Универзитет у Београду
Математички факултет

Мастер рад

КОХОМОЛОГИЈА ГРУПА
ОСНОВНИ ПОЈМОВИ И ПРИМЕРИ

Александар Шон Колинс

Ментор:

проф. др Зоран Петровић

Београд - 2025

Ментор

проф. др Зоран Петровић
Универзитет у Београду, Математички факултет

Чланови комисије

др Маја Рославцев
Универзитет у Београду, Математички факултет

др Александра Костић Матијевић
Универзитет у Београду, Математички факултет

Изјаве захвалности

Велику захвалност дугујем свом ментору, професору Зорану Петровићу, на великој подршци и стрпљењу од самог избора теме, до последњих исправки. Од почетка ме је мотивисао да радим, а то ми је пуно значило. Захваљујем се и осталим члановима комисије, доценткињама др Маји Рославцев и др Александри Костић Матијевић на уложеном времену и труду при читању рада. Коначно се захваљујем породици, нарочито родитељима.

Садржај

1 Увод

1.1 Предговор

Циљ ове тезе је да се представи кохомологију група и неке једноставне примене. Пажљиво пратим два извора да бих поставио подлогу за рад – „Кохомологија група“ Кенета С. Брауна из 1982. године, текст заснован на постдипломском курсу који је држао на Универзитету Корнел; и „Карактеристичне класе и кохомологија коначних група“ Ч.Б. Томаса из 1986. године. Након тога, обрадићу неколико примера, углавном преузетих из проблема и вежби наведених у тим књигама.

1.2 Историја

Прве идеје модерне хомолошке алгебре потичу још од Римана у другој половини 19. века, када је проучавао затворене криве на површима. Овај ток размишљања наставио је Бети, а затим Поенкаре у свом раду „Analysis Situs“ из 1895. године. Тамо је увео релацију названу „хомологија“, засновану на формалним збировима подмногострукости. Такође је увео Бетијеве бројеве многострукости, као и своју истоимену теорему, Поенкареову теорему дуалности. У његовим наредним радовима 1899. и 1900. године, појавио се концепт који ће касније бити познат као ланчани комплекс, заједно са граничним пресликавањима, које је увео кроз линеарну алгебру и појам торзионих коефицијената.

На почетку 20. века, математичари попут О. Веблена, Ц. В. Александера и Х. Кунета радили су на разумевању и разјашњавању Поенкареових револуционарних идеја. Међутим, област је остала дисциплина за тополоте, који су манипулисали матрицама инциденције да би одредили Бетијеве бројеве и торзионе коефицијенте. Тек 1925. године, Еми Нетер је известила да је хомологија заправо Абелова група, а не само Бетијеви бројеви и торзиони коефицијенти. Полако, перцепције су почеле да се померају ка алгебарском приступу. Године 1929. Л. Мајер је увео ланчане комплексе и хомолошке групе комплекса чисто алгебарски. Током деценије 1925-1935, неколико математичара је створило сопствене верзије хомологије. Међу овим математичарима су Александер, Александров, Чех, Лефшец, Колмогоров, Вијеторис, де Рам. Сваки случај је био сличан, дат је рецепт за конструисање ланчаног комплекса и њихове хомолошке групе би биле дефинисане као хомологија тог комплекса. Затим би показали да је резултат независан од избора и дали би уобичајене Бетијеве бројеве за компактне многострукости.

Године 1935. било је неколико великих продора у развоју теорије хомологије. Понтрјагин и Брауер су израчунали хомологију класичних Лијевих

група, резултате које је Хопф користио у ономе што ће касније постати теорија Хопфових алгебри. Чех је развио Теорему о универзалним коефицијентима. Последњи велики резултат који ћемо за сада поменути било је откриће теорије кохомологије и куп производа. Ово су независно развили Александар и Колмогоров, који су своје резултате представили један за другим на Московској међународној конференцији о топологији у септембру 1935. године.

Такође 1935. године, Хуревич је дефинисао више хомотопске групе $\pi_n(X)$ простора X. Конструисао је Хуревичева пресликавања $h : \pi_n(X) \to H_n(X; \mathbb{Z})$. Затим се фокусирао на асферичне просторе, оне просторе чије су више хомотопске групе ($n \geq 2$) све тривијалне, али чија фундаментална група $\pi_1(X)$ не мора бити тривијална. Доказао је, између осталог, да хомолошке групе простора X зависе само од фундаменталне групе простора X. Конкретно, то значи да су, за дату групу π, хомолошке групе асферичног простора X са фундаменталном групом π заправо независне од избора простора X.

Током наредног периода, до 1950. године, тополози су почели да схватају импликације које хомолошка теорија тополошких простора има у алгебарским системима. Откривено је да се одређене кохомологије ослањају искључиво на алгебарске податке, као што је кохомологија асферичног простора која зависи само од његове фундаменталне групе, или кохомологија Лијеве групе која зависи само од њене придружене Лијеве алгебре. То је довело до размишљања у алгебарски дефинисанијим терминима, без ослањања на топологију. Први пример је оно што је довело до стварања кохомологије група.

Кохомолошке групе ниже димензије групе G су раније интерпретиране на различите начине, дајући класичне резултате. На пример, у димензији нула, $H^0(G; A) = A^G$, група инваријантних елемената. У димензији 1, група хомологије $H_1(G; \mathbb{Z}) = G/[G, G]$, абелизација групе. Група кохомологије $H^1(G; A)$ је била већ проучавани класични објекат, група укрштених хоморфизама G у репрезентацију A. Хилбертова „Теорема 90“ из 1897. године је прорачун да је $H^1(G; L^\times) = 0$ када је G Галоаова група цикличног раширења поља L/K, а име потиче од њене улоге у проучавању укрштених производних алгебри. У димензији 2, група $H^2(G; A)$ је заправо класификација раширења над G са нормалном подгрупом A преко фактор скупова. Фактор скупови се појављују у концепту већ 1893. године у раду Хелдера, студији Шура из 1904. године или 1906. године код Дикинсона. Године 1926, Шрајер је дао први систематски приступ фактор скуповима, који је Брауер наставио 1928. Године 1934, Бер је приметио да када је A Абелов, ови фактор скупови могу се сабирати по члановима, тако да раширења формирају Абелову групу. Ово је довело до првог третмана раширења без коришћења фактор скупова.

Године 1941, Хајнц Хопф је поднео рад у којем је показао да фундаментална група $\pi = \pi_1(X)$ простора X одређује којезгро Хуревичевог пресликавања $h : \pi_2(X) \to H_2(X; \mathbb{Z})$. Представљајући π као количник F/R слободне групе F подгрупом R релација, Хопф је дао експлицитну формулу:

$$\frac{H_2(X;\mathbb{Z})}{h(\pi_2(X))} \cong \frac{R \cap [F,F]}{[F,R]},$$

где $[A, B]$ за $A, B \subseteq F$ означава подгрупу генерисану комутаторима $[a, b] = aba^{-1}b^{-1}$ ($a \in A, b \in B$). Конкретно, ако је $\pi_2(X) = 0$ (као што је у случају асферичних простора), ово показује да $H_2(X; \mathbb{Z})$ зависи само од $\pi_1(X)$. У том случају, ова формула се назива Хопфова формула за $H_2(\pi; \mathbb{Z})$.

Хопфов рад и рад Хуревича инспирисали су многе математичаре да проучавају хомологију и кохомологију асферичних простора и да изразе резултате у терминима фундаменталне групе. Маклејновим речима: „Ова линија истраживања пружила је оправдање за проучавање кохомологије група у **свим** димензијама и била је полазна тачка хомолошке алгебре“. Тако су Ајленберг, Маклејн, Фројдентал и Хопф, а затим и Екманом, сви истовремено, али независно, дефинисали хомологију и/или кохомологију групе.

Ајленберг и Маклејн су 1942. године заједно радили на открићу онога што је сада познато као Теорема о универзалним коефицијентима за сингуларну кохомологију, тачније да је кохомологија одређена хомологијом са целовројним коефицијентима. Хопфов рад те године је оставио велики утисак на њих, па су затим заједно радили на проучавању асферичних простора. Користећи Хуревичев резултат, да су, за дату групу π, групе хомологије и кохомологије асферичног простора Y независне од избора Y, све док је $\pi_1(Y) = \pi$, узели су ове групе, као дефиниције за $H_n(\pi; A)$ и $H^n(\pi; A)$. За израчунавања, креирали су специфичан апстрактни симплицијални комплекс $K(\pi)$ за избор асферичног простора Y. Његове n-ћелије су уређени низови $[x_1, \ldots, x_n]$ елемената у групи. Стога су израчунали кохомолошке групе π као кохомолошке групе ћелијског коланчаног комплекса $K(\pi)$. Екманов рад је такође дефинисао кохомолошки прстен на сличан начин, дефинишући кохомолошки куп производ у терминима овог комплекса. Оба рада су показала да $H^2(G; A)$ класификује раширења група.

Истовремено, Хопф је створио потпуно другачију дефиницију. Ова дефиниција је била много ближа модерној дефиницији. Он је разматрао модул M над прстеном R, а затим је конструисао слободно разрешење F од M помоћу R-модула. За I идеал од R, разматрао је хомологију језгра $F \to F \otimes (R/I)$ и показао да је независна од избора разрешења. У ствари, специјализовао се за случај групног прстена $R = \mathbb{Z}\pi$, идеала проширења I и $M = \mathbb{Z}$. Овде је показао да ако је Y асферични ћелијски простор са фундаменталном

групом π, онда $H_n(Y;\mathbb{Z}) = H_n(\pi;\mathbb{Z})$. Фројденталов метод је био сличан, али мање општи.

У почетку су прорачуни били ограничени на групе које су биле фундаменталне групе познатих тополошких простора, користећи „преградни“ комплекс. Касније, 1946. године, Линдон је пронашао други метод, који је Сер реализовао 1950. године користећи спектрални низ. Завршио је овај опис са Хохшилдом 1953. године, а сада је познат као Линдон-Хохшилд-Серов спектрални низ.

Хохшилд је применио нове дефиниције кохомологије група у својој студији теорије локалних класних поља, да би створио Галоаову кохомологију. Проучавајући ову Галоаову кохомологију, Тејт је дефинисао Тејтову кохомологију, индексирану свим целим бројевима, спајањем кохомологије и хомологије групе.

Године 1950, у Семинару Картан, Ајленберг је дао аксиоматску карактеризацију теорија хомологије и кохомологије за групу и утврдио постојање поменутих теорија користећи фиксирано слободно разрешење, а Картан је доказао Теорему поређења за ланчане комплексе. То је довело до њихове сарадње, са циљем поновног писања основа свих ад хок алгебарских теорија хомологије и кохомологије које су се до тада појавиле. Управо су овде увели термин „Хомолошка алгебра“, користећи га за наслов свог уџбеника из 1956. године. Ова књига означава прво појављивање нотација Tor_n и Ext^n, као и концепта пројективног модула. У својој рецензији њихове књиге, Хохшилд је изјавио да „Појава ове књиге мора да значи да је експериментална фаза хомолошке алгебре сада превазиђена“.

Књига је користила појам ланчаних комплекса и разрешења, који се такође развијао током времена. ланчане комплексе је први пут формално увео Мајер 1929. године, инспирисан Нетериним извештајем из 1925. године. Кели и Пичер су 1947. године сковали термин „тачан низ“. Ланчане комплексе су даље развили Ајленберг и Стинрод у својој књизи из 1945. године, у којој се први пут појављује лема о пет хомоморфизама (у даљем кратко пет-лема) и Мајер-Вијеторисов низ. Лема о змији се први пут појавила у књизи Картана и Ајленберга из 1950. године. Слободна разрешења су се дуго користила у алгебри, почевши од Хилберта у његовом раду из 1890. године. Бер је имплицитно користио слободна разрешења у својој студији о проширењима група из 1934. године. Слично томе, као што је раније поменуто, Хопф их је користио у свом опису хомологије групе. Инјективне модуле и разрешења имплицитно су користили Бер у својој карактеризацији полупростих прстена и Маклејн у раду о проширењима група из 1948. године.

На основу Хопфовог рада, Картан и Ајленберг су користили слободна $\mathbb{Z}G$-разрешења G-модула A како би дали аксиоматски опис за хомо-

логију групе $H_*(G;A)$. Међутим, наставили су са дефинисањем концепта пројективног модула. Затим су дефинисали пројективне и инјективна разрешења. Они користе ове дефиниције у својим дефиницијама $Tor_n^R(M,N)$ и $Ext_R^n(M,N)$ као изведених функтора $M \otimes_R N$ и $\mathrm{Hom}_R(M,N)$. Ово је довело до обједињавања многих претходно проучаваних теорија хомологије и кохомологије. Показано је да су групе хомологије и кохомологије групе G Tor и Ext групе над групним прстеном $\mathbb{Z}G$. Слично, показано је да су Хохшилдова хомологија и кохомологија асоцијативне алгебре Λ Tor и Ext групе над омотачком алгебром $\Lambda \otimes \Lambda^{\mathrm{op}}$, а хомологија и кохомологија Лијеве алгебре $\mathfrak{g}$ су показале да су Tor и Ext групе над омотачком алгебром $U_{\mathfrak{g}}$.

