UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Domen Keglevič

Kohomološki pogled na osnovnošolsko aritmetiko

Delo diplomskega seminarja

Mentor: izr. prof. dr. Primož Moravec

Ljubljana, 2015

Kazalo

Kohomološki pogled na osnovnošolsko aritmetiko

Povzetek

V osnovni šoli se naučimo seštevanja dveh števil tako, da najprej seštejemo enice po modulu 10 in 1 pišemo dalje, če je vsota večja od 10. Nato po istem postopku seštejemo desetice, stotice, itd. Ta postopek seštevanja lahko opišemo z razširitvami grup. Na grupo $\mathbb{Z}_{100}$ lahko gledamo kot na razširitev grupe $\mathbb{Z}_{10}$ z grupo $\mathbb{Z}_{10}$. Poleg te obstajajo še druge razširitve in med njimi so nekatere ekvivalentne. Če je prva grupa Abelova, potem ima množica razredov vseh neekvivalentnih razširitev strukturo grupe, ki ji rečemo druga kohomološka grupa. Enica te grupe ustreza poldirektnemu produktu. V delu bomo definirali razširitve grup, dokazali osnovne rezultate in izpeljali definicijo druge kohomološke grupe. Na koncu bomo s programskim paketom GAP izračunali nekaj primerov.

A cohomological viewpoint on elementary school arithmetic

Abstract

We learn addition of two numbers in elementary school by adding first two digits by modulo 10 and carry over 1 if sum exceeds 10. Then we repeat calculation for the second two digits, third, and so forth. This algorithm can be described by group extensions. The group $\mathbb{Z}_{100}$ can be viewed as an extension of $\mathbb{Z}_{10}$ by $\mathbb{Z}_{10}$. There are also other extensions of this kind and some are equivalent. If the first group is Abelian, then the set of all equivalence classes of extensions has a group structure and it is called the second cohomology group. Identity element of this group corresponds to semidirect product. In this paper we will define group extensions and prove some basic results which will lead us to definition of second cohomology group. In the end we will compute some examples with the help of GAP, a system for computational algebra.

Math. Subj. Class. (2010): 20E22, 20J06

Ključne besede: razširitve grup, druga kohomološka grupa

Keywords: group extensions, second cohomology group

1. Uvod

Ena prvih stvari, ki se jih naučimo pri matematiki v osnovni šoli, je seštevanje. Če se omejimo na takšne pare naravnih števil, da njihova vsota ne presega 100, potem se osnovnošolsko seštevanje ujema s seštevanjem v grupi $\mathbb{Z}_{100}$. Npr.

$$\begin{array}{rr} & 2\ \ 6 \\ +\ & 5_1\ \ 7 \\ \hline & 8\ \ 3 \end{array}$$

Števili 26 in 57 smo sešteli tako, da smo najprej sešteli enici po modulu 10 in ker je njuna vsota presegla 10, smo 1 pisali dalje. Potem smo sešteli desetici in 1 iz prejšnjega koraka. Ta postopek seštevanja bi lahko opisali tudi na naslednji način.

Označimo z D podgrupo edinko vseh desetic v $\mathbb{Z}_{100}$. Torej kot množica je $D = \{0, 10, 20, \ldots, 90\}$ in kot grupa je $D \cong \mathbb{Z}_{10}$. Obstaja kvocientna grupa $E = \mathbb{Z}_{100}/D \cong \mathbb{Z}_{10}$, ki nam bo predstavljala enice. Naj funkcija $z : E \times E \to D$ pove, koliko pri seštevanju enic pišemo dalje. Podana je s tabelo

z	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	0	0	1	1
3	0	0	0	0	0	0	0	1	1	1
4	0	0	0	0	0	0	1	1	1	1
5	0	0	0	0	0	1	1	1	1	1
6	0	0	0	0	1	1	1	1	1	1
7	0	0	0	1	1	1	1	1	1	1
8	0	0	1	1	1	1	1	1	1	1
9	0	1	1	1	1	1	1	1	1	1

S številom n v tabeli mislimo na ustrezno enico oz. desetico. Če element $de \in \mathbb{Z}_{100}$ pišemo kot urejeni par (d, e), potem lahko seštevanje v $\mathbb{Z}_{100}$ opišemo s predpisom:

$$(d_1, e_1) + (d_2, e_2) = (d_1 + d_2 + z(e_1, e_2), e_1 + e_2),$$

kjer se seštevanje na prvem mestu ravna po seštevanju v D in na drugem v E. Na primer:

$$26 + 57 = (2, 6) + (5, 7) = (2 + 5 + z(6, 7), 6 + 7) = (8, 3) = 83.$$

Nekaj več o tem je v [2]. V delu nas bo zanimalo, kakšna je splošna zveza med grupo $\mathbb{Z}_{100}$ in grupama E, D ter funkcijo z. Nato bomo pogledali, če lahko funkcijo z malo spremenimo, da bi z opisanim seštevanjem prišli do kakšne druge grupe (ne nujno $\mathbb{Z}_{100}$), in kako takšne grupe klasificirati. Na koncu bomo pogledali še nekaj primerov s pomočjo programa GAP.

2. Razširitve grup

Naj bodo E, D in $\mathbb{Z}_{100}$ kot v uvodu. Zvezo med E in D v $\mathbb{Z}_{100}$ lahko zapišemo s kratkim eksaktnim zaporedjem

$$1 \longrightarrow D \xrightarrow{i} \mathbb{Z}_{100} \xrightarrow{s} E \longrightarrow 1, \tag{1}$$

kjer je i vložitev, dana z $i(n) = n$, in s epimorfizem, definiran s $s(n) = n + D$. Zaporedje je res kratko eksaktno, saj je $\operatorname{im} i = \ker s$. Takšno zvezo med grupami lahko posplošimo v naslednjo definicijo.

Definicija 2.1. *Razširitev grupe N z grupo G* je kratko eksaktno zaporedje grup in homomorfizmov

$$1 \longrightarrow N \xrightarrow{\mu} R \xrightarrow{\epsilon} G \longrightarrow 1.$$

Krajše pišemo $N \rightarrowtail^{\mu} R \xrightarrow{\epsilon} \!\!\!\!\rightarrow G$.

Za naš primer enic in desetic bi lahko rekli, da je grupa $\mathbb{Z}_{100}$ (neka) razširitev desetic z enicami. To ni edina možna razširitev D z E. Lahko imamo tudi zaporedje

$$D \rightarrowtail^{i'} \mathbb{Z}_{10} \oplus \mathbb{Z}_{10} \xrightarrow{s'} \!\!\!\!\rightarrow E,$$

kjer je $i'(n) = (\frac{n}{10}, 0)$ in $s'(n_1, n_2) = n_2 + D$. Preslikava i' je injektivna in s' surjektivna (saj je $e + D = s'(0, e)$). Ker je $s'(i'(d)) = s'(\frac{d}{10}, 0) = 0 + D$, velja $\operatorname{im} i' \subseteq \ker s'$. Velja tudi $\ker s' \subseteq \operatorname{im} i'$, saj za poljuben $(n, 0) \in \ker s'$ velja $i'(10n) = (n, 0)$. Od tod sledi $\operatorname{im} i' = \ker s'$. Zaporedje je torej kratko eksaktno in dobili smo neko drugo razširitev D z E.

Ker je $D \cong \mathbb{Z}_{10}$ in $E \cong \mathbb{Z}_{10}$, je ta primer kar razširitev z direktno vsoto. Splošneje velja, da vedno obstaja vsaj kakšna razširitev, ker imamo vedno vsaj razširitev z direktnim produktom $N \rightarrowtail^{\mu} N \times G \xrightarrow{\epsilon} \!\!\!\!\rightarrow G$, kjer je $\mu(n) = (n, 1)$ in $\epsilon(n, g) = g$.

Oglejmo si še zaporedje

$$D \rightarrowtail^{i''} \mathbb{Z}_{100} \xrightarrow{s} \!\!\!\!\rightarrow E, \tag{2}$$

kjer je preslikava $i''(n) = 3n$, preslikava s pa kot v (1). Preslikava i'' je injektivna, saj iz $n_1 \neq n_2$ sledi $3n_1 \neq 3n_2 \mod 100$ oz. $i''(n_1) \neq i''(n_2)$. Je tudi homomorfizem, saj je $i''(n_1 + n_2) = 3(n_1 + n_2) = 3n_1 + 3n_2 = i''(n_1) + i''(n_2)$. Velja $\operatorname{im} i'' = \operatorname{im} i$ in zato $\operatorname{im} i'' = \ker s$. Torej smo spet dobili $\mathbb{Z}_{100}$ kot razširitev D z E, ampak preslikava i'' ni ista kot i.

2.1. **Morfizmi razširitev.** Videli smo, da lahko v razširitvah nastopajo iste grupe, vendar ni nujno, da so vse nastopajoče preslikave enake. Morfizmi razširitev nam omogočajo, da te in druge razširitve med seboj primerjamo.

Definicija 2.2. Označimo z $\mathcal{R}_1$ razširitev $N_1 \rightarrowtail^{\mu_1} R_1 \xrightarrow{\epsilon_1} \!\!\!\!\rightarrow G_1$ in z $\mathcal{R}_2$ razširitev $N_2 \rightarrowtail^{\mu_2} R_2 \xrightarrow{\epsilon_2} \!\!\!\!\rightarrow G_2$. *Morfizem iz razširitve $\mathcal{R}_1$ v razširitev $\mathcal{R}_2$* je trojica takšnih homomorfizmov (α, β, γ), da naslednji diagram komutira:

$$\begin{array}{ccccc} N_1 & \rightarrowtail^{\mu_1} & R_1 & \xrightarrow{\epsilon_1} \!\!\!\!\rightarrow & G_1 \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ N_2 & \rightarrowtail^{\mu_2} & R_2 & \xrightarrow{\epsilon_2} \!\!\!\!\rightarrow & G_2 \end{array} \tag{3}$$

Morfizem oblike $(\mathrm{id}, \beta, \mathrm{id})$ imenujemo *ekvivalenca razširitev* in tedaj pravimo, da sta razširitvi *ekvivalentni*. Če je pa oblike $(\alpha, \beta, \mathrm{id})$, kjer je α izomorfizem grup, mu rečemo *izomorfizem razširitev*. V tem primeru pravimo, da sta razširitvi *izomorfni*.

Opomba 2.3. Ekvivalenca razširitev in izomorfizem razširitev sta ekvivalenčni relaciji.

Dokaz. Preverili bomo, da je izomorfizem razširitev ekvivalenčna relacija. Naj bosta dve razširitvi v relaciji $\sim$ natanko tedaj, ko med njima obstaja kakšen izomorfizem razširitev. Naj bodo $\mathcal{R}_1$ razširitev $N_1 \rightarrowtail^{\mu_1} R_1 \twoheadrightarrow^{\epsilon_1} G_1$, $\mathcal{R}_2$ razširitev $N_2 \rightarrowtail^{\mu_2} R_2 \twoheadrightarrow^{\epsilon_2} G_2$ in $\mathcal{R}_3$ razširitev $N_3 \rightarrowtail^{\mu_3} R_3 \twoheadrightarrow^{\epsilon_3} G_3$. Refleksivnost relacije $\sim$ nam da izomorfizem $(\mathrm{id}, \mathrm{id}, \mathrm{id})$. Naj bo $\mathcal{R}_1 \sim \mathcal{R}_2$ in $(\alpha, \beta, \mathrm{id})$ pripadajoč izomorfizem. Za $\mathcal{R}_2 \sim \mathcal{R}_1$ si ogledamo trojico $(\alpha^{-1}, \beta^{-1}, \mathrm{id})$. Ta obstaja, saj sta α in β izomorfizma (β je izomorfizem po kratki lemi o petih). Iz diagrama (3) dobimo enakost

$$\mu_2 \circ \alpha = \beta \circ \mu_1$$
$$\beta^{-1} \circ (\mu_2 \circ \alpha) \circ \alpha^{-1} = \beta^{-1} \circ (\beta \circ \mu_1) \circ \alpha^{-1}$$
$$\beta^{-1} \circ \mu_2 = \mu_1 \circ \alpha^{-1}$$

Podobno dobimo $\epsilon_1 \circ \beta^{-1} = \epsilon_2$ in dobili smo komutativnost diagrama za trojico $(\alpha^{-1}, \beta^{-1}, \mathrm{id})$. Sledi simetričnost relacije $\sim$. Naj bo $\mathcal{R}_1 \sim \mathcal{R}_2$ in $(\alpha_1, \beta_1, \mathrm{id})$ pripadajoč izomorfizem ter $\mathcal{R}_2 \sim \mathcal{R}_3$ in $(\alpha_2, \beta_2, \mathrm{id})$ pripadajoč izomorfizem. Za $\mathcal{R}_1 \sim \mathcal{R}_3$ si ogledamo trojico $(\alpha_2 \circ \alpha_1, \beta_2 \circ \beta_1, \mathrm{id})$. Preslikavi $\alpha_2 \circ \alpha_1$ in $\beta_2 \circ \beta_1$ sta izomorfizma, saj so α_i in β_i izomorfizmi. S pomočjo diagrama (3) in relacij $\mathcal{R}_1 \sim \mathcal{R}_2$ in $\mathcal{R}_2 \sim \mathcal{R}_3$ dobimo

$$\beta_2 \circ \beta_1 \circ \mu_1 = \beta_2 \circ \mu_2 \circ \alpha_1 = \mu_3 \circ \alpha_2 \circ \alpha_1.$$

Podobno za $\epsilon_3 \circ \beta_2 \circ \beta_1 = \epsilon_1$. Zato pripadajoči diagram trojice $(\alpha_2 \circ \alpha_1, \beta_2 \circ \beta_1, \mathrm{id})$ komutira in dobili smo tranzitivnost relacije $\sim$. Sledi, da je izomorfizem razširitev ekvivalenčna relacija. Za ekvivalenco razširitev postopamo podobno. □

