UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jure Vogrinc

Razširitve grup

Delo diplomskega seminarja

Mentor: doc. dr. Aleš Vavpetič

Ljubljana, 2011

Kazalo

Razširitve grup

Povzetek

V delu dokažemo, da so ekvivalenčni razredi razširitev grupe G po G-modulu A v bijektivni korespondenci z elementi druge kohomološke grupe $H^2(G, A)$ grupe G s koeficienti v A. Predstavimo pojma razširitve grupe in delovanja grupe ter se seznanimo s problemom iskanja vseh razširitev. V nadaljevanju se osredotočimo le na razširitve z abelovim jedrom. Spoznamo pojem kohomologije grupe in ga povežemo s problemom iskanja vseh razširitev z abelovim jedrom. Izpeljemo, kaj predstavljajo ničta, prva in druga kohomološka grupa, ter preko tega pridemo še do metode, kako za dano grupo G in dani G-modul A poiščemo vse razširitve.

Group extensions

Abstract

It is proven in this work that there is a bijection between equivalence classes of extensions of group G by G-module A and elements of second cohomology group $H^2(G, A)$ of group G with coefficients in A. The notions of group extension and group action are presented and we familiarize ourselves with the problem of finding all extensions. Later on we focus only on extensions with abelian kernel. The notion of group cohomology is introduced and linked to the problem of finding all extensions with abelian kernel. It is deduced what zero, first and second cohomology groups represent and through it a method for finding all extensions for a given group G and G-modul A is derived.

Math. Subj. Class. (2010): 20J06

Ključne besede: razširitev grupe, kohomologija grupe, razširitev z abelovim jedrom, semidirektni produkt, razcepna razširitev, delovanje grupe

Keywords: group extension, group cohomology, extension with abelian kernel, semidirect product, split extension, group action

1. Osnovni pojmi

Poznamo grupi G in N. Kaj lahko povemo o grupi E, za katero velja $N \triangleleft E$ in $E/N \cong G$? To vprašanje bi lahko označili kot osrednji problem tega dela. Področje, v katerega spada, je seveda teorija grup, močno pa je povezano tudi z algebraično topologijo. Rezultati v zvezi s tem vprašanjem nam pomagajo pri problemih, kot je, recimo, klasifikacija vseh končnih p-grup.

V prvem razdelku bomo spoznali osnovne pojme in se naučili jezika, v katerem bomo v kasnejših razdelkih o problemu resneje spregovorili. V drugem razdelku se bomo srečali z delovanjem grupe, še enim pojmom, ki ima za nas bistven pomen. V tretjem razdelku se bomo ukvarjali z algebraično topološkim ozadjem problema. Razumevanje tega razdelka za razumevanje glavnih rezultatov v tem delu sicer ni potrebno, predstavlja pa zanimivo povezavo med matematičnimi področji, s katero si včasih lahko pomagamo tudi pri izračunih. V zadnjem razdelku pa se bomo zares lotili razširitev grup in izpeljali tudi nekaj rezultatov.

Osrednji objekt, ki ga bomo študirali, je razširitev grupe G po grupi N. Treba je razjasniti tudi, kdaj bomo imeli dva takšna objekta za enaka, torej kdaj sta dve razširitvi G po N ekvivalentni.

Definicija 1.1. *Razširitev grupe* G po grupi N, oziroma grupe G z jedrom N, je kratko eksaktno zaporedje grup

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1.$$

Velja omeniti, da iz definicije eksaktnosti sledi, da je i monomorfizem, π epimorfizem in velja $\ker \pi = \operatorname{im} i \cong N$ ter $E/N \cong \operatorname{im} \pi = G$. Čeprav je razširitev pravzaprav trojica (E, i, π), jo bomo na kratko označevali le z E.

Pravimo, da sta dve razširitvi E_1 in E_2 grupe G po N *ekvivalentni*, če obstaja takšen homomorfizem grup φ iz E_1 v E_2, da spodnji diagram komutira:

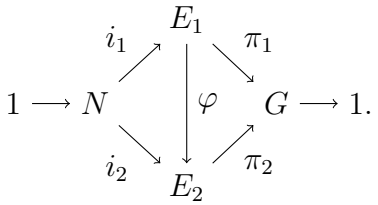


Diagram 1: Ekvivalenca razširitev

Če je jasno, da gre za dve razširitvi G po N, potem ponavadi rečemo kar, da je grupa E_1 ekvivalentna grupi E_2 in to označimo z $E_1 \equiv E_2$.

Trditev 1.2. *Če sta E_1 in E_2 ekvivalentni grupi in φ tak homomorfizem med njima, da diagram 1 komutira, potem je φ izomorfizem.*

Dokaz. Trditev je očitna posledica kratke leme o petih, vseeno pa jo dokažimo tudi bolj elementarno. Najprej dokažimo, da je homomorfizem φ injektiven. Naj bo $x \in E_1$ in naj velja $\varphi(x) = 1 \in E_2$. Ker diagram 1 komutira, velja

$$\pi_1(x) = \pi_2(\varphi(x)) = \pi_2(1) = 1.$$

Sledi, da je $x \in \ker \pi_1$. Zaporedje grup $N \to E_1 \to G$ je eksaktno pri E_1, zato je $x \in \operatorname{im} i_1$. Torej obstaja $y \in N$, da velja $i_1(y) = x$. Ker pa diagram 1 komutira,

velja tudi

$$i_2(y) = \varphi(i_1(y)) = \varphi(x) = 1.$$

Ker je zaporedje grup $1 \to N \to E_2 \to G \to 1$ kratko eksaktno, je homomorfizem i_2 injektiven, iz česar dobimo $y = 1$ in $x = i_1(y) = i_1(1) = 1$. Zato je φ injektiven.

Dokazati moramo še, da je surjektiven. Naj bo $z \in E_2$. Ker je π_1 surjektivna, obstaja $w \in E_1$, da velja $\pi_1(w) = \pi_2(z)$. Označimo $t := \varphi(w)$. Velja

$$\pi_2(t) = \pi_2(\varphi(w)) = \pi_1(w) = \pi_2(z).$$

Ker pa je π_2 homomorfizem, velja tudi

$$\pi_2(t^{-1}z) = \pi_2(t)^{-1}\pi_2(z) = \pi_2(t)^{-1}\pi_2(t) = 1.$$

Zato je $t^{-1}z \in \ker \pi_2 = \operatorname{im} i_2$, kar pomeni, da obstaja $v \in N$, za katerega velja $i_2(v) = t^{-1}z$. Oglejmo si sedaj $\varphi(wi_1(v))$. Iz komutativnosti diagrama sledi

$$\varphi(w \cdot i_1(v)) = \varphi(w)\varphi(i_1(v)) = \varphi(w)i_2(v) = t \cdot t^{-1}z = z.$$

Ker je z poljuben element iz E_2, je φ surjektiven. □

Pokazali smo, da ekvivalentnost dveh razširitev G po N implicira izomorfnost grup E_1 in E_2. Naslednji zgled bo pokazal, da obratno ne drži. Celo enakost grup $E_1 = E_2$ ni nujno dovolj za ekvivalenco razširitev.

Primer 1.3. Naj bo $p > 2$ praštevilo. Naslednji razširitvi $\mathbb{Z}_p$ po $\mathbb{Z}_p$ nista ekvivalentni:

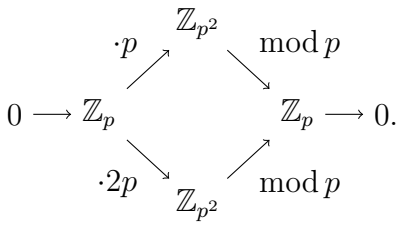


Diagram 2: Neekvivalentni razširitvi

Tu grupi $\mathbb{Z}_p$ in $\mathbb{Z}_{p^2}$ pišemo aditivno, njune elemente pa opišemo standardno, z množicama $\{0, 1, \ldots, p-1\}$ in $\{0, 1, \ldots, p^2-1\}$, oznaki $\cdot p$ in $\cdot 2p$ predstavljata homomorfizma množenje s p in množenje z $2p$. Prvi na primer slika $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ v $\{0, p, 2p \ldots, p(p-1)\} < \mathbb{Z}_{p^2}$. Oznaka $\bmod p$ pa predstavlja homomorfizem, ki $x \in \{0, 1, \ldots, p^2-1\}$ pripiše njegov ostanek pri deljenju s p.

Dokaz. Trivialno je preveriti, da sta obe zaporedji res kratki eksaktni. Denimo, da obstaja tak homomorfizem φ (ki slika iz zgornjega $\mathbb{Z}_{p^2}$ v spodnjega), da diagram 2 komutira. Označimo $x := \varphi(1)$. Ker desna polovica diagrama komutira, mora veljati

$$(\bmod p)(x) = (\bmod p)\varphi(1) = (\bmod p)(1) = 1,$$

oziroma $x \equiv 1 \pmod{p}$.

Po drugi strani lahko iz leve polovice komutativnega diagrama sklepamo

$$\varphi(p) = \varphi((\cdot p)(1)) = (\cdot 2p)(1) = 2p.$$

Drži pa tudi

$$\varphi(p) = \varphi(1 + 1 + \cdots + 1) = p \cdot \varphi(1) = px.$$

To pa pomeni $2p \equiv px \pmod{p^2}$ in posledično $2 \equiv x \pmod{p}$. Dobimo $1 \equiv x \equiv 2 \pmod{p}$, kar je protislovje.

□

2. Delovanje grupe

Sedaj smo predstavili matematični koncept, ki ga bomo obravnavali. Zdaj je potrebno vpeljati še nekaj konceptov, s katerimi si bomo pomagali pri dokazovanju.

Definicija 2.1. *Delovanje* grupe G na grupi N je preslikava iz $G \times N$ v N, ki paru $n \in N$, $g \in G$ priredi element $gn \in N$, obenem pa za vse n, $m \in N$ in vse g, $h \in G$ zadošča naslednjim pogojem:

$$\begin{aligned} 1n &= n, \\ h(gn) &= (hg)n, \\ g(nm) &= (gn)(gm). \end{aligned}$$

Delovanje grupe lahko ekvivalentno podamo tudi drugače. Delovanje grupe G na grupi N je homomorfizem χ iz grupe G v grupo $\operatorname{Aut} N$ avtomorfizmov grupe N, ki elementu $g \in G$ priredi avtomorfizem χ_g, definiran s predpisom $\chi_g(n) = gn$. Trivialno je preveriti, da sta definiciji res ekvivalentni.

Primer 2.2. Naj bo $N \triangleleft G$. Potem je homomorfizem $\chi : G \to \operatorname{Aut} N$, ki elementu $g \in G$ priredi avtomorfizem χ_g, definiran s predpisom $\chi_g(n) = gng^{-1}$, delovanje grupe G na podgrupi edinki N. Temu konkretnemu pravimo *delovanje* grupe G na podgrupi edinki N *s konjugiranjem*, avtomorfizme oblike $n \mapsto gng^{-1}$ za $g \in G$ pa imenujemo *notranji avtomorfizmi*. Če je grupa G abelova (splošneje, če je $N \leq Z(G)$), je χ trivialni homomorfizem (preslikava $n \mapsto gng^{-1}$ je identiteta).

Če imamo dano razširitev

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1,$$

potem velja $E/i(N) \cong G$. Iz vsakega odseka grupe $E/i(N)$ si lahko izberemo predstavnika. Za vsak $g \in G$ torej obstaja fiksirani predstavnik $s(g) \in E$, da velja $\pi s(g) = g$. Na s lahko gledamo kot na preslikavo iz G v E, ki je desni inverz, v smislu preslikav, epimorfizma π. Takšni preslikavi s pravimo transverzala.

Definicija 2.3. Za dano razširitev

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1, \\ & & & & = \downarrow & \swarrow & s & & \\ & & & & E & & & & \end{array}$$

je *transverzalna funkcija* oziroma *transverzala* s vsaka takšna preslikava $s : G \to E$, da velja $\pi s = id_G$.

Velja omeniti, da transverzala ni nujno homomorfizem. To lahko enostavno vidimo na naslednjem primeru.

Primer 2.4. V razširitvi spodaj, kjer za n, $m \in \mathbb{Z}$ velja $i(n) = (n, 0)$ in $\pi(n, m) = m$, imamo tako transverzalo $s_1(m) = (0, m)$, ki je homomorfizem, kot tudi na primer transverzalo $s_2(m) = (2m^2 + 3, m)$, ki očitno ni homomorfizem.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Z} \times \mathbb{Z} \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

Vemo tudi, da je $\pi(1_E) = 1_G$, saj je π homomorfizem. Zaradi tega lahko kot predstavnika trivialnega odseka $i(N) \in E/i(N)$ vedno vzamemo 1_E. Da bodo stvari enostavnejše, bomo od tu naprej vedno privzemali $s(1_G) = 1_E$.