Објављивање књиге „Хомолошка алгебра“ Картана и Ајленберга довело је до невероватне количине истраживања инспирисаних овим делом. У ствари, као резултат тога, појавила су се и процветала многа нова поља проучавања. Нека од ових поља укључују области пројективних модула; теорије у теорији прстена као што су регуларни локални прстени, локални прстени, Матлисова дуалност и локална кохомологија и дуалност; теорије у алгебарској геометрији као што су Галоаова кохомологија и Етална кохомологија; области у изведеним категоријама; и многе друге. Ова књига је остала популарна до 1970-их и, заједно са Маклејновом књигом „Хомологија“ из 1963. године, помогла је да ова тема постане стандардни материјал за курсеве.

2 G-модули

2.1 Групни прстени и G-модули

Нека је G група, не нужно коначна. Дефинишемо интегрални групни прстен од G са $\Lambda = \mathbb{Z}G$, који се састоји од формалних сума $\Sigma_i n_i g_i$ где су $n_i \in \mathbb{Z}$, $g_i \in G$ и i елементи коначног индексног скупа, са операцијама

$$\Sigma_i n_i g_i + \Sigma_i m_i g_i = \Sigma_i (n_i + m_i) g_i$$

и

$$(\Sigma_i n_i g_i)(\Sigma_i m_j g'_j) = \Sigma_{i,j}(n_i m_j)(g_i g'_j).$$

Леви G-модул A је дефинисан као Абелова група A заједно са G-дејством на A које поштује сабирање у A: $g \cdot (a+b) = g \cdot a + g \cdot b$. Пошто је A Абелова група, можемо је сматрати $\mathbb{Z}$-модулом. Понекад ћемо тај основни $\mathbb{Z}$-модул означити са A_0.

Пошто G-дејство на A поштује сабирање, можемо линеарно проширити G-дејство на Λ-дејство на A: за елемент $\lambda = \Sigma_i n_i g_i \in \Lambda$, $\lambda \cdot a = (\Sigma n_i g_i) \cdot a = \Sigma n_i (g_i \cdot a)$. Нека је $a \in A$. Јасно је да је $1 \cdot a = a$. За λ и $\mu = \Sigma_j m_j g'_j$ имамо

$$(\lambda\mu) \cdot a = \big((\Sigma_i n_i g_i)(\Sigma_j m_j g'_j)\big) \cdot a = \big(\Sigma_{i,j}(n_i m_j)(g_i g'_j)\big) \cdot a =$$
$$\Sigma_{i,j}(n_i m_j)(g_i g'_j) \cdot a = \Sigma_{i,j}(n_i m_j) g_i \cdot (g'_j \cdot a) = \Sigma_{i,j} n_i g_i \cdot (m_j g'_j \cdot a) =$$
$$\Sigma_i n_i g_i \cdot (\Sigma_j m_j g'_j \cdot a) = (\Sigma_{i,j} n_i g_i) \cdot \big((\Sigma_j m_j g'_j) \cdot a\big) = \lambda \cdot (\mu \cdot a)$$

Ово дејство такође поштује сабирање:

$$\begin{aligned} \lambda \cdot (a+b) &= (\Sigma_i n_i g_i) \cdot (a+b) \\ &= \Sigma_i n_i g_i \cdot (a+b) \\ &= \Sigma_i n_i (g_i \cdot a + g_i \cdot b) \\ &= (\Sigma_i n_i g_i \cdot a) + (\Sigma_i n_i g_i \cdot b) \\ &= \lambda \cdot a + \lambda \cdot b. \end{aligned}$$

Дакле, A, заједно са G-дејством, је Λ-модул, у класичном смислу. Обрнуто је такође очигледно тачно. Стога, од сада па надаље користимо термине G-модул и Λ-модул наизменично.

Кроз цео овај текст, G, Λ и A ће бити као горе наведено, осим ако није другачије прецизирано. Обично означавамо неутрални елемент G као 1, тако да у Λ можемо једноставно написати 2 уместо $2e_g$, и слично. Са $\mathcal{U}_G$ означавамо категорију левих Λ-модула и Λ-хомоморфизама. Такође ћемо често третирати $\mathbb{Z}$ као G-модул са тривијалним G-дејством.

Можемо направити G-модул из било ког произвољног скупа са G-дејством. Такав скуп X са G-дејством називамо G-скупом. Из X формирамо слободну Абелову групу (или, еквивалентно, $\mathbb{Z}$-модул) $\mathbb{Z}X$, понекад означену као $\mathbb{Z}[X]$, и проширујемо G-дејство на X на $\mathbb{Z}$-линеарно дејство G на $\mathbb{Z}X$. Добијени G-модул називамо пермутационим модулом.

Даље, како су орбите X_i G-дејства на X саме дисјунктни G-скупови, имамо следећу декомпозицију:

$$\mathbb{Z}[\bigsqcup X_i] = \bigoplus \mathbb{Z}X_i.$$

Наравно, користећи теорему о орбитама и стабилизаторима имамо

$$\mathbb{Z}X \cong \bigoplus \mathbb{Z}[G/G_{x_i}]$$

где су $x_i \in X_i$ представници за G-орбите у X, а G_x је стабилизаторска подгрупа од G у односу на x. Дакле, представници x_i формирају генераторни скуп за $\mathbb{Z}X$ као Λ-модул.

Посебно, за слободан G-скуп, тј. када је G-дејство на X слободно, стабилизаторске подгрупе су тривијалне. То значи да сваки $\mathbb{Z}[G/G_{x_i}] \cong \mathbb{Z}G$, из чега добијамо следећи став:

Став 1 *Нека је X слободан G-скуп и нека је E скуп представника за G-орбите у X. Тада је $\mathbb{Z}X$ слободан $\mathbb{Z}G$-модул са базом E.*

2.2 Инваријанте и коинваријанте

Подскуп инваријанти у G-модулу A је дефинисан као

$$A^G = \{a \in A : g \cdot a = a \text{ за све } g \in G\}.$$

Овај подмодул је највећи подмодул модула A на којем G делује тривијално.

Нека су A и A' два G-модула. Можемо дефинисати G-дејство на $\mathbb{Z}$-хомоморфизмима из $\mathrm{Hom}(A, A')$ по правилу

$$(g \cdot f)(a) = g \cdot f(g^{-1} \cdot a)$$

за све $g \in G$, $f \in \mathrm{Hom}(A, A')$ и $a \in A$. Овде смо користили G-дејства на A и A'.

Да бисмо проверили да ли је ово дејство добро дефинисано, проверавамо следеће важење за све $g, h \in G$, $f \in \mathrm{Hom}(A, A')$ и $a \in A$:

1. $(1 \cdot f)(a) = 1 \cdot f(1^{-1} \cdot a) = f(a)$

2. $(g\cdot(h\cdot f))(a) = g\cdot(h\cdot f)(g^{-1}\cdot a) = g\cdot(h\cdot f(h^{-1}\cdot(g^{-1}\cdot a))) = (gh)\cdot f((gh)^{-1}\cdot a) = ((gh)\cdot f)(a)$ за све $g, h \in G$.

Инваријантни елемент $\mathrm{Hom}(A, A')$ је елемент f који задовољава $(g \cdot f)(a) = f(a)$ за све $g \in G$ и $a \in A$, то јест $g \cdot f(g^{-1} \cdot a) = f(a)$, за све $g \in G$ и $a \in A$. Заменом a са $g \cdot a$ (што обухвата цео A) добијамо еквивалентни услов $g \cdot f(a) = f(g \cdot a)$, за све $g \in G$ и $a \in A$. Дакле, f је инваријантни елемент ако и само ако је хомоморфизам модула између G-модула A и A'. Дакле,

$$\mathrm{Hom}_G(A, A') = \mathrm{Hom}(A, A')^G.$$

Ова формула доводи до другог описа A^G, датог следећим својством:

$$A^G \cong \mathrm{Hom}_G(\mathbb{Z}, A). \tag{1}$$

Овде $\mathbb{Z}$ сматрамо G-модулом са тривијалним G-дејством. Заиста, како је $\mathrm{Hom}_G(\mathbb{Z}, A) = \mathrm{Hom}(\mathbb{Z}, A)^G$, довољно је показати $\mathrm{Hom}(\mathbb{Z}, A) \cong A$. Сваки хомоморфизам је одређен сликом $1 \in \mathbb{Z}$ због линеарности, па пресликајмо хомоморфизме f у $f(1)$. Ово пресликавање је очигледно изоморфизам, све што је преостало је да проверимо да ли G-структуре одговарају. Ово се лако проверава: $(g \cdot f)(1) = g \cdot f(g^{-1} \cdot 1) = g \cdot f(1)$, уз напомену да је G-дејство на $\mathbb{Z}$ тривијално.

Следећа лема приказује корисно својство функтора инваријанти:

Лема 2 *Функтор $A \to A^G$ је лево тачан на категорији левих Λ-модула, тј. ако је*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

кратак тачан низ левих Λ-модула, низ

$$0 \longrightarrow A^G \xrightarrow{\phi^G} B^G \xrightarrow{\psi^G} C^G$$

је тачан у категорији Абелових група.

Доказ: Ако је $\ker\phi = 0$ онда је $\ker\phi^G = 0$ јер је подскуп од $\ker\phi$.

Покажимо да је $\ker\psi = \mathrm{im}\,\phi$. Наравно, $\mathrm{im}\,\phi^G \subseteq \ker\psi^G$, јер је њихова композиција 0. Сада, нека је $b \in \ker\psi^G$, па је $b \in B^G$ и $\psi^G b = 0$, што значи $\psi b = 0$, јер је ψ^G рестрикција од ψ на B^G. Како је $\ker\psi = \mathrm{im}\,\phi$ имамо $b = \phi a$ за неко $a \in A$. Сада, како је ϕ хомоморфизам модула, за произвољни $g \in G$ имамо

$$\phi(g \cdot a) = g \cdot (\phi a) = g \cdot b = b$$

јер је b инваријантни елемент од B. Дакле, $\phi(g \cdot a)$ има исту слику као $\phi(a)$. Међутим, ϕ је мономорфизам, што значи да је $g \cdot a = a$. Пошто је g произвољан, то значи да је a инваријантни елемент од A, или $a \in A^G$. Дакле, $b \in \operatorname{im} \phi^G$. Стога, $\ker \psi = \operatorname{im} \phi$. □

Подскуп коинваријантних елемената у A је дефинисан као количник модула A подмодулом коју генеришу елементи облика $g \cdot a - a$ за све $g \in G$ и $a \in A$. Овај количник је означен са A_G. Где је A^G био највећи подмодул модула A на коме G делује тривијално, A_G је највећи количник модула A на коме G делује тривијално.

Еквивалентно можемо да дефинишемо A_G као:

$$A_G \cong \mathbb{Z} \otimes_\Lambda A. \tag{2}$$

Напоменимо да, да би тензорски производ имао смисла, $\mathbb{Z}$ сматрамо десним Λ-модулом, са тривијалним G-дејством. Докажимо да је горњи идентитет еквивалентан оригиналној дефиницији. На основу универзалног својства тензорског производа, постоји јединствено пресликавање $\varphi : \mathbb{Z} \otimes_\Lambda A \to A_G$ дато са $n \otimes a \mapsto n\bar{a}$, где $\bar{a}$ означава слику a у количнику A_G. Обрнуто, размотримо пресликавање $\theta : A_G \to \mathbb{Z} \otimes_\Lambda A$ дато са $\bar{a} \mapsto 1 \otimes a$ Проверавамо да је θ добро дефинисано пресликавање Λ-модула. Пошто је G-дејство на $\mathbb{Z}$ тривијално, имамо

$$1 \otimes (g \cdot a) = (1 \cdot g) \otimes a = 1 \otimes a,$$

што значи да имамо $1 \otimes (g \cdot a - a) = 0$. Дакле, пресликавање θ је добро дефинисано, јер су два елемента $\bar{a_1}, \bar{a_2}$, иста ако се разликују за збир елемената облика $g \cdot a - a$, па је $1 \otimes a_1 = 1 \otimes a_2$. Пресликавања φ и θ су инверзна једно другом, па су A_G и $\mathbb{Z} \otimes_\Lambda A$ изоморфни као Λ-модули, уз напомену да је G-дејство тривијално у оба случаја.

Напоменимо да се, због билинеарности, сваки елемент $\mathbb{Z} \otimes_\Lambda A$ може представити као $1 \otimes a$, за неко $a \in A$. Овај запис не мора бити јединствен.

Уопштено говорећи, можемо да радимо са тензорским производом $A \otimes_\Lambda A'$ два лева G-модула A и A'. То радимо тако што A посматрамо као десни G-модул са десним G-дејством дефинисаним као $a \cdot g = g^{-1} \cdot a$, за све $a \in A$ и $g \in G$. У овом случају, $A \otimes_\Lambda N$ се добија из $A \otimes A'$ количником по релацији $g^{-1} \cdot a \otimes a' = a \otimes g \cdot a'$ (уместо уобичајеног $a \cdot g \otimes a' = a \otimes g \cdot a'$). Заменом a са $g \cdot a$, ове релације добијају облик $a \otimes a' = g \cdot a \otimes g \cdot a'$.