Zgled 2.4. Naj bo $D \rightarrowtail^{i} \mathbb{Z}_{100} \twoheadrightarrow^{s} E$ kot v (1) in $D \rightarrowtail^{i''} \mathbb{Z}_{100} \twoheadrightarrow^{s} E$ kot v (2). Videli bomo, da sta ti dve razširitvi izomorfni, nista pa ekvivalentni. Naj bo $a : D \to D$ homomorfizem s predpisom $a(n) = 3n$. Je injektiven, saj iz $n_1 \neq n_2$ sledi $3n_1 \neq 3n_2 \mod 100$. Je tudi surjektiven, saj za poljuben $n = 10k \in D$ ($k \in \{0, 1, \ldots, 9\}$) lahko vzamemo $m = 7n$ in bo veljalo $a(m) = 21n = 200k + 10k \mod 100 = n$. Torej je a avtomorfizem z inverzom a^{-1}. Oglejmo si diagram

$$\begin{array}{ccccc} D & \rightarrowtail^{i} & \mathbb{Z}_{100} & \twoheadrightarrow^{s} & E \\ \downarrow{\scriptstyle a^{-1}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\ D & \rightarrowtail^{i''} & \mathbb{Z}_{100} & \twoheadrightarrow^{s} & E \end{array}$$

Iz definicije preslikave a sledi, da je $i'' = i \circ a$, in od tod dobimo $i'' \circ a^{-1} = i$. Torej zgornji diagram komutira in razširitvi sta izomorfni. Če bi bili ekvivalentni, bi moral obstajati tak izomorfizem β, da bi komutiral diagram

$$\begin{array}{ccccc} D & \rightarrowtail^{i} & \mathbb{Z}_{100} & \twoheadrightarrow^{s} & E \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \mathrm{id}} \\ D & \rightarrowtail^{i''} & \mathbb{Z}_{100} & \twoheadrightarrow^{s} & E \end{array}$$

Premislimo, da tak β ne obstaja. Če bi obstajal, bi moral izpolnjevati enačbi $\beta \circ i = i''$ in $s \circ \beta = s$. Po prvi enačbi dobimo $\beta(i(10)) = \beta(10) = i''(10) = 30$. Ker je β izomorfizem, je $\beta(10) = 10\beta(1) = 30$. Če označimo $\beta(1) = x$, potem nas zanima enačba $10x = 30$ v $\mathbb{Z}_{100}$. Ker x lahko pišemo kot $x = 10k_1 + k_2$ za $k_1, k_2 \in \{0, 1, \ldots, 9\}$, je $10x = 100k_1 + 10k_2 = 30$ in po modulu 100 dobimo $k_2 = 3$.

Zato so $3, 13, 23, \ldots, 93$ edina števila v $\mathbb{Z}_{100}$, ki zadoščajo enačbi $10x = 30$. Ampak za poljubno od teh števil enačba $s \circ \beta = s$ ni izpolnjena, saj je po eni strani $s(\beta(1)) = s(1) = 1+D$, po drugi pa $s(\beta(1)) = s(x) = 3+D$. Razširitvi torej nista ekvivalentni.

2.2. **Transverzalna funkcija.** Zanima nas, če obstaja kakšna invarianta za razširitve, ki so ekvivalentne. V ta namen si oglejmo, kaj je transverzalna funkcija, ki nas bo kasneje vodila k taki invarianti.

Definicija 2.5. Naj bo $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ razširitev grup. Množica T je *transverzala glede na* $M = \operatorname{im}\mu = \ker\epsilon$, če vsebuje natanko en element iz vsakega odseka grupe R/M.

Definicija 2.6. Funkciji $\tau : G \to R$ rečemo *transverzalna funkcija k transverzali* T, če za $t \in T$, za katerega je $\epsilon(t) = g$, velja $\tau(g) = t$.

Opomba 2.7. Velja $\epsilon \circ \tau = \mathrm{id}_G$, saj je $\epsilon(\tau(g)) = \epsilon(t) = g$. V splošnem vsaka funkcija $\tau' : G \to R$ z lastnostjo $\epsilon \circ \tau' = \mathrm{id}_G$ določa transverzalo $T' = \{\tau'(g) \mid g \in G\}$ glede na M v R. Res, saj za $g_1, g_2 \in G$ velja, da iz $g_1 \neq g_2$ sledi $\epsilon(\tau'(g_1)) \neq \epsilon(\tau'(g_2))$, torej sta $\tau'(g_1)$ in $\tau'(g_2)$ v različnih odsekih.

Transverzalna funkcija je injektivna (v nasprotnem pogoj $\epsilon \circ \tau = \mathrm{id}_G$ ne more biti izpolnjen), ni pa nujno homomorfizem. Oglejmo si najprej take razširitve, ko obstaja kakšna transverzalna funkcija, ki je homomorfizem.

Zgled 2.8. Naj bosta N in G grupi in

$$N \overset{\mu}{\rightarrowtail} N \times G \overset{\epsilon}{\twoheadrightarrow} G$$

razširitev z direktnim produktom, kjer je $\mu(n) = (n, 1)$ in $\epsilon(n, g) = g$. Potem je preslikava $\tau : G \to N \times G$ s predpisom $\tau(g) = (1, g)$ transverzalna funkcija, ki je homomorfizem. Res, saj je $\epsilon(\tau(g)) = s(1, g) = g$ in $\tau(g_1 g_2) = (1, g_1 g_2) = (1, g_1)(1, g_2) = \tau(g_1)\tau(g_2)$.

Transverzalna funkcija, ki je homomorfizem, ne nastopa le v razširitvah z direktnim produktom. Lahko pa direktni produkt posplošimo in dobimo splošni primer takih razširitev.

2.2.1. *Poldirektni produkt in razcepne razširitve.* Poldirektni produkt je posplošitev direktnega produkta. Pomagal nam bo najti vse takšne razširitve, kjer obstaja transverzalna funkcija, ki je homomorfizem. Tem razširitvam bomo rekli razcepne razširitve.

Trditev 2.9. *Naj bosta N in G grupi ter $\varphi : G \to \operatorname{Aut} N$ homomorfizem. Označimo $\varphi(g) = \varphi_g$. Potem množica $N \times G$ z operacijo $(n_1, g_1) \cdot (n_2, g_2) = (n_1\varphi_{g_1}(n_2), g_1 g_2)$ postane grupa.*

Dokaz. Množica $N \times G$ je zaprta za operacijo, saj je $n_1\varphi_{g_1}(n_2) \in N$ in $g_1 g_2 \in G$. Preverimo asociativnost operacije. Velja:

$$\Big[(n_1, g_1)(n_2, g_2)\Big](n_3, g_3) = (n_1\varphi_{g_1}(n_2), g_1 g_2)(n_3, g_3) = (n_1\varphi_{g_1}(n_2)\varphi_{g_1 g_2}(n_3), g_1 g_2 g_3).$$

Upoštevamo, da je $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$, saj je φ homomorfizem, in nadaljujemo:

$$\begin{aligned}
(n_1\varphi_{g_1}(n_2)\varphi_{g_1 g_2}(n_3), g_1 g_2 g_3) &= (n_1\varphi_{g_1}(n_2)\varphi_{g_1}(\varphi_{g_2}(n_3)), g_1 g_2 g_3) \\
&= (n_1\varphi_{g_1}(n_2\varphi_{g_2}(n_3)), g_1 g_2 g_3) \\
&= (n_1, g_1)(n_2\varphi_{g_2}(n_3), g_2 g_3) \\
&= (n_1, g_1)\Big[(n_2, g_2)(n_3, g_3)\Big]
\end{aligned}$$

Element $(1,1)$ je enica, saj je $(n,g)(1,1) = (n \cdot \varphi_g(1), g \cdot 1) = (n,g)$. Pri tem smo upoštevali, da je $\varphi_g(1) = 1$, saj je φ_g avtomorfizem. Podobno dokažemo za množenje enice z leve. Inverzni element je $(n,g)^{-1} = (\varphi_{g^{-1}}(n^{-1}), g^{-1})$, saj je

$$\begin{aligned}(n,g)(\varphi_{g^{-1}}(n^{-1}), g^{-1}) &= (n\varphi_g(\varphi_{g^{-1}}(n^{-1})), 1)\\ &= (n\varphi_{gg^{-1}}(n^{-1}), 1)\\ &= (nn^{-1}, 1) = (1,1)\end{aligned}$$

Pri tem smo upoštevali, da je $\varphi_{gg^{-1}} = \varphi_1 = \mathrm{id}$. Podobno velja za množenje inverza z leve. □

Definicija 2.10. Naj bodo N, G in φ kot v prejšnji trditvi. Dobljeno grupo P označimo s $P = N \rtimes_\varphi G$ in jo imenujemo *zunanji poldirektni produkt N z G po φ.*

Če je $\varphi \equiv 1$, potem je $N \rtimes_\varphi G$ že znani (zunanji) direktni produkt grup N in G.

Definicija 2.11. Grupa P je *notranji poldirektni produkt N z G*, če je $N \lhd P$, $G \leq P$, $N \cap G = \{1\}$ in $N \cdot G = P$. Označimo jo s $P = N \rtimes G$.

Opomba 2.12. Vsak element $p \in P$ se da enolično zapisati kot $p = ng$, kjer je $n \in N$ in $g \in G$. Recimo, da je $p = n_1g_1 = n_2g_2$. Potem je $n_2^{-1}n_1 = g_2g_1^{-1}$. Ampak ker je $N \cap G = \{1\}$, je $n_2^{-1}n_1 = g_2g_1^{-1} = 1$ oziroma $n_2 = n_1$ in $g_2 = g_1$.

Če je tudi G podgrupa edinka grupe P, potem je to že znani (notranji) direktni produkt.

Trditev 2.13. *Grupa P je notranji poldirektni produkt N z G natanko tedaj, ko obstaja takšen homomorfizem $\varphi : G \to \mathrm{Aut}(N)$, da je P izomorfen zunanjemu poldirektnemu produktu N z G po φ.*

Dokaz. ($\Longrightarrow$) Iščemo ustrezno preslikavo $\varphi : G \to \mathrm{Aut}(N)$. Naj bo $\varphi(g) = \varphi_g$, kjer je $\varphi_g(n) = gng^{-1}$. Tako definiran φ_g je avtomorfizem in velja

$$\begin{aligned}\varphi_{g_1g_2}(n) = g_1g_2n(g_1g_2)^{-1} = g_1g_2ng_2^{-1}g_1^{-1} = g_1\varphi_{g_2}(n){g_1}^{-1} = \varphi_{g_1}(\varphi_{g_2}(n))\\ = (\varphi_{g_1} \circ \varphi_{g_2})(n),\end{aligned}$$

torej je φ homomorfizem. Najti moramo še izomorfizem med P in $N \rtimes_\varphi G$. Naj bo preslikava $\Phi : N \rtimes_\varphi G \to P$ podana s predpisom $\Phi(n,g) = ng$. Preverimo, da je Φ homomorfizem:

$$\begin{aligned}\Phi((n_1,g_1)(n_2,g_2)) = \Phi(n_1\varphi_{g_1}(n_2), g_1g_2) = n_1\varphi_{g_1}(n_2)g_1g_2 =\\ = n_1g_1n_2g_1^{-1}g_1g_2 = n_1g_1n_2g_2 = \Phi(n_1,g_1)\Phi(n_2,g_2)\end{aligned}$$

Oglejmo si jedro $\ker\Phi = \{(n,g) \in N \rtimes_\varphi G \,|\, ng = 1\}$. Ker je $N \cap G = \{1\}$, je $ng = 1$ natanko tedaj, ko je $n = g = 1$. Sledi, da je $\ker\Phi = \{1\}$ in Φ je injektivna. Preverimo še surjektivnost. Poljuben $p \in P$ se da po opombi 2.12 enolično zapisati v obliki $p = ng$ za neka $n \in N$ in $g \in G$. Zato je $\Phi(n,g) = p$ in Φ je surjektivna.
($\Longleftarrow$) Iščemo podgrupo edinko $H \lhd P$ in podgrupo $K \leq P$, ki zadostita pogojem za notranji poldirektni produkt. Vzamemo $H = \{(n,1) \in P \,|\, n \in N\}$ in $K = \{(1,g) \in P \,|\, g \in G\}$. Iz definicije množenja v P sledi, da sta to podgrupi in da je $H \cong N$ ter $K \cong G$. Preverimo, da je H podgrupa edinka. Za poljuben $p = (n,g) \in P$ in $h = (h_1,1) \in H$ velja

$$\begin{aligned}php^{-1} = (n,g)(h_1,1)(\varphi_{g^{-1}}(n^{-1}), g^{-1}) = (n\varphi_g(h_1), g)(\varphi_{g^{-1}}(n^{-1}), g^{-1}) =\\ = (h_2\varphi_g(\varphi_{g^{-1}}(n^{-1})), gg^{-1}) = (h_3, 1) \in H\end{aligned}$$

Pri tem smo označili s $h_2 = n\varphi_g(h_1)$ in s $h_3 = h_2\varphi_g(\varphi_{g^{-1}}(n^{-1}))$. Sledi, da je H podgrupa edinka. Enakost $H \cap K = \{1\}$ sledi iz definicije H in K. Naj bo $p = (n, g) \in P$ poljuben. Potem za $(n, 1) \in H$ in $(1, g) \in K$ velja $(n, 1)(1, g) = (n\varphi_1(1), g) = (n, g) = p$ in od tod sledi $H \cdot K = P$. □

Zgled 2.14. Naj bo preslikava $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ definirana s predpisoma $\varphi(0) = \mathrm{id}$ in $\varphi(1) = \varphi_1$, kjer je $\varphi_1(a) = -a$. Preslikava φ_1 je avtomorfizem, saj je invertiranje v Abelovi grupi. Velja še $\varphi_1 \circ \varphi_1 = \mathrm{id}$ in od tod sledi, da je φ dobro definiran homomorfizem. Torej obstaja (zunanji) poldirektni produkt $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$. Poglejmo ali je to komutativna grupa. Po eni strani imamo $(1, 0)(1, 1) = (1 + 1, 1) = (2, 1)$ in po drugi $(1, 1)(1, 0) = (1 + \varphi_1(1), 1) = (1 - 1, 1) = (0, 1)$. Torej je $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$ nekomutativna grupa s 6 elementi, edina taka (do izomorfizma) pa je diedrska grupa D_6.

