H_2(G), A) \longrightarrow 0, \tag{2.5.1}$$

pentru orice G-modul trivial A. Teorema spunea că el este natural în A şi că scindează, dar scindarea nu este naturală.

Mai ştim din Teorema 2.1.4 că $H^2(G, A)$ clasifică până la echivalenţă extensiile centrale ale lui A prin G (centrale în sensul că A este subgrup central în extensia rezultată, pentru că G acţionează trivial pe A). Vom nota cu $\mathcal{E}xt_c(G, A)$ mulţimea claselor de echivalenţă pentru asemenea extensii. Functorul $H^2(G, -) \cong \mathcal{E}xt_c(G, -)$ este un endofunctor al categoriei $\mathcal{A}b$, şi se pune în mod firesc întrebarea când/dacă el este reprezentabil.

Dacă G_{ab} este liber abelian, atunci este clar că $H^2(G, -)$ va fi reprezentat chiar de $M(G)$. Partea interesantă este că are loc şi reciproca:

Propoziţia 2.5.2. *$\mathcal{E}xt_c(G, -)$ este reprezentabil dacă şi numai dacă abelianizatul $G_{ab} \cong H_1(G)$ este abelian liber, caz în care obiectul care reprezintă functorul este multiplicatorul Schur $M(G) = H_2(G)$.*

Demonstraţie. Am observat deja că dacă $G_{ab} = 0$, nu e nimic de arătat: $\operatorname{Ext}(H_1(G), -)$ se anulează, şi (2.5.1) arată că avem un izomorfism natural $H^2(G, -) \cong \operatorname{Hom}(M(G), -)$.

Reciproc, să presupunem că $H^2(G, -)$ este reprezentat de un grup abelian X. Ultimul morfism din şirul (2.5.1) spune că avem o transformare naturală de la $\operatorname{Hom}(X, -)$ la $\operatorname{Hom}(M(G), -)$. Din lema Yoneda ([MacL, III §2]; funcţionează şi pentru categoria $\mathcal{A}b$, nu numai pentru **Set**), transformarea respectivă este dată de un morfism de grupuri $f : M(G) \to X$.

Acum vom considera functorii coinduşi $\operatorname{Hom}(M(G), -)$ şi $\operatorname{Hom}(X, -)$ ca functori nu pe întreg $\mathcal{A}b$, ci numai pe categoria $\mathcal{C}$ a grupurilor abeliene injective (sau echivalent, divizibile). Dar pe $\mathcal{C}$ functorul $\operatorname{Ext}(H_1(G), -)$ e nul, deci (2.5.1) spune că $f : M(G) \to X$ induce un izomorfism natural f^* între functorii reprezentaţi de cele două grupuri pe categoria $\mathcal{C}$. De aici rezultă însă că f este izo: dacă nu ar fi surjectiv atunci incluziunea lui $X/f(M(G))$ într-un grup divizibil ar fi un morfism nenul care compus cu f devine nul, şi dacă f nu este injectiv atunci scufundarea lui $M(G)$ într-un grup divizibil nu s-ar afla în imaginea lui f^*.

Rezultă din toate acestea că de fapt ultimul morfism din şirul (2.5.1) ne dă un izomorfism natural de functori (când A variază), şi deci $\operatorname{Ext}(G_{ab}, -)$ se anulează. Dar asta e echivalent cu a spune că G_{ab} este grup abelian proiectiv, deci abelian liber. ■

Observaţia 2.5.3. Demonstraţia funcţionează şi pentru cazul general dat de Teorema Coeficienţilor Universali, când n este arbitrar (Teorema 1.7.1, şirul (1.7.2)). Puteam, cu alte cuvinte, să arătăm că endofunctorul $H^n(G, -)$ pe categoria $\mathcal{A}b$ este reprezentabil dacă şi numai dacă $H_{n-1}(G)$ este abelian liber, şi în acest caz obiectul de reprezentare este $H_n(G)$. Ne-a interesat însă cazul $n = 2$ pentru că avem o interpretare alternativă a lui $H^2(G, -)$ ca $\mathcal{E}xt_c(G, -)$.

Propoziţia anterioară ne dă, în cazul când G_{ab} este abelian liber, o extensie centrală

$$(U) : 0 \longrightarrow M(G) \longrightarrow U \longrightarrow G \longrightarrow 0$$

cu următoarea proprietate de universalitate: pentru orice extensie centrală

$$(E) : 0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0,$$

există un unic morfism $f : M(G) \to A$ astfel încât următoarea diagramă să fie comutativă:

$$\begin{tikzcd}
0 \arrow[r] & M(G) \arrow[r] \arrow[d, "f"'] & U \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\
0 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 0
\end{tikzcd}$$

Să observăm însă că morfismul $U \to E$ rezultat ne e neapărat universal. De această proprietate mai tare de universalitate ne ocupăm mai departe.

Vom nota cu $\mathcal{E}xt_c(G)$ categoria morfismelor surjective $\pi : E \to G$ cu proprietatea că nucelul lui π este central în E. Se subînţelege că morfismele de la $\pi : E \to G$ la $\pi' : E' \to G$ sunt morfismele de grupuri $f : E \to E'$ cu $\pi' \circ f = \pi$. Se vede imediat că proprietatea de universalitate despre care am vorbit în paragraful precedent se rezumă la a da un obiect iniţial în $\mathcal{E}xt_c(G)$. Avem

Definiţia 2.5.4. O *extenie centrală universală* a lui G este o extensie

$$0 \longrightarrow X \longrightarrow U \xrightarrow{\pi} G \longrightarrow 0$$

pentru care π este obiect iniţial în $\mathcal{E}xt_c(G)$.