Инспирисани овим, можемо дати $A \otimes A'$ G структуру. Дефинишемо G-дејство на $A \otimes A'$ са $g(a \otimes a') = ga \otimes ga'$ за све $a \otimes a' \in A \otimes A'$. Дакле, имамо

$$A \otimes_\Lambda A' = (A \otimes A')_G.$$

Слично леми 2, имамо следеће својство функтора коинваријанти:

Лема 3 *Функтор $A \to A_G$ је десно тачан на категорији левих Λ-модула, тј. ако је*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

кратак тачан низ левих Λ модула, низ

$$A_G \xrightarrow{\phi_G} B_G \xrightarrow{\psi_G} C_G \longrightarrow 0$$

је тачан у категорији Абелових група.

Доказ: Пресликавања ϕ_G и ψ_G су та која чине следећи дијаграм комутативним:

$$\begin{array}{ccccc} A & \xrightarrow{\phi} & B & \xrightarrow{\psi} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle r} \\ A_G & \xrightarrow{\phi_G} & B_G & \xrightarrow{\psi_G} & C_G, \end{array}$$

где p, q и r одговарају количничким пресликавањима из дефиниције коинваријанти. Другим речима, имамо $\phi_G p = q\phi$ и $\psi_G q = r\psi$. Видимо да за било које $a \in A$ и $g \in G$ имамо

$$\phi(g \cdot a - a) = g \cdot \phi(a) - \phi(a),$$

тј. ϕ шаље елементе из $\ker p$ у $\ker q$. Ово нам омогућава да дефинишемо ϕ_G на природан начин, шаљући елементе облика $p(a) \in A_G$ у $q\phi(a) \in B_G$. Слично за ψ.

Прво ћемо показати $\operatorname{im} \psi_G = C_G$. Претпоставимо да нам је дат произвољни елемент из C_G. Он је облика $r(c)$, за неко $c \in C$. Пошто је ψ сурјективно, то значи да постоји неко $b \in B$ такво да је $\psi b = c$. Дакле, $r(c) = r(\psi b) = \psi_G q(b) \in \operatorname{im} \psi_G$, па је $\operatorname{im} \psi_G = C_G$.

Сада, хајде да покажемо $\ker \psi_G = \operatorname{im} \phi_G$. Пре свега, имамо да је њихова копмозиција 0. Заиста, нека је дат произвољан елемент $p(a) \in A_G$. Добија се

$$\psi_G \phi_G p(a) = \psi_G q(\phi a) = r(\psi\phi(a)) = r(0) = 0.$$

Дакле, $\operatorname{im} \phi_G \subseteq \ker \psi_G$. Покажимо обрнуто.

Нека је $q(b) \in \ker \psi_G$ произвољан. Тада је $\psi_G q(b) = 0$, тј. $r(\psi b) = 0$, по чему имамо $\psi b \in \ker r$. Из дефиниције пресликавања r, то значи да је ψb у подгрупи C генерисаној елементима облика $g \cdot c - c$, где су $g \in G$ и $c \in C$. Дакле, за неке $g_i \in G$, $c_i \in C$ и $n \geq 1$, имамо

$$\psi b = \sum_{i=1}^{n} (g_i \cdot c_i - c_i).$$

Како је сваки $c_i \in C$ за све $1 \leq i \leq n$, и ψ је сурјективан, то значи да постоје $b_i \in B$ такви да је $c_i = \psi b_i$ за све $1 \leq i \leq n$. Дакле,

$$\psi b = \sum_{i=1}^{n}(g_i \cdot \psi b_i - \psi b_i) = \psi(\sum_{i=1}^{n}(g_i \cdot b_i - b_i)) = \psi m,$$

тј. $\psi(b-m) = 0$, где означавамо $m = (\sum_{i=1}^{n}(g_i \cdot b_i - b_i))$. Дакле, $b - m \in \ker\psi = \operatorname{im}\phi$ према тачности почетног низа. Дакле, сада имамо $b - m = \phi a$ за неко $a \in A$. Како је m у подгрупи наведеној у дефиницији B_G, следи $m \in \ker q$. Сада имамо

$$q(b) = q(b-m) = q(\phi a) = \phi_G p(a) \in \operatorname{im}\phi_G.$$

Дакле, показали смо $\ker\psi_G \in \ker\phi_G$. □

2.3 Коиндуковани и индуковани Λ-модули

Из G-структуре добијене из горе наведених G-дејстава на резултујућим објектима, функтори $\mathrm{Hom}(\_,\_)$ и $\_ \otimes \_$ дају појмове индукованих и коиндукованих Λ-модула.

Дефиниција 1 *Λ-модул A се сматра коиндукованим ако постоји Абелова група X са тривијалним G-дејством таква да је $A = \mathrm{Hom}(\Lambda, X)$, а индукованим ако је $A = \Lambda \otimes X$.*

Став 4 *Ако је G коначан, дефиниције коиндукованих и индукованих модула се поклапају.*

Доказ: Нека је X Абелова група са тривијалним G-дејством. Нека су A и A' модули из дефиниција индукованих и коиндукованих модула редом, то јест $A = \Lambda \otimes X$ и $A' = \mathrm{Hom}(\Lambda, X)$.

Нека је n број елемената у G, а елементе G означимо као $\{g_1, g_2, \ldots, g_n\}$. Како је $\Lambda = \mathbb{Z}G$ скуп формалних сума над елементима у G, којих има $n < \infty$, очигледно је изоморфан $\mathbb{Z}^n$. Значи, имамо

$$A = \Lambda \otimes X \cong \mathbb{Z}^n \otimes X \cong (\mathbb{Z} \otimes X)^n \cong X^n$$

Добијени изоморфизам $A = \Lambda \otimes X \to X^n$ је дат на произвољном елементу $\sum_{g\in G} g \otimes x_g \in \Lambda$ са

$$\sum_{g\in G} g \otimes x_g \mapsto (x_{g_1}, x_{g_2}, \ldots, x_{g_n}).$$

Следи да се било који елемент у A може јединствено представити као $\sum_{g\in G} g\otimes x_g$ за одговарајуће $x_g \in X$.

С друге стране, како је хомоморфизам из $\mathbb{Z}^n$ на неку групу јединствено одређен сликама n базних елемената од $\mathbb{Z}^n$, имамо

$$A' = \mathrm{Hom}(\Lambda, X) \cong \mathrm{Hom}(\mathbb{Z}^n, X) \cong (\mathrm{Hom}(\mathbb{Z}, X))^n \cong X^n$$

где последњи изоморфизам настаје тако што је сваки хомоморфизам из $\mathbb{Z}$ у X јединствено одређен тиме куда се слика 1.

Стога, као $\mathbb{Z}$ модули, видимо да су A' и A изоморфни. Све што је преостало је да покажемо да постоји изоморфизам између њих који поштује њихова G-дејства. Да бисмо то урадили, конструисаћемо изоморфизам између A' и A и директно показати да он чува G-дејство.

Како је G коначан, можемо записати произвољни елемент $\lambda \in \Lambda$ као збир над свим елементима G, тј. $\lambda = \sum_{g\in G} k_g g$, где је $k_g \in \mathbb{Z}$. Размотримо пресликавање $\varphi\colon A \to A'$ које пребацује елемент $g \times x$ у хомоморфизам $x\chi_g$, где је χ_g индикаторски хомоморфизам за g, тј. ако је $\lambda = \sum_{h\in G} k_h h$, онда је $\chi_g(\lambda) = k_g$. φ адитивно проширујемо на остатак A.

Ако је $a = \sum_{g\in G} g\otimes x_g \in A$, и $\lambda = \sum_{g\in G} k_g g$, онда

$$f_a(\lambda) = f_{\sum_{g\in G} g\otimes x_g}(\lambda) = \sum_{g\in G} f_{g\otimes x_g}(\lambda) = \sum_{g\in G} x_g\chi_g(\lambda) = \sum_{g\in G} k_g x_g.$$

Како се сваки елемент у A може јединствено представити у облику $\sum_{g\in G} g\otimes x_g$, пресликавање φ је добро дефинисано.

Да бисмо показали да је инјективно, претпоставимо да φ има исту слику на елементима $a = \sum_{g\in G} g\otimes x_g$ и $b = \sum_{g\in G} g\otimes y_g$, тј. $f_a = f_b$. То значи да имају исту слику на било ком произвољном елементу $g \in G$, тј. $f_a(g) = f_b(g)$. Дакле, $x_g = y_g$ за све $g \in G$. Дакле, $a = b$ и φ је инјективно.

Сада проверимо да ли је пресликавање такође сурјективно. Претпоставимо да је $f \in A' = \mathrm{Hom}(\Lambda, X)$. За свако $g \in G$, нека је $f(g) = x_g$. Нека је $a = \sum_{g\in G} g\otimes x_g \in X$. Сада, $f = f_a$ на G, па се по линеарности подударају и на Λ.

Све што преостаје је да се провери да ли се G дејства на A' и A подударају, то јест $h \cdot f_a = f_{h\cdot a}$ за све $h \in G$. Као и раније, било који произвољни елемент $a \in A$ може се једноставно написати као $a = \sum_{g\in G} g\otimes x_g$. Нека је $h \in G$. Имајући у виду да је G-дејство тривијално на X, сада израчунавамо:

$$h\cdot a = h\cdot(\sum_{g\in G} g\otimes x_g) = \sum_{g\in G} h\cdot(g\otimes x_g) = \sum_{g\in G} h\cdot g\otimes h\cdot x_g = \sum_{g\in G} h\cdot g\otimes x_g.$$

Како G делује на Λ множењем слева, и како је G коначан, можемо идентификовати дејство множења слева са елементом h из G са пермутацијом $\sigma \in \mathrm{Aut}(G)$.

$$h \cdot a = \sum_{g \in G} hg \otimes x_g = \sum_{g \in G} \sigma(g) \otimes x_g = \sum_{g \in G} g \otimes x_{\sigma^{-1}(g)}.$$

Сада израчунавамо како h делује на f_a за било који произвољни $\mu \in \Lambda$:

$$(h \cdot f_a)(\mu) = h \cdot f(h^{-1} \cdot \mu) = f(h^{-1} \cdot \mu)$$

као $f(g^{-1} \cdot \mu) \in X$. Ограничавајући се на слике елемената из G, имамо

$$(h \cdot f_a)(g) = f_a(h^{-1} \cdot g) = f_a(\sigma^{-1}(g)) = x_{\sigma^{-1}(g)} = f_{h \cdot a}(g)$$

где коначну једнакост закључујемо из горњих прорачуна $h \cdot a$. Стога, како се обе стране слажу на G, морају се сложити и на својим раширењима на Λ. □

Лема 5 *Сваки G-модул се утапа у коиндуковани модул.*

Доказ: Нека је A произвољан G-модул. Приказаћемо да се A утапа у $\mathrm{Hom}(\Lambda, A_0)$, где је A_0 основни $\mathbb{Z}$-модул од A, што значи да има тривијално G-дејство. Размотримо пресликавање $A \to \mathrm{Hom}(\Lambda, A_0)$ дато са $a \mapsto f_a$ где је $f_a(g) = g^{-1} \cdot a$ за све $g \in G$ као подскуп Λ (како је дејство G на A_0 тривијално, разматрамо резултат деловања g^{-1} на a у A, што је елемент A_0), а f_a се проширује на остатак Λ линеарно, то јест, $f_a(\lambda) = f_a(\sum_{i=1}^n k_i g_i) = \sum_{i=1}^n k_i g_i^{-1} \cdot a$. Ово пресликавање је инјективно, јер ако је $f_a = f_b$, онда је $f_a(1) = f_b(1)$, што значи $a = b$. Такође морамо показати да се G-дејства слажу, то јест, $g \cdot f_a = f_{g \cdot a}$. Стога морамо имати $(g \cdot f_a)(\lambda) = f_{g \cdot a}(\lambda)$ за све λ.

$$(g \cdot f_a)(\lambda) = g \cdot f_a(g^{-1} \cdot \lambda) = f_a(g^{-1} \cdot \lambda) = f_a(g^{-1} \cdot \sum_{i=1}^n k_i g_i) = f_a(\sum_{i=1}^n k_i g^{-1} g_i)$$

$$= \sum_{i=1}^n k_i (g^{-1} g_i)^{-1} \cdot a = \sum_{i=1}^n k_i (g_i^{-1} g) \cdot a = \sum_{i=1}^n k_i g_i^{-1} \cdot (g \cdot a) = f_{g \cdot a}(\lambda).$$

Друга једнакост важи, јер је у $g \cdot f_a(g^{-1} \cdot \lambda)$ спољашње дејство одговара G-дејству на A_0, што је тривијално. □

Лема 6 *Сваки G-модул је хомоморфан слици пројекције индукованог G-модула.*

Доказ: Нека је A произвољан G-модул и означимо са A_0 његов основни $\mathbb{Z}$-модул. Размотримо пресликавање из $\Lambda \otimes A_0$ у A које пресликава $g \otimes a$ у $g \cdot a$ и проширује се на све $\Lambda \otimes A_0$ линеарно. Показаћемо да је то епиморфизам. Сурјективно је, јер је сваки $a \in A$ слика $1 \otimes a$. Да бисмо показали да се G-дејства слажу, показујемо да се $g' \cdot (g \otimes a)$ пресликава у $g' \cdot (g \cdot a)$. Дакле,

$$g' \cdot (g \otimes a) = (g'g \otimes g' \cdot a) = (g'g \otimes a)$$

како G делује на A_0 тривијално. Овај резултат се пресликава на $(g'g) \cdot a = g' \cdot (g \cdot a)$. □

3 Разрешења

3.1 Слободна разрешења

Осим G-модула, друга основна структура у теорији групне кохомологије је пројективно разрешење. За сада ћемо почети са разрешењима слободних модула, а пројективне модуле ћемо касније правилно дефинисати.