Definicija 2.15. Razširitev $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ je *razcepna*, če obstaja transverzalna funkcija $\tau : G \to R$, ki je homomorfizem.

Opomba 2.16. Ker je τ vedno injektivna, je v tem primeru τ izomorfizem med G in $\mathrm{im}\,\tau$.

Trditev 2.17. *Naj bodo N, R in G grupe. Razcepna razširitev $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ obstaja natanko tedaj, ko je R poldirektni produkt N z G.*

Dokaz. ($\Longrightarrow$) Naj bo $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ razcepna razširitev in $\tau : G \to R$ transverzalna funkcija, ki je homomorfizem. Potem je $T = \mathrm{im}\,\tau$ podgrupa grupe R. Naj bo $M = \mathrm{im}\,\mu = \ker\epsilon$. Za poljuben $r \in R$ je

$$\epsilon(\tau(\epsilon(r^{-1})) \cdot r) = (\epsilon \circ \tau)(\epsilon(r^{-1})) \cdot \epsilon(r) = \epsilon(r)^{-1}\epsilon(r) = 1.$$

Pri tem smo upoštevali, da je $\epsilon \circ \tau = \mathrm{id}_G$. Od tod sledi $\tau(\epsilon(r^{-1})) \cdot r \in M$. Zato lahko poljuben element $r \in R$ zapišemo v obliki

$$r = \tau(\epsilon(r^{-1}))^{-1} \cdot \tau(\epsilon(r^{-1})) \cdot r,$$

kjer je $\tau(\epsilon(r^{-1}))^{-1} \in T$ in $\tau(\epsilon(r^{-1})) \cdot r \in M$. Sledi $R = T \cdot M$. Za poljuben $t \in T \cap M$ je $t = \tau(g)$ za neki $g \in G$. Če na tej enakosti uporabimo ϵ in upoštevamo $\epsilon \circ \tau = \mathrm{id}_G$, dobimo $1 = g$. Ker je τ homomorfizem, je $t = 1$ in zato $T \cap M = \{1\}$. Vemo tudi, da je M podgrupa edinka. Sledi, da je R (notranji) poldirektni produkt $M \cong N$ z $T \cong G$.
($\Longleftarrow$) Naj bo $R = N \rtimes_\varphi G$ (zunanji) poldirektni produkt N z G. Naj bo preslikava $\mu : N \to N \rtimes_\varphi G$ dana s predpisom $\mu(n) = (n, 1)$, preslikava $\epsilon : N \rtimes_\varphi G \to G$ pa s predpisom $\epsilon(n, g) = g$. Tako definirana μ in ϵ sta homomorfizma, saj je

$$\mu(n_1n_2) = (n_1n_2, 1) = (n_1\varphi_1(n_2), 1) = (n_1, 1)(n_2, 1) = \mu(n_1)\mu(n_2)$$

in

$$\epsilon((n_1, g_1)(n_2, g_2)) = \epsilon(n_1\varphi_{g_1}(n_2), g_1g_2) = g_1g_2 = \epsilon(n_1, g_1)\epsilon(n_2, g_2).$$

Zaporedje $N \overset{\mu}{\rightarrowtail} N \rtimes_\varphi G \overset{\epsilon}{\twoheadrightarrow} G$ je kratko eksaktno, saj je $\ker\mu = \{1\}$, $\mathrm{im}\,\epsilon = G$, enakost $\ker\epsilon = \mathrm{im}\,\mu$ pa sledi iz $\epsilon(\mu(n)) = \epsilon(n, 1) = 1$ in $(n, 1) = \mu(n)$ za poljubna $n \in N$ in $(n, 1) \in \ker\epsilon$. Funkcija $\tau : G \to N \rtimes_\varphi G$, definirana s predpisom $\tau(g) := (1, g)$, je transverzalna funkcija, ki je homomorfizem. Res, saj je

$$\tau(g_1)\tau(g_2) = (1, g_1)(1, g_2) = (1\varphi_{g_1}(1), g_1g_2) = (1, g_1g_2) = \tau(g_1g_2)$$

in $\epsilon(\tau(g)) = \epsilon(1, g) = g$, torej $\epsilon \circ \tau = \mathrm{id}_G$. □

V splošnem ni nujno, da obstaja transverzalna funkcija, ki je homomorfizem. V tem primeru v razširitvah lahko nastopajo tudi grupe, ki niso poldirektni produkti. Takšna je razširitev (1) iz uvoda, kjer je nastopala grupa $\mathbb{Z}_{100}$. Ta ne more biti poldirektni produkt $D \cong \mathbb{Z}_{10}$ in $E \cong \mathbb{Z}_{10}$, saj ima le eno podgrupo reda 10. Nobena transverzalna funkcija zato ni homomorfizem. Pogledali bomo kaj več o teh primerih.

2.3. **Sklopitve.** Naj bo $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ razširitev in $\tau : G \to R$ poljubna transverzalna funkcija. Potem je za vsak $g \in G$ preslikava $\tau_g : R \to R$ s predpisom $\tau_g(r) = \tau(g)r\tau(g)^{-1}$ notranji avtomorfizem R. Ker je $M = \operatorname{im}\mu = \ker\epsilon$ podgrupa edinka v R, je za vsak $m \in M$ tudi $\tau(g)m\tau(g)^{-1} \in M$. Torej je zožitev $\tau_g|_M : M \to M$ avtomorfizem grupe M. Ker je $N \cong M$ in μ izomorfizem na svojo sliko, lahko definiramo $\lambda_g \in \operatorname{Aut} N$ s predpisom

$$\lambda_g := \mu^{-1} \circ \tau_g \circ \mu.$$

Če λ_g uporabimo na $n \in N$, dobimo zvezo

$$\begin{aligned} \lambda_g(n) &= (\mu^{-1} \circ \tau_g \circ \mu)(n) \\ \mu(\lambda_g(n)) &= \tau(g)\mu(n)\tau(g)^{-1} \end{aligned} \tag{4}$$

Definiramo lahko preslikavo $\lambda : G \to \operatorname{Aut} N$ s predpisom $\lambda(g) = \lambda_g$, ki pa je odvisna od izbire transverzalne funkcije τ (druga transverzalna funkcija bi inducirala drugačen λ). Preslikavo λ želimo preoblikovati tako, da ne bi bila odvisna od izbire transverzalne funkcije.

Spomnimo se, da so notranji avtomorfizmi podgrupa grupe $\operatorname{Aut} N$. Podgrupa notranjih avtomorfizmov je podgrupa edinka, saj je

$$(\alpha \circ \sigma_k \circ \alpha^{-1})(n) = \alpha(k\alpha^{-1}(n)k^{-1}) = \alpha(k)n\alpha(k)^{-1} = \sigma_{\alpha(k)}(n)$$

za poljuben avtomorfizem $\alpha \in \operatorname{Aut} N$ in notranji avtomorfizem $\sigma_k : N \to N$.

Definicija 2.18. Naj bo N grupa. Označimo z $\operatorname{Inn} N$ podgrupo edinko notranjih avtomorfizmov in kvocientno grupo z $\operatorname{Out} N = \operatorname{Aut} N / \operatorname{Inn} N$.

Trditev 2.19. *Naj bodo oznake kot zgoraj. Preslikava $\chi : G \to \operatorname{Out} N$, definirana s predpisom $\chi(g) = \lambda(g) \operatorname{Inn} N$, je neodvisna od izbire transverzalne funkcije.*

Dokaz. Naj bo τ' neka druga transverzalna funkcija. Ker je ϵ homomorfizem, je

$$\epsilon(\tau(g)\tau'(g)^{-1}) = (\epsilon \circ \tau)(g)(\epsilon \circ \tau')(g)^{-1} = gg^{-1} = 1.$$

Torej je $\tau(g)\tau'(g)^{-1} \in M$ oz. $\tau'(g) = \tau(g)m_g$ za neki $m_g \in M$. Če τ' inducira λ', potem po enačbi (4) dobimo

$$\mu(\lambda'_g(n)) = \tau'(g)\mu(n)\tau'(g)^{-1} = (\tau(g)m_g)\mu(n)(\tau(g)m_g)^{-1} = \tau(g)m_g\mu(n)m_g^{-1}\tau(g)^{-1}.$$

Označimo z $\bar{m}_g$ konjugacijo z m_g (kot preslikavo). Potem je

$$\begin{aligned} \mu^{-1}(\mu(\lambda'_g(n))) &= (\mu^{-1} \circ \tau_g \circ \bar{m}_g \circ \mu)(n) \\ &= (\mu^{-1} \circ \tau_g \circ \mu \circ \mu^{-1} \circ \bar{m}_g \circ \mu)(n) \\ &= (\lambda_g \circ \mu^{-1} \circ \bar{m}_g \circ \mu)(n) \end{aligned}$$

Ampak $\mu^{-1} \circ \bar{m}_g \circ \mu \in \operatorname{Inn}(N)$, saj je μ izomorfizem na M in zožitev $\bar{m}_g|_M : M \to M$ notranji avtomorfizem M. Sledi, da je $\lambda'_g \equiv \lambda_g \operatorname{Inn} N$ oz. $\chi(g) = \lambda(g) \operatorname{Inn} N$ ni odvisna od transverzalne funkcije. □

Trditev 2.20. *Preslikava χ je homomorfizem.*

Dokaz. Po osnovnem izreku o izomorfizmih obstaja izomorfizem $\alpha : R/M \to G$, saj je ϵ surjektiven in $\ker \epsilon = M$. Naj bo $\beta = \alpha^{-1}$. Za $g_1, g_2 \in G$ je $\beta(g_1)\beta(g_2) = \beta(g_1 g_2)$. Ker so $\tau(g_i)$ predstavniki odsekov, dobimo $\tau(g_1)M\tau(g_2)M = \tau(g_1 g_2)M$. Po definiciji množenja odsekov je $\tau(g_1)M\tau(g_2)M = \tau(g_1)\tau(g_2)M$. Od tod dobimo $\tau(g_1 g_2) = \tau(g_1)\tau(g_2)m_{g_1 g_2}$ za neki $m_{g_1 g_2} \in M$. S pomočjo te enakosti in enačbe (4) za $n \in N$ izračunamo

$$\begin{aligned} \mu(\lambda_{g_1 g_2}(n)) &= \tau(g_1 g_2)\mu(n)\tau(g_1 g_2)^{-1} \\ &= \tau(g_1)\tau(g_2)m_{g_1 g_2}\mu(n)(\tau(g_1)\tau(g_2)m_{g_1 g_2})^{-1} \\ &= \tau(g_1)\tau(g_2)m_{g_1 g_2}\mu(n)m_{g_1 g_2}^{-1}\tau(g_2)^{-1}\tau(g_1)^{-1} \end{aligned} \tag{5}$$

Označimo s τ_{g_1} konjugacijo s $\tau(g_1)$, s τ_{g_2} konjugacijo s $\tau(g_2)$ in z $\bar{m}_{g_1 g_2}$ konjugacijo z $m_{g_1 g_2}$ (kot preslikave). Upoštevamo, da je M podgrupa edinka in μ izomorfizem na M, in iz (5) dobimo

$$\begin{aligned} \lambda_{g_1 g_2} &= \mu^{-1} \circ \tau_{g_1} \circ \tau_{g_2} \circ \bar{m}_{g_1 g_2} \circ \mu \\ &= \mu^{-1} \circ \tau_{g_1} \circ (\mu \circ \mu^{-1}) \circ \tau_{g_2} \circ (\mu \circ \mu^{-1}) \circ \bar{m}_{g_1 g_2} \circ \mu \\ &= \lambda_{g_1} \circ \lambda_{g_2} \circ \mu^{-1} \circ \bar{m}_{g_1 g_2} \circ \mu = \lambda_{g_1} \circ \lambda_{g_2} \circ \eta \end{aligned}$$

Preslikava $\eta = \mu^{-1} \circ \bar{m}_{g_1 g_2} \circ \mu$ je notranji avtomorfizem N, saj je μ izomorfizem na M in zožitev $\bar{m}_{g_1 g_2}|_M : M \to M$ notranji avtomorfizem M. Dobili smo $\lambda_{g_1 g_2} = \lambda_{g_1}\lambda_{g_2} \operatorname{Inn} N$ oz. $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. □

Definicija 2.21. Naj bosta G in N poljubni grupi. Homomorfizem $\chi : G \to \operatorname{Out} N$, ne glede na to ali je induciran iz kakšne razširitve ali ne, imenujemo *sklopitev* N *z* G (ang. *coupling*).

Videli smo, da vsaka razširitev grupe N z G inducira sklopitev $\chi : G \to \operatorname{Out} N$. Po drugi strani obstajajo različne razširitve istih grup. V primeru, da so razširitve ekvivalentne, se sklopitev χ ne spremeni.

Trditev 2.22. *Ekvivalentne razširitve inducirajo isto sklopitev* χ.