Denimo, da za razširitev

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

izberemo transverzalo $s : G \to E$ in označimo $S = \{s(g), g \in G\} \subset E$ ter $M = \operatorname{im} i$. Potem velja $M \triangleleft E$ in z elementi množice S lahko konjugiramo podgrupo M. Prek transverzale s lahko za vsak $g \in G$ definiramo avtomorfizem $\lambda_{g,s}$ grupe N, ki vsakemu $n \in N$ pripiše $i^{-1}(s(g)i(n)s(g)^{-1})$. Slednje lahko zapišemo tudi kot

$$i(\lambda_{g,s}(n)) = s(g)i(n)s(g)^{-1}.$$

Recimo, da je t neka druga transverzala za isto razširitev. Oglejmo si enakost:

$$\pi(t(g)s(g)^{-1}) = \pi t(g)(\pi s(g))^{-1} = gg^{-1} = 1.$$

Iz nje sledi $t(g)s(g)^{-1} \in \ker \pi = \operatorname{im} i$. To upoštevamo in dobimo $t(g) = m_g s(g)$ za nek $m_g \in M$.

Definirajmo še $i(\lambda_{g,t}(n)) = t(g)i(n)t(g)^{-1}$, uporabimo zgornji rezultat in dobimo

$$i(\lambda_{g,t}(n)) = m_g s(g)i(n)(m_g s(g))^{-1} = m_g i(\lambda_{g,s}(n))m_g^{-1}.$$

To lahko prepišemo v

$$\lambda_{g,t}(n) = n_g \lambda_{g,s}(n) n_g^{-1},$$

kjer je $n_g := i^{-1}(m_g) \in N$. Avtomorfizma $\lambda_{g,s}$ in $\lambda_{g,t}$ se torej razlikujeta le za notranji avtomorfizem. Označimo z $\operatorname{Inn} N$ *grupo notranjih avtomorfizmov grupe* N. Znano dejstvo je, da je to res grupa in da velja $\operatorname{Inn} N \triangleleft \operatorname{Aut} N$. Zato lahko vpeljemo še *grupo zunanjih avtomorfizmov* $\operatorname{Out} N := \operatorname{Aut} N / \operatorname{Inn} N$. Ravnokar smo dokazali, da je naslednja definicija neodvisna od izbire transverzale.

Definicija 2.5. Naj bo dana razširitev

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1.$$

Naj bo s neka transverzala za to razširitev. Preslikavi $\chi : G \to \operatorname{Out} N$ s predpisom $\chi(g) = \lambda_{g,s}\operatorname{Inn} N$ pravimo *parčkanje*.

Parčkanje je neodvisno od izbire transverzale, zato je upravičeno pisati $\chi(g) = \lambda_g \operatorname{Inn} N$. Tu je λ_g le nova oznaka za $\lambda_{g,s}$, le da s izpustimo, saj ni bistven.

Trditev 2.6. *Parčkanje $\chi : G \to \operatorname{Out} N$ je homomorfizem.*

Dokaz. Vemo, da je parčkanje neodvisno od transverzale. Za razširitev izberimo neko transverzalo s, s katero bomo računali. Naj bosta g, $h \in G$ poljubna. Ker je π homomorfizem in s transverzala, velja

$$\pi(s(gh)s(h)^{-1}s(g)^{-1}) = ghh^{-1}g^{-1} = 1.$$

Od tod pa sledi $s(gh)s(h)^{-1}s(g)^{-1} \in \ker \pi = \operatorname{im} i$, kar lahko prepišemo v $s(gh) = m_{g,h}s(g)s(h)$, kjer je $m_{g,h} = i(n_{g,h})$ za nek $n_{g,h} \in N$. Poračunajmo:

$$\begin{aligned} i(\lambda_{gh}(n)) &= s(gh)i(n)s(gh)^{-1} = \\ &= m_{g,h}s(g)s(h)i(n)s(h)^{-1}s(g)^{-1}m_{g,h}^{-1} = \\ &= m_{g,h}i(\lambda_g(\lambda_h(n)))m_{g,h}^{-1}. \end{aligned}$$

Ker je v zgornjem izračunu n poljuben element iz N, se avtomorfizma λ_{gh} in $\lambda_g\lambda_h$ razlikujeta le za notranji avtomorfizem. Zares velja $\chi(gh) = \chi(g)\chi(h)$. □

3. Kohomologija grupe

Definicija 3.1. Naj bo G grupa in R komutativni kolobar z enoto. *Grupni kolobar* RG je množica formalnih vsot $RG = \{\sum_{g\in G} r_g g : r_g \in R, g \in G\}$, kjer je $r_g \neq 0$ le za končno mnogo $g \in G$, ki jo opremimo z operacijama seštevanja in množenja na samoumeven način:

$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G} (r_g + s_g)g,$$
$$\Big(\sum_{g\in G} r_g g\Big)\Big(\sum_{g\in G} s_g g\Big) = \sum_{g\in G}\sum_{h\in G} (r_g s_h)gh.$$

Definicija 3.2. Naj bo A abelova grupa in naj grupa G deluje na grupi A. Množenje elementov grupe A z elementi grupnega kolobarja $\mathbb{Z}G$ lahko podamo s predpisom $(\sum_{g\in G} n_g g)\cdot a = \sum_{g\in G} n_g(ga)$. S tem A postane *levi $\mathbb{Z}G$-modul*, ki mu na kratko pravimo tudi *G-modul*. G-linearni preslikavi med dvema G-moduloma pravimo kar *G-homomorfizem*.

Trivialno je preveriti, da sta zgornji definiciji zares smiselni.

Primer 3.3. Imejmo razširitev

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

grupe G po grupi N. Kot smo videli v trditvi 2.6 ta razširitev poraja homomorfizem $\chi : G \to \operatorname{Out} N$. Oglejmo si zožitve avtomorfizmov grupe N na njen center $Z(N)$. Vsak notranji avtomorfizem, zožen na center, je trivialen (saj za $g \in G$ in $z \in Z(N)$ velja $gzg^{-1} = gg^{-1}z = z$). Zato vsak element $\operatorname{Out} N$ enolično določa element $\operatorname{Aut} Z(N)$. S pomočjo $\chi(g) = \lambda_g \operatorname{Inn} N$ lahko dobro definiramo homomorfizem $\bar{\chi} : G \to \operatorname{Aut} Z(N)$ s predpisom $\bar{\chi}(g) = \lambda_g|_{Z(N)}$. Grupa G torej deluje na center $Z(N)$, ki je seveda abelova grupa. Tako $Z(N)$ postane G-modul.

V primeru razširitve z abelovim jedrom A grupa G deluje na $Z(A) = A$. Imamo delovanje G na celi grupi A, drugače povedano A postane G-modul. Iz definicije 2.5 sledi, da ima to delovanje predpis $\chi(g) = \lambda_g$. Naj bo s neka transverzala za razširitev. Potem lahko to delovanje zapišemo s formulo

$$ga = i^{-1}(s(g)i(a)s(g)^{-1}).$$

Izkaže se, da je analiza G-modula $Z(N)$ ključen korak v teoriji razširitev, vendar pa je to za nas nekoliko pretežek problem. Zato se bomo osredotočili le na nekoliko lepši podprimer. Privzeli bomo, da je grupa N abelova. Od tu dalje se bomo v tem delu ukvarjali samo še z razširitvami z abelovim jedrom. Namesto N bomo od zdaj naprej vedno pisali A in s tem mislili abelovo grupo.

Sedaj se lahko seznanimo s pojmom kohomologije, najpomembnejšim konceptom v algebraično topološkem ozadju naše teme.

Definicija 3.4. Naj bo R kolobar. *R-koverižni kompleks* $C = (C^*, d^*)$ je zaporedje levih R-modulov $\ldots, C^{-2}, C^{-1}, C^0, C^1, C^2, \ldots$ skupaj z R-linearnimi preslikavami med njimi $d^n : C^n \to C^{n+1}$ in z dodatno lastnostjo, da je kompozitum poljubnih dveh zaporednih preslikav trivialen: $\forall n \in \mathbb{Z}$: $d^{n+1}d^n = 0$. Kompleks C bomo včasih zapisali kot

$$\cdots \longrightarrow C^{-1} \xrightarrow{d^{-1}} C^0 \xrightarrow{d^0} C^1 \longrightarrow \cdots \longrightarrow C^n \xrightarrow{d^n} C^{n+1} \longrightarrow \cdots.$$

Za ta verižni kompleks definirajmo še naslednja zaporedja levih R-modulov:

$$\begin{aligned}
&\textit{kocikle } Z^*(C) = \ker d^* = (\ker d^n)_{n\in\mathbb{Z}},\\
&\textit{korobove } B^*(C) = \operatorname{im} d^* = (\operatorname{im} d^{n-1})_{n\in\mathbb{Z}},\\
&\textit{kohomologijo } H^*(C) = Z^*(C)/B^*(C) = (\ker d^n/\operatorname{im} d^{n-1})_{n\in\mathbb{Z}}.
\end{aligned}$$

Omenimo še, da elementom R-modulov $\ker d^n = Z^n(C)$ in $\operatorname{im} d^{n-1} = B^n(C)$ pravimo *n-kocikli* in *n-korobovi*.

Definicija 3.5. Naj bo R kolobar z enoto in M levi R modul. *R-resolucija* $F = (F_{n-1}, \delta_n)_{n\in\mathbb{N}}$ levega R-modula M je zaporedje levih R-modulov F_n in R-linearnih preslikav $\delta_n : F_n \to F_{n-1}$ med njimi, za katero obstaja R-linearna preslikava $\delta_0 \colon F_0 \to M$, da je

$$\cdots \longrightarrow F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

eksaktno zaporedje. Če je vsak F_n prost R-modul, ji pravimo *prosta resolucija*.

Čeprav je resolucija definirana drugače, bomo zaradi enostavnosti tudi eksaktnemu zaporedju

$$\cdots \longrightarrow F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

rekli kar resolucija.

Primer 3.6. $\mathbb{Z}$-modul $\mathbb{Z}_2$ dopušča prosto resolucijo

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\bmod 2} \mathbb{Z}_2 \longrightarrow 0.$$

Kako je vse to povezano z razširitvami grup? Imamo razširitev grupe G po abelovi grupi A. Vemo že, da je A levi G-modul. $\mathbb{Z}$ obravnamo kot trivialni G-modul (homomorfizem $\chi : G \to \operatorname{Aut}\mathbb{Z}$ je trivialen). Denimo, da imamo neko prosto resolucijo F:

$$\cdots \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow \mathbb{Z}$$

za G-modul $\mathbb{Z}$.

Spomnimo se, da je za G-modula N in M množica $\operatorname{Hom}_G(N, M)$ vseh G-homomorfizmov ($\mathbb{Z}G$-linearnih preslikav) med njima abelova grupa. Ker ima A strukturo G-modula, lahko na prosti resoluciji F uporabimo kontravariantni funktor $\operatorname{Hom}_G(-, A)$. Ta funktor G-modul M preslika v $\operatorname{Hom}_G(M, A)$, G-homomorfizem $\alpha : M \to N$ med dvema G-moduloma M in N pa preslika v preslikavo $\operatorname{Hom}_G(N, A) \to \operatorname{Hom}_G(M, A)$, ki $\rho \in \operatorname{Hom}_G(N, A)$ slika v kompozitum $\rho\alpha \in \operatorname{Hom}_G(M, A)$. Tako dobimo naslednji koverižni kompleks abelovih grup ($\mathbb{Z}$-modulov):

$$\cdots \leftarrow \operatorname{Hom}_G(F_n, A) \leftarrow \operatorname{Hom}_G(F_{n-1}, A) \leftarrow \cdots \leftarrow \operatorname{Hom}_G(F_0, A) \leftarrow \operatorname{Hom}_G(\mathbb{Z}, A).$$

Če v tem koverižnem kompleksu na -1-vem mestu zamenjamo $\operatorname{Hom}_G(\mathbb{Z}, A)$ z 0, dobimo nov koverižni kompleks, ki ga označimo s $\operatorname{Hom}_G(F, A)$.

Definicija 3.7. Naj bo F neka prosta resolucija G-modula $\mathbb{Z}$. *Kohomologijo* grupe G s koeficienti v G-modulu A definiramo kot kohomologijo verižnega kompleksa $\operatorname{Hom}_G(F, A)$ in jo označimo z $H^*(G, A)$. Za $n \geq 0$ grupi

$$H^n(G, A) := H^n(\operatorname{Hom}_G(F, A))$$

pravimo *n-ta kohomološka grupa* grupe G s koeficienti v A (pri $n < 0$ so vse kohomološke grupe trivialne).

Da bo ta definicija smiselna, mora biti neodvisna od izbire proste resolucije. Izkaže se, da tudi je. Ne glede na to, kakšno prosto resolucijo izberemo, bodo kohomološke grupe izomorfne (velja celo za vse projektivne resolucije). Gre za znan izrek, dokaza katerega pa tu ne bom vključil, saj je precej obsežen in zahteva razumevanje nekaterih algebraično topoloških pojmov, recimo verižne homotopije. Dokaz lahko najdete na primer v [1]. Namesto tega rajši dokažimo korektnost dveh drugih zgoraj omenjenih zadev.