Дефиниција 2 *Нека је R прстен, а M R-модул. Скуп E је база за M ако генерише M и ако је линеарно независан. Ако такав скуп постоји, онда кажемо да је M слободан модул.*

Дефиниција 3 *Нека је R прстен и M леви R-модул. Разрешење за M је тачан низ R-модула*

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Ако је сваки F_i слободан, онда се то назива слободним разрешењем M над R.

Можемо показати да постоји слободно разрешење за било који произвољни модул M, једноставном конструкцијом: Нека је F_0 слободан модул генерисан елементима M као генераторима, а $\varepsilon : F_0 \to M$ очигледна сурјекција. Затим, поновимо поступак да бисмо направили слободан модул F_1 генерисан елементима $\ker \varepsilon$ као генераторима и сурјекцијом $F_1 \to \ker \varepsilon$. Овај поступак се затим може понављати бесконачно да би се креирало слободно разрешење за M.

Углавном ћемо се бавити случајем када је $M = \mathbb{Z}$ а R је $\Lambda = \mathbb{Z}G$ за дату групу G.

3.2 Пресликавање проширења

Дефинишемо пресликавање проширења као хомоморфизам прстена $\varepsilon : \Lambda \to \mathbb{Z}$ такво да је $\varepsilon(g) = 1$ за све $g \in G$. Језгро од ε се назива иедал проширења λ и означава се са I.

Нека $\lambda = \sum_i^n k_i g_i$ буде произвољан елемент у Λ. Израчунавамо

$$\varepsilon(\lambda) = \varepsilon(\sum_i^n k_i g_i) = \sum_i^n k_i \varepsilon(g_i) = \sum_i^n k_i.$$

Дакле, ако је $\lambda \in I$, онда је $\sum_i^n k_i = 0$, што значи

$$\lambda = \lambda - \sum_i^n k_i = \sum_i^n k_i g_i - \sum_i^n k_i = \sum_i^n k_i (g_i - 1).$$

Дакле, сваки елемент скупа I је генерисан елементима облика $g-1$, тј. елементи $\{g-1|\ g\in G,\ g\neq 1\}$ чине базу за I као $\mathbb{Z}$-модул.

Сада, претпоставимо да је S скуп генератора за G. Показаћемо да елементи $\{s-1|\ s\in S\}$ генеришу I као леви идеал. Како елементи $\{g-1|\ g\in G,\ g\neq 1\}$ генеришу I, довољно је показати да су ови елементи генерисани са $\{s-1|\ s\in S\}$. Елемент $g\in G$ је облика $g=s_1s_2\cdots s_k$ где $s_1,\ldots,s_k\in S$ нису нужно различити. Сада, додавањем чланова који се скрате, добијамо следећу суму:

$$\begin{aligned} g-1 &= s_1s_2\cdots s_k-1 \\ &= s_1s_2\cdots s_k-\sum_{i=1}^{k-1}s_1\cdots s_i+\sum_{i=1}^{k-1}s_1\cdots s_i-1 \\ &= \sum_{i=1}^{k}(s_1\cdots s_i-s_1\cdots s_{i-1}) \\ &= \sum_{i=1}^{k}(s_1\cdots s_{i-1})\cdot(s_i-1). \end{aligned}$$

Дакле, елементи $\{s-1|\ s\in S\}$ генеришу I као леви идеал.

Важи и обрнуто, ако елементи $\{s-1|\ s\in S\}$ генеришу I као леви идеал, онда је S скуп генератора за G. Заиста, претпоставимо да је H подгрупа од G генерисана скупом S. Размотримо пермутациони модул $\mathbb{Z}[G/H]$. Неутрални елемент $\bar{1}\in G/H$ је фиксиран са H. Дакле, како S генерише H као подгрупу, а елементи $\{s-1|\ s\in S\}$ генеришу I као идеал, $\bar{1}$ се поништава свим елементима из I. Према томе, за све елементе $g\in G$, $(g-1)\bar{1}=0$, па $gH=H$ тј. $g\in H$. Дакле, $G\subset H$, што значи $G=H$. Другим речима, S генерише G.

Дефинисали смо групу коинваријантних елемената A_G од A као количник од A по адитивној подгрупи генерисаној елементима облика $ga-a$ за све $g\in G$, $a\in A$. Ови елементи су заправо производи елемента $g-1\in I$ и $a\in A$. Ови елементи тако генеришу идеал $IA=\{\sum_i^n a_ib_i\mid n\geq 1,\ a_i\in I,\ b_i\in A\}$, и тако имамо други облик за коинваријантну групу.

Лема 7 *$A_G=A/IA$.*

3.3 Пример: слободно разрешење од $\mathbb{Z}$ над неком цикличном групом

Конструишемо сада основни пример слободног разрешења.

Пример 1 *Слободно разрешење $\mathbb{Z}$ над цикличном групом.*

Напомена: Означимо са C_r^T цикличну групу реда r генерисану са T, за цео број r, $2 \leq r \leq \infty$.
Доказ: Поделићемо доказ на два случаја у зависности од тога да ли је ред дате цикличне групе, r, бесконачан или коначан.

Случај 1: $r = \infty$. На крају нашег разрешења мора бити пресликавање проширења $\varepsilon : \mathbb{Z}C_\infty^T \longrightarrow \mathbb{Z}$, где се генератор T слика у 1. То значи да се $T-1$ слика у 0. Према томе, нека конструишемо претходни слободни модул као $\mathbb{Z}C_\infty^S \cong \mathbb{Z}C_\infty^T \cong \Lambda$, са граничним пресликавањем $d : S \mapsto T-1$, где смо генератор преименовали у S чисто ради јасноће.

Једноставно је показати да је d инјективан: нека је $a+bS, c+dS \in \mathbb{Z}C_\infty^S$ са $d(a+bS) = d(c+ds)$. Дакле,

$$a + bT - b = c + dT - d,$$

па је

$$(a-c) + (d-b) = (d-b)T.$$

Због линеарне независности добијамо да је $d = b$ и $c = a$, тј. $a+bS = c+dS$.

Дакле, низ

$$0 \longrightarrow \mathbb{Z}C_\infty^S \xrightarrow{d} \mathbb{Z}C_\infty^T \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

је тачан, па је ово слободно разрешење од $\mathbb{Z}$ над $\mathbb{Z}C_\infty^T$.

Случај 2: $r < \infty$. Нека је $N = 1 + T + T^2 + \cdots + T^r$. Показаћемо да је следеће једно слободно разрешење $\mathbb{Z}$ над $\mathbb{Z}C_r^T$:

$$\ldots \xrightarrow{T-1} \Lambda_{(2k)} \xrightarrow{N} \Lambda_{(2k-1)} \xrightarrow{T-1} \ldots \xrightarrow{N} \Lambda_{(1)} \xrightarrow{T-1} \Lambda_{(0)} \longrightarrow \mathbb{Z}.$$

Сваки модул $\Lambda_{(i)}$ је копија слободног модула Λ. Проверимо да ли је низ тачан, тј. да ли се језгра и слике пресликавања $N : \Lambda_{(2k)} \longrightarrow \Lambda_{(2k-1)}$ и $T-1 : \Lambda_{(2k+1)} \longrightarrow \Lambda_{(2k)}$ поклапају. $N(T-1) = (T-1)N = T^r - 1 = 0$, тако да слика сваког прселикавања лежи унутар језгра следећег. Покажимо да је и обрнуто тачно.

За непаран случај, нека је $\lambda = \sum_{i=0}^{r-1} a_i T^i \in \Lambda_{(2k+1)}$. Како је λ у $\ker(T-1)$, имамо

$$\begin{aligned}
(T-1)\cdot\lambda &= 0 \\
(T-1)\cdot\sum_{i=0}^{r-1} a_i T^i &= 0 \\
T\cdot\sum_{i=0}^{r-1} a_i T^i - 1\cdot\sum_{i=0}^{r-1} a_i T^i &= 0
\end{aligned}$$

$$\begin{aligned}\sum_{i=0}^{r-1} a_i T^{i+1} - \sum_{i=0}^{r-1} a_i T^i &= 0\\ a_{r-1}T^r + \sum_{i=1}^{r-1}(a_{i-1} - a_i)T^i - a_0 &= 0\end{aligned}$$

из чега, уз напомену да је $T^r = 1$, следи $a_0 = a_1 = \cdots = a_{r-1} = a_0$ по линеарној независности. Дакле, λ је облика $\sum_{i=0}^{r-1} a_0 T^i = a_0 N$ и стога $\lambda \in \operatorname{im} N$.

За парни случај, поново нека је $\lambda = \sum_{i=0}^{r-1} a_i T^i$, овог пута, међутим, у $\Lambda_{(2k)}$. Претпоставимо $\lambda \in \ker N$. Затим,

$$\begin{aligned}N \cdot \lambda &= 0\\ N \cdot \sum_{i=0}^{r-1} a_i T^i &= 0\\ \sum_{j=0}^{r-1} \big(T^j \cdot \sum_{i=0}^{r-1} a_i T^i\big) &= 0\\ \sum_{j=0}^{r-1}\sum_{i=0}^{r-1} a_i T^{i+j} &= 0\\ \sum_{i=0}^{r-1} \big(a_i \sum_{j=0}^{r-1} T^{i+j}\big) &= 0\\ \big(\sum_{i=0}^{r-1} a_i\big)\big(\sum_{i=0}^{r-1} T^i\big) &= 0.\end{aligned}$$

Због линеарне независности елемената a_i, ово даје r идентичних једначина: $a_0 + \cdots + a_{r-1} = 0$, или $a_0 = -a_1 - \cdots - a_{r-1}$. Враћањем овога у λ, добијамо

$$\lambda = \sum_{i=0}^{r-1} a_i T^i = a_0 + \sum_{i=1}^{r-1} a_i T^i = \sum_{i=1}^{r-1} a_i (T^i - 1) = \sum_{i=1}^{r-1} a_i (T-1)(1 + \cdots + T^{i-1}).$$

Дакле, $\lambda = (T-1)\cdot\mu$ за неко $\mu \in \Lambda$ (или боље речено $\Lambda_{(2k+1)}$), и стога $\lambda \in \operatorname{im}(T-1)$.

Стога је наш низ тачан, па је према томе слободно разрешење $\mathbb{Z}$ над $\mathbb{Z}C_r^T$. □

3.4 Стандардно разрешење

Иако смо већ показали да у општем случају слободно разрешење неког модула над прстеном R увек постоји, за случај за прстен R имамо пр-

стен $\Lambda = \mathbb{Z}G$, постоји једна практичнија конструкција, наиме стандардно разрешење. Нека је $\bar{P}_k$ слободан $\mathbb{Z}$-модул са базом датом $(k+1)$-торкама $(g_0, \ldots, g_k)$ елемената из G, и нека сваки $g \in G$ дејствује на произвољну $(k+1)$-торку са

$$g \cdot (g_0, \ldots, g_k) = (gg_0, \ldots, gg_k).$$

Напоменимо да је $\bar{P}_0$ заправо $\mathbb{Z}G$, тј. Λ.