Dokaz. Naj bosta $N \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ in $N \overset{\bar{\mu}}{\rightarrowtail} \bar{R} \overset{\bar{\epsilon}}{\twoheadrightarrow} G$ ekvivalentni razširitvi ter $(\mathrm{id}, \varphi, \mathrm{id})$ pripadajoči morfizem. Imamo komutativen diagram

$$\begin{array}{ccccc} N & \overset{\mu}{\rightarrowtail} & R & \overset{\epsilon}{\twoheadrightarrow} & G \\ {\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle \varphi}\downarrow & & {\scriptstyle \mathrm{id}}\downarrow \\ N & \overset{\bar{\mu}}{\rightarrowtail} & \bar{R} & \overset{\bar{\epsilon}}{\twoheadrightarrow} & G \end{array}$$

Naj bo $\chi : G \to \operatorname{Out} N$ sklopitev, ki jo inducira prva razširitev, in $\bar{\chi} : G \to \operatorname{Out} N$ sklopitev, ki jo inducira druga razširitev. Izberimo transverzalno funkcijo $\tau : G \to R$ za prvo razširitev. Potem je $\bar{\tau} = \varphi \circ \tau$ (neka) transverzalna funkcija za drugo razširitev, saj zaradi komutativnosti diagrama velja $\bar{\epsilon} \circ \bar{\tau} = \bar{\epsilon} \circ (\varphi \circ \tau) = \epsilon \circ \tau = \mathrm{id}_G$. Vemo, da za vsak $n \in N$ preslikava λ_g zadošča enakosti $\mu(\lambda_g(n)) = \tau(g)\mu(n)\tau(g)^{-1}$. Na tej enakosti uporabimo φ in upoštevamo $\varphi \circ \mu = \bar{\mu}$:

$$\begin{aligned} \varphi(\mu(\lambda_g(n))) &= \varphi(\tau(g)\mu(n)\tau(g)^{-1}) \\ (\varphi \circ \mu)(\lambda_g(n)) &= (\varphi \circ \tau)(g)(\varphi \circ \mu)(n)(\varphi \circ \tau)(g)^{-1} \\ \bar{\mu}(\lambda_g(n)) &= \bar{\tau}(g)\bar{\mu}(n)\bar{\tau}(g)^{-1} \\ \bar{\mu}(\lambda_g(n)) &= \bar{\mu}(\bar{\lambda}_g(n)) \end{aligned}$$

Sledi $\lambda(g) = \bar{\lambda}(g)$ in zato $\chi(g) = \bar{\chi}(g)$. $\square$

2.3.1. *Grupni kolobar.* Grupni kolobar nam bo pomagal, da z danima dvema grupama in sklopitvijo skonstruiramo razširitve. Tu si oglejmo definicijo in par trditev, ki jih bomo kasneje potrebovali.

Definicija 2.23. Naj bo G grupa. Na množico formalnih vsot oblike

$$\mathbb{Z}G = \left\{ \sum_{g \in G} r_g g \;\middle|\; r_g \in \mathbb{Z}, \text{ le končno mnogo } r_g \neq 0 \right\}$$

uvedemo operaciji

$$\begin{aligned} (\Sigma_g r_g g) + \left(\Sigma_g r'_g g\right) &= \Sigma_g (r_g + r'_g) g \\ (\Sigma_g r_g g) \cdot \left(\Sigma_g r'_g g\right) &= \Sigma_g \Sigma_h \left(r_g r'_h gh\right) \end{aligned}$$

S tema operacijama $\mathbb{Z}G$ postane kolobar. Pravimo mu *grupni kolobar.*

Opomba 2.24. Vlogo ničle igra vsota samih ničel. Za nasprotni element vzamemo nasprotne koeficiente iz $\mathbb{Z}$. Asociativnost in distributivnost operacij sledita iz osnovnih lastnosti seštevanja in množenja. Preverimo distributivnost z leve (ostalo podobno):

$$\begin{aligned} a(b+c) &= \Sigma_g r_g g \cdot \left(\Sigma_g r'_g g \; + \Sigma_g r''_g g\right) = \Sigma_g r_g g \cdot \Sigma_g (r'_g + r''_g) g \\ &= \Sigma_g \Sigma_h r_g (r'_h + r''_h) gh = \Sigma_g \Sigma_h (r_g r'_h gh + r_g r''_h gh) \\ &= \Sigma_g \left(\Sigma_h r_g r'_h gh + \Sigma_h r_g r''_h gh\right) = \Sigma_g \Sigma_h r_g r'_h gh + \Sigma_g \Sigma_h r_g r''_h gh = ab + ac \end{aligned}$$

Zgled 2.25. Za G vzemimo $\mathbb{Z}$ in namesto $n \in G$ pišimo x^n. Potem so elementi grupnega kolobarja oblike

$$a_0 x^{n_0} + a_1 x^{n_1} + \ldots + a_k x^{n_k} \in \mathbb{Z}G,$$

kar so ravno Laurentovi polinomi v eni spremenljivki s celoštevilskimi koeficienti. Seštevanje in množenje se ujema s seštevanjem in množenjem v kolobarju polinomov.

Trditev 2.26. *Naj bosta N in G grupi, $\chi : G \to \operatorname{Out} N$ sklopitev in C center grupe N. Potem sklopitev χ na C določa modul nad grupnim kolobarjem $\mathbb{Z}G$. Pri tem je množenje s skalarji definirano s predpisom $g \cdot c := \chi_g(c)$, kjer je χ_g neki element odseka $\chi(g)$.*

Dokaz. Najprej si oglejmo, ali je predpis $g \cdot c = \chi_g(c)$ dobro definiran. Naj bo $\chi_g = \alpha_g \circ \sigma_k$ poljuben element odseka $\chi(g) = \alpha_g \operatorname{Inn} N$, kjer je $\alpha_g \in \operatorname{Aut}(N)$ in $\sigma_k \in \operatorname{Inn}(N)$. Notranji avtomorfizem σ_k naj bo dan z $\sigma_k(n) = knk^{-1}$. Potem za $c \in C$ velja

$$\alpha_g(\sigma_k(c)) = \alpha_g(kck^{-1}) = \alpha_g(ckk^{-1}) = \alpha_g(c),$$

saj je c iz centra grupe N. Torej $\operatorname{Inn} N$ deluje trivialno na C in zato je $g \cdot c$ dobro definiran. Zdaj lahko definiramo operacije modula C. Seštevanje naj bo kar seštevanje v C. Množenje s skalarji definiramo s predpisom ($c \in C$ in $\sum_g n_g g \in \mathbb{Z}G$)

$$\left(\sum_{g \in G} n_g g\right) \cdot c := \sum_{g \in G} n_g (g \cdot c).$$

Preveriti moramo, ali ta predpis zadošča pogojem za module. Dovolj je, če pogledamo samo množenje z elementi iz G. Naj bodo $c, c_1, c_2 \in C$ in $g, g_1, g_2 \in G$. Potem je

$$g(c_1 + c_2) = \chi_g(c_1 + c_2) = \chi_g(c_1) + \chi_g(c_2) = gc_1 + gc_2$$

in

$$(g_1g_2)c = \chi_{g_1g_2}(c) = (\chi_{g_1}\chi_{g_2})(c) = \chi_{g_1}(g_2c) = g_1(g_2c).$$

Ostalo preverimo podobno. S tem C postane $\mathbb{Z}G$-modul. □

Namesto $\mathbb{Z}G$-modul običajno pišemo le G-modul. V primeru, da je N Abelova grupa, dobimo G-modul N. Ta primer nas bo v naslednjem razdelku najbolj zanimal.

Trditev 2.27. *Če je G grupa in N levi G-modul, potem je preslikava $\varphi : G \to \operatorname{Aut} N$ s predpisom $\varphi(g) = (n \mapsto gn)$ homomorfizem.*

Dokaz. Označimo $\varphi(g) = \varphi_g$. Preslikava φ_g ima predpis $\varphi_g(n) = gn$. Je homomorfizem, saj je $\varphi_g(n_1 + n_2) = g(n_1 + n_2) = gn_1 + gn_2 = \varphi_g(n_1) + \varphi_g(n_2)$. Je injektivna, saj iz $gn_1 = gn_2$ sledi $n_1 = n_2$ in surjektivna, saj je $n = gg^{-1}n = \varphi_g(g^{-1}n)$. Sledi, da je φ_g avtomorfizem in zato je φ dobro definirana. Preslikava φ je homomorfizem, saj velja $\varphi_{g_1g_2}(n) = g_1g_2n = g_1\varphi_{g_2}(n) = (\varphi_{g_1} \circ \varphi_{g_2})(n)$. □

Opomba 2.28. Ker je φ homomorfizem, obstaja poldirektni produkt $N \rtimes_\varphi G$. Množenje v $N \rtimes_\varphi G$ je oblike $(n_1, g_1)(n_2, g_2) = (n_1 + g_1n_2, g_1g_2)$.

Opomba 2.29. Poseben primer G-modula je trivialni G-modul ($gn = n$ za vsak $g \in G$ in $n \in N$). V tem primeru se poldirektni produkt poenostavi v direktni produkt.

2.4. **Razširitve z Abelovim jedrom.** Naj bo v tem razdelku A Abelova grupa, $A \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ razširitev, $M = \operatorname{im}\mu$ in $\tau : G \to R$ transverzalna funkcija. Vemo, da za vsak $g_1, g_2 \in G$ obstaja takšen $m_{g_1g_2} \in M$, da velja $\tau(g_1)\tau(g_2) = \tau(g_1g_2)m_{g_1g_2}$ (kot v dokazu trditve 2.20). To lahko preuredimo v

$$\tau(g_1)\tau(g_2)\tau(g_1g_2)^{-1} = \tau(g_1g_2)m_{g_1g_2}\tau(g_1g_2)^{-1} = \tilde{m}_{g_1g_2},$$

kjer je $\tilde{m}_{g_1g_2} \in M$, saj je M podgrupa edinka v R. Ker je μ injektivna, lahko definiramo preslikavo $\varphi : G \times G \to A$ s predpisom $\varphi(g_1, g_2) = \mu^{-1}(\tilde{m}_{g_1g_2})$. Tako definiran φ zadošča enačbi

$$\tau(g_1)\tau(g_2)\tau(g_1g_2)^{-1} = \mu(\varphi(g_1, g_2)). \tag{6}$$

Želimo najti kakšno enačbo, ki ji zadošča funkcija φ, v kateri ne bi nastopala μ in τ. Do nje bomo prišli tako, da bomo s pomočjo zgornje enačbe razpisali naslednjo enakost:

$$\begin{aligned}
(\tau(g_1)\tau(g_2))\tau(g_3) &= \tau(g_1)(\tau(g_2)\tau(g_3)) \\
(\tau(g_1)\tau(g_2))\tau(g_1g_2)^{-1}\tau(g_1g_2)\tau(g_3)\tau(g_1g_2g_3)^{-1} &= \tau(g_1)(\tau(g_2)\tau(g_3)\cdot \\
&\quad \cdot \tau(g_2g_3)^{-1}\tau(g_1)^{-1}\tau(g_1)\tau(g_2g_3))\tau(g_1g_2g_3)^{-1} \\
\mu(\varphi(g_1, g_2)\mu(\varphi(g_1g_2, g_3)) &= \tau(g_1)\mu(\varphi(g_2, g_3))\tau(g_1)^{-1}\mu(\varphi(g_1, g_2g_3))
\end{aligned} \tag{7}$$

To enakost lahko še nekoliko poenostavimo. Vemo, da transverzalna funkcija inducira sklopitev $\chi : G \to \operatorname{Out} A$. Po trditvi 2.26 χ na A inducira množenje s skalarji

s predpisom $g \cdot a = \chi_g(a)$. Potrebovali bomo še zvezo (4), iz katere smo izpeljali definicijo sklopitve:

$$\mu(\lambda_g(a)) = \tau(g)\mu(a)\tau(g)^{-1}.$$

Ker imamo tokrat komutativno grupo A, je $\operatorname{Inn} A$ trivialna in zato $\lambda_g = \chi_g$. Inducirano množenje s skalarji nam da zvezo

$$\mu(g \cdot a) = \tau(g)\mu(a)\tau(g)^{-1}. \tag{8}$$

S to zvezo lahko enakost (7) poenostavimo v

$$\mu(\varphi(g_1, g_2))\mu(\varphi(g_1g_2, g_3)) = \mu(g_1\varphi(g_2, g_3))\mu(\varphi(g_1, g_2g_3))$$
$$\mu(\varphi(g_1, g_2) + \varphi(g_1g_2, g_3)) = \mu(g_1\varphi(g_2, g_3) + \varphi(g_1, g_2g_3))$$

Ker je μ injektivna, lahko argumente enačimo in dobimo pogoj za φ:

$$\varphi(g_1, g_2) + \varphi(g_1g_2, g_3) = g_1\varphi(g_2, g_3) + \varphi(g_1, g_2g_3). \tag{9}$$

Definicija 2.30. Naj bo G grupa in A levi G-modul. Vsaka funkcija $\varphi : G \times G \to A$, ki zadošča enačbi (9) za vse $g_1, g_2, g_3 \in G$, se imenuje 2-*kocikel*. Množico vseh takšnih funkcij označimo z $Z^2(G, A)$.