Trditev 3.8. *Naj bo F neka G-resolucija trivialnega G-modula $\mathbb{Z}$.* $\mathrm{Hom}_G(F, A)$ *je $\mathbb{Z}$-koverižni kompleks.*

Dokaz. Vemo že, da so grupe $\mathrm{Hom}_G(F_n, A)$ abelove, torej so res $\mathbb{Z}$-moduli. Za preslikave δ iz resolucije $F = (F_n, \delta_n)_{n\in\mathbb{N}_0}$ velja $\delta_{n-1}\delta_n = 0$, saj je zaporedje G-modulov v resoluciji eksaktno. Ko na resoluciji

$$\cdots \longrightarrow F_n \xrightarrow{\delta_n} F_{n-1} \xrightarrow{\delta_{n-1}} F_{n-2} \longrightarrow \cdots \xrightarrow{\delta_0} \mathbb{Z} \longrightarrow 0$$

uporabimo funktor $\mathrm{Hom}_G(-, A)$, dobimo

$$\leftarrow \mathrm{Hom}_G(F_n, A) \xleftarrow{\sigma_n} \mathrm{Hom}_G(F_{n-1}, A) \xleftarrow{\sigma_{n-1}} \mathrm{Hom}_G(F_{n-2}, A) \leftarrow \cdots \xleftarrow{\sigma_1} \mathrm{Hom}_G(F_0, A).$$

Tu σ_n predstavlja preslikavo iz $\mathrm{Hom}_G(F_{n-1}, A)$ v $\mathrm{Hom}_G(F_n, A)$, ki element $\rho \in \mathrm{Hom}_G(F_{n-1}, A)$ preslika v $\rho\delta_n$. Če želimo dokazati, da je $\mathrm{Hom}_G(F, A)$ koverižni kompleks, moramo dokazati, da velja $\sigma_n\sigma_{n-1} = 0$. Naj bo $\rho \in \mathrm{Hom}_G(F_{n-2}, A)$. Poračunajmo: $\sigma_n\sigma_{n-1}\rho = \sigma_n(\rho\delta_{n-1}) = \rho\delta_{n-1}\delta_n$. To pa je seveda ničelni homomorfizem, saj je $\delta_{n-1}\delta_n = 0$. □

Naslednje vprašanje je, kako vemo, da prosta resolucija trivialnega G-modula $\mathbb{Z}$ vedno obstaja. Za različne dovolj lepe grupe G obstajajo zelo lepe proste resolucije, za poljubno grupo G pa bo dobra naslednja konstrukcija.

Izrek 3.9. *Obstaja prosta G-resolucija trivialnega G-modula $\mathbb{Z}$.*

Dokaz. Najprej definiramo $\mathbb{Z}$-module $F_n = \mathbb{Z}\langle G^{n+1}\rangle$ (proste $\mathbb{Z}$-module generirane z G^{n+1}) in morfizme $f_n : \mathbb{Z}\langle G^{n+1}\rangle \to \mathbb{Z}\langle G^n\rangle$ med njimi, ki jih na baznih elementih definiramo takole

$$(g_0, g_1, \ldots, g_n) \mapsto \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_n)$$

in nato aditivno razširimo (strešica pomeni, da g_i izpustimo, tako da res dobimo element iz $\mathbb{Z}\langle G^n\rangle$). V istem slogu definiramo še predpis $f_0 : \mathbb{Z}\langle G\rangle \to \mathbb{Z}$ s predpisom $f_0(\sum_{g\in G} n_g g) = \sum_{g\in G} n_g$. Imamo torej naslednje zaporedje $\mathbb{Z}$-modulov:

$$\cdots \longrightarrow F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} \mathbb{Z} \longrightarrow 0.$$

Najprej dokažimo, da je $F = (F_{n-1}, f_n)_{n\in\mathbb{N}_0}$ prosta G-resolucija $\mathbb{Z}$. Očitno so vsi F_n prosti $\mathbb{Z}$-moduli in vse preslikave f_n homomorfizmi. Dokazati moramo torej, da je zaporedje res eksaktno. Očitno je f_0 surjektiven in je zaporedje zato eksaktno pri

$\mathbb{Z}$. Na $\mathbb{Z}$ lahko gledamo kot na $\mathbb{Z}\langle G^0\rangle$ oziroma kot na prosti $\mathbb{Z}$-modul $\mathbb{Z}\langle 1\rangle$ z enim samim baznim elementom. Zato je naslednji sklep veljaven za vse $n \geq 1$.

Oglejmo si kompozitum $f_{n-1}f_n$ na poljubnem baznem elementu $(g_0, g_1, \ldots, g_n)$. Velja

$$\begin{aligned} f_{n-1}f_n(g_0, g_1, \ldots, g_n) &= f_{n-1}\sum_{i=0}^{n}(-1)^i(g_0, \ldots, \hat{g}_i, \ldots, g_n) \\ &= \sum_{i=0}^{n}(-1)^i f_{n-1}(g_0, \ldots, \hat{g}_i, \ldots, g_n). \end{aligned}$$

Ko bomo upoštevali še predpis preslikave f_{n-1}, bomo dobili neko vsoto členov oblike $(\pm 1)(g_0, \ldots, \hat{g}_i, \ldots, \hat{g}_j, \ldots, g_n)$. Tu je g_j element, ki izgine zaradi f_{n-1}. Imamo dve možnosti $j > i$ ali $j < i$. Temu ustrezno lahko zadnjo vsoto razbijemo na dve vsoti. Napisano s točno formulo, dobimo vsoti

$$\Sigma_1 = \sum_{0\leq j<i\leq n}(-1)^i(-1)^j(g_0, \ldots, \hat{g}_j, \ldots, \hat{g}_i, \ldots, g_n)$$

in

$$\Sigma_2 = \sum_{0\leq i<j\leq n}(-1)^i(-1)^{j-1}(g_0, \ldots, \hat{g}_i, \ldots, \hat{g}_j, \ldots, g_n).$$

V drugi vsoti imamo eksponent $j-1$ zato, ker je g_j dejansko na $(j-1)$-vem mestu, saj vmes že manjka g_i. To se v prvi vsoti ne zgodi, saj je $j < i$. Če povzamemo, velja $f_{n-1}f_n(g_0, g_1, \ldots, g_n) = \Sigma_1 + \Sigma_2$.

Ampak če v drugi vsoti samo preimenujemo sumacijska indeksa (i, j) v (j, i), dobimo

$$\Sigma_2 = \sum_{0\leq j<i\leq n}(-1)^j(-1)^{i-1}(g_0, \ldots, \hat{g}_j, \ldots, \hat{g}_i, \ldots, g_n) = -\Sigma_1.$$

Zato velja $f_{n-1}f_n = 0$, kar pomeni $\operatorname{im} f_n \leq \ker f_{n-1}$. Da dokažemo eksaktnost, moramo dokazati še obratno.

Naj bo $x = \sum_{i=1}^{N} n_i(x_0^i, x_1^i, \ldots, x_{n-1}^i)$ iz $\ker f_{n-1}$ (tu i predstavlja drugi indeks, ne potence). Torej velja $f_{n-1}\sum_{i=1}^{N} n_i(x_0^i, x_1^i, \ldots, x_{n-1}^i) = 0$. Ob upoštevanju predpisa preslikave f_{n-1} sklepamo

$$\sum_{i=1}^{N} n_i \sum_{j=0}^{n}(-1)^j(x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) = 0.$$

Poskusimo poiskati element F_n, ki se z f_n slika v x. Ustrezen element bo $y = \sum_{i=1}^{N} n_i(g, x_0^i, x_1^i, \ldots, x_{n-1}^i)$, kjer je g nek element grupe G. Motivacija za izbor y, ki za razumevanje samega dokaza sicer ni potrebna, prihaja iz algebraične topologije. Če $(x_0, x_1, \ldots, x_{n-1})$ predstavlja nek $(n-1)$-simpleks, je njegova slika pri f_{n-1} ravno njegov rob. Element x je nek $(n-1)$-dimenzionalni simplicialni kompleks, f_{n-1} pa slika x v njegov rob δx, ki mora biti enak 0. Zato je topološko gledano smiseln izbor n-dimenzionalnega simplicialnega kompleksa y, katerega rob $\delta y = f_n(y)$ je enak x, ravno stožec nad x. Poračunajmo:

$$
\begin{aligned}
f_n(y) &= f_n \sum_{i=1}^{N} n_i(g, x_0^i, x_1^i, \ldots, x_{n-1}^i) = \\
&= \sum_{i=1}^{N} n_i f_n(g, x_0^i, x_1^i, \ldots, x_{n-1}^i) = \\
&= \sum_{i=1}^{N} n_i \left[(x_0^i, x_1^i, \ldots, x_{n-1}^i) - \sum_{j=0}^{n} (-1)^j (g, x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) \right] = \\
&= \sum_{i=1}^{N} n_i (x_0^i, x_1^i, \ldots, x_{n-1}^i) - \sum_{i=1}^{N} n_i \sum_{j=0}^{n} (-1)^j (g, x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) = \\
&= x - \sum_{i=1}^{N} n_i \sum_{j=0}^{n} (-1)^j (g, x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i).
\end{aligned}
$$

Ker pa je $x \in \ker f_{n-1}$, vemo, da velja

$$\sum_{i=1}^{N} n_i \sum_{j=0}^{n} (-1)^j (x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) = 0.$$

To je $\mathbb{Z}$-linearna kombinacija baznih elementov, ki je enaka 0. Ker so bazni elementi neodvisni, mora biti celoštevilski koeficient pred vsakim baznim elementom, ko vsoto razvijemo, enak 0. Potemtakem pa drži tudi

$$\sum_{i=1}^{N} n_i \sum_{j=0}^{n} (-1)^j (g, x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) = 0,$$

saj je $\mathbb{Z}$-linearna kombinacija enaka kot prejšnja, le da smo bazne elemente preimenovali po predpisu

$$(x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i) \mapsto (g, x_0^i, x_1^i, \ldots, \hat{x_j}^i, \ldots, x_{n-1}^i).$$

Dokazali smo $f_n(y) = x$, zato drži $\ker f_{n-1} \leq \operatorname{im} f_n$ in nazadnje $\ker f_{n-1} = \operatorname{im} f_n$. Zaporedje modulov je zato zares eksaktno.

Resolucija F je torej res prosta $\mathbb{Z}$-resolucija. Vpeljimo zdaj delovanje grupe G na abelovi grupi ($\mathbb{Z}$-modulu) F_n. Definiramo ga na baznih elementih na samoumeven način $g(g_0, g_1, \ldots, g_n) = (gg_0, gg_1, \ldots, gg_n)$. Trivialno je preveriti, da gre zares za delovanje. Zato so F_n pravzaprav G-moduli. $\mathbb{Z}$ seveda obravnavamo kot trivialni G-modul. Očitno so pri takšni definicji delovanja tudi homomorfizmi f_n pravzaprav G-linearne preslikave. Enostavno je preveriti, da velja $gf_n(g_0, g_1, \ldots, g_n) = f_n g(g_0, g_1, \ldots, g_n)$.

Tako F postane G-resolucija. Ali je ta resolucija tudi prosta? Da! Za bazo F_n lahko vzamemo elemente oblike $(1, g_1, \ldots, g_n)$. Očitno so neodvisni, vsak element F_n pa lahko tudi zapišemo kot njihovo G-linearno kombinacijo. Element $(g_0, g_1, \ldots, g_n)$ si lahko namreč predstavljamo kot $g_0(1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n)$. Zato je F zares prosta G-resolucija trivialnega G-modula $\mathbb{Z}$. □

Iz razlogov, ki bodo postali jasni kasneje, pa se ponavadi to isto resolucijo predstavi nekoliko drugače. Zgoraj smo definirali bazo $\mathbb{Z}$-modula F_n, zdajle pa bomo definirali bazo $\mathbb{Z}G$-modula F_n, in sicer v obliki $(1, g_1, g_1g_2 \ldots, g_1g_2 \ldots g_n)$, le da to

označimo kot $[g_1|g_2|\dots|g_n]$. Posebej zapišemo $(g) = g(1) = g[\ ]$. Temu zapisu pravimo *bar notacija*, resoluciji F pa *standardna* oziroma *bar resolucija* grupe G.