Гранични хомоморфизам $d : \bar{P}_k \to \bar{P}_{k-1}$ је дефинисан на бази:

$$d(g_0, \ldots, g_k) = \sum_{j=0}^{k} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_k),$$

где читамо $\hat{g_j}$ као „изоставимо елемент g_j“. У димензији нула користимо пресликавање проширења $\epsilon : \bar{P}_0 \to \mathbb{Z}$ дато са $\varepsilon(g_0) = 1$. Ова дефиниција d је аналогна дефиницији симплицијалне границе симплекса са теменима $g_0, \ldots, g_k$. Стога је низ

$$\cdots \longrightarrow \bar{P}_k \xrightarrow{d_k} \bar{P}_{k-1} \xrightarrow{d_{k-1}} \cdots \xrightarrow{d_1} \bar{P}_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

тачан, и према томе представља слободно разрешење $\mathbb{Z}$ над Λ. Такође можемо директно да проверимо ово користећи контрахујућу хомотопију $h : \bar{P}_k \to \bar{P}_{k+1}$ за проширени комплекс $\mathbb{Z}$-модула у основи. Дефинишемо h са $h(g_0, \ldots, g_k) = (1, g_0, \ldots, g_k)$ ако је $n \geq 0$ и $h(1) = (1)$ за $k = -1$. Заиста, имамо

$$\begin{aligned} d_{k+1}h(g_0, \ldots, g_k) &= d_{k+1}(1, g_0, \ldots, g_k) \\ &= (g_0, \ldots, g_k) + \sum_{j=1}^{k+1} (-1)^j (1, g_0, \ldots, g_j \hat{} - 1, \ldots, g_k) \\ &= (g_0, \ldots, g_k) + \sum_{j=0}^{k+1} (-1)^{j+1} (1, g_0, \ldots, \hat{g_j}, \ldots, g_k) \end{aligned}$$

и

$$\begin{aligned} hd_k(g_0, \ldots, g_k) &= h \sum_{j=0}^{k} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_k) \\ &= \sum_{j=0}^{k} (-1)^j (1, g_0, \ldots, \hat{g_j}, \ldots, g_k). \end{aligned}$$

Одатле је $(d_{k+1}h + hd_k)(1, g_0, \ldots, g_k) = (g_0, \ldots, g_k)$, тј. $dh + hd = id_C$, и стога је h заправо контрахујућа хомотопија.

Као базу за слободни Λ-модул $\bar{P}_k$ можемо узети $(n+1)$-торке чији је први елемент 1, пошто оне представљају G-орбите $(n+1)$-торки. Често је корисно написати такву $(n+1)$-торку у облику $(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_n)$ и увести „преградну“ нотацију (eng. "bar"notation)

$$[g_1|g_2|\ldots|g_n] = (1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_n).$$

За $k = 0$, постоји само један такав елемент у бази, означен са $[\,]$. Како смо већ идентификовали $\bar{P}_0$ са Λ, онда је $[\,] = 1$ при овој идентификацији.

Сада ћемо тражити како изгледа гранични хомоморфизам ∂_* у овој нотацији.

$$\begin{aligned}\partial_*[g_1|\ldots|g_k] &= d(1, h_1, \ldots, h_k)\\ &= \sum_{j=0}^{k}(-1)^j(1, h_1, \ldots, \hat{h}_j, \ldots, h_k)\end{aligned}$$

где је свако $h_i = g_1 \ldots g_i$ и узимајући $1 = h_0$. Израчунајмо сада сваки сабирак.

За $j = 0$:

$$\begin{aligned}(h_1, h_2, \ldots, h_k) &= (g_1, g_1g_2, \ldots, g_1\ldots g_k)\\ &= g_1 \cdot (1, g_2, \ldots, g_2\ldots g_k)\\ &= g_1 \cdot [g_2|\ldots|g_k].\end{aligned}$$

За $1 \le j \le k-1$:

$$\begin{aligned}(1, h_1, \ldots, \hat{h}_j, \ldots, h_k) &= (1, g_1, \ldots, g_1\ldots g_{j-1}, g_1\ldots g_jg_{j+1}, \ldots, g_1\ldots g_k)\\ &= [g_1|\ldots|g_{j-1}|g_jg_{j+1}|g_{j+2}|\ldots|g_k].\end{aligned}$$

Другу једнакост добијамо тиме што смо формирали $(k-1)$-торку од $g_1, \ldots, g_k$ „лепљењем“ g_j и g_{j+1}.

За $j = k$:

$$\begin{aligned}(1, h_1, \ldots, h_{k-1}) &= (1, g_1, \ldots, g_1\ldots g_{k-1})\\ &= [g_1|\ldots|g_{k-1}].\end{aligned}$$

Дакле, наша резултујућа формула за гранични хомоморфизам је:

$$\begin{aligned}d_*[g_1|\ldots|g_{k+1}] &= g_1 \cdot [g_2|\ldots|g_{k+1}]\\ &\quad + \sum_{j=1}^{k}(-1)^j[g_1|\ldots|g_jg_{j+1}|\ldots|g_{k+1}]\end{aligned}$$

$$
\begin{aligned}
& +(-1)^{k+1}[g_1|\dots|g_k] \\
= \; & g_1 \cdot [g_2|\dots|g_{k+1})] - [g_1g_2|g_3|\dots|g_{k+1}] \\
& +[g_1|g_2g_3|\dots|g_{k+1}] - \dots \\
& +(-1)^{j}[g_1|\dots|g_jg_{j+1}|\dots|g_{k+1}] + \dots \\
& +(-1)^{k+1}[g_1|\dots|g_k].
\end{aligned}
$$

Ова верзија стандардног разрешења се често назива преградним разрешењем. У ниским димензијама има облик

$$\cdots \to \bar{P}_2 \xrightarrow{d_2} \bar{P}_1 \xrightarrow{d_1} \bar{P}_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

где је $d_2([g|h]) = g \cdot [h] - [gh] + [g]$, $d_1([g]) = g[\,] - [\,] = g - 1$, и $\varepsilon([\,]) = 1$.

Друга верзија стандардног разрешења је нормализовано стандардно (или преградно) разрешење $\bar{F}_* = F_*/D_*$, где је D_* дегенерисани поткомплекс од $\bar{P}_*$, поткомплекс генерисан елементима $(g_0, \cdots, g_n)$ таквим да је $g_i = g_{i+1}$ за неке i. У ознакама преградне нотације, D_* се може описати као G-поткомплекс од F_* генерисан елементима $[g_1|\dots|g_n]$ таквим да је $g_i = 1$ за неко i. Дакле, $\bar{F}_*$ је слободан Λ модул са једним базисним елементом (још увек означен као $[g_1|\dots|g_n]$) за сваку n-торку нетривијалних елемената од G. Ланчани комплекс $\bar{F}_*$ је тачан јер је контрактибилан коришћењем исте контрахујуће хомотопије h од раније, пошто слика $\bar{F}_*$ у себе.

3.5 Тополошка тачка гледишта

Дефиниција 4 *G-комплекс је CW-комплекс заједно са дејством G на X које пермутује ћелије. Дакле, за сваки $g \in G$, имамо хомеоморфизам $x \mapsto g \cdot x$ од X за који је слика $g \cdot \sigma$ било које ћелије σ у X такође ћелија. Ако је дејство G на X слободно, онда кажемо да је X слободан G-комплекс.*

Ако је X један G-комплекс, онда дејство G на X индукује дејство G на ћелијски ланчани комплекс $C_*(X)$, којим он постаје ланчани комплекс G-модула.

Ако је X слободан G-комплекс, онда сваки модул $C_n(X)$ у придруженом ланчаном комплексу има $\mathbb{Z}$-базу која је слободно пермутована од стране G. Другим речима, X је G-скуп, и можемо одредити специфичну Λ-базу користећи става 1. Добијамо да је сваки модул C_n придруженог ланчаног комплекса Λ-модул са базним елементом за сваку G-орбиту ћелија. Да бисмо добили одређену базу, морали бисмо да изаберемо ћелију представника из сваке орбите и оријентацију за сваку од њих.

За G-комплекс X, орбитални комплекс Y је количнички простор X/G. Тачке у Y одговарају орбитама тачака у X. Дакле, ако је X слободан G

комплекс, $C_*(Y)$ има $\mathbb{Z}$-базу са базним елементом за сваку G-орбиту ћелија од X. Међутим, $C_*(X)$ је комплекс слободних Λ-модула са базним елементом за сваку G-орбиту ћелија. Дакле, $C_*(Y)$ је еквивалентан слици $C_*(X)$ при количничком пресликавању које је одређено G-дејством, другим речима група коинваријанти. Да резимирамо:

Став 8 *Нека је X слободан G-комплекс и нека је Y орбитални комплекс X/G. Тада је $C_*(Y) \cong C_*(X)_G$.*

Ако је X контрактибилан, онда је $H_*(X) \cong H_*(pt.)$. То јест, низ

$$\cdots \longrightarrow C_k \xrightarrow{\partial} C_{k-1} \longrightarrow \cdots \longrightarrow C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

је тачан. Дакле, следи нам следећи став:

Став 9 *Нека је X контрактибилан слободан G-комплекс. Тада је проширени ћелијски ланчани комплекс од X слободно разрешење од $\mathbb{Z}$ над $\mathbb{Z}G$.*

Пример 2 *Тополошки начин посматрања стандардног разрешења.*

Нека је X линеарни омотач над G при чему се сматра да су елементи из G у простору довољно велике димензије да су у општем положају. Темена од X су елементи G, при чему дејствује множењем слева. Сваки коначан подскуп од G чини симплекс у X. Ако је G коначна, тада је X заправо и сам симплекс, а ако је бесконачна, онда је X бесконачно димензионални аналог. Група G дејствује на X симплицијално, шаљући симплексе у друге симплексе исте димензије, а дејство је очигледно слободно. Видимо да се у оба случаја резултујући симплицијални ланчани комплекси (а самим тим и гранични оператор) поклапају са раније наведеним дефиницијама стандардног разрешења.

У оба случаја, X је контрактибилан праволинијском контрахујућом хомотопијом. Дакле, према ставу 9, проширени целуларни ланчани комплекс X је слободно разрешење од $\mathbb{Z}$ над $\mathbb{Z}G$. Ово је тополошки начин да се докаже тачност стандардног разрешења.

Стандардно разрешење је користан теоријски алат. На пример, користићемо га да докажемо постојање кохомолошке екстензије за групе. Али, често га није практично користити за прорачуне. У пракси нам је углавном корисније да пронађемо најбољи избор за ту одређену групу која се проучава. То је често повезано са тополошким просторима. На пример, у примеру 1, тополошка мотивација долази разматрањем дејства C_∞^T на $\mathbb{R}$ по правилу $T \cdot x = x + 1$. Слично, за коначну цикличну групу C_r^T, разматрамо дејство групе T на круг $S^1 = \{e^{i\varphi} : \phi \in \mathbb{R}\}$ пресликавањем $T : e^{i\varphi} \mapsto e^{i(\varphi + 2\pi/r)}$. Или, еквивалентно, могли бисмо да размотримо правилан r-угао на који делује његова група ротација.

3.6 Ајленберг-Маклејнови простори

Један природан начин да се конструишу G-комплекси јесте да се узме група аутомофизама нормалног наткривања. Нека је $p : \widetilde{X} \to X$ нормално наткривање CW-комплекса X и G група аутоморфизама $\widetilde{X}$. Простор $\widetilde{X}$ наслеђује CW-структуру од X, где G слободно и транзитивно пермутује скуп $p^{-1}\sigma$ за било коју ћелију $\sigma \in X$, тј. ћелије преслике σ. Дакле, $\widetilde{X}$ је слободан G-комплекс. Орбите G-дејства су скупови преслика $p^{-1}\sigma$, тако да је према ставу 1, $C_*\widetilde{X}$ комплекс слободних $\mathbb{Z}G$-модула са једним базним елементом за сваку ћелију од X. Гранична пресликавања се затим добијају из граничних пресликавања у ћелијском ланчаном комплексу од X.

Сада је сасвим природно размотрити ефекте става 9, када је то применљиво. Да бисмо то урадили, разматрамо повезан простор Y са фундаменталном групом $\pi_1 Y \cong G$ са контрактибилним универзалним наткривањем X. Такав простор се назива Ајленберг-Маклејнов простор $K(G, 1)$. Стога добијамо из 9 следеће:

Став 10 *Нека је Y $K(G, 1)$. Тада је проширени ћелијски ланчани комплекс универзалног покривача X од Y слободно разрешење од $\mathbb{Z}$ над $\mathbb{Z}G$.*

Уопштено, Ајленберг-Маклејнов простор $K(G, n)$ је повезан простор са $\pi_n K(G, n) = G$ и свим осталим хомотопским групама тривијалним. За димензију 1, ова дефиниција је еквивалентна нашој горњој дефиницији. То је због следеће леме:

Лема 11 *За повезан простор X, следећа тврђења су еквивалентна:*

1. *универзално наткривање од X је контрактибилно,*
2. *$H_i(X) = 0$ за $i \geq 2$,*
3. *$\pi_i(X) = 0$ за $i \geq 2$.*

Ова лема је последица резултата из основне теорије хомотопије. Слично томе, постојање простора $K(G, n)$ може се доказати конструкцијом, још једним познатим резултатом из теорије хомотопије.

Посматрајмо сада неки основни пример:

Пример 3 *Разрешење $\mathbb{Z}$ над $\mathbb{Z}G$ за $G = \mathbb{Z}_2$.*

Бесконачно димензиони реални пројективни простор $\mathbb{R}\mathrm{P}^\infty$ је добро познат пример $K(G, 1)$ простора, јер има $\pi(\mathbb{R}\mathrm{P}^\infty) = \mathbb{Z}_2$ а све остале хомотопске

групе су тривијалне. Универзално наткривање реалног пројективног простора $\mathbb{R}\mathrm{P}^\infty$ је бесконачна сфера S^∞, где наткривајуће пресликавање идентификује две супротне тачке. То значи да нетривијални елемент од G делује као антиподално пресликавање. Према ставу 10, ћелијски ланчани комплекс од S^∞ заједно са дејством G формира разрешење за $\Lambda = \mathbb{Z}G$ над $\mathbb{Z}$.