Zgled 2.31. Spomnimo se na razširitev iz uvoda $D \overset{i}{\rightarrowtail} \mathbb{Z}_{100} \overset{s}{\twoheadrightarrow} E$, kjer sta bila $D \cong \mathbb{Z}_{10}$ in $E \cong \mathbb{Z}_{10}$. Seštevanje v $\mathbb{Z}_{100}$ smo opisali s pari števil $(d, e) \in D \times E$ in funkcijo $z : E \times E \to D$. Predpis se je glasil $(d_1, e_1)(d_2, e_2) = (d_1 + d_2 + z(e_1, e_2), e_1 + e_2)$. Vzemimo števila $(0, e_1), (0, e_2)$ in $(0, e_3)$ in poglejmo enakost za asociativnost:

$$((0, e_1) + (0, e_2)) + (0, e_3) = (0, e_1) + ((0, e_2) + (0, e_3))$$
$$(z(e_1, e_2), e_1 + e_2) + (0, e_3) = (0, e_1) + (z(e_2, e_3), e_2 + e_3)$$
$$(z(e_1, e_2) + z(e_1 + e_2, e_3), e_1 + e_2 + e_3) = (z(e_1, e_2 + e_3) + z(e_2, e_3), e_1 + e_2 + e_3)$$

Funkcija z zadošča enakosti $z(e_1, e_2) + z(e_1 + e_2, e_3) = z(e_1, e_2 + e_3) + z(e_2, e_3)$, kar je ravno pogoj za 2-kocikel, če za množenje s skalarji vzamemo trivialno delovanje.

Še en primer 2-kocikla je trivialni 2-kocikel (konstanta 0). Ta se pojavi v razširitvi z direktnim produktom.

Trditev 2.32. *Množica $Z^2(G, A)$ je Abelova grupa za operacijo $(\varphi_1 + \varphi_2)(g_1, g_2) = \varphi_1(g_1, g_2) + \varphi_2(g_1, g_2)$.*

Dokaz. Preverimo, če tak $(\varphi_1 + \varphi_2)(g_1, g_2)$ zadošča enačbi (9):

$$(\varphi_1 + \varphi_2)(g_1, g_2) + (\varphi_1 + \varphi_2)(g_1g_2, g_3) = g_1(\varphi_1 + \varphi_2)(g_2, g_3) + (\varphi_1 + \varphi_2)(g_1, g_2g_3)$$
$$\varphi_1(g_1, g_2) + \varphi_2(g_1, g_2) + \varphi_1(g_1g_2, g_3) + \varphi_2(g_1g_2, g_3) = g_1(\varphi_1(g_2, g_3) + \varphi_2(g_2, g_3)) + \varphi_1(g_1, g_2g_3) + \varphi_2(g_1, g_2g_3)$$

Po definiciji množenja s skalarji velja $g_1(\varphi_1(g_2, g_3) + \varphi_2(g_2, g_3)) = g_1\varphi_1(g_2, g_3) + g_1\varphi_2(g_2, g_3)$ in od tod sledi, da $(\varphi_1 + \varphi_2)(g_1, g_2)$ zadošča (9). Asociativnost in komutativnost operacije sledi iz asociativnosti in komutativnosti v A. Vlogo ničle igra trivialni 2-kocikel, nasprotni element pa je $(-\varphi)(g_1, g_2) = -\varphi(g_1, g_2)$. □

Zgoraj smo pogoj za 2-kocikel φ izpeljali v odvisnosti od transverzalne funkcije τ. Poglejmo, kako se φ spremeni, če spremenimo transverzalno funkcijo. Naj bodo oznake kot prej in naj bo τ' neka druga transverzalna funkcija, ki vodi do 2-kocikla φ'. Za vsak $g \in G$ lahko zapišemo $\tau'(g) = \tau(g)m_g$ za neki $m_g \in M$ (kot v dokazu 2.19). To preuredimo v $\tau'(g)\tau(g)^{-1} = \tau(g)m_g\tau(g)^{-1} = \tilde{m}_g \in M$. Definirajmo

funkcijo $\psi : G \to A$ s predpisom $\psi(g) = \mu^{-1}(\tilde{m}_g)$. Tako definiran ψ zadošča enačbi $\tau'(g) = \mu(\psi(g))\tau(g)$. S pomočjo te enačbe in enačbe (6) izračunamo:

$$\begin{aligned}
\tau'(g_1)\tau'(g_2)\tau'(g_1g_2)^{-1} &= \mu(\varphi'(g_1, g_2)) \\
\mu(\psi(g_1))\tau(g_1)\mu(\psi(g_2))\tau(g_2) &= \mu(\varphi'(g_1, g_2))\mu(\psi(g_1g_2))\tau(g_1g_2) \\
\mu(\psi(g_1))\tau(g_1)\mu(\psi(g_2))\tau(g_1)^{-1} &= \mu(\varphi'(g_1, g_2))\mu(\psi(g_1g_2))\tau(g_1g_2)\tau(g_2)^{-1}\tau(g_1)^{-1} \\
\mu(\psi(g_1))\mu(g_1\psi(g_2)) &= \mu(\varphi'(g_1, g_2))\mu(\psi(g_1g_2))\mu(-\varphi(g_1, g_2)) \\
\mu(\psi(g_1) + g_1\psi(g_2)) &= \mu(\varphi'(g_1, g_2) + \psi(g_1g_2) - \varphi(g_1, g_2))
\end{aligned}$$

Ker je μ injektivna, lahko enačimo argumente in po preureditvi dobimo

$$\varphi'(g_1, g_2) - \varphi(g_1, g_2) = g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1).$$

Razlika dveh kociklov iz iste razširitve je tako določena z izrazom na desni.

Definicija 2.33. Naj bo G grupa in A levi G-modul. Za poljubno funkcijo $\psi : G \to A$ definiramo $\psi^* : G \times G \to A$ s predpisom $\psi^*(g_1, g_2) = g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1)$. Funkcijo ψ^* imenujemo 2-*korob*. Množico vseh 2-korobov označimo z $B^2(G, A)$.

Posledica 2.34. *V dani razširitvi 2-kocikli pripadajo množici $\varphi + B^2(G, A)$.*

Trditev 2.35. *Množica vseh 2-korobov $B^2(G, A)$ je podgrupa grupe $Z^2(G, A)$.*

Dokaz. Preverimo, če predpis za 2-korob ψ^* zadošča enačbi (9):

$$\begin{aligned}
\psi^*(g_1, g_2) + \psi^*(g_1g_2, g_3) &= g_1\psi^*(g_2, g_3) + \psi^*(g_1, g_2g_3) \\
g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1) + g_1g_2\psi(g_3) - \psi(g_1g_2g_3) + \psi(g_1g_2) &= g_1g_2\psi(g_3) - \\
&\quad -g_1\psi(g_2g_3) + g_1\psi(g_2) + g_1\psi(g_2g_3) - \psi(g_1g_2g_3) + \psi(g_1)
\end{aligned}$$

Člani se odštejejo in enačba se izide. Preverimo še ali je $\psi_1^* - \psi_2^* \in B^2(G, A)$. Velja

$$\begin{aligned}
&{\psi_1}^*(g_1, g_2) - \psi_2^*(g_1, g_2) = \\
&\quad = g_1\psi_1(g_2) - \psi_1(g_1g_2) + \psi_1(g_1) - g_1\psi_2(g_2) + \psi_2(g_1g_2) - \psi_2(g_1) \\
&\quad = g_1(\psi_1(g_2) - \psi_2(g_2)) - (\psi_1(g_1g_2) - \psi_2(g_1g_2)) + \psi_1(g_1) - \psi_2(g_1)
\end{aligned}$$

Če vzamemo $\psi(g) = \psi_1(g) - \psi_2(g)$ je $\psi^* = \psi_1^* - \psi_2^*$ in $\psi^* \in B^2(G, A)$. □

Sedaj lahko definiramo kvocientno grupo 2-kociklov po 2-korobovih.

3. Druga kohomološka grupa

Definicija 3.1. Naj bo G grupa in A levi G-modul. Potem kvocientni grupi $Z^2(G, A)/B^2(G, A)$ pravimo *druga kohomološka grupa G s koeficienti v A*. Označimo jo s $H^2(G, A)$.

Opomba 3.2. Da se definirati tudi n-to kohomološko grupo $H^n(G, A)$ za poljuben $n \in \mathbb{N}_0$. Splošno definicijo lahko najdemo v [4, poglavje 11].

V prejšnjem razdelku smo videli, da lahko vsaki razširitvi priredimo en element grupe $H^2(G, A) = Z^2(G, A)/B^2(G, A)$. Velja tudi obratno; to bomo izpeljali v dveh korakih.

Trditev 3.3. *Naj bo G grupa, A levi G-modul in $\varphi : G \times G \to A$ 2-kocikel. Potem obstaja takšna razširitev grupe A z G, ki inducira G-modul A in ji pripada 2-kocikel φ.*

Dokaz. Označimo množico $R_\varphi = A \times G$. Na to množico uvedemo operacijo s predpisom $(a_1, g_1)(a_2, g_2) := (a_1 + g_1 a_2 + \varphi(g_1, g_2), g_1 g_2)$. Je asociativna, saj je

$$\begin{aligned}[(a_1, g_1)(a_2, g_2)](a_3, g_3) &= (a_1 + g_1 a_2 + \varphi(g_1, g_2), g_1 g_2)(a_3, g_3) \\ &= (a_1 + g_1 a_2 + \varphi(g_1, g_2) + g_1 g_2 a_3 + \varphi(g_1 g_2, g_3), g_1 g_2 g_3) \\ &= (a_1 + g_1(a_2 + g_2 a_3 + \varphi(g_2, g_3)) + \varphi(g_1, g_2 g_3), g_1 g_2 g_3) \\ &= (a_1, g_1)(a_2 + g_2 a_3 + \varphi(g_2, g_3), g_2 g_3) \\ &= (a_1, g_1)[(a_2, g_2)(a_3, g_3)]\end{aligned}$$

Pokazali bomo, da je $(-\varphi(1,1), 1)$ enica, inverz elementa (a, g) pa je dan z $(a, g)^{-1} = (-g^{-1}a - \varphi(1,1) - \varphi(g^{-1}, g), g^{-1})$. Preden to preverimo, rabimo nekaj zvez, ki sledijo iz pogoja za 2-kocikel (9). Če v njem vstavimo

(i) $g_2 = g_3 = 1$, dobimo $\varphi(g, 1) = g\varphi(1, 1)$;
(ii) $g_1 = g_2 = 1$, dobimo $\varphi(1, g) = \varphi(1, 1)$;
(iii) $g_1 = g_3$ in $g_2 = g_1^{-1}$, dobimo $\varphi(g, g^{-1}) + \varphi(1, g) = g\varphi(g^{-1}, g) + \varphi(g, 1)$.

S pomočjo (i) preverimo, da je $(-\varphi(1,1), 1)$ desna enica:

$$(a, g)(-\varphi(1,1), 1) = (a - g\varphi(1,1) + \varphi(g, 1), g) = (a, g).$$

Z (ii), da je tudi leva enica:

$$(-\varphi(1,1), 1)(a, g) = (-\varphi(1,1) + a + \varphi(1, g), g) = (a, g).$$

Preverimo, da je $(-g^{-1}a - \varphi(1,1) - \varphi(g^{-1}, g), g^{-1})$ desni inverz (a, g):

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

Pri tem smo v drugi vrstici upoštevali, da iz (i) sledi $g\varphi(1,1) = \varphi(g, 1)$ in v tretji, da iz (iii) dobimo $-\varphi(g, 1) - g\varphi(g^{-1}, g) = -\varphi(g, g^{-1}) - \varphi(1, g)$. Preverimo še inverz z leve:

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

Sledi, da je R_φ grupa. Zdaj konstruiramo razširitev $A \rightarrowtail^{\mu} R_\varphi \overset{\epsilon}{\twoheadrightarrow} G$, kjer je $\mu(a) = (a - \varphi(1,1), 1)$ in $\epsilon(a, g) = g$. Preslikava μ je homomorfizem, saj je

$$\begin{aligned}\mu(a + b) &= (a + b - \varphi(1,1), 1) = (a - \varphi(1,1) + b - \varphi(1,1) + \varphi(1,1), 1) \\ &= (a - \varphi(1,1), 1)(b - \varphi(1,1), 1) = \mu(a)\mu(b)\end{aligned}$$

Je injektivna, saj iz $a - \varphi(1,1) = b - \varphi(1,1)$ sledi $a = b$. Preslikava ϵ je homomorfizem, saj je $\epsilon((a, g_1)(b, g_2)) = \epsilon(c, g_1 g_2) = g_1 g_2 = \epsilon(a, g_1)\epsilon(b, g_2)$. Je surjektivna, saj je $g = \epsilon(0, g)$ za poljuben $g \in G$. Velja $\operatorname{im}\mu = \ker\epsilon = \{(a, 1) \mid a \in A\}$, saj je enačba $b = a - \varphi(1,1)$ enolično rešljiva na a. Dokazati moramo še, da ta razširitev inducira G-modul A in da ji pripada 2-kocikel φ. Vzemimo transverzalno funkcijo

$\tau : G \to R_\varphi$ s predpisom $\tau(g) = (0, g)$. Iz induciranega množenja s skalarji (enačba (8), tu ga označimo z $*$) in definicije množenja v R_φ dobimo

$$\begin{aligned}
\mu(g*a) &= \tau(g)\mu(a)\tau(g)^{-1} = (0,g)(a - \varphi(1,1), 1)(0,g)^{-1} \\
&= (ga - g\varphi(1,1) + \varphi(g,1), g)(-\varphi(1,1) - \varphi(g^{-1}, g), g^{-1}) \\
&= (ga - g\varphi(1,1) + \underbrace{\varphi(g,1)}_{=g\varphi(1,1)} \overbrace{\underbrace{-g\varphi(1,1)}_{=-\varphi(g,1)} \underbrace{-g\varphi(g^{-1},g)}_{=-\varphi(g,g^{-1})-\varphi(1,g)}}^{} + \varphi(g,g^{-1}), 1) \\
&= (ga - g\varphi(1,1) + g\varphi(1,1) \underbrace{-\varphi(1,g)}_{=-\varphi(1,1)}, 1) \\
&= (ga - \varphi(1,1), 1) = \mu(g \cdot a)
\end{aligned}$$