Se pune întrebarea când un grup G are o asemenea extensie centrală universală. Răspunsul este dat de

Propoziţia 2.5.5. *Grupul G are o extensie centrală universală $U \to G$ dacă şi numai dacă este perfect, adică $G_{ab} = 0$.*

Demonstraţie. Să presupunem că avem o extensie centrală universală $\pi : U \to G$. Dacă abelianizatul G_{ab} nu e nul, atunci există morfisme netriviale de la G la un grup abelian A. Dar grupul acestor morfisme este chiar $Z^1(G, A) \cong \mathrm{Hom}(G, A)$ (cociclii sunt morfisme pentru că A este G-modul trivial), care, aşa cum am remarcat ceva mai sus în Observaţia 2.1.7, poate fi identificat cu grupul automorfismelor stabilizatoare ale unei estensii (centrale în cazul de faţă) E a lui A prin G. Dar atunci morfismul de la U la E care face comutativă diagrama

$$\begin{tikzcd}
U \arrow[r, "\pi"] \arrow[d] & G \\
E \arrow[ur] &
\end{tikzcd}$$

nu va mai fi unic, putând fi compus cu automorfisme stabilizatoare netriviale ale lui E. Cum $U \to G$ a fost presupusă universală, trebuie într-adevăr să avem $G_{ab} = 0$.

Reciproc, să presupunem că G este perfect. Atunci Propoziţia 2.5.2 ne spune că $H^2(G,-)$ este reprezentat de $M(G)$. Afirm că extensia

$$0 \longrightarrow M(G) \longrightarrow U \longrightarrow G \longrightarrow 0$$

dată de proprietatea de universalitate a lui $M(G)$ este extensie centrală universală în sensul mai strict al definiţiei precedente. Într-adevăr, reprezentabilitatea lui $H^2(G,-)$ spune că pentru orice extensie centrală

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0$$

vom avea o diagramă

$$\begin{tikzcd} 0 \arrow[r] & M(G) \arrow[r] \arrow[d, "f"] & U \arrow[r] \arrow[d, "g"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 0 \end{tikzcd}$$

f este unic din universalitatea lui $M(G)$. Tot faptul că $H^2(G,-)$ este reprezentat de $M(G)$ prin intermediul extensiei $U \to G$ ne mai spune şi că g este unic până la compuneri cu automorfisme stabilizatoare ale extensiei $E \to G$. Ca şi în implicaţia precedentă, identificăm grupul de automorfisme stabilizatoare cu $Z^1(G,-) \cong \mathrm{Hom}(G,-)$, grup care este trivial pentru că G este perfect. ∎

Observaţia 2.5.6. Am folosit până acum în mod tacit următoarea descriere a morfismului $f_* : H^2(G,A) \to H^2(G,B)$ indus de un morfism de G-module $f : A \to B$ în interpretarea lui H^2 ca extensii: clasa extensiei

$$(F) : 0 \longrightarrow B \longrightarrow F \longrightarrow G \longrightarrow 0$$

este f_* aplicat clasei de echivalenţă a extensiei

$$(E) : 0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0$$

dacă şi numai dacă avem o diagramă comutativă

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & E \arrow[r] \arrow[d, "g"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & B \arrow[r] & F \arrow[r] & G \arrow[r] & 0 \end{tikzcd}$$

În acest caz se vede uşor că g este unic până la compuneri cu automorfisme stabilizatoare ale extensiei (F).

Următorul rezultat pe care îl vom trata nu este propriu-zis o aplicaţie a noţiunilor universale de mai sus; el ar putea apărea de exemplu în Secţiunea 2.1, unde apare clasificarea extensiilor prin intermediul lui H^2. Pare însă natural să îl includem aici, pentru că în demonstraţie apar mai ales extensii centrale şi tehnici foarte asemănătoare celor folosite până acum în această secţiune.

Ne punem următoarea problemă foarte naturală: există oare grupuri finite arbitrar de mari cu puţine automorfisme? Pentru a formula riguros, introducem o notaţie. Pentru un număr natural $n \in \mathbb{N}^*$ fie $\phi(n)$ cel mai mic număr de forma $|\mathrm{Aut}(G)|$ cu G grup de ordin n, unde $\mathrm{Aut}(G)$ este grupul automorfismelor lui G. Întrebarea este: e adevărat că limita la infinit a lui ϕ este infinit? Răspunsul se dovedeşte a fi afirmativ.

Propoziţia 2.5.7. *Pentru orice număr natural N există un număr natural n_0 astfel încât orice grup finit cu $\geq n_0$ elemente să aibă cel puţin N automorfisme.*

Demonstraţie. Începem cu observaţia că este foarte uşor de arătat că afirmaţia din enunţ are loc dacă lucrăm cu grupuri abeliene. Cu alte cuvinte, dacă în enunţ înlocuim cuvântul "grupurile" cu "grupurile abeliene", afirmaţia rezultată este uşor de demonstrat. Se foloseşte teorema de structură a grupurilor abeliene finite, etc.