Индуктивно конструишемо CW-комплекс за S^∞. Сваки скелет X_k је хомеоморфан k-сфери, где је $(k-1)$-сфера X_{k-1} екватор, а хемисфере су формиране од две k-ћелије a_k и b_k спојене дуж наведеног екватора. Дакле, у $\mathbb{Z}$ коефицијентима имамо следећи ћелијски ланчани комплекс:

$$\cdots \longrightarrow \mathbb{Z}\oplus\mathbb{Z} \xrightarrow{\partial_k} \mathbb{Z}\oplus\mathbb{Z} \xrightarrow{\partial_{k-1}} \ldots \xrightarrow{\partial_1} \mathbb{Z}\oplus\mathbb{Z} \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

Гранична пресликавања ∂_k су одређена степеном пресликавања лепљења k-ћелија. Пошто је свака k-ћелија b_k антиподална слика a_k, степен њеног лепљења је $(-1)^k$ пута већи од a_k. Дакле, имамо

$$\begin{aligned} \partial_1 a_1 &= a_0 - b_0, & \partial_1 b_1 &= b_0 - a_0, \\ \partial_2 a_2 &= a_1 + b_1, & \partial_2 b_2 &= b_1 + a_1, \\ \partial_3 a_3 &= a_2 - b_2, & \partial_3 b_3 &= b_2 - a_2. \\ &\vdots & &\vdots \end{aligned}$$

У општем облику, имамо

$$\begin{aligned} \partial_k a_k &= a_{k-1} + (-1)^k b_{k-1} \\ \partial_k b_k &= b_{k-1} + (-1)^k a_{k-1} \end{aligned}$$

У свакој димензији k, a_k и b_k су антиподалне слике један другог, што значи да нетривијални елемент T у G делује на њих замењивањем. Стога можемо написати $b_k = Ta_k$. Према томе, $\mathbb{Z}$-модул у димензији k, $\mathbb{Z}\oplus\mathbb{Z}$ генерисан са a_k и b_k, постаје G-модул $\mathbb{Z}\oplus T\mathbb{Z} = \Lambda$ генерисан са a_k. Овиме, гранично пресликавање постаје

$$\partial_k a_k = (1 + (-1)^k T)a_{k-1} = \begin{cases} 1+T, & 2 \mid k, \\ 1-T, & 2 \nmid k. \end{cases}$$

Дакле, имамо следеће разрешење $\mathbb{Z}G$ над $\mathbb{Z}$:

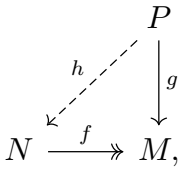
$$\ldots \xrightarrow[1+T]{\partial_4} \Lambda \xrightarrow[1-T]{\partial_3} \Lambda \xrightarrow[1+T]{\partial_2} \Lambda \xrightarrow[1-T]{\partial_1} \Lambda \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

Ово разрешење се поклапа са већ добијеним разрешењем у примеру 1, за ред $r = 2$.

3.7 Пројективни модули

Вратимо се сада на општији случај, разрешења R-модула M где је R произвољан прстен. R-модул M дозвољава много слободних разрешења, наш циљ до краја ове главе је да покажемо да су сва таква разрешења хомотопски еквивалентна. Заправо важи и општије, за пројективна разрешења.

Дефиниција 5 *Размотримо проблем комплетирања дијаграма облика*

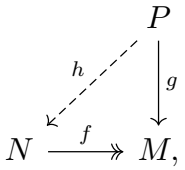


где је f сурјекција, и желимо да конструишемо h тако да дијаграм комутира, тј. $fh = g$. Модул P се назива пројективним ако решење постоји за сваки проблем комплетирања дијаграма овог облика.

Покажимо зашто ово генерализује појам слободних модула:

Лема 12 *Слободни модули су пројективни.*

Доказ: Нека је F слободан модул са базом (e_γ) и размотримо проблем пресликавања



где је f сурјекција. Тада је $g(e_\gamma) \in M = \operatorname{im} f$, тако да можемо изабрати $x_\gamma \in N$ са $f(x_\gamma) = g(e_\gamma)$. Нека сада h буде јединствено пресликавање R-модула задато са $g(e_\gamma) = x_\gamma$. □

У дефиницији 3, заменом свуда „слободно“ са „пројективно“, добијамо дефиницију пројективног разрешења; разрешења где су сви модули пројективни. Стога, свако слободно разрешење је такође пројективно разрешење.

Постоје и други, еквивалентни начини за дефинисање пројективних модула. Један који ће нам касније бити користан је коришћење „цепајућих“ низова.

Дефиниција 6 *Нека је*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0.$$

кратак тачан низ R-модула. Дефинишемо следеће:

а) низ се цепа здесна ако постоји хомоморфизам $s : C \to B$ такав да је $\beta s = id_C$;

б) низ се цепа слева ако постоји хомоморфизам $r : B \to A$ такав да је $r\alpha = id_A$;

ц) низ је „цепајуће“ тачан ако постоји изоморфизам $h : B \to A \oplus C$ такав да је $h\alpha = i_A$ и $hp_C = \beta$, где је $i_A : A \to A \oplus C$ природна инклузија, а $p_C : A \oplus C$ природна пројекција.

Уствари, све ове дефиниције су еквивалентне. Према томе, ако важи било која од њих, кажемо само да се низ цепа. Ово представљамо у леми опште познатој као Лема о цепању низова:

Лема 13 *Случајеви наведени у дефиницији 6 су еквивалентни.*

Доказ: Током доказа, позиваћемо се на пресликавања дата следећим дијаграмом:

$$\begin{array}{ccccc} A & \underset{r}{\overset{\alpha}{\rightleftarrows}} & B & \underset{s}{\overset{\beta}{\rightleftarrows}} & C \\ {\scriptstyle \mathrm{id}_A}\downarrow & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \mathrm{id}_C} \\ A & \xrightarrow{i_A} & A \oplus C & \xrightarrow{p_C} & C. \end{array}$$

Пуне стрелице означавају α и β из почетног кратког тачног низа, идентичко пресликавање на A и C, природна инклузија $i_A : A \to A \oplus C$ и пројекција $p_C : A \oplus C \to C$. Испрекидане стрелице су пресликавања из случајева (а), (б) и (ц). Докажимо како сваки случај имплицира други.

(а) $\Rightarrow$ (б): Претпоставимо да постоји инјекција $s : C \to B$ таква да је $\beta s = \mathrm{id}_C$. Нека је $b \in B$ и размотримо $b' = b - s\beta b$. Сада имамо

$$\beta b' = \beta b - \beta s \beta b = \beta b - \mathrm{id}_C \beta b = \beta b - \beta b = 0.$$

Дакле, $b' \in \ker \beta$. Међутим, због тачности почетног низа, $\ker \beta = \mathrm{im}\, \alpha$. Пошто је α инјекција, можемо дефинисати α^{-1} на $\mathrm{im}\, \alpha$. Дакле, можемо дефинисати пресликавање $r : B \to A$ на произвољном елементу $b \in B$ са

$$r(b) = \alpha^{-1}(b - s\beta b).$$

Јасно је да имамо $r\alpha = \mathrm{id}_A$. Пошто r има десни инверз, мора бити сурјекција. Приметимо да је

$$rsc = \alpha^{-1}(sc - s\beta sc) = \alpha^{-1}(sc - sc) = 0,$$

за све $c \in C$, стога је $rs = 0$.

(b) $\Rightarrow$ (a): Претпоставимо сада да постоји сурјекција $r : B \to A$ таква да је $r\alpha = \mathrm{id}_A$. Нека је $c \in C$. Пошто је β сурјекција, постоји неко $b \in B$ такво да је $c = \beta b$. Дефинишемо $s : C \to B$ на c као

$$s(c) = b - \alpha rb.$$

Дакле, $\beta sc = \beta b - \beta\alpha rb = c - 0 = c$, тј. $\beta s = \mathrm{id}_C$. Пошто s има леви инверз, мора бити инјекција. Поново, напоменимо да

$$rsc = rb - r\alpha rb = rb - rb = 0,$$

тј. $rs = 0$.

До сада смо показали да су случајеви (а) и (б) еквивалентни. Покажимо сада следеће.

(a) $\Rightarrow$ (c): Претпоставимо да постоји пресликавање $s : C \in B$ такво да је $\beta s = \mathrm{id}_C$. Одмах следи да је s инјективно, и стога $\operatorname{im} s \cong C$. Такође, како је $\beta s = \mathrm{id}_C$, то значи $\ker\beta \cap \operatorname{im} s = 0$, тј. $\operatorname{im}\alpha \cap \operatorname{im} s = 0$.

Нека је $b \in B$ произвољан. Нека је $b' = b - s\beta b$. У доказу (a) $\Rightarrow$ (b) показали смо да је $b' \in \operatorname{im}\alpha$. Такође, узимајући r дефинисано из нашег доказа за (a) $\Rightarrow$ (b), имамо $b' = \alpha rb$. Јасно је да имамо $b'' = s\beta b \in \operatorname{im} s$. Значи, записали смо b као збир $b' + b''$ за неке $b' \in \operatorname{im}\alpha$ и $b'' \in \operatorname{im} s$.

Претпоставимо да имамо други начин да запишемо b као збир два елемента из $\operatorname{im}\alpha$ и $\operatorname{im} s$, рецимо $b = c' + c''$, где је $c' \in \operatorname{im}\alpha$ и $c'' \in \operatorname{im} s$. Дакле, $b' + b'' = c' + c''$, тј. $b' - c' = c'' - b''$. Лева страна је садржана у $\operatorname{im}\alpha = \ker\beta$, а десна страна је у $\operatorname{im} s$. Међутим, $\ker\beta \cap \operatorname{im} s = 0$, и стога $c' = b'$ и $c'' = b''$. Зато је декомпозиција b као збира елемената из $\operatorname{im}\alpha$ и $\operatorname{im} s$ јединствена.

Овиме смо показали да је $B = \operatorname{im}\alpha \oplus \operatorname{im} s \cong A \oplus C$. Изоморфизам $h : B \to A \oplus C$ је дат на елементу $b \in B$ са јединственом композицијом $b = b' + b''$, за $b' \in \operatorname{im}\alpha$ и $b'' \in \operatorname{im} s$, као $h(b) = i_A r(b') + i_C\beta(b'')$. Како је $\operatorname{im}\beta = \ker\alpha$, имамо $b' \in \operatorname{im}\beta = \ker\alpha$, и, као што смо раније напоменули $rs = 0$, тако да је $b'' \in \operatorname{im} s \subseteq \ker r$. То значи да је хомоморфизам h дефинисан као $h = i_A r + i_C\beta$. Да бисмо видели да h заиста испуњава услове у (c), израчунавамо следеће:

$$h\alpha = i_A r\alpha + i_C\beta\alpha = i_A\mathrm{id}_A + i_C \circ 0 = i_A,$$

и

$$p_C h = p_C i_A r + p_C i_C\beta = 0r + \mathrm{id}_C\beta = \beta.$$

Коначно, покажимо **(c) ⇒ (a)**. Претпоставимо да имамо изоморфизам $h : B \to A \oplus C$ такав да је $h\alpha = i_A$ и $p_C h = \beta$. Можемо дефинисати $s : C \to B$ као $s = h^{-1} i_C$. Сада, из $p_C h = \beta$, имамо $p_C = \beta h^{-1}$. Дакле,

$$\beta s = \beta h^{-1} i_C = p_C i_C = \mathrm{id}_C.$$

Дакле, показали смо да су (a), (b) и (c) еквивалентни. □

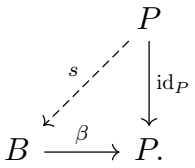
За пројективне модуле имамо следеће својство.

Лема 14 *Ако је P пројективни модул, онда се сваки кратки тачан низ који се завршава са P цепа. То јест, за било које R-модуле A и B, за које је низ*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} P \longrightarrow 0.$$

тачан, овај се низ цепа.

Доказ: Neka је дат такав низ, размотримо следећи дијаграм:

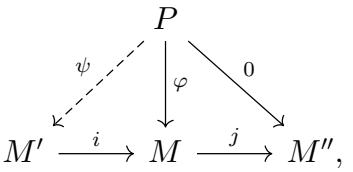


Како је P пројективан, мора постојати R-хомоморфизам $s : P \to B$ такав да дијаграм комутира. Стога је $\beta s = \mathrm{id}_P$. □

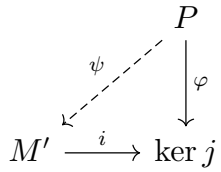
Заправо важи и обрнуто, и ово можемо узети за алтернативну дефиницију пројективних модула. Међутим, нама је само потребна импликација из горе наведене леме у даљем, па ћемо прескочити доказ обрнуте.