Ker je μ injektivna, sledi, da se inducirano množenje s skalarji ujema z množenjem s skalarji v G-modulu A. Preveriti moramo še, ali tej razširitvi in transverzalni funkciji pripada 2-kocikel φ. Drugače rečeno, zanima nas, ali izpolnjuje enačbo (6):

$$\tau(g_1)\tau(g_2)\tau(g_1g_2)^{-1} = \mu(\varphi(g_1, g_2)).$$

Izračunamo:

$$\begin{aligned}
\tau(g_1)\tau(g_2) &= (0, g_1)(0, g_2) = (\varphi(g_1, g_2), g_1g_2) \\
&= (\varphi(g_1, g_2) - \varphi(1,1) + \varphi(1, g_1g_2), g_1g_2) \\
&= (\varphi(g_1, g_2) - \varphi(1,1), 1)(0, g_1g_2) \\
&= \mu(\varphi(g_1, g_2))\tau(g_1g_2)
\end{aligned}$$

Zato je pri tej izbiri transverzalne funkcije φ res pripadajoči 2-kocikel. □

Izrek 3.4. *Naj bo G grupa in A levi G-modul. Potem obstaja bijektivna preslikava med ekvivalenčnimi razredi vseh ekvivalentnih razširitev A z G, ki inducirajo dani G-modul A, in grupo $H^2(G, A)$.*

Dokaz. Naj bosta $A \overset{\mu_i}{\rightarrowtail} R_i \overset{\epsilon_i}{\twoheadrightarrow} G$ $(i = 1, 2)$ ekvivalentni razširitvi in τ_i ter φ_i transverzalni funkciji in 2-kocikla. Imamo komutativen diagram

$$\begin{array}{ccccc}
A & \overset{\mu_1}{\rightarrowtail} & R_1 & \overset{\epsilon_1}{\twoheadrightarrow} & G \\
\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \mathrm{id}} \\
A & \overset{\mu_2}{\rightarrowtail} & R_2 & \overset{\epsilon_2}{\twoheadrightarrow} & G
\end{array}$$

kjer je β izomorfizem.

Najprej si oglejmo funkcijo $\bar{\tau_2} := \beta \circ \tau_1$, ki je transverzalna funkcija za drugo razširitev, saj je $\epsilon_2 \circ \bar{\tau_2} = \epsilon_2 \circ \beta \circ \tau_1 = \epsilon_1 \circ \tau_1 = \mathrm{id}_G$. Če uporabimo β na enačbi $\tau_1(g_1)\tau_1(g_2) = \mu_1(\varphi_1(g_1, g_2))\tau_1(g_1g_2)$, dobimo $\bar{\tau_2}(g_1)\bar{\tau_2}(g_2) = \mu_2(\varphi_1(g_1, g_2))\bar{\tau_2}(g_1g_2)$. Torej $\bar{\tau_2}$ določa 2-kocikel φ_1 za drugo razširitev. Ampak vemo, da vsi 2-kocikli ene razširitve pripadajo istemu odseku $\varphi + B^2(G, A)$ (za neki φ). Sledi $\varphi_1 + B^2(G, A) = \varphi_2 + B^2(G, A)$. S tem smo pokazali, da ekvivalentni razširitvi določata isti element v $Z^2(G, A)/B^2(G, A)$.

Poglejmo še obratno: naj bo $\varphi_1 + B^2(G, A) = \varphi_2 + B^2(G, A)$. Torej je $\varphi_1 = \varphi_2 + \psi^*$ za neki $\psi^* \in B^2(G, A)$ (s pripadajočim $\psi : G \to A$). Naj φ_i inducira razširitev $A \overset{\mu_i}{\rightarrowtail} R_i \overset{\epsilon_i}{\twoheadrightarrow} G$. Poljuben $r \in R_1$ lahko enolično zapišemo v obliki $r = \mu_1(a)\tau_1(g)$ za neka $a \in A$ in $g \in G$, saj je $G \cong R_1/A$. Sedaj definiramo

preslikavo $\alpha : R_1 \to R_2$ s predpisom $\alpha(r) = \alpha(\mu_1(a)\tau_1(g)) := \mu_2(a + \psi(g))\tau_2(g)$. Z upoštevanjem definicije induciranih 2-kociklov in zveze $\varphi_1 = \varphi_2 + \psi^*$ preverimo, da je α homomorfizem:

$$\begin{aligned}
\alpha(\mu_1(a_1)\tau_1(g_1)\mu_1(a_2)\tau_1(g_2)) &= \alpha(\mu_1(a_1)\tau_1(g_1)\mu_1(a_2)\tau_1(g_1)^{-1}\tau_1(g_1)\tau_1(g_2)) \\
&= \alpha(\mu_1(a_1)\mu_1(g_1a_2)\mu_1(\varphi_1(g_1,g_2))\tau_1(g_1g_2)) \\
&= \mu_2(a_1 + g_1a_2 + \varphi_1(g_1,g_2) + \psi(g_1g_2))\tau_2(g_1g_2) \\
&= \mu_2(a_1 + g_1a_2 + \varphi_2(g_1,g_2) + g_1\psi(g_2) + \psi(g_1))\mu_2(-\varphi_2(g_1,g_2))\tau_2(g_1)\tau_2(g_2) \\
&= \mu_2(a_1 + \psi(g_1))\tau_2(g_1)\mu_2(a_2)\tau_2(g_1)^{-1}\tau_2(g_1)\mu_2(\psi(g_2))\tau_2(g_1)^{-1}\tau_2(g_1)\tau_2(g_2) \\
&= \mu_2(a_1 + \psi(g_1))\tau_2(g_1)\mu_2(a_2 + \psi(g_2))\tau_2(g_2) \\
&= \alpha(\mu_1(a_1)\tau_1(g_1))\alpha(\mu_1(a_2)\tau_1(g_2))
\end{aligned}$$

Preverimo, da je $\alpha \circ \mu_1 = \mu_2$. Velja enakost $\tau_1(1) = \mu_1(\varphi_1(1,1))$, saj je $\tau_1(1)\tau_1(1) = \mu_1(\varphi_1(1,1))\tau_1(1)$ in $\tau_1(1) \in \operatorname{im}\mu_1$ (podobno za τ_2). Za vsak $a \in A$ obstaja natanko en $\tilde{a} \in A$, da je $\mu_1(a) = \mu_1(\tilde{a})\tau_1(1)$. Od tod dobimo $\mu_1(a) = \mu_1(\tilde{a})\mu_1(\varphi_1(1,1)) = \mu_1(\tilde{a} + \varphi_1(1,1))$ oz. $a = \varphi_1(1,1) + \tilde{a}$. S to zvezo in enakostjo $\psi^*(1,1) = \psi(1)$ izračunamo

$$\begin{aligned}
(\alpha \circ \mu_1)(a) = \alpha(\mu_1(\tilde{a})\tau_1(1)) &= \mu_2(\tilde{a} + \psi(1))\tau_2(1) \\
&= \mu_2(a - \varphi_1(1,1) + \psi^*(1,1))\mu_2(\varphi_2(1,1)) \\
&= \mu_2((\varphi_2 - \varphi_1)(1,1) + a + \psi^*(1,1)) \\
&= \mu_2(a)
\end{aligned}$$

Po definiciji α in zaradi $\operatorname{im}\mu_i = \ker\epsilon_i$ sledi, da je $\epsilon_1 = \epsilon_2 \circ \alpha$. Torej imamo komutativen diagram

$$\begin{array}{ccccc}
A & \xrightarrow{\mu_1} & R_1 & \xrightarrow{\epsilon_1} & G \\
{\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle \alpha}\downarrow & & {\scriptstyle \mathrm{id}}\downarrow \\
A & \xrightarrow{\mu_2} & R_2 & \xrightarrow{\epsilon_2} & G
\end{array}$$

Po kratki lemi o petih je α izomorfizem. Od tod sledi, da vsak element grupe $Z^2(G,A)/B^2(G,A)$ določa razred ekvivalentnih razširitev A z G. Torej je funkcija, ki slika razred ekvivalentnih razširitev v odsek $\varphi + B^2(G,A)$, kjer je φ 2-kocikel od ene izmed razširitev, bijektivna. S tem je trditev dokazana. □

Posledica 3.5. *Razcepna razširitev ustreza elementu $B^2(G,A)$.*

Dokaz. Naj bo $A \xrightarrow{\mu} R \xrightarrow{\epsilon} G$ razcepna razširitev in $\tau : G \to R$ transverzalna funkcija, ki je homomorfizem. Naj bo φ 2-kocikel za to transverzalno funkcijo. Iz enačbe $\tau(g_1)\tau(g_2) = \mu(\varphi(g_1,g_2))\tau(g_1g_2)$ dobimo $\mu(\varphi(g_1,g_2)) = 1$ za vsak $g_1, g_2 \in G$. Ker je μ injektivna, je $\varphi(g_1,g_2) = 0$. Sledi $\varphi = 0$ oz. $\varphi + B^2(G,A) = B^2(G,A)$.

Poglejmo še obratno. Izberimo poljuben $\psi^* \in B^2(G,A)$ s pripadajočim $\psi : G \to A$. Vemo, da je ψ^* 2-kocikel in da zato obstaja neka razširitev, za katero je $\tau(g_1)\tau(g_2) = \mu(\psi^*(g_1,g_2))\tau(g_1g_2)$. Definirajmo novo transverzalno funkcijo $\tau' : G \to R$ s predpisom $\tau'(g) = \mu(-\psi(g))\tau(g)$. To je res transverzalna funkcija, saj je

$$(\epsilon \circ \tau')(g) = \epsilon(\mu(-\psi(g))\tau(g)) = (\epsilon \circ \mu)(-\psi(g))(\epsilon \circ \tau)(g) = g.$$

Zadnja enakost velja, saj je $(\epsilon \circ \mu)(-\psi(g)) = 1$ in $\epsilon \circ \tau = \mathrm{id}_G$. Sedaj razpišemo

$$\begin{aligned}
\tau(g_1)\tau(g_2) &= \mu(\psi^*(g_1, g_2))\tau(g_1 g_2) \\
\tau(g_1)\tau(g_2) &= \mu(g_1\psi(g_2) - \psi(g_1 g_2) + \psi(g_1))\mu(\psi(g_1 g_2))\tau'(g_1 g_2) \\
\tau(g_1)\tau(g_2) &= \tau(g_1)\mu(\psi(g_2))\tau(g_1)^{-1}\mu(\psi(g_1))\tau'(g_1 g_2) \\
\mu(-\psi(g_1))\tau(g_1)\mu(-\psi(g_2))\tau(g_2) &= \tau'(g_1 g_2) \\
\tau'(g_1)\tau'(g_2) &= \tau'(g_1 g_2)
\end{aligned}$$

Sledi, da je razširitev razcepna. □

Zgled 3.6. Naj bodo $D \cong \mathbb{Z}_{10}$, $E \cong \mathbb{Z}_{10}$ in funkcija z kot v zgledu 2.31 oz. uvodu (skupaj s trivialnim delovanjem). Videli smo že, da je z 2-kocikel. Zato z določa en razred ekvivalentnih razširitev D z E. Zanimajo nas še druge razširitve. Funkcija $\underbrace{z + \ldots + z}_{k\text{-krat}}$ zadošča pogoju za 2-kocikel za vsak $k \in \{0, 1, \ldots, 9\}$. Po trditvi 3.3 obstajajo razširitve

$$D \rightarrowtail^{\mu_k} R_k \twoheadrightarrow^{\epsilon_k} E,$$

za katere je operacija v R_k določena s predpisom $(d_1, e_1)(d_2, e_2) = (d_1 + d_2 + kz(e_1, e_2), e_1 + e_2)$ (množenje s skalarji vzamemo trivialno). Za $k = 0$ in $k = 1$ že vemo, da dobimo razširitev z direktnim produktom in $\mathbb{Z}_{100}$, zato nas bodo zanimali le primeri za $k \in \{2, \ldots 9\}$. Ker je $R_k / \ker \epsilon_k \cong E$ in $\ker \epsilon_k \cong D$, mora biti grupa R_k končna grupa reda 100, saj sta D in E reda 10. Iz definicije z sledi $z(e_1, e_2) = z(e_2, e_1)$, saj je seštevanje v $\mathbb{Z}_{100}$ komutativno. Zato je tudi operacija v R_k komutativna. Do izomorfizma natančno obstajajo štiri komutativne grupe reda 100: $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$, $\mathbb{Z}_{20} \oplus \mathbb{Z}_5$, $\mathbb{Z}_{50} \oplus \mathbb{Z}_2$ in $\mathbb{Z}_{100}$. Radi bi ugotovili, katera izmed teh grup se pojavi v razširitvi z 2-kociklom kz (ista grupa se lahko pojavi tudi v več neekvivalentnih razširitvah).