Presupunem acum contrariul afirmaţiei din enunţ. Asta înseamnă că există un şir infinit de grupuri E_n, $n \geq 1$ cu proprietatea că ordinul lui E_n tinde la infinit, dar $|\mathrm{Aut}(E_n)|$ este mărginit. Asta înseamnă în primul rând că grupurile $\mathrm{Out}(E_n) = \mathrm{Aut}(E_n)/\mathrm{Inn}(E_n)$ ale automorfismelor exterioare ale grupurilor E_n au ordine mărginite. Dar $\mathrm{Out}(E_n)$ este izomorf cu câtul lui E_n prin centrul său $A_n = Z(E_n)$, deci indicii $|E_n/A_n|$ formează un şir mărginit. Asta înseamnă că grupurile E_n/A_n parcurg numai o mulţime finită de clase de izomorfism, deci putem presupune că E_n/A_n sunt toate izomorfe cu un acelaşi grup finit G. Lucrăm deci acum cu extensii centrale ale unor grupuri A_n prin grupul G.

Grupurile A_n se scriu ca sume directe de grupuri ciclice. Extensia $E_n \to G$ este dată de o clasă de coomologie din $H^2(G, A_n)$, deci este reprezentată de un 2-cociclu al lui G cu valori în G-modulul trivial A_n. Vom presupune că divizorii primi ai lui $|A_n|$ se află printre cei ai lui $|G|$, pentru că Propoziţia 2.1.8 arată uşor că oricum sumandul lui A_n ce constă din elementele de ordin prim cu $|G|$ este sumand direct şi al lui E_n. Avem acum două variante: fie numărul sumanzilor tinde la infinit, fie nu.

Tratăm mai întâi primul caz. Cociclul f_n ia valori într-o mulţime de ordin cel mult $|G|^2$ a lui A_n. Pentru orice element al unui grup abelian finit, putem găsi o descompunere a grupului ca sumă directă de grupuri ciclice astfel încât acel element să aparţină unui sumand. Asta înseamnă că putem presupune că pentru orice n, f_n ia valori într-o sumă directă B_n de $\leq |G|^2$ sumanzi din A_n. extensia E_n va fi atunci produsul direct dintre extensia lui B_n prin G indusă de cociclul nostru f_n şi grupul abelian A_n/B_n. Ordinul acestuia tinde la infinit, pentru că numărul sumanzilor săi tinde la infinit. Din observaţia din primul paragraf al demonstraţiei, $|\mathrm{Aut}(A_n/B_n)|$ tinde la infinit, deci şi $|\mathrm{Aut}(E_n)|$. Asta contrazice presupunerea făcută la început.

Acum tratăm al doilea caz, anume cel când numărul sumanzilor lui A_n nu tinde la infinit; putem presupune atunci că acest număr este mărginit. Grupul $H^2(G, A_n)$ este anihilat de înmulţirea cu $|G|$ (Propoziţia 1.3.5). Cum am presupus că divizorii primi ai lui $|A_n|$ sunt printre cei ai lui $|G|$, înmulţirea în A_n cu $1 - N$ pentru $|G| \mid N$ este un automorfism. Mai mult, acest automorfism induce identitatea pe $H^2(G, A_n)$. Asta înseamnă (Observaţia 2.5.6) că avem o diagramă comutativă

$$\begin{tikzcd}
0 \arrow[r] & A_n \arrow[r] \arrow[d, "1-N"'] & E_n \arrow[r] \arrow[d, "g"'] & G \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\
0 \arrow[r] & A_n \arrow[r] & E_n \arrow[r] & G \arrow[r] & 0
\end{tikzcd}$$

Desigur, g va fi automorfism al lui E_n, şi la automorfisme $1-N$ diferite corespund automorfisme g diferite. Din presupunerea că numărul sumanzilor lui A_n este mărginit va rezulta că maximumul ordinului unui sumand ciclic al lui A_n tinde la infinit cu n, şi asta implică imediat faptul că numărul automorfismelor lui A_n de forma (înmulţire cu $1-N$ pentru N număr natural divizibil cu $|G|$) tinde şi el la infinit cu n. Din nou, am obţinut contradicţia căutată. ■

Ne vor interesa acum extensiile centrale prin G ale grupului $\mathbb{C}^*$, grupul multiplicativ al corpului numerelor complexe. Vom vedea că ele apar natural în studiul aşa-numitelor reprezentări proiective. Introducem acum definiţiile şi noţiunile relevante.

Pentru un număr natural nenul n şi un corp k, $\mathrm{Gl}_n(k)$ va reprezenta, ca de obicei, grupul general liniar al matricelor inversabile de dimensiune n. Cu $\mathrm{PGl}_n(k)$ vom nota câtul lui Gl_n prin centrul său, adică grupul proiectiv liniar. Este binecunoscut că centrul constă exact din matricele scalare nenule. Printr-o reprezentare (complexă)liniară de grad n a unui grup G înţelegem pur şi simplu un morfism de la G la $\mathrm{Gl}_n(\mathbb{C})$, şi printr-o reprezentare (complexă) proiectivă de grad n înţelegem un morfism $G \to \mathrm{PGl}_n(\mathbb{C})$. Când corpul este $\mathbb{C}$ (adică peste tot în această porţiune a secţiunii), scriem pur şi simplu Gl_n şi PGl_n.