3.8 Јединственост разрешења

Сада се усредсређујемо на показивање јединствености пројективних (и самим тим слободних) разрешења. Користићемо модификовану дефиницију пројективног модула: размотримо проблем комплетирања дијаграма



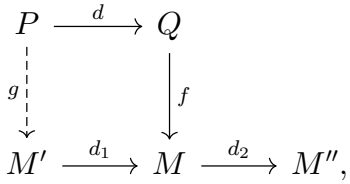
где је $j\varphi = 0$. Модул P се назива пројективним ако постоји решење за сваки такав проблем допуњавања дијаграма у коме је низ на дну тачан. Ово је еквивалентно оригиналној дефиницији једноставним ограничавањем на



јер $j\varphi = 0$ имплицира $\operatorname{im}\varphi \in \ker j$.

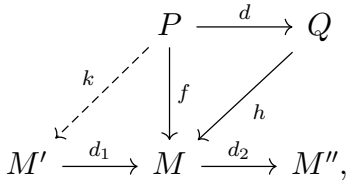
Докажимо сада следећу лему која ће нам после помоћи:

Лема 15 *(а) Претпоставимо да је дат дијаграм*



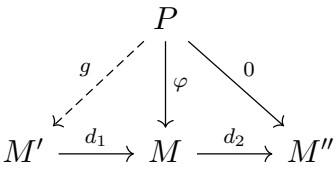
где је $d_2fd = 0$, и желимо да нађемо g такав да је $d_1g = fd$. Ако је P пројективан и доњи ред је тачан, онда такав g постоји.

(б) Претпоставимо да је дат дијаграм (не нужно комутативан)



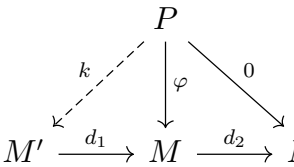
где је $d_2hd = d_2f$ и желимо да нађемо k такав да је $d_1k + hd = f$. Ако је P пројективан и доњи ред је тачан, онда такав k постоји.

Доказ: (а) Постављањем $\varphi = fd$ трансформишемо проблем у



где је $d_2\varphi = 0$ када је $d_2\varphi = d_2fd = 0$. Дакле, за пројективни P, постоји g такав да је $d_1g = \varphi$ тј. $d_1g = fd$.

(б) Овог пута, поставимо $\varphi = f - hd$. Сада, како је $d_2\varphi = d_2(f - hd) = 0$, имамо



Дакле, за пројективни P, постоји k такав да је $\varphi = d_1 k$ тј. $d_1 k = f - hd$. Дакле, $d_1 k + hd = f$. □

Следећа лема је о ланчаним пресликавањима и хомотопијама из пројективног комплекса у тачан.

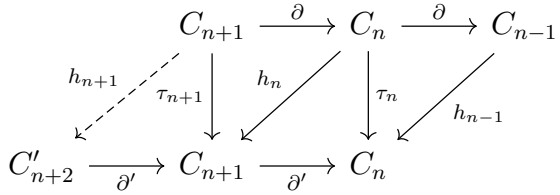
Лема 16 *Нека су (C, ∂) и (C', ∂') ланчани комплекси и нека је r цео број. Нека је $(f_i : C_i \to C'_i)_{i \le r}$ фамилија пресликавања таква да је $\partial'_i f_i = f_{i-1}\partial_i$ за $i \le r$. Ако је C_i пројективно за $i > r$ и $H_i(C') = 0$ за $i \ge r$, онда се $(f_i)_{i \le r}$ проширује на ланчано пресликавање $f : C \to C'$, а f је јединствено до на хомотопију. Прецизније, било која два проширења су хомотопска помоћу хомотопије h такве да је $h_i = 0$ за $i \le r$.*

Доказ: Претпоставимо индуктивно да је f_i дефинисано за $i \le n$, где је $n \ge r$, и да је $\partial'_i f_i = f_{i-1}\partial_i$ за $i \le n$. Онда имамо проблем допуњавања дијаграма

$$\begin{array}{ccccc} C_{n+1} & \xrightarrow{\partial} & C_n & \xrightarrow{\partial} & C_{n-1} \\ \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\ C'_{n+1} & \xrightarrow{\partial'} & C_n & \xrightarrow{\partial'} & C_{n-1}, \end{array}$$

где је $\partial' f_n \partial = f_{n-1}\partial\partial = 0$. Стога f_{n+1} постоји по леми 15а.

Претпоставимо сада да је g неко друго проширење од $(f_i)_{i \le r}$. Желимо да пронађемо хомотопију h између f и g. Поступимо индуктивно. Индукцију започињемо постављањем $h_i = 0$ за $i \le r$. Сада, претпоставимо да је $h_i : C_i \to C''_{i+1}$ дефинисано за $i \le n$, где је $n \ge r$, и да је $\partial' h_i + h_{i-1}\partial = f_i - g_i$. Ако поставимо $\tau = f_i - g_i$, добијамо проблем допуњавања дијаграма



са $\partial' h_n \partial = (\tau_n - h_{n-1}\partial)\partial$ по индуктивној хипотези. Пошто је $\partial^2 = 0$, ово је једнако $\tau_n \partial$. Пошто је τ ланчано пресликавање, имамо $\partial' h_n \partial = \partial' \tau_{n+1}$. Сада,

како је C_{n+1} пројективан, можемо применити Лему 15b, по којој постоји h_{n+1} са $\partial' h_{n+1} + h_n \partial = \tau_{n+1}$, што смо тражили. □

Ова лема је идејна сржи која се користи за да се постигне наш циљ проналажења јединствености пројективних разрешења, што ћемо окончати следећем теоремом:

Теорема 17 *За дата пројективна разрешења F и F' модула M, постоји ланчано пресликавање $f : F \to F'$ које чува проширење (тј. задовољава $\varepsilon' f_0 = \varepsilon$), јединствено до хомотопије, и f је хомотопска еквиваленција.*

Доказ: Размотримо следећи дијаграм:

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & F_1 & \longrightarrow & F_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \vdots & & \vdots & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow \\ \ldots & \longrightarrow & F'_1 & \longrightarrow & F'_0 & \xrightarrow{\varepsilon'} & M & \longrightarrow & 0. \end{array}$$

Примењујемо Лему 16 на проширена разрешења F и F' са $r = -1$ и пресликавањем $f_{-1} = \mathrm{id}_M$. Закључујемо да постоји (јединствено до на хомотопију) ланчано пресликавање $f : F \to F'$ које чува проширење јер је $\varepsilon' f_0 = \mathrm{id}_M \varepsilon = \varepsilon$. Штавише, закључујемо да је f јединствено до на хомотопију. Аналогно, имамо пресликавање које чува проширење $f' : F' \to F$. Сада, како су $f'f$ и id_F оба проширења id_M између две копије F, према другом делу леме 16, имамо $f'f \simeq \mathrm{id}_F$. Слично, имамо $ff' \simeq \mathrm{id}_{F'}$. Дакле, f је заиста хомотопска еквиваленција. □

4 Кохомологија група

4.1 Кохомолошке и хомолошке групе групе

Нека је G група и нека је $\varepsilon : F \to \mathbb{Z}$ пројективно разрешење $\mathbb{Z}$ над Λ. Дефинишемо кохомолошку и хомолошку групу од G респективно са

$$H^iG = H^i(F^G),\ H_iG = H_i(F_G).$$

Инваријантни и коинваријантни функтори $(\_)^G$ и $(\_)_G$ су адитивни, тј. за било које $\psi, \phi : A \to A'$, имамо $(\psi+\phi)^G = \psi^G+\phi^G$ и $(\psi+\phi)_G = \psi_G+\phi_G$. Ово следи из алтернативних дефиниција користећи Hom и тензорски функтор респективно, тј. $(\_)^G = \mathrm{Hom}_\Lambda(\mathbb{Z}, \_)$ и $(\_)_G = \mathbb{Z} \otimes_\Lambda \_$. Дакле, ови функтори чувају ланчане хомотопије. Заиста, претпоставимо да је $\varphi : F \to F'$ ланчана хомотопија од ψ до ϕ, тј. $d'\varphi + \varphi d = \psi - \phi$. Затим, када применимо функтор на обе стране ове једначине, имамо

$$\begin{aligned} (d'\varphi + \varphi d)^G &= (\psi - \phi)^G \\ (d'\varphi)^G + (\varphi d)^G &= \psi^G - \phi^G \\ d'^G\varphi^G + \varphi^G d^G &= \psi^G - \phi^G. \end{aligned}$$

Дакле, φ^G је ланчана хомотопија од ψ^G до ϕ^G. Аналогно, φ_G је ланчана хомотопија од ψ_G до ϕ_G.

Претпоставимо да имамо друго слободно разрешење $\varepsilon' : F' \to \mathbb{Z}$ од $\mathbb{Z}$ над Λ. Према теореми 17, постоји хомотопска еквиваленција која чува проширење $f : F \to F'$. Према горњем резоновању, $f^G : F^G \to F'^G$ и $f_G : F_G \to F'_G$ су такође хомотопске еквиваленције. Стога, наше дефиниције H^iG и H_iG не зависе од избора пројективног разрешења $\varepsilon : F \to \mathbb{Z}$.

Кохомолошке и хомолошке групе од G увек постоје, због постојања слободног разрешења. Конкретно, можемо узети стандардно разрешење, или преградно разрешење, или неко повољно разрешење инспирисано топологијом, итд.

Са тачке гледишта топологије, размотримо $K(G,1)$-комплекс Y са универзалним покривачем X. Према ставу 10, $C_*(X)$ је слободно разрешење од $\mathbb{Z}$ над Λ. Простор Y је орбитални комплекс од X, стога је $C_*(X)_G \cong C_*(Y)$ према ставу 8. Дакле, рачунајући хомологије обе стране, добијамо:

Став 18 *Ако је Y $K(G,1)$-комплекс, онда је $H_*G \cong H_*Y$.*

4.2 Тачност функтора Hom и тензорског производа

Да бисмо израчунали кохомологију и хомологију са коефицијентима у Λ-модулу A уместо у $\mathbb{Z}$, применићемо функторе $\mathrm{Hom}_\Lambda(\_, A)$ и $\_ \otimes_\Lambda A$ на

пројективно разрешење редом и израчунаћемо хомологију ових ланчаних комплекса. Ово поглавље је посвећено неколиким основним својствима ових функтора.

Као што смо видели у претходном одељку, ови функтори су адитивни и чувају ланчане хомотопије. Сада ћемо испитати како се понашају на кратким тачним низовима. Претпоставимо, у остатку овог одељка, да је A дати леви R-модул.

Лема 19 *Контраваријантни функтор* $\mathrm{Hom}_R(\_, A)$ *је лево тачан на категорији левих* R*-модула. То јест, ако је*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

кратак тачан низ левих R *модула, низ*

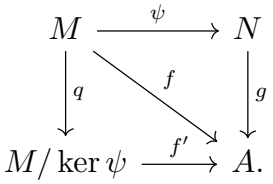
$$0 \longrightarrow \mathrm{Hom}_R(N, A) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, A) \xrightarrow{\phi^*} \mathrm{Hom}_R(L, A)$$

је тачан у категорији Абелових група.

Доказ: За елемент $f \in \mathrm{Hom}_R(M, A)$, слика елемента f при ϕ^* је дефинисана у свакој тачки $a \in A$ као $(\phi^* f)(a) = f(\phi(a))$, тј. $\phi^* f = f\phi$. Слично за ψ^*.

Прво ћемо показати да је $\ker \psi^* = 0$. Претпоставимо да је $f \in \ker \psi^*$, тј. $\psi^* f = 0$. Дакле, $f\psi = 0$. Следи, $\mathrm{im}\, \psi \subseteq \ker f$. Како је $\mathrm{im}\, \psi = N$, према тачности првог низа, то значи $f(n) = 0$ за све $n \in N$, тј. $f = 0$.

Покажимо сада да је $\ker \phi^* = \mathrm{im}\, \psi^*$. Прво, за елемент $f \in \mathrm{Hom}_R(M, A)$, $\phi^*\psi^* f = \phi^* f\psi = f\psi\phi = 0$, тј. $\mathrm{im}\, \psi^* \subseteq \ker \phi^*$. Сада ћемо показати супротну инклузију. Претпоставимо да је $f \in \ker \phi^*$, тј. $\phi^* f = 0$. То значи $f\phi = 0$, по чему је $\mathrm{im}\, \phi \subseteq \ker f$. Како је $\mathrm{im}\, \phi = \ker \psi$ према тачности почетног низа, то значи $\ker \psi \subseteq \ker f$. Дакле, f можемо третирати као композицију количничког пресликавања $q : M \to M/\ker \psi$, дефинисаног преко ψ, и $f' : M/\ker \psi \to A$. Како је $M/\ker \psi \cong N$, можемо заменити $M/\ker \psi$ са N у горњим пресликавањима, па добијамо пресликавања $\psi : M \to N$ и $g : N \to A$, помоћу којих имамо $f = g\psi = \psi^* g$. Према томе, $f \in \mathrm{im}\, \psi^*$. Дакле, $\ker \phi^* = \mathrm{im}\, \psi^*$.



□

Сличну причу имамо и за функторе тензорског производа, само што су десно тачни уместо лево. Доказ је веома сличан као код Hom функтора, иако мало сложенији.