Navedene štiri grupe lahko ločimo glede na prisotnost ali odsotnost elementa reda 4 in 25. Najprej si oglejmo, kaj mora veljati za element reda 4. Naj bo $(d, e) \in R_k$. Dobimo enačbo

$$\underbrace{(d, e) + \ldots + (d, e)}_{4\text{-krat}} = (4d + kz(e, e) + kz(2e, e) + kz(3e, e), 4e) = (0, 0).$$

Edini števili v $\mathbb{Z}_{10}$, ki zadoščata $4e = 0$, sta 0 in 5. V primeru $e = 0$ iz prve komponente dobimo $4d = 0$. Spet sta možni rešitvi 0 in 5, ampak noben od elementov $(0, 0)$ in $(5, 0)$ ni reda 4. Zato za element reda 4 pride v poštev le $e = 5$. Od tod dobimo

$$4d + kz(5, 5) + kz(0, 5) + kz(5, 5) = 4d + 2k = 0.$$

Oglejmo si primer za $k = 2$. Rešitvi enačbe $4d + 4 = 0$ v $\mathbb{Z}_{10}$ sta 4 in 9. Ampak oba elementa $(4, 5)$ in $(9, 5)$ imata red 2. Za $k = 2$ zato ne obstaja noben element reda 4 in v poštev prideta le grupi $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ in $\mathbb{Z}_{50} \oplus \mathbb{Z}_2$. Poglejmo še prisotnost elementa reda 25:

$$\underbrace{(d, e) + \ldots + (d, e)}_{25\text{-krat}} = (25d + k \sum_{i=1}^{24} z(ie, e), 25e) = (0, 0).$$

Še vedno opazujmo le primer $k = 2$. Rešitev enačbe $25e = 0$ v $\mathbb{Z}_{10}$ je 0, 4 ali 8. V primeru $e = 0$ še z upoštevanjem prve komponente dobimo kandidate $(0, 0)$, $(4, 0)$ in

$(8,0)$. Ampak noben od teh ni reda 25. Vzamemo $e = 4$ in poskusimo rešiti enačbo

$$25d + 2\sum_{i=1}^{24} z(4i,4) = 5d + 8\sum_{i=1}^{5} z(4i,4) + 2\sum_{i=1}^{4} z(4i,4) = 5d + 8\cdot 2 + 2\cdot 2 = 0.$$

Če je $d = 0$ ali $d = 2$, se enačba izide. V primeru $(0,4)$ res dobimo element reda 25, saj sta $2 \cdot \sum_{i=1}^{j-1} z(4i,4)$ in $4j$ prvič hkrati enaka 0 šele pri $j = 25$. Ker v $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ ni elementa reda 25, sledi, da kocikel $2z$ pripada razširitvi, v kateri nastopa grupa $\mathbb{Z}_{50} \oplus \mathbb{Z}_2$.

Na podoben način izračunamo, da tudi pri $4z, 6z$ in $8z$ nastopa grupa $\mathbb{Z}_{50} \oplus \mathbb{Z}_2$. Ker je $8z - 6z = 2z$ in $2z$ pripada razširitvi, ki ni ekvivalentna razširitvi z direktnim produktom, tudi ostale med seboj niso ekvivalentne. Drugače rečeno, imamo štiri razširitve, pri katerih nastopa grupa $\mathbb{Z}_{50} \oplus \mathbb{Z}_2$, ampak med seboj niso ekvivalentne. Podobno lahko izračunamo, da pri $3z, 7z$ in $9z$ nastopa grupa $\mathbb{Z}_{100}$ in da pripadajoče razširitve niso ekvivalentne, ter pri $5z$ grupa $\mathbb{Z}_{20} \oplus \mathbb{Z}_5$.

Sledi, da $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$ vsebuje podgrupo, ki je izomorfna $\mathbb{Z}_{10}$, pri čemer je $z + B^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$ generator te podgrupe. V naslednjem poglavju bomo s programom GAP videli, da je to celotna grupa $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$.

Izrek 3.7 (Schur-Zassenhaus)**.** *Naj bo G končna grupa, A končna Abelova grupa in $D(|A|, |G|) = 1$. Potem je vsaka razširitev A z G razcepna.*

Dokaz. Naj bo $|A| = m$, $|G| = n$, $A \overset{\mu}{\rightarrowtail} R \overset{\epsilon}{\twoheadrightarrow} G$ poljubna razširitev in $\varphi : G \times G \to A$ pripadajoč 2-kocikel. Spomnimo se, da iz Evklidovega algoritma sledi, da za tuji si števili m in n obstajata taki celi števili a in b, da je $am + bn = 1$. Ker je $|A| = m$, je $m\varphi = 0$ in zato $(am + bn)\varphi = bn\varphi$. Želimo dokazati, da je $n\varphi \in B^2(G, A)$. Definirajmo preslikavo $d : G \to A$ s predpisom

$$d(g) = \sum_{g_2 \in G} \varphi(g, g_2).$$

Oglejmo si enačbo (9) za 2-kocikle:

$$\varphi(g_1, g_2) + \varphi(g_1 g_2, g_3) = g_1\varphi(g_2, g_3) + \varphi(g_1, g_2 g_3).$$

To enačbo seštejemo po vseh $g_3 \in G$:

$$\begin{aligned}
\sum_{g_3 \in G} \varphi(g_1, g_2) + \sum_{g_3 \in G} \varphi(g_1 g_2, g_3) &= g_1 \sum_{g_3 \in G} \varphi(g_2, g_3) + \sum_{g_3 \in G} \varphi(g_1, g_2 g_3) \\
n\varphi(g_1, g_2) + d(g_1 g_2) &= g_1 d(g_2) + \sum_{g_2 g_3 \in G} (g_1, g_2 g_3) \\
n\varphi(g_1, g_2) &= g_1 d(g_2) - d(g_1 g_2) + d(g_1)
\end{aligned}$$

Po definiciji 2-korobov je $n\varphi \in B^2(G, A)$. □

Opomba 3.8. Izrek velja tudi v primeru, če A ni Abelova grupa, vendar je dokaz daljši. Zassenhaus je dokazal, da je namesto komutativnosti grupe A dovolj predpostaviti, da je A ali G rešljiva grupa. Iz znamenitega Feit-Thompsonovega izreka, ki pravi, da je vsaka končna grupa lihe moči rešljiva, pa sledi, da je tudi predpostavka o rešljivosti odveč. Več o tem je v [4, poglavje 9].

Posledica 3.9. *Naj bosta m in n tuji si števili. Potem je $H^2(\mathbb{Z}_m, \mathbb{Z}_n) = 0$.*

4. Primeri v GAP-u

Programski paket GAP je odprtokodni sistem za računsko diskretno algebro. Sestavljen je iz jezika GAP, knjižic s funkcijami in podatkovne baze algebraičnih objektov. Namenjen je predvsem računski teoriji grup. Paket in priročnik sta dostopna na naslovu [5].

4.1. **Policiklične in elementarne Abelove grupe.** Paket GAP bomo uporabili za iskanje razširitev grupe A z grupo G, za iskanje grupe 2-kociklov in 2-korobov ter za računanje druge kohomološke grupe. Funkcije v GAP-u nam omogočajo, da to lahko izračunamo, če je grupa A elementarna Abelova grupa in grupa G policiklična grupa.

Definicija 4.1. Naj bo p praštevilo in $n \in \mathbb{N}$. Grupa A oblike $A = \mathbb{Z}_p^n = \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{n\text{-krat}}$ se imenuje *elementarna Abelova grupa*.

Opomba 4.2. Če je A elementarna Abelova grupa, potem je A vektorski prostor nad obsegom $\mathbb{Z}_p$. Njegovi elementi so n-terice oblike $(a_1, \ldots, a_n)$ in njegova baza množica $\{e_1, \ldots, e_n\}$, kjer je $e_i = (0, \ldots, 1, \ldots, 0)$ (enica na i-tem mestu). Od tod sledi, da je grupa avtomorfizmov $\operatorname{Aut} A$ izomorfna grupi matrik $\mathrm{GL}_n(\mathbb{Z}_p)$.

Opomba 4.3. Ker je elementarna Abelova grupa A Abelova, je $\operatorname{Out} A = \operatorname{Aut} A$ in zato je za poljubno grupo G sklopitev $\chi : G \to \operatorname{Out} A$ kar $\chi : G \to \mathrm{GL}_n(\mathbb{Z}_p)$. Z drugimi besedami, sklopitev χ vsakemu $g \in G$ priredi $n \times n$ matriko nad $\mathbb{Z}_p$, ki deluje na A.

S tem si pri delovanju G na A pomaga GAP, ker matrike je enostavno predstaviti in z njimi hitro računati.

Definicija 4.4. Grupa G je *policiklična grupa*, če obstaja zaporedje podgrup $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{m+1} = \{1\}$ ($m \in \mathbb{N}$), za katerega je G_i/G_{i+1} ciklična grupa.

Definicija 4.5. Množica $\{g_1, \ldots, g_m\} \subset G$ je množica *policikličnih generatorjev* policiklične grupe G, če velja $G_i = \langle g_i, g_{i+1}, \ldots, g_m \rangle$ za vsak $i \in \{1, \ldots, m\}$.

Opomba 4.6. Policiklični generatorji niso nujno enolično določeni.

Lema 4.7. *Naj bo $\{g_1, \ldots, g_m\}$ (fiksna) množica policikličnih generatorjev policiklične grupe G. Potem lahko poljuben $g \in G$ enolično zapišemo v obliki $g = g_1^{e_1} g_2^{e_2} \ldots g_m^{e_m}$, kjer so $e_i \in \{0, \ldots, r_i - 1\}$, pri čemer r_i označuje red elementa $g_i G_{i+1} \in G_i/G_{i+1}$ (lahko je tudi ∞).*

Dokaz. Poljubna podgrupa G_i iz zaporedja $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{m+1} = \{1\}$ je policiklična, saj zaporedje $G_i \triangleright G_{i+1} \triangleright \cdots \triangleright G_{m+1}$ izpolnjuje zahtevo iz definicije. Lemo dokazujemo z indukcijo (padajočo in končno) po indeksu i. Za $i = m$ je podgrupa G_m ciklična grupa in lema velja. Predpostavimo, da lema velja za podgrupo z indeksom $i = k$ za neki $k \in \{2, \ldots, m\}$. Ker je G_{k-1}/G_k ciklična grupa, obstaja generator tG_k za neki $t \in G_{k-1}$. Po drugi strani je $G_{k-1} = \langle g_{k-1}, g_k, \ldots, g_m \rangle$ in zato je $t = g_{\lambda(1)} g_{\lambda(2)} \cdots g_{\lambda(n)}$ za neko preslikavo $\lambda : \{1, \ldots, n\} \to \{k-1, \ldots, m\}$. Naj bo $r = |\lambda^{-1}(\{k-1\})|$ (število pojavitev g_{k-1} v produktu za t). Potem je $t = h_0 g_{k-1} h_1 g_{k-1} h_2 \cdots h_{r-1} g_{k-1} h_r$ za neke $h_i \in G_k$. Od tod vidimo, da je $t \in G_k (g_{k-1} G_k)^r$. Sledi, da je $tG_k = G_k (g_{k-1} G_k)^r = g_{k-1}^r G_k$ in zato je $g_{k-1} G_k$ generator grupe G_{k-1}/G_k. Od tod sledi, da za poljuben $g \in G_{k-1}$ obstaja $e_{k-1} \in \{0, \ldots, r_{k-1} -$

1}, da je $g \in g_{k-1}^{e_{k-1}} G_k$ oz. da je $g = g_{k-1}^{e_{k-1}} g_k^{e_k} \cdots g_m^{e_m}$. Po indukcijski predpostavki so člani $g_k^{e_k} \cdots g_m^{e_m}$ enolično določeni in zato je tudi $g_{k-1}^{e_{k-1}}$ enolično določen. □

Opomba 4.8. Policiklični generatorji nam omogočajo, da delovanje policiklične grupe G na elementarno Abelovo grupo A opišemo tako, da vsakemu policikličnemu generatorju priredimo matriko iz $\mathrm{GL}_n(\mathbb{Z}_p)$. Pri tem pazimo, da se redi in produkti matrik ujemajo z redi in produkti policikličnih generatorjev. Ker se da po prejšnji lemi poljuben element iz G enolično zapisati kot produkt policikličnih generatorjev, je njegovo delovanje enako produktu matrik, ki smo jih predpisali policikličnim generatorjem.

S tako definiranim delovanjem dobimo G-modul A, ki ga v GAP uporabimo pri iskanju razširitev.

4.2. **Nekaj funkcij v GAP-u.** Osnovni objekti v GAP-u, ki jih bomo uporabljali v primerih, so seznam (list), zapis (record), matrika in policiklična grupa (pc group). Moduli bodo podani v obliki zapisa. Pri vsakem objektu lahko dostopamo do njegovih delov, na primer elementov v seznamu, posameznih komponent zapisa, generatorjev grupe, ipd. Pri uporabi funkcij pazimo, da so vhodni in izhodni podatki usklajeni s tipom objekta.

`CyclicGroup(n)` - poda ciklično grupo moči n. Ker so ciklične grupe policiklične, GAP vrne rezultat kot objekt policiklična grupa (pc group). Podobno za `DihedralGroup`.

`Pcgs(G)` - seznam policikličnih generatorjev policiklične grupe G.

`RelativeOrders(pcgs)` - seznam relativnih redov policikličnih generatorjev.

`PermutationMat(perm,n,F)` - vrne permutacijsko matriko dimenzije n nad obsegom F, ki je določena s permutacijo `perm`.

`GF(n)` - označuje obseg moči n (če obstaja).

`GModuleByMats(gens,F)` - vrne modul $M = F^n$ nad obsegom, ki ga generirajo obrnljive matrike `gens`. Pri tem je `F` obseg, n dimenzija matrik `gens` in delovanje je določeno z delovanjem matrik na elemente M. Če so matrike usklajene s policikličnimi generatorji kakšne policiklične grupe G, potem dobimo G-modul M. Funkcija vrne rezultat v obliki objekta zapis (record).

`TwoCocycles(G,M)` - seznam vektorjev, ki generirajo grupo 2-kociklov policiklične grupe G in G-modula M. Podobno `TwoCoboundaries`.

`TwoCohomology(G,M)` - izračuna drugo kohomološko grupo $H^2(G, M)$ kot kvocientni prostor 2-kociklov po 2-korobovih. Rezultat vrne kot zapis s številnimi komponentami.

`SplitExtension(G,M)` - grupa iz razcepne razširitve G z M, kjer je M podan kot G-modul.