Na F_n lahko zdaj gledamo kot na prosti G-modul z bazo G^n, torej kot na $\mathbb{Z}G\langle G^n\rangle$. Posebej na F_0 lahko gledamo kot na prost G-modul, generiran z enim elementom. Zato je $F_0 \cong \mathbb{Z}G$. V takšnem zapisu se spremeni tudi predpis G-homomorfizmov f_n. Sedaj se $f_n[g_1|g_2|\dots|g_n]$ slika v

$$g_1[g_2|g_3|\dots|g_n] + \Big(\sum_{i=1}^{n-1}(-1)^i[g_1|\dots|g_ig_{i+1}|\dots|g_n]\Big) + (-1)^n[g_1|g_2|\dots|g_{n-1}].$$

Oglejmo si preslikave f_n za majhne vrednosti n:

$$\begin{aligned} f_3[x|y|z] &= x[y|z] - [xy|z] + [x|yz] - [x|y],\\ f_2[x|y] &= x[y] - [xy] + [x],\\ f_1[x] &= x[\ ] - [\ ] = x - 1,\\ f_0(1) &= 1. \end{aligned}$$

S pomočjo trditve 3.8 in izreka 3.9 si lahko pogledamo, kako izgleda nekaj kohomoloških grup za majhne n pri standardni resoluciji. Naj bo $F = (F_{n-1}, f_n)_{n\in\mathbb{N}}$ standardna resolucija grupe G. Če sledimo dokazu trditve 3.8, za $n \geq 1$ dobimo $\sigma_n : \mathrm{Hom}_G(F_{n-1}, A) \to \mathrm{Hom}_G(F_n, A)$ s predpisom $\sigma_n(\rho) = \rho f_n$. Preslikava $\sigma_n(\rho)$ je torej G-homomorfizem iz F_n v A, ki bazni element $[g_1|g_2|\dots|g_n]$ preslika v

$$g_1\rho[g_2|g_3|\dots|g_n] + \Big(\sum_{i=1}^{n-1}(-1)^i\rho[g_1|\dots|g_ig_{i+1}|\dots|g_n]\Big) + (-1)^n\rho[g_1|g_2|\dots|g_{n-1}].$$

Kohomološko grupo $H^n(G, A) = H^n(\mathrm{Hom}_G(F, A))$ za $n \geq 1$ po definiciji dobimo kot kvocient $\ker\sigma_{n+1}/\mathrm{im}\,\sigma_n$. Za $n = 0$ pa velja $H^0(G, A) = \ker\sigma_1$, saj smo na mestu -1 v koverižnem kompleksu $\mathrm{Hom}_G(\mathbb{Z}, A)$ zamenjali z 0.

Kaj so elementi $\ker\sigma_{n+1}$? Vse funkcije $\vartheta \in \mathrm{Hom}_G(F_n, A)$, za katere je izraz

$$g_1\vartheta[g_2|g_3|\dots|g_{n+1}] + \Big(\sum_{i=1}^{n}(-1)^i\vartheta[g_1|\dots|g_ig_{i+1}|\dots|g_{n+1}]\Big) + (-1)^{n+1}\vartheta[g_1|g_2|\dots|g_n]$$

identično enak 0 za vse $g_1, g_2, \dots, g_{n+1} \in G$. Kaj pa so elementi $\mathrm{im}\,\sigma_n$? Ravno vsi G-homomorfizmi iz F_n v A, ki so oblike $\sigma_n(\rho)$ za G-homomorfizem $\rho : F_{n-1} \to A$. Formulo za $\sigma_n(\rho)$ pa lahko najdete nekaj vrstic višje.

Elementi $H^n(G, A)$ (za $n \geq 1$) so ravno vsi ekvivalenčni razredi G-homomorfizmov $\vartheta : F_n \to A$, za katere je izraz

$$g_1\vartheta[g_2|g_3|\dots|g_{n+1}] + \Big(\sum_{i=1}^{n}(-1)^i\vartheta[g_1|\dots|g_ig_{i+1}|\dots|g_{n+1}]\Big) + (-1)^{n+1}\vartheta[g_1|g_2|\dots|g_n]$$

identično enak 0, dva takšna G-homomorfizma ϑ_1 in ϑ_2 pa štejemo za ekvivalentna, če obstaja takšen G-homomorfizem $\rho : F_{n-1} \to A$, da se ϑ_1 in ϑ_2 razlikujeta za $\sigma_n(\rho)$.

Primer 3.10. Če je, denimo, $n = 2$, je jedro $\ker\sigma_3$ enako

$$\{f \in \mathrm{Hom}_G(F_2, A) | \forall x, y, z \in G : xf[y|z] - f[xy|z] + f[x|yz] - f[x|y] = 0\},$$

pri $n = 1$ je jedro $\ker\sigma_2$ enako

$$\{f \in \mathrm{Hom}_G(F_1, A) | \forall x, y \in G : xf[y] - f[xy] + f[x] = 0\},$$

pri $n = 0$ pa velja

$$\ker \sigma_1 = \{f \in \mathrm{Hom}_G(F_0, A) | \forall x \in G : xf[\,] - f[\,] = 0\}.$$

Podobno je slika $\mathrm{im}\,\sigma_2$ enaka

$$\{f \in \mathrm{Hom}_G(F_2, A) | \exists \varphi \in \mathrm{Hom}_G(F_1, A) : \forall x, y \in G : f[x|y] = x\varphi[y] - \varphi[xy] + \varphi[x]\}$$

in slika $\mathrm{im}\,\sigma_1$ enaka

$$\{f \in \mathrm{Hom}_G(F_1, A) | \exists \varphi \in \mathrm{Hom}_G(F_0, A) : \forall x \in G : f[x] = x\varphi[\,] - \varphi[\,]\}.$$

Definicija 3.11. Naj grupa G deluje na abelovi grupi A. Podmnožici grupe A $\{a \in A | \forall g \in G : ga = a\}$ pravimo *grupa negibnih točk delovanja* grupe G na grupi A in jo označimo s $\mathrm{Fix}(G, A)$.

Trivialno je preveriti, da je zares grupa in da drži $\mathrm{Fix}(G, A) \leq A$.

Trditev 3.12. *Naj bo G grupa in A abelova grupa. Fiksirajmo delovanje G na A (določimo G-modul A). Velja $H^0(G, A) \cong \mathrm{Fix}(G, A)$.*

Dokaz. Že iz primera 3.10 vemo, da velja

$$H^0(G, A) = \ker \sigma_1 = \{f \in \mathrm{Hom}_G(F_0, A) | \forall x \in G : xf[\,] - f[\,] = 0\}.$$

Vemo tudi, da je $F_0 \cong \mathbb{Z}G\langle G^0 \rangle \cong \mathbb{Z}G\langle [\,] \rangle \cong \mathbb{Z}G$. Grupo F_0 zato obravnavamo kot prost G-modul nad generatorjem $[\,]$. Ker za vsak $x \in G$ velja $xf[\,] = f[\,]$, mora biti $f[\,]$ negibna točka delovanja. Vsak G-homomorfizem iz $\ker \sigma_1$ je natančno določen z $f[\,]$, saj za $\sum_{g \in G} n_g g \in \mathbb{Z}G$ velja

$$f\Big(\sum_{g \in G} n_g g[\,]\Big) = \sum_{g \in G} n_g g f[\,] = \sum_{g \in G} n_g f[\,].$$

Definirajmo zdaj izomorfizem $\alpha : H^0(G, A) \to \mathrm{Fix}(G, A)$ in sicer s predpisom $\alpha(f) = f[\,]$. Očitno je α homomorfizem, saj velja

$$\alpha(f + g) = (f + g)[\,] = f[\,] + g[\,] = \alpha(f) + \alpha(g).$$

Homomorfizem α je injektiven, ker je $f \in H^0(G, A)$ natančno določen z $f[\,]$. Dokazati moramo še, da je surjektiven. Naj bo $a \in \mathrm{Fix}(G, A)$ negibna točka. Definirajmo preslikavo $f_a : F_0 \to A$ s predpisom

$$f_a\Big(\sum_{g \in G} n_g g[\,]\Big) = \sum_{g \in G} n_g a.$$

Očitno je f_a G-homomorfizem in velja $f_a[\,] = a$. Ker je a negibna točka, tudi za vsak $x \in G$ velja $xf_a[\,] = xa = a = f_a[\,]$. Zato je $f_a \in H^0(G, A)$ in res drži $H^0(G, A) \cong \mathrm{Fix}(G, A)$. □

4. Razširitve grup z abelovim jedrom

V nadaljevanju se bomo ukvarjali s problemom, kako za dani A in G poiskati vse takšne grupe E, ki imajo za edinko abelovo grupo A, kvocientna grupa E/A pa je izomorfna G. To lahko preformuliramo v iskanje vseh razširitev

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1.$$

Kot smo že videli v primeru 3.3 potem grupa G deluje na grupo A s predpisom $i(ga) = s(g)i(a)s(g)^{-1}$ in ta predpis je neodvisen od izbire transverzale. A je torej nek G-modul. Ampak kateri? G namreč lahko deluje na A na več različnih načinov. Vsako delovanje G na A, torej vsak homomorfizem $\chi : G \to \operatorname{Aut} A$, rezultira v drugačnem G modulu A. Kateri homomorfizem χ je torej tisti, ki določa delovanje $i(ga) = s(g)i(a)s(g)^{-1}$?

Izkaže se, da katerikoli homomorfizem χ določa delovanje takšne oblike. To pomeni, da moramo, če želimo poiskati vse razširitve, najprej poiskati vsa delovanja, torej vse homomorfizme $\chi : G \to \operatorname{Aut} A$ in nato še vsako delovanje fiksirati ter za fiksni G-modul A poiskati vse razširitve.

Definicija 4.1. Naj grupa G deluje na abelovi grupi A. Naj bo $\chi : G \to \operatorname{Aut} A$ ustrezni homomorfizem, ki predstavlja to delovanje. Grupi, ki je kot množica enaka $A \times G$, grupno operacijo pa definiramo takole $(a, g) \circ (b, h) = (a + gb, gh)$, pravimo *semidirektni produkt* grup A in G in jo označimo $A \rtimes_\chi G$.

Običajno je jasno, za katero delovanje gre, in pišemo samo $A \rtimes G$. V kolikor je delovanje trivialno ($\forall g \in G : \chi(g) = id_A$), velja kar $A \rtimes_\chi G = A \times G$.

Izrek 4.2. *Za vsako delovanje grupe G na grupi A obstaja razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1,$$

ki jo realizira.

Dokaz. Naj bo χ neko delovanje. Ustrezna razširitev bo kar

$$0 \longrightarrow A \xrightarrow{i} A \rtimes_\chi G \xrightarrow{\pi} G \longrightarrow 1.$$

Tu sta $i(a) := (a, 1)$ in $\pi(a, g) = g$. Dokazati moramo le, da je semidirektni produkt $A \rtimes G = A \rtimes_\chi G$ zares grupa in da G prek $A \rtimes G$ z zvezo $i(g \bullet a) = s(g)i(a)s(g)^{-1}$ (to drugo delovanje začasno pišimo kot $g \bullet a$) na A res porodi delovanje χ.

Operacija je asociativna:

$$\begin{aligned}((a, g)(b, h))(c, k) &= (a + gb, gh)(c, k) = \\ &= (a + gb + ghc, ghk), \\ (a, g)((b, h)(c, k)) &= (a, g)(b + hc, hk) = \\ &= (a + g(b + hc), ghk) = \\ &= (a + gb + ghc, ghk).\end{aligned}$$

Element $(0, 1)$ je enota grupe:

$$\begin{aligned}(a, g)(0, 1) &= (a + g \cdot 0, g \cdot 1) = \\ &= (a + 0, g) = \\ &= (a, g), \\ (0, 1)(a, g) &= (0 + 1 \cdot a, 1 \cdot g) = \\ &= (a, g).\end{aligned}$$

Vsak element (a, g) ima inverz $(g^{-1}(-a), g^{-1})$:

$$\begin{aligned}(a,g)(g^{-1}(-a),g^{-1}) &= (a+gg^{-1}(-a), gg^{-1}) = \\ &= (a+(-a),1) = \\ &= (0,1), \\ (g^{-1}(-a),g^{-1})(a,g) &= (g^{-1}(-a)+g^{-1}a, g^{-1}g) = \\ &= (g^{-1}(-a+a),1) = \\ &= (0,1).\end{aligned}$$

$A \rtimes G$ je zato res grupa. Definirajmo preslikavo $s := G \to A \rtimes G$ s predpisom $s(g) = (0, g)$. Ker je $\pi s(g) = \pi(0, g) = g$, je $\pi s = id_G$ in je s transverzala. Spomnimo se zveze $i(g \bullet a) = s(g)i(a)s(g)^{-1}$. Ob upoštevanju, kaj sta i in s, se zveza glasi

$$(g \bullet a, 1) = (0, g)(a, 1)(0, g^{-1}) = (ga, g)(0, g^{-1}) = (ga, 1).$$

Ker je i injektiven, velja $g \bullet a = ga$ in delovanji zares sovpadata. □

Primer 4.3. Oglejmo si razširitev

$$0 \longrightarrow \mathbb{Z} \longrightarrow E \longrightarrow \mathbb{Z}_2 \longrightarrow 0.$$

Celoten avtomorfizem grupe $\mathbb{Z}$ je določen s sliko generatorja 1, ki se mora slikati v generator, torej v 1 ali -1. Zato sta edina avtomorfizma celih števil $id_{\mathbb{Z}}(n) = n$ in $\lambda(n) = -n$ in velja $\operatorname{Aut}\mathbb{Z} \cong \mathbb{Z}_2$. Obstajata dva homomorfizma iz $\mathbb{Z}_2$ v $\mathbb{Z}_2$, trivialni in identiteta, ter zato tudi dva homomorfizma iz $\mathbb{Z}_2$ v $\operatorname{Aut}\mathbb{Z}$. Sledi, da obstajata dve delovanji $\mathbb{Z}_2$ na $\mathbb{Z}$.