Fiind dată o reprezentare proiectivă $G \to \mathrm{PGl}_n$, se pune în mod firesc întrebarea dacă ea provine dintr-una liniară $G \to \mathrm{Gl}$ prin compunere cu proiecţia $\mathrm{Gl}_n \to \mathrm{PGl}_n$. Răspunsul la această întrebare este controlat într-o oarecare măsură de $H^2(G, \mathbb{C}^*)$, lucru care se poate vedea după cum urmează: G acţionează trivial pe grupurile necomutative Gl_n şi PGl_n şi pe grupul comutativ $\mathbb{C}^*$, care este izomorf cu centrul lui Gl_n. Vom avea deci un şir exact scurt de G-module triviale

$$0 \longrightarrow \mathbb{C}^* \longrightarrow \mathrm{Gl}_n \longrightarrow \mathrm{PGl}_n \longrightarrow 0,$$

unde 0 desemnează grupul trivial, chiar dacă folosim notaţie multiplicativă. Mai mult, nucleul $\mathbb{C}^*$ este central în Gl_n. Putem aplica aşadar Teorema 1.5.3 pentru a obţine un şir lung exact de coomologie necomutativă. Noţiunile acestea sunt definite în Secţiunea 1.5. Porţiunea care conţine H^0 oricum nu ne interesează, pentru că acţiunea lui G este trivială peste tot. Partea relevantă pentru noi este

$$H^1(G, \mathrm{Gl}_n) \longrightarrow H^1(G, \mathrm{PGl}_n) \xrightarrow{\Delta} H^2(G, \mathbb{C}^*). \tag{2.5.2}$$

Pentru că acţiunea lui G este trivială, $H^1(G, gl_n)$ este mulţimea morfismelor de grupuri de la G în Gl_n, adică mulţimea reprezentărilor liniare complexe de grad n, şi analog pentru PGl. Şirul (2.5.2) spune că un morfism $G \to \mathrm{PGl}_n$ poate fi ridicat la unul $G \to \mathrm{Gl}$ dacă şi numai dacă imaginea lui prin Δ este clasa trivială de coomologie din $H^2(G, \mathbb{C}^*)$. Reamintim descrierea lui Δ dată în Secţiunea 1.5: fiind dat un morfism

$\rho \in H^1(G, \mathrm{PGl}_n)$, se alege o ridicare ϕ a funcţiei ρ la Gl_n, şi $\Delta(\rho)$ va fi atunci clasa de coomologie reprezentată de 2-cociclul $f(s,t) = \phi(s)\phi(t)\phi(st)^{-1}$.

Ne vor interesa aici mai ales grupurile finite G. Teorema Coeficienţilor Universali (Teorema 1.7.1) ne dă un şir exact scurt

$$0 \longrightarrow \mathrm{Ext}(H_1(G), \mathbb{C}^*) \longrightarrow H^2(G, \mathbb{C}^*) \longrightarrow \mathrm{Hom}(M(G), \mathbb{C}^*) \longrightarrow 0.$$

Primul termen este nul, pentru că $\mathbb{C}^*$ este grup divizibil şi deci obiect injectiv în $\mathcal{A}b$. Avem aşadar un izmorfism $H^2(G, \mathbb{C}^*) \cong \mathrm{Hom}(M(G), \mathbb{C}^*)$. Dacă G este finit şi A este un G-modul finit generat, este uşor de văzut că $H^*(G, A)$, $H_*(G, A)$ sunt grupuri abeliene finite (este clar că sunt finit generate din definiţie, şi sunt de torsiune din Propoziţia 1.3.5). Asta înseamnă că $H^2(G, \mathbb{C}^*)$ este natural izomorf cu *dualul* grupului abelian finit $M(G)$ în sensul dualităţii Pontrjagin, deci izomorf (nenatural) cu $M(G)$. De aceea vom scrie uneori $M(G)$ în loc de $H^2(G, \mathbb{C}^*)$, pentru că în restul acestei secţiuni grupul G va fi finit, dacă nu specificăm contrariul. Dualul unui grup abelian finit A va fi notat cu A^*; am observat deja că el este izomorf cu A, dar nenatural, aşa că vom folosi notaţia A^* când este importantă naturalitatea aplicaţiilor.

În [Ro2, Cap. 7] se face studiul multiplicatorului Schur pentru un grup finit din acest punct de vedere al reprezentărilor proiective, şi se demonstrează un rezultat al lui Schur ([Ro2, Teorema 7.66]) care afirmă că orice grup finit G are cea ce se numeşte o "acoperire", adică o extensie centrală (finită) prin grupul respectiv la care se pot ridica mereu reprezentările proiective ale lui G şi care are în plus o proprietate de minimalitate. Detaliez mai jos.

Pentru o extensie centrală

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0$$

în care toate grupurile sunt finite, şirul exact cu cinci termeni în coomologie cu valori în E-modulul trivial $\mathbb{C}^*$ arată astfel ((1.7.8) adaptat la situaţia de faţă, când A este central în E):

$$0 \to H^1(G, \mathbb{C}^*) \to H^1(E, \mathbb{C}^*) \to A^* \xrightarrow{\delta^*} H^2(G, \mathbb{C}^*) \to H^2(E, \mathbb{C}^*). \tag{2.5.3}$$

Pe de altă parte, şirul în omologie ((1.7.9)) asociat E-modulului trivial $\mathbb{Z}$ este pur şi simplu dualul acestuia, după cum am observat mai sus:

$$H_2(E) \to H_2(G) \xrightarrow{\delta} A \to H_1(E) \to H_1(G) \to 0, \tag{2.5.4}$$

unde δ^* este dualul lui δ. Am asociat deci fiecărei extensii centrale a lui A prin G un morfism $\delta : M(G) \to A$ cu dual $\delta^* : A^* \to M(G)^*$. δ^* de exemplu poate fi descris foarte simplu: dacă $f \in A^*$ este morfism de la A la $\mathbb{C}^*$ (sau echivalent, $\mathbb{S}^1$) şi extensia $E \to G$ este descrisă de un 2-cociclu $h \in Z^2(G, A)$, atunci $\delta^*(f)$ este elementul lui $H^2(G, \mathbb{C}^*) \cong M(G)^*$ descris de 2-cociclul $f \circ h$. De aici se vede imediat că δ nu depinde decât de clasa de echivalenţă a extensiei $E \to G$, şi că aplicaţia care asociază unei extensii acest morfism δ este morfism de grupuri de la $H^2(G, A)$ la $\mathrm{Hom}(M(G), A)$.