`Extension(G,M,co)` - grupa iz razširitve G z M, ki je določena z 2-kociklom `co`, kjer je M podan kot G-modul.

`Extensions(G,M)` - seznam grup vseh neekvivalentnih razširitev G z M, kjer je M podan kot G-modul.

`StructureDescription(G)` - delno izpiše strukturo grupe G (ni nujno do izomorfizma natančno).

Poleg vgrajenih funkcij lahko definiramo tudi svoje funkcije in zanke. Poglejmo, kako bi definirali funkcijo, ki vrne direktni produkt n kopij grupe G:

```
gap> direktnaPotenca:=function (G,n)
> local i,H;
```

```
> H:=G;
> for i in [2..n] do H:=DirectProduct(H,G); od;
> return H;
> end;;
gap> direktnaPotenca(CyclicGroup(2),5);
<pc group of size 32 with 5 generators>
gap> StructureDescription(last);
"C2 x C2 x C2 x C2 x C2"
```

Nekaj zgledov uporabe GAP je v [3].

4.3. **Primeri.**

(1) *Razcepna razširitev grupe $\mathbb{Z}_5$ z grupo $\mathbb{Z}_{10}$ s trivialnim delovanjem in druga kohomološka grupa $H^2(\mathbb{Z}_{10}, \mathbb{Z}_5)$.*

Najprej definiramo grupo $\mathbb{Z}_{10}$ in v seznam `mats` njenim policikličnim generatorjem priredimo matrike identitete (ki predstavljajo trivialno delovanje). Nato konstruiramo $\mathbb{Z}_{10}$-modul $\mathbb{Z}_5$ in pogledamo razcepno razširitev (ki je v tem primeru kar direktni produkt). Funkcija `TwoCohomology` vrne zapis (record) druge kohomološke grupe. V komponenti `cohom` je podana linearna preslikava med modulom 2-kociklov in kvocientnim modulom 2-kociklov po 2-korobovih. Zanima nas kvocientni modul oz. kvocientna grupa. Iz slike in dimenzije razberemo, da je $H^2(\mathbb{Z}_{10}, \mathbb{Z}_5) = \mathbb{Z}_5$.

```
gap> G:=CyclicGroup(10);
<pc group of size 10 with 2 generators>
gap> mats:=List(Pcgs(G),x->IdentityMat(1,GF(5)));;
gap> A:=GModuleByMats(mats,GF(5));;
gap> S:=SplitExtension(G,A);;
gap> StructureDescription(S);
"C10 x C5"
gap> H:=TwoCohomology(G,A);;
gap> H.cohom;
<linear mapping by matrix, <vector space of dimension 2
   over GF(5)> -> ( GF(5)^1 )>
gap> Image(H.cohom);
( GF(5)^1 )
gap> Dimension(Image(H.cohom));
1
```

(2) *Razširitve $\mathbb{Z}_{10}$ z $\mathbb{Z}_{10}$ s trivialnim delovanjem in $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$.*

V zgledu 3.6 smo že videli, da je $\mathbb{Z}_{10} \leq H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$ in da 2-kocikel z iz uvoda služi kot generator za to podgrupo. Zanimajo nas še ostali elementi v $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10})$. Vendar GAP zna izračunati drugo kohomološko grupo le, kadar je druga grupa elementarna Abelova grupa, $\mathbb{Z}_{10}$ pa to ni. Zato si pomagamo s pomožno lemo, ki pravi, da če sta A_1 in A_2 G-modula, potem je $H^2(G, A_1 \oplus A_2) = H^2(G, A_1) \oplus H^2(G, A_2)$. Splošen primer te leme lahko najdemo v [1, poglavje VI]. V našem primeru je $\mathbb{Z}_{10} = \mathbb{Z}_2 \oplus \mathbb{Z}_5$ oz. $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10}) = H^2(\mathbb{Z}_{10}, \mathbb{Z}_2) \oplus H^2(\mathbb{Z}_{10}, \mathbb{Z}_5)$ in vsakega od členov v tej direktni vsoti lahko izračunamo z GAP-om.

Za grupo $H^2(\mathbb{Z}_{10}, \mathbb{Z}_5)$ že vemo, da je enaka $\mathbb{Z}_5$. Grupo $H^2(\mathbb{Z}_{10}, \mathbb{Z}_2)$ izračunamo podobno kot v prejšnjem zgledu. Dobimo $H^2(\mathbb{Z}_{10}, \mathbb{Z}_2) = \mathbb{Z}_2$ in od tod $H^2(\mathbb{Z}_{10}, \mathbb{Z}_{10}) = \mathbb{Z}_{10}$. V zgledu 3.6 smo torej že našli vse razširitve grupe $\mathbb{Z}_{10}$ z grupo $\mathbb{Z}_{10}$.

```
gap> G:=CyclicGroup(10);;
gap> mats:=List(Pcgs(G),x->IdentityMat(1,GF(2)));;
gap> A:=GModuleByMats(mats,GF(2));;
gap> H:=TwoCohomology(G,A);;
gap> Image(H.cohom);
( GF(2)^1 )
gap> Dimension(Image(H.cohom));
1
```

(3) *Razširitve $\mathbb{Z}_2$ z $D_4 \oplus \mathbb{Z}_3$ s trivialnim delovanjem, 2-kocikli, 2-korobovi in $H^2(D_4 \oplus \mathbb{Z}_3, \mathbb{Z}_2)$.*

Najprej definiramo $D_4 \oplus \mathbb{Z}_3$ in modul $\mathbb{Z}_2$. S funkcijo `Extensions` dobimo grupe v vseh neekvivalentnih razširitvah, in jih izpišemo. Dobili smo štiri različne grupe, ki nastopajo v osmih neekvivalentnih razširitvah.

Nadaljujemo s funkcijo `TwoCocycles`, ki vrne seznam vektorjev, ki generirajo grupo vseh 2-kociklov (podobno `TwoCoboundaries`). Za konkreten 2-kocikel (ali korob) lahko konstruiramo razširitev in pogledamo katera grupa nastopa. S funkcijo `AdditiveGroupByGenerators` nato konstruiramo grupo 2-kociklov $Z^2(D_4 \oplus \mathbb{Z}_3, \mathbb{Z}_2)$, vendar ta funkcija vrne rezultat v obliki objekta `magma`. Objekt `magma` je množica, ki je zaprta za operacijo. V splošnem ni nujno grupa (niti polgrupa), vendar v našem primeru GAP po konstrukciji vrne grupo. Za ta tip objekta večina funkcij za grupe ne deluje (tudi `StructureDescription`), vendar si lahko pomagamo z naslednjim premislekom. Če je G grupa in $A = \mathbb{Z}_p^n$ elementarna Abelova grupa, potem za vsak 2-kocikel $\varphi : G \times G \to A$ velja $p\varphi = 0$. Ker je p praštevilo, sledi, da je grupa 2-kociklov oblike $Z^2(G, A) = \mathbb{Z}_p^r$ za neki $r \in \mathbb{N}$. Njena moč je $|Z^2(G, A)| = p^r$. V GAP-u lahko pogledamo njeno moč z ukazom `Length(Elements())`. Ker poznamo tudi p, lahko izračunamo r in izvemo, katera grupa je $Z^2(G, A)$. V našem primeru je $p = 2$ in $|Z^2(D_4 \oplus \mathbb{Z}_3, \mathbb{Z}_2)| = 16$ in zato je iskana grupa 2-kociklov enaka $\mathbb{Z}_2^4$. Podobno dobimo $B^2(D_4 \oplus \mathbb{Z}_3, \mathbb{Z}_2) = \mathbb{Z}_2$ in od tod sledi, da je $H^2(D_4 \oplus \mathbb{Z}_3, \mathbb{Z}_2) = \mathbb{Z}_2^3$. To preverimo še s funkcijo `TwoCohomology` in rezultat se ujema.

```
gap> G:=DirectProduct(DihedralGroup(4),CyclicGroup(3));;
gap> mats:=List(Pcgs(G),x->IdentityMat(1,GF(2)));;
gap> A:=GModuleByMats(mats,GF(2));;
gap> ext:=Extensions(G,A);;
gap> for i in [1..Length(ext)] do
> Print(StructureDescription(ext[i]),"\n");
> od;
C6 x C2 x C2
C12 x C2
C3 x D8
C3 x D8
C12 x C2
C12 x C2
C3 x D8
C3 x Q8
gap> co:=TwoCocycles(G,A);;
gap> cb:=TwoCoboundaries(G,A);;
gap> ext1:=Extension(G,A,co[3]+co[4]);;
```

```
gap> StructureDescription(ext1);
"C12 x C2"
gap> ext2:=Extension(G,A,cb[1]);;
gap> StructureDescription(ext2);
"C6 x C2 x C2"
gap> Z2:=AdditiveGroupByGenerators(co);;
gap> B2:=AdditiveGroupByGenerators(cb);;
gap> Length(Elements(Z2));
16
gap> Length(Elements(B2));
2
gap> H:=TwoCohomology(G,A);;
gap> Image(H.cohom);
( GF(2)^3 )
```

(4) *Razširitve $\mathbb{Z}_2^m$ z $\mathbb{Z}_m$ ($m \in \mathbb{N}$) z danim netrivialnim delovanjem.*

Naj bo $\{e_1, \ldots, e_m\}$ baza Abelove grupe $\mathbb{Z}_2^m$ in $a \in \mathbb{Z}_m$ generator ciklične grupe $\mathbb{Z}_m$. Delovanje grupe $\mathbb{Z}_m$ na grupo $\mathbb{Z}_2^m$ naj bo definirano z enačbami $ae_i = e_{i+1}$ in $ae_m = e_1$ ($i = 1, \ldots, m-1$). To delovanje permutira bazne vektorje s permutacijo $(1 \;\; 2 \;\; 3 \;\; \ldots \;\; m)$.

Za opis delovanja bomo v GAP-u napisali novo funkcijo `matsact`. Ta funkcija za argument vzame ciklično grupo G in vrne seznam permutacijskih matrik. Prva matrika predstavlja permutacijo $(1 \;\; 2 \;\; \ldots \;\; m)$ in ustreza prvemu policikličnemu generatorju. Generiramo jo s funkcijo `PermutationMat`, pri čemer si pomagamo s `PermList`, ki iz našega seznama `perm` naredi ustrezno permutacijo. Prvo matriko shranimo v `mats[1]`. Vsaka naslednja matrika je potenca prejšnje in ustreza naslednjemu policikličnemu generatorju. Pri tem pazimo, da se matrike potencirajo z isto potenco kot policiklični generatorji. Ustrezne potence policikličnih generatorjev dobimo s funkcijo `RelativeOrders`. Matrike shranjujemo v seznam `mats`, ki ga funkcija na koncu vrne.

```
gap> matsact:=function(G)
> local perm,mats,ord,m,i;
> m:=Length(Elements(G));
> perm:=[]; for i in [1..m] do Append(perm,[(i mod m)+1]);
   od;
> mats:=[]; mats[1]:=PermutationMat(PermList(perm),m,GF(2))
   ;
> ord:=RelativeOrders(Pcgs(G));
> for i in [2..Length(ord)] do
> mats[i]:=mats[i-1]^ord[i-1];
> od;
> return mats;
> end;;
```

Sedaj funkcijo `matsact` uporabimo za konstrukcijo modula in iskanje razširitev. Za dovolj majhne m lahko izpišemo vse razširitve, za večje pa postane funkcija `StructureDescription` zelo počasna. Izkaže se, da pri vseh m, ki jih računalnik še lahko izračuna (npr. $m = 100$), dobimo le eno razširitev in zato trivialno drugo kohomološko grupo.

```
gap> for i in [1..7] do
> G:=CyclicGroup(i);
> mats:=matsact(G);
> A:=GModuleByMats(mats,GF(2));
> ext:=Extensions(G,A);
> Print("m=", i, ": ", List(ext,StructureDescription),"\n")
   ;
> od;
m=1: [ "C2" ]
m=2: [ "D8" ]
m=3: [ "C2 x A4" ]
m=4: [ "((C8 : C2) : C2) : C2" ]
m=5: [ "C2 x ((C2 x C2 x C2 x C2) : C5)" ]
m=6: [ "(C2 x C2 x ((C2 x C2 x C2 x C2) : C3)) : C2" ]
m=7: [ "C2 x ((C2 x C2 x C2 x C2 x C2 x C2) : C7)" ]
gap> m:=100;
gap> G:=CyclicGroup(m);;
gap> mats:=matsact(G);;
gap> A:=GModuleByMats(mats,GF(2));;
gap> Extensions(G,A);
[ <pc group of size 126765060022822940149670320537600 with
   104 generators> ]
gap> H:=TwoCohomology(G,A);;
gap> H.cohom;
ZeroMapping( <vector space of dimension 301 over GF(2)>, (
   GF(2)^0 ) )
```

Literatura

[1] P. J. Hilton in U. Stammbach, *A course in homological algebra*, Graduate Texts in Mathematics **4**, Springer-Verlag, New York, 1970.

[2] D. C. Isaksen, *A Cohomological Viewpoint on Elementary School Arithmetic*, Amer. Math. Monthly **109** (2002) 796–805.

[3] P. Moravec, *Some topics in the theory of finite groups*, verzija 21. 8. 2014 [ogled 20. 11. 2014], dostopno na http://www.fmf.uni-lj.si/~moravec/Papers/rogla2014_moravec.pdf.

[4] D. J. S. Robinson, *A course in the theory of groups*, 2nd ed., Graduate Texts in Mathematics **80**, Springer-Verlag, New York, 1996.

[5] The GAP Group, *GAP - Groups, Algorithms, and Programming, Version 4. 7. 4*, 2014 [ogled 15. 11. 2014], dostopno na http://www.gap-system.org.