Iz trivialnega homomorfizma $\mathbb{Z}_2 \to \operatorname{Aut}\mathbb{Z}$ dobimo trivialno delovanje $gn = n$ in navadni kartezični produkt $= \mathbb{Z} \times \mathbb{Z}_2$. Pri identičnem homomorfizmu pa dobimo delovanje, ki ga lahko povzamemo s formulo $gn = (-1)^g n$ (če na $\mathbb{Z}_2$ gledamo kot na $\{0, 1\}$) in grupo $\mathbb{Z} \rtimes \mathbb{Z}_2$, ki je kot množica enaka $\mathbb{Z} \times \mathbb{Z}_2$, operacija na njej pa je enaka $(n, g)(m, h) = (n + (-1)^g m, g + h)$. Ta grupa je izomorfna tako imenovani neskončni diedrski grupi $D_\infty = \langle x, y | y^2 = 1, xy = yx^{-1} \rangle$. Generatorja lahko prepoznamo v $x = (1, 0)$ in $y = (0, 1)$.

Ker obstajata samo 2 delovanji $\mathbb{Z}_2$ na $\mathbb{Z}$, sta edini grupi E, ki ju lahko prepoznamo kot semidirektna produkta, ravno $\mathbb{Z} \times \mathbb{Z}_2$ in D_∞. Vendar pa

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

in

$$0 \longrightarrow \mathbb{Z} \longrightarrow D_\infty \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

nista edini neekvivalentni razširitvi grupe. Obstaja vsaj še naslednja:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\bmod 2} \mathbb{Z}_2 \longrightarrow 0.$$

Ker $\mathbb{Z} \ncong \mathbb{Z} \times \mathbb{Z}_2$ in $\mathbb{Z} \ncong D_\infty$ ter ekvivalentnost implicira izomorfnost, ta razširitev ne more biti evivalentna kateri od zgornjih dveh. Samo s pomočjo semidirektnih produktov torej ne bomo dobili vseh možnih razširitev. Ravno tako se lahko zgodi, da za fiksno delovanje G na A obstaja več grup E, ki ga realizirajo. To lahko vidimo ravno iz zgornjega primera, saj $\mathbb{Z}_2$ na $\mathbb{Z}$ deluje trivialno tako v primeru $E = \mathbb{Z} \times \mathbb{Z}_2$ kot v primeru $E = \mathbb{Z}$.

Izrek 4.4. *Denimo, da imamo neko razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

grupe G po abelovi grupi A. Potem ima grupa E enako moč kot $A \times G$.

Dokaz. Poiskati moramo neko bijektivno preslikavo $F : A \times G \to E$. Izberimo neko transverzalo s. Zanjo velja $\pi s = id_G$. Definirajmo $F(a, g) := i(a)s(g)$. Pokažimo, da je takšna preslikava res injektivna in surjektivna.

Denimo, da za neka (a, g) in $(b, h) \in A \times G$ velja $i(a)s(g) = i(b)s(h)$. Potem velja tudi

$$g = \pi(i(a)s(g)) = \pi(i(b)s(h)) = h,$$

saj je $\pi i(a) = 1$ ($\operatorname{im} i = \ker \pi$) in $\pi s = id_G$. Če velja $g = h$, potem mora veljati tudi $s(g) = s(h)$ in posledično $i(a) = i(b)$. Ampak morfizem i je injektiven, zato drži tudi $a = b$. Preslikava F je res injektivna.

Naj bo $x \in E$ poljuben. Označimo $g = \pi(x)$ in $y = s(g)$. Velja $\pi(y) = g$ in zato $\pi(xy^{-1}) = \pi(x)\pi(y)^{-1} = 1$. Zaradi eksaktnosti pri E lahko sklepamo $xy^{-1} \in \ker \pi = \operatorname{im} i$. Obstajati mora takšen $a \in A$, da velja $xy^{-1} = i(a)$, kar pa pomeni $x = i(a)y = i(a)s(g)$. Preslikava F je zato tudi surjektivna. □

Rezultat tega izreka je zelo pomemben, saj pomeni, da lahko na vsako grupo E iz razširitve G po A gledamo kot na množico $A \times G$ z neko čudno grupno operacijo. Tako lahko, recimo, v primeru 4.3 na D_∞ gledamo kot na $\mathbb{Z} \times \mathbb{Z}_2$ z operacijo $(n, g)(m, h) = (n + (-1)^g m, g + h)$. Takojšnja zanimiva posledica tega izreka je naslednji izrek.

Izrek 4.5. *Naj bo E razširitev grupe G po abelovi grupi A:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G \longrightarrow 1. \\ & & & & = \downarrow & \swarrow_{s} & \\ & & & & E & & \end{array}$$

Grupa E je ekvivalentna $A \rtimes G$ natanko takrat, ko za razširitev obstaja transverzala s, ki je homomorfizem.

Dokaz. Če je $E \equiv A \rtimes G$, je očitno transverzala $s : G \to A \rtimes G$ podana s predpisom $s(g) = (0, g)$ homomorfizem. Dokažimo še drugo smer.

Naj bo s transverzalni homomorfizem. Kot v prejšnjem dokazu definirajmo bijekcijo $F : A \times G \to E$ s predpisom $F(a, g) = i(a)s(g)$. Po prejšnjem izreku lahko na E gledamo kot na $A \times G$ z neko čudno operacijo. Bijekcija F je v bistvu ravno prenos iz enega zapisa v drugega. Denimo, da imamo dva poljubna elementa $x, y \in E$. Zanima nas njun produkt. Zapišemo ju lahko kot $x = i(a)s(g)$ in $y = i(b)g(h)$ za neka $a, b \in A$ in neka $g, h \in G$. Izraz $xy = i(a)s(g)i(b)s(h)$ želimo pretvoriti v obliko $i(c)s(k)$ za neka $c \in A$ in $k \in G$.

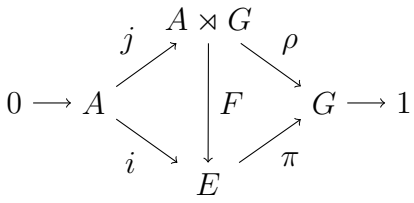
Spomnimo se, kako grupa G deluje na grupo A. Natančneje, spomnimo se zveze $i(ga) = s(g)i(a)s(g)^{-1}$. To zvezo lahko prepišemo v pravilo $i(ga)s(g) = s(g)i(a)$, ki ga nato uporabimo na srednjih dveh členih izraza $i(a)s(g)i(b)s(h)$, da dobimo $i(a)i(gb)s(g)s(h)$. Tako i kot s sta homomorfizma, zato je to enako $i(a + gb)s(gh)$. Če vse skupaj strnemo, ugotovimo, da velja

$$i(a)s(g)i(b)s(h) = i(a + gb)s(gh).$$

Če na zadnjo enakost pogledamo še v $A \times G$ s čudno operacijo (če potegnemo nazaj s F^{-1}), smo dobili ravno zvezo

$$(a, g) \circ (b, h) = (a + gb, gh),$$

kar pa je ravno operacija v semidirektnem produktu. Zato velja $E \cong A \rtimes G$, izomorfizem med njima pa je kar F. Velja še več. Razširitvi sta ekvivalentni, saj diagram



komutira. Z j označimo vložitev na prvo, z ρ pa projekcijo na drugo komponento. Res za vsaka $a \in A$ in $g \in G$ drži

$$Fj(a) = F(a, 1) = i(a)s(1) = i(a)$$

in

$$\pi F(a, g) = \pi(i(a)s(g)) = \pi(i(a))\pi(s(g)) = g = \rho(a, g).$$

□

Takšnim razširitvam, kjer obstaja transverzala, ki je hkrati homomorfizem, pravimo tudi *razcepne razširitve*. Poglejmo si nekaj zanimivih dejstev o razcepnih razširitvah.

Definicija 4.6. Naj bo E grupa ter $M \triangleleft E$ in $H \leq E$ takšni podgrupi, da velja $E = HM$ in $M \cap H = 1_E$. Potem pravimo, da je grupa H *komplement* grupe M v grupi E.

Omenimo, da pod omenjenimi pogoji velja

$$E/M = HM/M \cong H/M \cap H = H/1 \cong H.$$

Kaj to pomeni v našem primeru? Recimo, da imamo grupo E in njeno abelovo podgrupo edinko A. Naj bo G komplement A v E. Po zgornjem velja $G \cong E/A$. Oglejmo si razširitev

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} E/A \longrightarrow 1,$$

kjer je i inkluzija A v E, π pa kvocientna preslikava z jedrom A. Pokažimo, da je π, zoženo na G, izomorfizem.

Denimo, da za dva elementa $g, h \in G$ velja $gA = hA$. To je ekvivalentno $h^{-1}g \in A$. Ker pa je $G \leq E$, velja tudi $h^{-1}g \in G$. Od tu dobimo $h^{-1}g \in G \cap A$, kar pomeni $h^{-1}g = 1$ in zato $g = h$. Sledi, da je homomorfizem π, zožen na G, injektiven.

Naj bo $e \in E$. Ker je G komplement A v E, velja $E = GA$. Zaradi tega obstajata $a \in A$ in $g \in G$, da velja $e = ga$. Sledi, da je homomorfizem π, zožen na G, surjektiven. Za poljuben element eA grupe E/A velja zveza

$$eA = gaA = gA = \pi(g).$$

Dokazali smo, da je $\pi|_G$ izomorfizem. Zato ima inverz s, ki je hkrati transverzala. Sledi, da je razširitev razcepna. Po izreku 4.5 sledi, da $E \equiv A \rtimes E/A$. Mimogrede smo dokazali naslednjo trditev.

Trditev 4.7. *Naj bo A abelova edinka v grupi E in razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \equiv A \rtimes G \xrightarrow{\pi} G \longrightarrow 1,$$

kjer je i inkluzija A v E, razcepna. Potem so vsi komplementi A v E izomorfni G in vsak komplement K poraja transverzalo $s_K : G \to K \leq E$, ki je hkrati izomorfizem.

Glede na to, da velja $E \equiv A \rtimes G$ in da je s_K transverzala, lahko $s_K \colon G \to A \rtimes G$ podamo s predpisom $s_K(g) = (d_K(g), g)$ za neko preslikavo $d_K : G \to A$. Transverzala s_K je tudi homomorfizem, zato morata biti izraza

$$s_K(gh) = (d_K(gh), gh)$$

in

$$s_K(g)s_K(h) = (d_K(g), g)(d_K(h), h) = (d_K(g) + gd_K(h), gh)$$

enaka. Veljati mora

$$d_K(gh) = d_K(g) + gd_K(h).$$

Definicija 4.8. Naj bo G grupa in A abelova grupa. Predpišimo delovanje G na A. Preslikavi $d : G \to A$, ki zadošča pogoju $d(gh) = d(g)+gd(h)$ pravimo *odvod* oziroma *odvajanje*. Množico vseh odvodov, ki slikajo iz G v A, označimo z $\mathrm{Der}(G, A)$.

Ker odvajanja slikajo v abelovo grupo A, je na množico $\mathrm{Der}(G, A)$ smiselno vpeljati operacijo seštevanja odvajanj. Enostavno je preveriti, da s tem množica $\mathrm{Der}(G, A)$ postane abelova grupa.

Zgoraj smo pokazali, da vsakemu komplementu K lahko pripišemo odvod d_K. Velja pa tudi obrat. Vsakemu odvodu lahko pripišemo komplement. Naj bo $d \in \mathrm{Der}(G, A)$. Potem je $s : G \to E \equiv A \rtimes G$ podana s predpisom $s(g) = (d(g), g)$ očitno transverzala in homomorfizem. Ta homomorfizem je očitno tudi injektiven zaradi druge komponente. Definirajmo $K_d := \operatorname{im} s$. Očitno $G \cong K_d \leq E$. Grupa K_d je enaka $\{(d(g), g)|g \in G\}$. Dokažimo, da je K_d komplement A v E.