Mai există un morfism natural de la $H^2(G, A)$ la $\mathrm{Hom}(M(G), A)$, anume ultimul morfism din şirul dat de Teorema Coeficienţilor Universali (Teorema 1.7.1, (1.7.2)):

$$0 \longrightarrow \mathrm{Ext}(H_1(G), A) \longrightarrow H^2(G, A) \longrightarrow \mathrm{Hom}(M(G), A) \longrightarrow 0.$$

După cum era firesc să ne aşteptăm, cele două morfisme coincid. Asta se vede foarte uşor din următoarea diagramă comutativă, în care săgeţile verticale sunt induse de un $f \in A^*$ arbitrar:

$$\begin{tikzcd} H^2(G,A) \arrow[r] \arrow[d] & \mathrm{Hom}(M(G),A) \arrow[d] \\ H^2(G,\mathbb{C}^*) \arrow[r, "\cong"] & \mathrm{Hom}(M(G),\mathbb{C}^*) \end{tikzcd}$$

Faptul că am identificat asocierea dintre extensii $E \to G$ ca mai sus şi δ cu morfismul $H^2(G,A) \to \mathrm{Hom}(M(G),A)$ din şirul coeficienţilor ne va permite mai târziu să dăm o demonstraţie foarte scurtă şi naturală pentru teorema lui Schur menţionată mai sus. Avem nevoie însă de câteva pregătiri.

Definiţia 2.5.8. Vom spune că o extensie centrală $U \to G$ a grupului G are *proprietatea de ridicare* dacă pentru orice n, orice reprezentare proiectivă $G \to \mathrm{PGl}_n$ poate fi completată la o diagramă

$$\begin{tikzcd} U \arrow[r] \arrow[d] & G \arrow[d] \\ \mathrm{Gl}_n \arrow[r] & \mathrm{PGl}_n \end{tikzcd}$$

Avem acum următoarea noţiune datorată lui Schur:

Definiţia 2.5.9. O *acoperire* a grupului finit G este o extensie centrală

$$0 \longrightarrow K \longrightarrow U \longrightarrow G \longrightarrow 0$$

care are proprietatea de ridicare şi astfel încât $K \leq U'$.

Legătura cu discuţia de până acum este următoarea:

Propoziţia 2.5.10. *O extensie centrală*

$$0 \longrightarrow K \longrightarrow U \longrightarrow G \longrightarrow 0$$

a grupului finit G este acoperire dacă şi numai dacă morfismul $\delta^* : K^* \to M(G)^*$ corespunzător extensiei este izomorfism.

Demonstraţie. Se vede imediat din şirul exact (2.5.3) că δ^* este injectiv dacă şi numai dacă restricţia oricărui morfism $U \to \mathbb{C}^*$ la K este nulă. Dar cum $\mathbb{C}^*$ este cogenerator în categoria grupurilor abeliene, această proprietate este echivalentă cu faptul că morfismul indus $K \to U/U'$ este nul, adică $K \leq U'$.

Din acelaşi şir (2.5.3) se vede că δ^* este surjectiv dacă şi numai dacă restricţia $H^2(G,\mathbb{C}^*) \to H^2(U,\mathbb{C}^*)$ este nulă. Deci dacă δ^* este surjectiv, atunci $U \to G$ are proprietatea de ridicare: asta reiese din comutativitatea diagramei

$$\begin{tikzcd} H^1(G, \mathrm{PGl}_n) \arrow[r, "\Delta"] \arrow[d] & H^2(G, \mathbb{C}^*) \arrow[d] \\ H^1(U, \mathrm{PGl}_n) \arrow[r, "\Delta"] & H^2(U, \mathbb{C}^*) \end{tikzcd}$$

, unde aplicaţiile verticale sunt cele naturale de "restricţie", iar cele orizontale sunt aplicaţiile Δ din (2.5.2) corespunzătoare grupurilor G şi respectiv U. Din ipoteză morfismul vertical din dreapta este nul, şi o clasă din $H^1(-, \mathrm{PGl}_n)$ se poate ridica dacă şi numai dacă are imagine nulă prin Δ.

Pentru reciprocă (proprietatea de ridicare implică δ^* surjectiv) ar fi suficient să arătăm că $\Delta : H^1(G, \mathrm{PGl}_n) \to H^2(G, \mathbb{C}^*)$ este surjecţie pentru un n (proprietatea de ridicare arată numai că suma imaginilor tuturor $\Delta : H^1(G, \mathrm{PGl}_n)$ pentru diverşi n este dusă în zero de $H^2(G, \mathbb{C}^*) \to H^2(U, \mathbb{C}^*)$). Asta e adevărat pentru $n = |G|$ de exemplu, pentru că atunci unui 2-cociclu $(s, t) \mapsto a_{s,t} \in \mathbb{C}^*$ al lui G îi putem asocia următoarea reprezentare proiectivă: se alege o bază e_s, $s \in G$ pentru $\mathbb{C}^{|G|}$, şi elementului $s \in G$ Îi asociem automorfismul $P_s \in \mathrm{Gl}_{|G|}$ definit prin $P_s e_t = a_{s,t} e_{st}$. După factorizarea prin scalari obţinem un morfism $G \to \mathrm{PGl}_{|G|}$ care este trimis de Δ exact în clasa de coomologie reprezentată de cociclul $a_{s,t}$. ∎

Observaţia 2.5.11. Propoziţia ne spune în particular că într-o acoperire, nucleul K trebuie să fie chiar $M(G)$.