Za odvod velja $d(1) = 0$, saj drži

$$d(1) = d(1 \cdot 1) = d(1) + 1 \cdot d(1) = 2d(1).$$

Če si E predstavljamo kot $A \rtimes G$, je $A \leq E$ enaka $\{(a, 1)|a \in A\} \leq A \rtimes G$. Če je

$$(b, h) \in \{(a, 1)|a \in A\} \cap \{(d(g), g)|g \in G\},$$

mora očitno veljati $h = 1$ in $b = d(h) = d(1) = 0$, zato je presek $A \cap K_d$ zares trivialen.

Dokazati moramo še $E = K_dA$. Naj bo (a, g) poljuben element $A \rtimes G$. Zapišemo ga lahko v obliki

$$(a, g) = (d(g), g)(g^{-1}a - g^{-1}d(g), 1),$$

kjer je očitno prvi faktor v K_d, drugi pa v A.

Odvodu d res lahko priredimo komplement K_d, komplementu K pa odvod d_K. Še več, preslikavi $K \to d_K$ in $d \to K_d$ sta si inverzni. Obstaja bijekcija med komplementi in odvodi.

Če pogledamo $Z^1(G, A) = \ker \sigma_2$ iz primera 3.10 in pogoj za odvod prepišemo v obliko $gd(h)-d(gh)+d(g) = 0$, opazimo sumljivo podobnost. Če to zapišemo v obliki $gd\,[h] - d\,[gh] + d\,[g] = 0$, lahko d zlahka razširimo do preslikave $d : \mathbb{Z}G\,\langle G\rangle \to A$ s predpisom

$$d\Big(\sum_{g\in G}\Big(\sum_{h\in G} n_h h\Big)\,[g]\Big) = \sum_{g\in G}\Big(\sum_{h\in G} n_h h\Big) d\,[g]\,.$$

Enostavno je preveriti, da je novo dobljeni d pravzaprav G-homomorfizem. Prav tako lahko preslikavi $d : \mathbb{Z}G\langle G\rangle \to A$, ki zadošča $gd[h] - d[gh] + d[g] = 0$ priredimo ustrezno preslikavo $d : G \to A$ preprosto tako, da jo zožimo le na bazne elemente. Dokazali smo, da so odvodi $\mathrm{Der}(G, A)$ v bijektivni korespondenci z 1-kocikli $Z^1(G, A)$ grupe G po grupi A pri standardni resoluciji. V resnici smo dokazali še več.

Trditev 4.9. *Če imamo abelovo edinko A v grupi E in razcepno razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \equiv A \rtimes G \xrightarrow{\pi} G \longrightarrow 1,$$

kjer je i inkluzija A v E, potem so komplementi A v E v bijektivni korespondenci z 1- *kocikli $Z^1(G, A)$ grupe G s koeficienti v A pri standardni resoluciji.*

Definicija 4.10. Naj bo G grupa in A abelova grupa. Predpišimo delovanje G na A. Preslikavi $\delta_a : G \to A$ s predpisom oblike $\delta_a(g) = a - ga$, za $a \in A$, pravimo *notranje odvajanje*. Množico vseh notranjih odvajanj, ki slikajo iz G v A, označimo z $\mathrm{InnDer}(G, A)$.

Enostavno je preveriti, da notranja delovanja tvorijo grupo. Notranje odvajanje je res odvajanje, saj velja:

$$\begin{aligned}\delta_a(gh) &= a - gha = \\ &= a - ga + ga - gha = \\ &= a - ga + g(a - ha) = \\ &= \delta_a(g) + g\delta_a(h).\end{aligned}$$

Trditev 4.11. *Naj bo A abelova edinka v grupi E in naj bosta K in L podgrupi E. Obstaja element $a \in A$, da velja $aKa^{-1} = L$ (za podgrupi K in L rečemo, da sta* A-konjugirani*) natanko tedaj, ko se odvajanji d_K in d_L razlikujeta za notranje odvajanje δ_a.*

Dokaz. Že od prej vemo, da lahko privzamemo $E = A \rtimes G$, $A = \{(a, 1)|a \in A\}$, $K = \{(d_K(g), g)|g \in G\}$ in $L = \{(d_L(g), g)|g \in G\}$.

Denimo, da obstaja $a \in A$, da velja $(a, 1)K(-a, 1) = L$. Če primerjamo drugi komponenti, ugotovimo, da mora za vsak $g \in G$ veljati zveza

$$(a, 1)(d_K(g), g)(-a, 1) = (d_L(g), g).$$

Poračunajmo levo stran zgornje enačbe:

$$\begin{aligned}(a, 1)(d_K(g), g)(-a, 1) &= (a + d_K(g), g)(-a, 1) = \\ &= (a + d_K(g) + g(-a), g) = \\ &= (d_K(g) + a - ga, g) = \\ &= (d_K(g) + \delta_a(g), g).\end{aligned}$$

Ker zgornja enačba velja za vsak $g \in G$, sledi $d_L - d_K = \delta_a$.

Obrat trditve je enostaven. Imamo dva komplementa $K = \{(d_K(g), g)|g \in G\}$ in $L = \{(d_L(g), g)|g \in G\}$, katerim pripadajoči delovanji se razlikujeta za δ_a. S praktično enakim računom kot zgoraj le preverimo, da velja

$$(a, 1)(d_K(g), g)(-a, 1) = (d_L(g), g).$$

□

Primerjajmo zdaj $B^1(G,A) = \operatorname{im}\sigma_1$ iz primera 3.10 s predpisom $\delta_a(g) = a - ga$ za notranje odvajanje. Namesto a pišimo $\varphi[\ ]$ in namesto δ_a pišimo le δ. Tu si lahko predstavljamo, da je φ nek G-homomorfizem $\mathbb{Z}G\langle[\ ]\rangle \to A$, ki je enolično določen s sliko $[\ ]$. Ta je lahko tudi a. Preslikavo δ lahko razširimo do preslikave $\mathbb{Z}G\langle G\rangle \to A$ s predpisom:

$$\delta\Big(\sum_{g\in G}\Big(\sum_{h\in G} n_h h\Big)[g]\Big) = \sum_{g\in G}\Big(\sum_{h\in G} n_h h\Big)\delta[g].$$

Enostavno je preveriti, da je novo dobljena δ res G-homomorfizem. Notranjemu odvajanju δ_a smo priredili 1-korob δ grupe G po A pri standardni resoluciji. Obratno lahko tudi 1-korobu priredimo notranje odvajanje, preprosto tako, da ga zožimo le na bazne elemente. Notranja odvajanja in 1-korobovi $B^1(G,A)$ so torej v bijektivni korespondenci. Dokazali smo naslednji izrek.

Izrek 4.12. *Naj bo A abelova edinka v grupi E. Naj bo $G \cong E/A$. Naj bo razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1,$$

kjer je i inkluzija, π pa kvocientna projekcija komponirana z izomorfizmom, razcepna. Obstaja bijekcija med množico ekvivalenčnih razredov komplementov A v E po ekvivalenčni relaciji A-konjugiranosti in prvo kohomološko grupo $H^1(G,A)$.

Velja omeniti, da vse komplemente, vsa odvajanja, vsa notranja odvajanja, ali število vseh danemu komplementu A-konjugiranih komplementov res lahko dobimo le tako, da poiščemo vse 1-kocikle ali vse 1-korobove grupe G po G-modulu A pri standardni resoluciji. Število A-konjugiranostnih razredov pa lahko dobimo tudi prek kakšne druge proste resolucije, prek katere izračunamo $H^1(G,A)$.

Navedli smo nekaj zanimivih dejstev o razcepnih razširitvah, sedaj pa se vrnimo spet na splošnejše, ne nujno razcepne, razširitve. Zares se posvetimo vprašanju, kako za dane G, A in delovanje G na A poiščemo vse raširitve G po A.

Izrek 4.13. *Denimo, da imamo razširitev*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

grupe G po abelovi grupi A. Obstaja takšna preslikava $f : G \times G \to A$, ki zadošča pogojema:

$$f(1,g) = f(g,1) = 0 \text{ za vsak } g \in G,$$
$$gf(h,k) + f(g,hk) = f(gh,k) + f(g,h) \text{ za vse } g,h,k \in G,$$

da je grupa E ekvivalentna grupi E_f, ki je kot množica enaka $A \times G$, množenje na njej pa je definirano s predpisom

$$(a,g)\circ(b,h) = (a + gb + f(g,h), gh).$$

Dokaz. Naj bo $s : G \to E$ transverzala za dano razširitev. Kot smo že omenili, lahko zanjo brez škode za splošnost privzamemo, da velja $s(1) = 1$. Ker je π homomorfizem, za vsaka $g,h \in G$ velja $\pi(s(g)s(h)) = \pi(s(gh))$. Zato je $\pi(s(g)s(h)s(gh)^{-1}) = 1$ oziroma $s(g)s(h)s(gh)^{-1} \in \ker\pi = \operatorname{im} i$.

Zato obstaja element grupe A, ki ga bomo označili z $f(g,h)$, da drži

$$s(g)s(h) = i(f(g,h))s(gh).$$

Na f lahko gledamo kot na preslikavo iz $G\times G$ v A, ki meri, kako blizu homomorfizmu je transverzala s. Če je s homomorfizem, velja $s(gh) = s(g)s(h)$ in $f(g,h) = 0$ za vsaka $g, h \in G$.

Če v zvezo $s(g)s(h) = i(f(g,h))s(gh)$ vstavimo $g = 1$ ali $h = 1$ in upoštevamo $s(1) = 1$, ugotovimo, da mora veljati

$$f(g,1) = f(1,g) = 0 \text{ za vsak } g \in G.$$

Kot pri dokazu izreka 4.5 upoštevajmo, da lahko na E gledamo kot na množico $A \times G$ z neko grupno operacijo. Denimo, da imamo dva poljubna elementa $x = i(a)s(g)$ in $y = i(b)s(h)$ grupe E. Oglejmo si njun produkt $xy = i(a)s(g)i(b)s(h)$. Enako kot v dokazu izreka 4.5 uporabimo zvezo

$$i(ga)s(g) = s(g)i(a),$$

ki jo dobimo iz pogoja delovanja G na A. Upoštevamo še, da je i homomorfizem in zvezo

$$s(g)s(h) = i(f(g,h))s(gh)$$

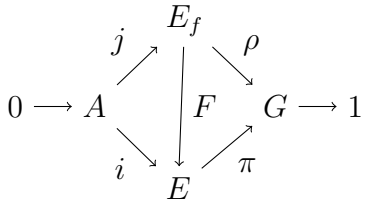
ter poračunamo:

$$\begin{aligned} i(a)s(g)i(b)s(h) &= i(a)i(gb)s(g)s(h) = \\ &= i(a+gb)s(g)s(h) = \\ &= i(a+gb)i(f(g,h))s(gh) = \\ &= i(a+gb+f(g,h))s(gh). \end{aligned}$$

Imamo $i(a)s(g)i(b)s(h) = i(a+gb+f(g,h))s(gh)$, kar pomeni, da je $E \cong E_f$. Grupa E_f je kot množica enaka $A \times G$, grupna operacija na njej pa je definirana takole:

$$(a,g) \circ (b,h) = (a+gb+f(g,h), gh).$$

Izmorfizem $F\colon E_f \to E$ med njima je podan s predpisom $F(a,g) = i(a)s(g)$. Velja še več. Diagram



komutira in rešitvi sta ekvivalentni. Z j smo označili vložitev na prvo, z ρ pa projekcijo na drugo komponento. Res, za vsaka $a \in A$ in $g \in G$ velja

$$Fj(a) = F(a,1) = i(a)s(1) = i(a)$$

in

$$\pi F(a,g) = \pi(i(a)s(g)) = g = \rho(a,g).$$

Ampak, ali je vsaka takšna funkcija f dobra? Kaj mora veljati za f, da bo zgornja operacija zadoščala ustreznim aksiomom, da bo asociativna ter bo imela enoto in inverz? Če želimo, da bo operacija asociativna morata biti produkta

$$\begin{aligned} ((a,g)(b,h))(c,k) &= (a+gb+f(g,h), gh)(c,k) = \\ &= (a+gb+f(g,h)+ghc+f(gh,k), ghk) = \\ &= (a+gb+ghc+f(g,h)+f(gh,k), ghk) \end{aligned}$$

in

$$\begin{aligned}(a,g)((b,h)(c,k)) &= (a,g)(b+hc+f(h,k),hk) = \\ &= (a+gb+ghc+gf(h,k)+f(g,hk),ghk)\end{aligned}$$

enaka. Če zgornja produkta primerjamo ugotovimo, da mora veljati

$$f(g,h)+f(gh,k) = gf(h,k)+f(g,hk).$$

Izkaže se, da je to že dovolj. Tako definirana grupna operacija ima enoto $(0,1)$:

$$\begin{aligned}(a,g)(0,1) &= (a+g\cdot 0+f(g,1),g\cdot 1) = \\ &= (a,g), \\ (0,1)(a,g) &= (0+1\cdot(0+a+f(1,g)),1\cdot g) = \\ &= (a,g).\end{aligned}$$

Element (a,g) ima levi inverz $(g^{-1}(-a)-f(g^{-1},g),g^{-1})$, saj je:

$$\begin{aligned}&(g^{-1}(-a)-f(g^{-1},g),g^{-1})(a,g) = \\ &= (g^{-1}(-a)-f(g^{-1},g)+g^{-1}a+f(g^{-1},g),g^{-1}g) = \\ &= (g^{-1}(a-a)+f(g^{-1},g)-f(g^{-}1,g),1) = \\ &= (0,1),\end{aligned}$$

in desni inverz $(g^{-1}(-a-f(g,g^{-1})),g^{-1})$, saj je:

$$\begin{aligned}&(a,g)(g^{-1}(-a-f(g,g^{-1})),g^{-1}) = \\ &= (a+gg^{-1}(-a-f(g,g^{-1}))+f(g,g^{-1}),gg^{-1}) = \\ &= (a-a-f(g,g^{-1})+f(g,g^{-1}),1) = \\ &= (0,1).\end{aligned}$$

Vemo, da sta v grupi, če obstajata, levi in desni inverz enaka. Zato je E_f res grupa. Preveriti moramo le še, da G preko E_f res poraja pravo delovanje na A. Oglejmo si razširitev

$$0 \longrightarrow A \xrightarrow{i} E_f \xrightarrow{\pi} G \longrightarrow 1,$$

kjer seveda velja $i(a) = (a,1)$ in $\pi(a,g) = g$. Transverzalo lahko še vedno definiramo kot $s(g) = (0,g)$. Ta zdaj ni več nujno homomorfizem. Porojeno delovanje je podano z zvezo

$$i(g\bullet a) = s(g)i(a)s(g)^{-1}.$$

Upoštevamo, kaj sta s in i in dobimo:

$$\begin{aligned}(g\bullet a,1) &= i(g\bullet a) = \\ &= s(g)i(a)s(g)^{-1} = \\ &= (0,g)(a,1)(-g^{-1}f(g,g^{-1}),g^{-1}) = \\ &= (ga,g)(-g^{-1}f(g,g^{-1}),g^{-1}) = \\ &= (ga-gg^{-1})f(g,g^{-1})+f(g,g^{-1}),gg^{-1}) = \\ &= (ga-f(g,g^{-1})+f(g,g^{-1}),1) = \\ &= (ga,1).\end{aligned}$$

Sledi, da je porojeno delovanje res pravo, saj velja $g \bullet a = ga$. Dokaz je s tem v celoti končan. □

Ugotovili smo, da če imamo podani grupi G in A ter fiksirano delovanje grupe G na grupi A, potem je vsaka grupa E ekvivalentna E_f za neko funkcijo $f : G \times G \to A$, ki zadošča ustreznima pogojema. Da torej poiščemo vse možne razširitve G po A, je dovolj poiskati vse funkcije $f : G \times G \to A$, ki zadoščajo pogojema:

$$f(1, g) = f(g, 1) = 0 \text{ za vsak } g \in G,$$
$$gf(h, k) + f(g, hk) = f(gh, k) + f(g, h) \text{ za vsake } g, h, k \in G.$$

Poimenujmo ju prvi in drugi *razširitveni pogoj*, da bomo vedeli, o čem je govora in ju ne bo zmeraj potrebno pisati. Funkcije, ki jima zadoščajo, pa poimenujmo *razširitvene funkcije*. Poudarimo, da tu ne gre za standardno poimenovanje, marveč le za način, kako si malo olajšamo pisanje.

Drugi razširitveni pogoj je bistven, prvi pa je zgolj lepotne narave. Je posledica tega, da si za transverzalo s vedno lahko izberemo $s(1_G) = 1_E$, saj poznamo nek element, natančneje 1_E iz $\pi^{-1}(1_G)$. S prvim razširitvenim pogojem naj bi si le poenostavili iskanje razširitev (kako točno bomo videli kasneje), v principu pa bi čisto lahko shajali tudi brez njega.

Omenimo, da razširitvene funkcije tvorijo abelovo grupo. Vse funkcije $G \times G \to A$ so namreč abelova grupa za seštevanje, saj slikajo v A, ki je tudi sam abelova grupa. Enostaven račun pokaže, da v kolikor f in g zadoščata razširitvenima pogojema, potem jim zadošča tudi $f - g$. Zato razširitvene funkcije tvorijo podgrupo v grupi vseh funkcij $G \times G \to A$.

Za trenutek si oglejmo razširitvene funkcije brez upoštevanja prvega razširitvenega pogoja, osredotočimo se torej na funkcije $G \times G \to A$, ki zadoščajo le drugemu pogoju. Sedaj primerjajmo drugi razširitveni pogoj s pogojem pri $Z^2(G, A) = \ker \sigma_3$ iz primera 3.10.

Tako kot v prejšnjih dveh podobnih situacijah se da pokazati, da obstaja bijekcija, celo izomorfizem (tudi prejšnje preslikave so bile izomorfizmi, le da tega nismo posebej navajali), med preslikavami $G \times G \to A$, ki zadoščajo drugemu razširitvenemu pogoju in 2-kocikli $Z^2(G, A)$ grupe G s koeficienti v G-modulu A pri standardni resoluciji.

Ugotovili smo že, da je, če želimo poiskati vse razširitve G po A pri danem delovanju, dovolj poiskati vse razširitvene funkcije. Ampak že v preprostih primerih je razširitvenih funkcij ogromno. Zato se je smiselno vprašati, ali je res potrebno izračunati vse? Ali se lahko zgodi, da bomo za dve razširitveni funkciji f_1 in f_2 dobili ekvivalentni grupi $E_{f_1} \equiv E_{f_2}$? Odgovor na to vprašanje podaja naslednji izrek.

Izrek 4.14. *Naj bo G grupa in A abelova grupa. Fiksirajmo delovanje G na A. Naj bosta f_1 in f_2 razširitveni funkciji. Grupi E_{f_1} in E_{f_2} sta ekvivalentni natanko tedaj, ko obstaja takšna funkcija $\varphi : G \to A$, da za vsaka g in h iz G drži $\varphi(1) = 0$ in*

$$f_1(g, h) - f_2(g, h) = \varphi(gh) - \varphi(g) - g\varphi(h).$$

Dokaz. Denimo, da sta grupi E_{f_1} in E_{f_2} ekvivalentni. Spodnji diagram komutira. Tu sta i_1 in i_2 uložitvi na prvo koordinato, π_1 in π_2 pa projekciji na drugo koordinato. Spomnimo se, da sta oba, E_{f_1} in E_{f_2}, kot množica enaki $A \rtimes G$ z neko grupno operacijo. Z F označimo izomorfizem med E_{f_1} in E_{f_2}. Zapišimo ga v obliki

$$F(a, g) := (\xi(a, g), \psi(a, g)),$$

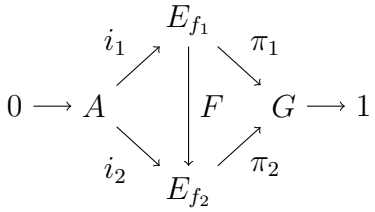


Diagram 3: Ekvivalenca E_{f_1} in E_{f_2}

za neki funkciji $\xi : E_{f_1} \to A$ in $\psi : E_{f_1} \to G$. Ker diagram 3 komutira mora veljati zveza

$$g = \pi_1(a, g) = \pi_2 F(a, g) = \pi_2(\xi(a, g), \psi(a, g)) = \psi(a, g).$$

Zaradi tega lahko izboljšamo našo formulo za F v

$$F(a, g) := (\xi(a, g), g).$$

Ker komutira tudi leva polovica diagrama 3, mora veljati tudi

$$F(a, 1) = Fi_1(a) = i_2(a) = (a, 1).$$

Zdaj, ko vemo tudi to, upoštevajmo še, da mora biti F homomorfizem:

$$\begin{aligned}(\xi(a + b, x), x) &= F(a + b, g) = \\ &= F((b, 1)(a, g)) = \\ &= (b, 1)(\xi(a, g), x) = \\ &= (b + \xi(a, g), x).\end{aligned}$$

Ugotovili smo, da velja $\xi(a + b, x) = b + \xi(a, g)$. Vstavimo $a = 0$ in ugotovimo $\xi(b, g) = b + \xi(0, g)$. Definirajmo funkcijo $\varphi : G \to A$ s predpisom $\varphi(g) = \xi(0, g)$ in spremenimo predpis za F v

$$F(a, g) = (a + \varphi(g), g).$$

Kaj velja za ta φ? Najprej opazimo $(a, 1) = F(a, 1) = (a + \varphi(1), 1)$ iz česar sledi $\varphi(1) = 0$. Nato pa upoštevamo še formuli za grupno operacijo v grupah E_{f_1} in E_{f_2}. Ker je F homomorfizem, morata biti vrednosti $F((a, g)(b, h))$ in $F(a, g)F(b, h)$ enaki. Ampak

$$\begin{aligned}F((a, g)(b, h)) &= F(a + gb + f_1(g, h), gh) = \\ &= (a + gb + f_1(g, h) + \varphi(gh), gh)\end{aligned}$$

in

$$\begin{aligned}F(a, g)F(b, h) &= (a + \varphi(g), g)(b + \varphi(h), h) = \\ &= (a + \varphi(g) + gb + g\varphi(h) + f_2(g, h), gh).\end{aligned}$$

Če primerjamo dobljeno, ugotovimo, da mora veljati zveza

$$f_1(g, h) - f_2(g, h) = \varphi(gh) - \varphi(g) - g\varphi(h),$$

s čimer smo dokazali eno od implikacij izreka.

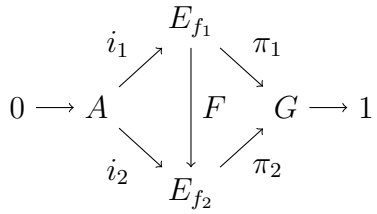
Velja pa tudi obrat. Recimo, da za razširitveni funkciji f_1 in f_2 velja

$$f_1(g, h) - f_2(g, h) = \varphi(gh) - \varphi(g) - g\varphi(h).$$

Tu je $\varphi(1) = 0$. Dokažimo, da sta grupi E_{f_1} in E_{f_2} ekvivalentni. Zgornjo zvezo preoblikujemo v

$$f_1(g,h) = f_2(g,h) + \varphi(gh) - \varphi(g) - g\varphi(h).$$

Dokazati moramo, da je diagram



komutativen. Kot ponavadi označujeta i_1 in i_2 vložitvi na prvo koordinato, π_1 in π_2 projekciji na drugo, homomorfizem F pa definiramo s predpisom $F(a,g) = (a + \varphi(g), g)$. Da je res homomorfizem sledi iz zveze $f_1(g,h) = f_2(g,h) + \varphi(gh) - \varphi(g) - g\varphi(h)$. Preverimo še, da je diagram res komutativen! Velja

$$Fi_1(a) = F(a,1) = (a + \varphi(1), 1) = (a,1) = i_2(a)$$

in

$$\pi_2 F(a,g) = \pi_2(a + \varphi(g), g) = g = \pi_1(a,g).$$

Diagram je res komutativen. S tem je dokaz zaključen. □

Naj bo $\varphi : G \to A$ neka funkcija, za katero velja $\varphi(1) = 0$. Funkciji $r : G \times G \to A$ s predpisom oblike

$$r(g,h) = \varphi(gh) - \varphi(g) - g\varphi(h)$$

bomo zaradi jasnosti rekli *ekvivalenča funkcija*. Tu spet ne gre za standardno poimenovanje. Zgoraj smo dokazali, da se razširitveni funkciji dveh ekvivalentnih razširitev razlikujeta za ekvivalenčno funkcijo.

Spet omenimo, da je pogoj $\varphi(1) = 0$ zgolj lepotne narave. Je posledica tega, da smo privzeli

$$f(g,1) = f(1,g) = 0,$$

in je namenjen zgolj enostavnejšemu računanju in ničemur drugemu. Če tega ne bi privzeli, bi lahko zgornji dokaz ravno tako izpeljali na zelo podoben način, le da se pogoj $\varphi(1) = 0$ ne bi nikjer pojavil.

Če primerjamo $B^2(G,A)\mathrm{im}\,\sigma_2$ iz primera 3.10 in kako smo definirali ekvivalenčno funkcijo, opazimo podobnost. Spet se da, na podoben način kot prej, poiskat izomorfizem med grupo ekvivalenčnih funkcij, ki ne zadoščajo nujno pogoju $\varphi(1) = 0$, in 2-korobovi $B^2(G,A)$ grupe G s koeficienti v G-modulu A pri standardni resoluciji.

Trditev 4.15. *Vsaka ekvivalenčna funkcija r je tudi razširitvena.*

Dokaz. Dokazati moramo, da r zadošča razširitvenim pogojem. Velja

$$r(1,g) = \varphi(g) - \varphi(1) - 1 \cdot \varphi(g) = 0$$

in

$$r(g,1) = \varphi(g) - \varphi(g) - g\varphi(1) = 0,$$

zato r zadošča prvemu pogoju.