Ajungem acum în sfârşit la rezultatul lui Schur:

Teorema 2.5.12 (Schur)**.** *Orice grup finit G are o acoperire $U \to G$.*

Demonstraţie. Am văzut în propoziţia precedentă că e suficient să găsim o extensie centrală U a lui $M(G)$ prin G astfel încât morfismul $\delta : M(G) \to M(G)$ este automorfism. Am identificat în discuţia de mai sus aplicaţia care asociază morfismul δ unei asemenea extensii privite ca element al lui $H^2(G, M(G))$ cu morfismul

$$H^2(G, M(G)) \to \mathrm{Hom}(M(G), M(G))$$

din şirul coeficienţilor universali. Dar acest morfism este surjectiv, deci există elemente ale lui $H^2(G, M(G))$ pe care el le aplică în $\mathrm{id}_{M(G)}$ de exemplu, şi am terminat. ∎

Observaţia 2.5.13. Din construcţia pentru acoperiri dată în demonstraţia precedentă se vede că atunci când grupul finit G este perfect, o acoperire este unică până la izomorfism (izo în categoria săgeţilor $U \to G$, cu care am lucrat şi mai sus), şi este şi extensie centrală universală (Definiţia 2.5.4).

Discuţia de până acum este utilă în studiul reprezentărilor proiective ale grupurilor finite. În particular, putem da condiţii suficiente asupra unui grup finit pentru ca acestea să se poată ridica întotdeauna la reprezentări liniare. Un exemplu de astfel de rezultat:

Propoziţia 2.5.14. *Fie G un grup finit cu subgrupuri Sylow ciclice. Atunci $M(G) = 0$, şi deci toate reprezentările proiective ale lui G se ridică la reprezentări liniare.*

Demonstraţie. Dacă arătăm că $M(G) = 0$ atunci a doua afirmaţie va rezulta din faptul că atunci identitatea $G \to G$ va fi acoperire a lui G (Teorema 2.5.12).

Pentru un număr prim p, fie G_p un subgrup Sylow al lui G. Să observăm că pentru orice G-modul A, restricţia $H^2(G, A) \to H^2(G_p, A)$ este injectivă pe componenta p-primară a grupului abelian de torsiune $H^2(G, A)$. Într-adevăr, corestricţia compusă cu restricţia (ambele corespunzătoare subgrupului $G_p \leq G$) dă înmulţirea cu $[G : G_p]$ (Propoziţia 1.3.5), care este un număr prim cu p. Componenta p-primară a grupului finit $H^2(G, \mathbb{C}^*)$ se scufundă aşadar în $H^2(G_p, \mathbb{C}^*)$. Cum G_p este ciclic (o ipoteză pe care nu am folosit-o până acum), Teorema 2.2.4 arată că $H^2(G_p, A)$ pentru orice G_p-modul trivial divizibil A este nul (în particular $A = \mathbb{C}^*$). ■

Vom spune că o reprezentare proiectivă $\rho : G \to \mathrm{PGl}_n$ a unui grup finit G este *ireductibilă* dacă o reprezentare liniară a unei acoperiri $U \to G$ obţinută prin ridicarea lui ρ este ireductibilă în sens clasic, adică nu există subspaţii liniare proprii nenule ale lui $\mathbb{C}^n$ invariante la acţiunea lui U. Să observăm că noţiunea nu depinde de acoperirea U sau de ridicarea liniară $U \to \mathrm{Gl}_n$ aleasă; într-adevăr, definiţia se mai poate reformula spunând că spaţiul proiectiv $\mathbb{P}^{n-1}(\mathbb{C})$ nu are subvarietăţi liniare proprii G-invariante. Avem următorul rezultat:

Propoziţia 2.5.15. *Fie G un grup netrivial de ordin $\leq n^2$ cu $M(G) = 0$. Atunci G nu are reprezentări proiective ireductibile de grad n.*

Demonstraţie. Dacă G ar avea o asemenea reprezentare, atunci ea s-ar ridica la una liniară ireductibilă de grad n a lui G, pentru că G este acoperire pentru G. Avem deci un grup netrivial de ordin $\leq n^2$ cu o reprezentare liniară ireductibilă de grad n. Se ştie însă ([Se1, §2.4, Cor. 2], de exemplu) că dacă n_i, $i = \overline{1, r}$ sunt gradele reprezentărilor liniare ireductibile ale unui grup finit G, atunci $\sum n_i^2 = |G|$. G are întotdeauna o reprezentare ireductibilă de grad 1, anume cea trivială. Cu alte cuvinte, unul dintre n_i este 1. Atunci, dacă G este netrivial, toţi n_i^2 vor fi strict mai mici decât $|G|$, şi obţinem contradicţia căutată. ■

Am inclus acest rezultat pentru a-l putea folosi într-o aplicaţie asupra produselor crossed de algebre cu grupuri. Ne interesează produsele crossed de grupuri cu algebre de operatori pe un spaţiu Hilbert. Pentru o introducere rapidă în subiect facem trimitere la [Tak1, § V.7] sau [Tak2, § X.1]. Ne interesează problema următoare: se dă o C^*-algebră A, care este factor (adică centrul ei constă numai din $\mathbb{C}$). Pentru un număr natural n avem algebra $B = M_n(A) = A \otimes M_n(\mathbb{C})$, care constă din matrice $n \times n$ cu elemente din A, cu structura evidentă de algebră. A se scufundă în mod natural în B ca algebra matricelor diagonale cu acelaşi element pe fiecare poziţie diagonală (scufundarea se poate descrie şi ca $A \ni x \mapsto x \otimes 1 \in A \otimes M_n(\mathbb{C})$). Este atunci adevărat că B este produs crossed $A \rtimes G$ pentru un grup G (obligatoriu de ordin n^2) care acţionează pe A?

Se poate arăta că răspunsul la această întrebare este afirmativ pentru unele grupuri (şi factori A care nu sunt de forma $M_k(\mathbb{C})$), dar aici voi demonstra un rezultat negativ folosind propoziţia precedentă. Mai precis:

Propoziţia 2.5.16. *Fie A un factor, şi $n > 1$ un număr natural. Dacă grupul G de ordin n^2 are multiplicator Schur trivial, atunci $B = M_n(A)$ nu are structură de produs crossed $A \rtimes G$ (pentru scufundarea standard a lui A).*

Demonstraţie. Vom presupune contrariul, şi vom arăta că G trebuie atunci să aibă o reprezentare proiectivă ireductibilă de grad n. Concluzia va rezulta atunci din propoziţia precedentă.

Presupunem deci că $M_n(A) \cong A \rtimes G$. Vom considera elementele G ca fiind scufundat în grupul elementelor unitare din C^*-algebra $A \rtimes G$, şi acţiunea lui $s \in G$ pe $a \in A$ o notăm cu $a \mapsto {}^s a$. Fiecare element $x \in M_n(A)$ se va scrie atunci în mod unic sub forma $\sum_{s\in G} x_s s$, cu $x_s \in A$. Pentru că A este factor, centralizatorul lui A în $M_n(A)$ este $M_n(\mathbb{C})$ (cu incluziunea evidentă). Fie $\sum x_s s$ un element care centralizează A. Atunci fiecare sumand $x_s s$ centralizează A, pentru că As este invariant şi la înmulţirea la dreapta cu A. Condiţia asupra lui x_s pentru ca $x_s s$ să centralizeze A este

$$a x_s = x_s {}^s a, \ \forall a \in A. \tag{2.5.5}$$

Aplicând involuţia $*$ din algebra A şi notând a^* cu a (pentru că oricum a va parcurge întreg A), vom avea

$$x_s^* a = {}^s a x_s^*, \ \forall a \in A.$$

Din aceste două relaţii se vede că $x_s x_s^* \in A$ (şi $x_s^* x_s$) centralizează A. Cu alte cuvinte, $x_s x_s^*$ este un scalar (nenegativ). Va fi un scalar strict pozitiv dacă şi numai dacă $x_s \neq 0$ (condiţia de algebră C^* este necesară în implicaţia $x_s \neq 0 \Rightarrow x_s x_s^* \neq 0$). Dar putem găsi elemente $x_s s$ nenule care centralizează A pentru toţi $s \in G$, pentru că altfel A-submodulul stâng al lui $M_n(A)$ generat de centralizatorul lui A ar fi strict mai mic decât $M_n(A)$, ceea ce nu e adevărat.

Putem găsi deci elemente inversabile $x_s \in A$ astfel încât $x_s s \in M_n(\mathbb{C})$. Aplicând (2.5.5) se vede că elementele x_{st} şi $x_s {}^s x_t$ au aceeaşi acţiune pe A prin conjugare, deci coincid până la un scalar. Asta înseamnă că aplicaţia $s \mapsto x_s s$ este morfism după trecerea la PGl_n. Am obţinut aşadar o reprezentare proiectivă de grad n a lui G. Că trebuie să fie ireductibilă este acum clar: cele n^2 elemente $x_s s \in M_n(\mathbb{C})$ trebuie să fie liniar indpendente, pentru că A-modulul stâng generat de ele este întreg $M_n(A)$. Asta înseamnă că G are o reprezentare proiectivă ireductibilă de grad n, şi deci demonstraţia este încheiată, conform observaţiei de la început. ∎

Concluzii

Pentru o perspectivă mai largă asupra omologiei şi coomologiei grupurilor facem referire la textele menţionate şi mai sus: [Th] pentru o prezentare a legăturilor dintre teoria reprezentărilor liniare ale grupurilor finite şi coomologie, cu aplicaţii la studiul ambelor domenii, [Gru] pentru aplicaţii în teoria clasică a grupurilor, ca de exemplu automorfisme de p-grupuri finite, [Se3] pentru teoria coomologică a grupurilor profinite şi coomologie Galois, "descent" în geometria algebrică şi domenii înrudite, [CFr, Cap. VI, VII, IX] pentru o prezentare a problemelor fundamentale ale teoriei corpului claselor în limbaj coomologic, [Se2] pentru o tratare mai detaliată a aceloraşi probleme în cazul corpurilor locale.