Dokazati moramo še, da drži

$$gr(h,k) + r(g,hk) = r(gh,k) + r(g,h).$$

Poračunajmo levo in desno stran! Leva je enaka

$$gr(h,k) + r(g,hk) = g(\varphi(hk) - \varphi(h) - h\varphi(k)) + \varphi(ghk) - \varphi(g) - g\varphi(hk) = \\ = \varphi(ghk) - \varphi(g) - g\varphi(h) - gh\varphi(k).$$

Desna pa

$$r(gh,k) + r(g,h) = \varphi(ghk) - \varphi(gh) - gh\varphi(k) + \varphi(gh) - \varphi(g) - g\varphi(h).$$

Vidimo, da za ekvivalenčno funkcijo r razširitveni pogoji res držijo. □

Enostavno je preveriti tudi, da je razlika dveh ekvivalenčnih funkcij spet ekvivalenčna funkcija. To pomeni, da tvorijo ekvivalenčne funkcije podgrupo v grupi razširitvenih. Ker sta obe grupi abelovi, je smiselno definirati kvocientno grupo razširitvenih funkcij po ekvivalenčnih.

Povzemimo zadnjih nekaj izrekov. Vsako razširitev lahko dobimo prek neke razširitvene funkcije. Dve razširitveni funkciji porodita isto razširitev, če se razlikujeta le za ekvivalenčno. Množica vseh ekvivalenčnih razredov razširitev grupe G po grupi A glede na relacijo ekvivalentnosti ima strukturo abelove grupe in je izomorfna kvocientni grupi razširitvenih funkcij po ekvivalentnih. Laično povedano to pomeni, da vse razširitve G po A pri fiksiranjem delovanju G na A lahko dobimo tako, da dobimo kvocientno grupo razširitvenih funkcij po ekvivalenčnih.

Kot smo omenili, pa lahko vse skupaj računamo ne da bi privzeli prvi razširitveni pogoj. V tem primeru ugotovimo, da je grupa ekvivalenčnih razredov razširitev pravzaprav ravno druga kohomološka grupa $H^2(G,A)$ grupe G s koeficienti v G-modulu A. Vendar pa je v tem primeru vsaka razširitvena funkcija ekvivalentna neki razširitveni funkciji, ki zadošča še prvemu razširitvenemu pogoju. Od tu sklepamo, da sta kvocienta enaka. Kvocientna grupa razširitvenih funkcij po ekvivalenčnih je torej izomorfna tako grupi ekvivalenčnih razredov razširitev kot tudi $H^2(G,A)$.

Z zadnjimi nekaj dokazi smo v resnici dokazali naslednje dejstvo, ki je glavni cilj tega dela.

Izrek 4.16. *Naj bo G grupa, A pa abelova grupa. Fiksirajmo delovanje G na A. Naj bo $\gamma(G,A)$ množica vseh ekvivalenčnih razredov razširitev G po A, ki porajajo ustrezno delovanje G na A. Obstaja takšna grupna operacija, da $\gamma(G,A)$ postane grupa in velja*

$$\gamma(G,A) \cong H^2(G,A).$$

Primer 4.17. Oglejmo si vso to teorijo še na nekem primeru. Naj bo p praštevilo. Poiščimo, vse možne razširitve $\mathbb{Z}_p$ po $\mathbb{Z}_p$. Zanimajo nas vse možne grupe E in homomorfizmi i ter π, da bo zaporedje grup

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{i} E \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0.$$

ekzaktno. Poiskati moramo torej vsa možna delovanja $\mathbb{Z}_p$ na $\mathbb{Z}_p$ in potem pri vsakem fiksnem $\mathbb{Z}_p$-modulu $\mathbb{Z}_p$ poiskati vse neekvivalentne razširitve.

Najprej premislimo, kako lahko $\mathbb{Z}_p$ sploh deluje na $\mathbb{Z}_p$. Ker je grupa $\mathbb{Z}_p$ ciklična, bo njen avtomorfizem $\mathbb{Z}_p$ natančno podan s sliko generatorja. Izberemo enega od generatorjev (katerokoli število tuje p, torej katerikoli element različen od 0), denimo 1. Če želimo, da bo naš avtomorfizem res bijektiven, se mora ta generator spet slikati v generator. Lahko se slika v 1, 2 ... ali v $p-1$. Imamo torej $p-1$ različnih avtomorfizmov grupe $\mathbb{Z}_p$. To pomeni $|\operatorname{Aut}\mathbb{Z}_p| = p-1$ (pravzaprav velja celo $\operatorname{Aut}\mathbb{Z}_p \cong \mathbb{Z}_{p-1}$, vendar to, da je grupa ciklična, zdaj ni pomembno). Delovanje

je homomorfizem iz grupe $\mathbb{Z}_p$ moči p v grupo $\operatorname{Aut}\mathbb{Z}_p$ moči $p-1$. Ampak moči p in $p-1$ sta si tuji, zato med grupama lahko obstaja le trivialni homomorfizem. Edino možno delovanje $\mathbb{Z}_p$ na $\mathbb{Z}_p$ je torej trivialno.

Imamo torej trivialni $\mathbb{Z}_p$-modul $\mathbb{Z}_p$ in naša naloga je poiskati vse neekvivalentne razširitve

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{i} E \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0.$$

Predstavljena teorija nam pove, da moramo poiskati vse ekvivalenčne razrede funkcij $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, ki zadoščajo (tokrat tudi drugo grupo $\mathbb{Z}_p$ pišemo aditivno in upoštevamo, da je delovanje trivialno)

$$f(0,x) = f(x,0) = 0 \text{ za vsak } x \in \mathbb{Z}_p$$

in

$$f(y,z) + f(x,y+z) = f(x+y,z) + f(x,y) \text{ za vsake } x,y,z \in \mathbb{Z}_p,$$

pri čemer imamo dve takšni funkciji za ekvivalentni, če se razlikujeta le za funkcijo $r : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ oblike $r(x,y) = \varphi(x+y) - \varphi(x) - \varphi(y)$, kjer je φ neka funkcija iz $\mathbb{Z}_p$ v $\mathbb{Z}_p$, za katero velja $\varphi(0) = 0$.

Funkcije f bomo predstavili kot $p \times p$ tabele, kjer na $i+1, j+1$-tem mestu najdemo $f(i,j)$ $(i,j = 0,1,\ldots p-1)$. Ideja je, da za poljubno razširitveno funkcijo f poiščemo ekvivalentno funkcijo g lepše oblike. Na začetku o f vemo le:

$$f = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & f(1,1) & \cdots & f(1,p-1) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & f(p-1,1) & \cdots & f(p-1,p-1) \end{bmatrix}.$$

Konstrukciji ekvivalenčne funkcije si bomo pomagali s funkcijo φ. Pri izbiri slednje imamo precej svobode. Zanjo mora veljati le $\varphi(0) = 0$, v vseh ostalih točkah pa jo lahko predpišemo. Predpišimo jo tako da velja:

$$\begin{aligned} r(1,1) &= \varphi(2) - \varphi(1) - \varphi(1) = f(1,1), \\ r(1,2) &= \varphi(3) - \varphi(2) - \varphi(1) = f(1,2), \\ r(1,3) &= \varphi(4) - \varphi(3) - \varphi(1) = f(1,3), \\ &\vdots \\ r(1,p-2) &= \varphi(p-1) - \varphi(p-2) - \varphi(1) = f(1,p-2). \end{aligned}$$

To lahko storimo tako, da v prvem koraku izberemo $\varphi(1)$ in izračunamo $\varphi(2)$, v drugem izračunamo $\varphi(3)$ in tako dalje. Za $k = 2,3,\ldots,p-2$ v k-tem koraku izračunamo $\varphi(k+1)$. S tem smo φ popolnoma določili. Ker v $\mathbb{Z}_p$ velja $p = 0$, smo s tem določili tudi

$$r(1,p-1) = \varphi(0) - \varphi(p-1) - \varphi(1) = -\varphi(p-1) - \varphi(1).$$

Posodobimo f v ekvivalentno funkcijo $g := f - r$. Označimo še $a := g(1,p-1)$. Tabela funkcije g izgleda takole:

$$g = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & a \\ 0 & g(2,1) & g(2,2) & \cdots & g(2,p-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & g(p-1,1) & g(p-1,2) & \cdots & g(p-1,p-1) \end{bmatrix}.$$

Tudi funkcija g zadošča drugemu razširitvenemu pogoju:

$$g(x,y) + g(x+y,z) = g(y,z) + g(x,y+z).$$

V pogoj vstavimo $x = y = 1$ in dobimo formulo

$$g(1,1) + g(2,z) = g(1,z) + g(1,z+1).$$

Vemo že, da velja $g(1,1) = 0$, zato lahko formulo izboljšamo v

$$g(2,z) = g(1,z) + g(1,z+1).$$

To pomeni, da je za vsak z element $g(2,z)$ vsota elementov zgoraj in desno zgoraj. Ker že poznamo drugo vrstico matrike funkcije g, lahko od tu izračunamo še tretjo in ugotovimo:

$$g = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & a \\ 0 & 0 & 0 & \cdots & a & a \\ 0 & g(3,1) & g(3,2) & \cdots & g(3,p-2) & g(3,p-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & g(p-1,1) & g(p-1,2) & \cdots & g(p-1,p-2) & g(p-1,p-1) \end{bmatrix}.$$

Če v pogoj razširitvene funkcije g vstavimo $y = 1, x = n < p-1$, dobimo

$$g(n,1) + g(n+1,z) = g(1,z) + g(n,z+1).$$

S pomočjo te zveze lahko iz n-te vrstice dobimo $(n+1)$-vo. Tako lahko induktivno napolnimo celotno tabelo funkcije g. Zaradi situacije v drugi vrstici lahko privzamemo $g(n,1) = 0$ in se pogoj poenostavi v

$$g(n+1,z) = g(1,z) + g(n,z+1).$$

Če $z \neq p-1$, je tudi $g(1,z) = 0$, zato velja, da je $g(n+1,z)$ enak elementu desno nad sabo $g(n,z+1)$. V primeru $z = p-1$ pa velja $g(n,z+1) = g(n,0) = 0$ in $g(n+1,p-1) = g(1,p-1) = a$.

Ugotovimo, da je v vsaki naslednji vrstici en neničelni element več. Tabela funkcije g je zato na spodnjem desnem trikotniku enaka a, na levem zgornjem pa 0. Izgleda torej takole:

$$g = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & a \\ 0 & 0 & 0 & \cdots & a & a \\ 0 & 0 & 0 & \cdots & a & a \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a & a & \cdots & a & a \end{bmatrix}.$$

Zaradi tega lahko definiramo funkcijo g kot

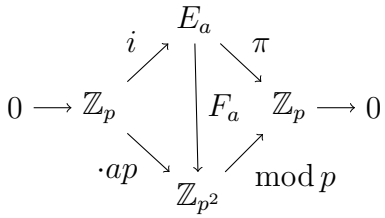
$$g_a(x,y) := \begin{cases} a, & x+y \geq p \\ 0, & \text{sicer.} \end{cases}$$

Neekvivalentnih razširitev je torej p, saj a lahko zavzame vrednost $0, 1, \ldots, p-1$, vsaka funkcija f pa je ekvivalentna funkciji g_a za nek $a \in A$. Velja $H^2(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p$.

Vse neekvivalentne razširitve E_a grupe $\mathbb{Z}_p$ po $\mathbb{Z}_p$ so zato kot množice enake $\mathbb{Z}_p \times \mathbb{Z}_p$ grupna operacija na njih pa je enaka

$$(n,x)(m,y) = (n+m+g_a(x,y), x+y).$$

Če je $a = 0$, očitno velja $E_0 \equiv \mathbb{Z}_p \times \mathbb{Z}_p$. V nasprotnem primeru ($a \neq 0$) pa diagram



komutira.

Tu sta i vložitev na prvo in π projekcija na drugo komponento, homomorfizma $\cdot ap$ in $\mathrm{mod}\, p$ predstavljata množenje z ap in ostanek pri deljenju s p, predpis izomorfizma F_a pa se glasi $F_a(n,x) = apn + x$. Enostavno je preveriti, da je F_a res izomorfizem in da diagram res komutira.

Literatura

[1] Kenneth S. Brown, *Cohomology of groups*, Graduate texts in mathematics 87, Springer-Verlag, New York, 1982.

[2] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[3] Derek J. S. Robinson, *A course in the theory of groups*, Graduate texts in mathematics 80, Springer-Verlag, New York, 1996.

[4] *Group cohomology*, [ogled 15. 9. 2011], dostopno na `http://en.wikipedia.org/wiki/Group_cohomology`.

[5] *Resolution (algebra)*, [ogled 15. 9. 2011], dostopno na `http://en.wikipedia.org/wiki/Resolution_(algebra)`.