Lipsa spaţiului şi a timpului au permis o prezentare care dă numai o idee vagă asupra versatilităţii metodelor omologice în teoria grupurilor şi domeniile adiacente. Utilizarea acestor metode omologice este o tehnică din ce în ce mai importantă în multe domenii ale matematicii, şi sperăm că prezentarea aceasta a arătat întrucâtva că rezultatele care pot fi obţinute pe această cale sunt multe şi variate.

Bibliografie

[AT] Artin, E. şi Tate, J. - *Class field theory*, Harvard (1961)

[Bo] Borel, A. - *Linear algebraic groups*, Springer-Verlag (ed. a 2-a, 1991)

[Br] Brown, K. S. - *Cohomology of groups*, Springer-Verlag (1982)

[Bu] Burnside, W. - *Theory of groups of finite order*, Dover (ed. a 2-a, 1955)

[CFr] Cassels, J. W. S. şi Fröhlich (editori) - *Algebraic Number Theory*, Academic Press (1967)

[CE] Cartan, H. şi Eilenberg, S. - *Homological Algebra*, Princeton University Press (1956)

[Eck] Eckmann, B. - *Cohomology of groups and transfer*, Ann. of Math. **58** (1953), pp. 481 - 493

[Fr] Freyd, P. - *Abelian categories*, Harper & Row (1964)

[Ga1] Gaschütz, W. - *Kohomologische Trivialitäten und äussere Automorphismen von p-Gruppen*, Math. Zeit. **88** (1965), pp. 432 - 433

[Ga2] ———- *Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen*, J. of Algebra **4** (1966), pp. 1 - 2

[GS] Golod, E. S. şi Šafarevič, I. - *On the class field tower*, Izv. Akad. Nauk USSR **28** (1964), pp. 261 - 272

[Gr] Grothendieck, A. - *Sur quelques points d'algèbre homologique*, Tôhoku Math. J. **9** (1957), pp. 119 - 221

[Gru] Gruenberg, K. W. - *Cohomological topics in group theory*, Springer-Verlga (1970)

[Ha] Hartshorne, R. - *Algebraic Geometry*, Springer-Verlag (ed. a 8-a, 1997)

[Hat] Hatcher, A. - *Algebraic Topology*, Cambridge University Press (2002)

[HSt] Hilton, P. J. şi Stammbach, U. - *A course in homological algebra*, Springer-Verlag (1971)

[Ho] Hopf, H. - *Fundamentalgruppe und zweite Bettische Gruppe*, Comment. Math. Helv. **14** (1942), pp. 257 - 309

[Hu] Hurewicz, W. - *Beiträge zur Topologie der Deformationen. IV. Asphärische Räume*, Nederl. Akad. Wetensch. Proc. **39** (1936), pp. 215 - 224

[Hus] Husemoller, D. - *Fibre bundles*, Springer-Verlag (ed. a 3-a, 1994)

[Iw] Iwasawa, K. - Local class field theory, Oxford University Press (1986)

[MacL] Mac Lane, S. - *Categories for the working mathematician*, Springer-Verlag (1971)

[McC] McCleary, J. - *A userguide to spectral sequences*, Cambridge University Press (ed. a 2-a, 2001)

[MTW] Madsen, I., Thomas, C. B. şi Wall, C. T. C. - *The topological spherical space form problem II*, Topology **15** (1978), pp. 375 - 382

[Mil1] Milnor, J. - *Groups which act on $\mathbb{S}^n$ without fixed points*, Amr. J. Math. **79** (1957), pp. 623 - 630

[Mil] ———- *Morse Theory*, Princeton University Press (1963)

[MZ] Montgomery, D. şi Zippin, L. - *Topological transformation groups*, Interscience (1955)

[Mu] Mumford, D. - *The red book of varieties and schemes*, Springer-Verlag (ed. a 2-a, 1999)

[Pas] Passman, D. - *Group rings, crossed products, and Galois theory*, American Mathematical Society (1986)

[Ro1] Rotman, Joseph J. - *An introduction to homological algebra*, Academic Press (1979)

[Ro2] ______- *An introduction to the theory of groups*, Springer-Verlag (ed. a 4-a, 1995)

[Sch] Schur, I. - *Neuer Beweis eines Satzes über endliche Gruppen*, Sitzungsber. Preuss. Akad. Wiss. (1902), pp. 1013 - 1019, Gessamelte Abhandlungen, I, 79 - 85

[Se1] Serre, J. P. - *Linear representations of finite groups*, Springer-verlag (1977)

[Se2] ______- *Local fields*, Springer-Verlag (1979, tradus din limba franceză)

[Se3] ______- *Cohomologie galoisienne*, Springer-Verlag, (ed. a 5-a, 1994)

[Sm] Smith, P. A. - *Permutable periodic transformations*, Proc. Nat. Acad. Sci. **30** (1944), pp. 105 - 108

[St] Stallings, J. - *On torsion-free groups with infinitely many ends*, Ann. Math. **88** (1968), pp. 312 - 334

[Sw] Swan, R. G. - *Groups of cohomological dimension one*, J. Algebra **12** (1969), pp. 585 - 610

[Th] Thomas, C. B. - *Characters and the cohomology of finite groups*, Cambridge University Press (2008)

[Tak1] Takesaki, M. - *Theory of operator algebras Vol. I*, Springer-Verlag (ed. a 2-a, 2002)

[Tak2] ______- *Theory of operator algebras Vol. II*, Springer-Verlag (2003)

[We] Weibel, Charles A. - *An introduction to homological algebra*, Cambridge University Press (1994)