Лема 20 *Коваријантни функтор* $\_ \otimes_R A$ *је десно тачан на категорији десних* R*-модула. То јест, ако*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

је кратак тачан низ десних R *модула, низ*

$$L \otimes_R A \xrightarrow{\phi_*} M \otimes_R A \xrightarrow{\psi_*} N \otimes_R A \longrightarrow 0$$

је тачан у категорији Абелових група.

Доказ: Индуковани хомоморфизми су дефинисани као $\phi_* = \phi \otimes \mathrm{id}_A$ и $\psi_* = \psi \otimes \mathrm{id}_A$. Ово је очигледно добро дефинисано.

Прво ћемо да покажемо $\operatorname{im}\psi_* = N \otimes_R A$. Прости тензори $m \otimes_R a \in M \otimes_R A$ се пресликавају у $\psi_*(m \otimes_R a) = \psi(m) \otimes_R a$. Дакле, због линеарности ψ_*, $\operatorname{im}\psi_*$ је генерисан свим таквим елементима, тј. $\operatorname{im}\psi_* = \operatorname{im}\psi \otimes_R A$. Пошто је ψ сурјективан, тј. $\operatorname{im}\psi = N$, то значи да је $\operatorname{im}\psi_* = N \otimes_R A$.

Сада, покажимо $\ker\psi_* = \operatorname{im}\phi_*$. Пре свега, њихова композиција је 0: за било који једноставан тензор $l \otimes_R a \in L \otimes_R A$,

$$\psi_*\phi_*(l \otimes_R a) = \psi(\phi(l) \otimes_R a) = \psi\phi(l) \otimes_R a = 0.$$

Ово се линарно проширује на остатак $L \otimes_R A$, и стога је $\psi_*\phi_* = 0$, тј. $\operatorname{im}\phi_* \subseteq \ker\psi_*$.

Даље, размотримо $(M \otimes_R A)/\ker\psi_*$ и $(M \otimes_R A)/\operatorname{im}\phi_*$. Како је $\operatorname{im}\phi_* \subseteq \ker\psi_*$, имамо природни хомоморфизам из $(M \otimes_R A)/\operatorname{im}\phi_*$ у $(M \otimes_R A)/\ker\psi_*$. Овај хомоморфизам је изоморфизам ако и само ако је $\operatorname{im}\phi_* = \ker\psi_*$. Стога ћемо да покажемо да је овај хомоморфизам заиста изоморфизам.

Према првој теореми о изоморфизму, имамо $(M \otimes_R A)/\ker\psi_* \cong \operatorname{im}\psi_* = N \otimes_R A$. Сада, аналогно првом делу доказа, имамо $\operatorname{im}\phi_* = \operatorname{im}\phi \otimes_R A$. Према тачности првог низа, $\operatorname{im}\phi = \ker\psi$, па је $(M \otimes_R A)/\operatorname{im}\phi_* = (M \otimes_R A)/(\ker\phi \otimes_R A)$.

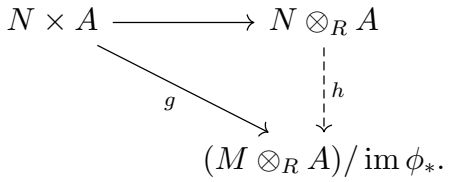
Како је $\operatorname{im}\phi_* \subseteq \ker\psi_*$, можемо да разлажемо ψ_* као

$$M \otimes_R A \xrightarrow{q} (M \otimes_R A)/\operatorname{im}\phi_* \xrightarrow{f} N \otimes_R A$$

где је q количничко пресликавање и f је дефинисано на следећи начин: како је било који елемент у $(M \otimes_R A)/\operatorname{im}\phi_*$ облика $q(t)$ за неко $t \in M \otimes_R A$,

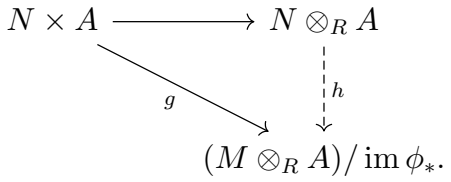
дефинишемо f на $q(t)$ као $\psi_*(t)$. Заиста, ако је $q(t') = q(t)$ за неко $t \in M \otimes_R A$, онда је $q(t' - t) = 0$ тј. $t' - t \in \ker q = \operatorname{im} \phi_*$. Међутим, $\operatorname{im} \phi_* \subseteq \ker \psi_*$, па је $\psi_*(t'-t) = 0$, и стога $f(t) = f(t')$, тако да је f добро дефинисано. Ако можемо да покажемо да је f изоморфизам, онда бисмо добили $(M \otimes_R A)/\operatorname{im} \phi_* \cong N \otimes_R A \cong (M \otimes_R A)/\ker \psi_*$, као што нам је и потребно.

Пронађимо инверз од f. То ћемо урадити користећи универзално својство тензорског производа. Размотримо следећи дијаграм:



На основу универзалног својства тензорског производа, ако је g билинеарно пресликавање, онда постоји пресликавање h које чини дијаграм комутативним.

Пронађимо инверз од f. То ћемо урадити користећи универзално својство тензорског производа. Размотримо следећи дијаграм:



На основу универзалног својства тензорског производа, ако је g билинеарно пресликавање, онда постоји пресликавање h које чини дијаграм комутативним.

Дефинишимо g са $(n, a) \mapsto q(m \otimes_R a)$, за све $(n, a) \in N \times A$, где је m неки елемент од M такав да је $\psi(m) = n$. Прво проверимо да ли је ово пресликавање добро дефинисано. Претпоставимо да за неко друго $m' \in M$ такође имамо $\psi(m') = n$. То значи $\psi(m') = \psi(m)$, па је $m' - m \in \ker \psi$. Дакле, $(m' - m) \otimes_R a \in \ker \psi \otimes_R A$. Сада, аналогно самом првом делу доказа, имамо $\operatorname{im} \phi_* = \operatorname{im} \phi \otimes_R A$. По тачности почетног низа је $\operatorname{im} \phi = \ker \psi$, и стога $(m' - m) \otimes_R a \in \operatorname{im} \psi_*$. Дакле, значи да је $q(m' \otimes_R a) = q(m \otimes_R a)$. Према томе, $g(n)$ има јединствену слику, па је g добро дефинисан.

Да бисмо користили универзално својство, морамо такође показати да је g билинеарно пресликавање. Претпоставимо да су $n, n' \in N$ и $a, a' \in A$. Нека су $m, m' \in M$ неки елементи из M такви да је $\psi(m) = n$ и $\psi(m') = n'$. То значи да је $\psi(m + m') = n + n'$. Дакле, имамо

$$g(n + n', a) = q((m + m') \otimes_R a) = q(m \otimes_R a) + q(m' \otimes_R a) = g(n, a) + g(n', a)$$

и

$$g(n, a+b) = q(m \otimes_R (a+b)) = q(m \otimes_R a) + q(m \otimes_R b) = g(n,a) + g(n,b).$$

Такође, за било који $r \in R$,

$$g(n \cdot r, a) = q(m \cdot r \otimes_R a) = q(m \otimes_R r \cdot a) = g(n, r \cdot a).$$

Стога је g билинеарно. Према томе, на основу универзалног својства, имамо добро дефинисано пресликавање $h : N \otimes_R A \to (M \otimes_R A)/\operatorname{im}\phi_*$ дефинисано са $h : n \otimes_R a \mapsto q(m \otimes a)$ на свим једноставним тензорима $n \otimes_R a \in N \otimes_R A$ са $m \in M$ таквим да је $\psi(m) = n$.

Покажимо сада да су ова пресликавања, h и f инверзи. Претпоставимо да је $n \otimes_R a \in N \otimes_R A$, и $m \in M$ такви да је $\psi(m) = n$. Тада,

$$f \circ h(n \otimes_R a) = f(q(m \otimes_R a)) = \psi_*(m \otimes_a) = \psi(m) \otimes_a = n \otimes_a$$

Са друге стране, размотримо неки елемент $q(m \otimes_R a) \in M \otimes_R A/\operatorname{im}\phi_*$. Сада,

$$h \circ f(q(m \otimes_R a)) = h(\psi_*(m \otimes_R a)) = h(\psi_*(m) \otimes_R a) = q(m \otimes_R a).$$

Дакле, f и h су инверзи, а стога су изоморфизми. □

Такође важи да је за десни R-модул A, функтор $\operatorname{Hom}_R(\_, A)$ лево тачан на категорији десних R-модула, а $A \otimes_R \_$ је десно тачан на категорији левих R-модула. Докази ових тврдњи су потпуно аналогни претходним доказима.

Лема 2 је директан резултат леме 19, као $A^G \cong \operatorname{Hom}_\Lambda(\mathbb{Z}, A)$. Слично, лема 3 је директан резултат леме 20, као $A_G \cong \mathbb{Z} \otimes_\Lambda A$.

На пројективним модулима, резултати претходне две леме могу да се даље усаврше.

Став 21 *Функтор* $\operatorname{Hom}_R(\_, A)$ *је тачан на категорији пројективних модула. То јест, ако је*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

кратак тачан низ пројективних левих R *модула, онда је низ*

$$0 \longrightarrow \operatorname{Hom}_R(N, A) \xrightarrow{\psi^*} \operatorname{Hom}_R(M, A) \xrightarrow{\phi^*} \operatorname{Hom}_R(L, A) \longrightarrow 0$$

тачан у категорији Абелових група.

Доказ: Лемом 19 имамо да је добијени низ лево тачан, тако да је једино преостало да се докаже да је ϕ^* сурјекција.

Према леми 14, како је N пројективан, имамо да се почетни низ цепа. Према томе, постоји сурјекција $r : M \to L$ таква да је $r\phi = \mathrm{id}_L$. Дакле, за било коју $f \in \mathrm{Hom}_R(L, A)$, нека је $g = fr$. Тада добијамо

$$\phi^*(fr) = fr\phi = f\mathrm{id}_L = f.$$

Дакле, $f \in \mathrm{im}\,\phi^*$, и стога је ϕ^* сурјекција. □

Став 22 *Функтор* $\_ \otimes_R A$ *је тачан у категорији пројективних модула. То јест, ако је*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

кратак тачан низ пројективних левих R *модула, онда је низ*

$$0 \longrightarrow L \otimes_R A \xrightarrow{\psi_*} M \otimes_R A \xrightarrow{\phi_*} N \otimes_R A \longrightarrow 0$$

тачан у категорији Абелових група.

Доказ: Лемом 20 имамо да је низ десно тачан, тако да је једино преостало да се докаже да је ϕ_* инјективан.

Према леми 14, како је N пројективан, имамо да се почетни низ раздваја. Дакле, постоји сурјекција $r : M \to L$ таква да је $r\phi = \mathrm{id}_L$. Сада имамо

$$r_*\phi_* = (r \otimes_R \mathrm{id}_A) \circ (\phi \otimes_R \mathrm{id}_A) = r\phi \otimes_R \mathrm{id}_A = \mathrm{id}_L \otimes_R \mathrm{id}_A = \mathrm{id}_{L \otimes_R A}$$

Дакле, r_* је леви инверз од ϕ_*, па је ϕ_* инјекција. □

Када је неки адитивни функтор тачан, он не само да чува тачност кратких низова, већ и тачне низове произвољних дужина, као што и само име имплицира. Штавише, он заправо комутира са функтором хомологије на било ком ланчаном комплексу.

Став 23 *Претпоставимо да имамо ланчани комплекс* (C_*, ∂_*)*:*

$$\cdots \to C_{k+1} \xrightarrow{\partial_{k+1}} C_k \xrightarrow{\partial_k} C_{k-1} \to \dots$$

Онда, за ланчани комплекс

$$\cdots \to FC_{k+1} \xrightarrow{F\partial_{k+1}} FC_k \xrightarrow{F\partial_k} FC_{k-1} \to \dots$$

имамо

$$H_k(FC) = FH_k(C).$$

Доказ: Нека F и C буду као горе. Пре свега, имамо

$$\operatorname{im} F\partial_{k+1} = F \operatorname{im} \partial_{k+1}.$$

Затим, размотримо кратак тачан низ

$$0 \to \ker \partial_k \xrightarrow{i_k} C_k \xrightarrow{\partial_k} \operatorname{im} \partial_k \to 0.$$

Како је F тачан, онда је и следећи низ такође кратак тачан низ:

$$0 \to F \ker \partial_k \xrightarrow{Fi_k} FC_k \xrightarrow{F\partial_k} F \operatorname{im} \partial_k \to 0.$$

Дакле,

$$\ker F\partial_k = F \ker \partial_k.$$

Сада, размотримо кратки тачан низ који дефинише k-ту хомолошку групу:

$$0 \to \operatorname{im} \partial_{k+1} \xrightarrow{j_k} \ker \partial_k \xrightarrow{\pi_k} H_k(C) \to 0.$$

Поново, како је F тачан, онда је следећи низ такође кратак тачан низ:

$$0 \to F \operatorname{im} \partial_{k+1} \xrightarrow{Fj_k} F \ker \partial_k \xrightarrow{F\pi_k} FH_k(C) \to 0.$$

Дакле, по тачности, имамо

$$\frac{F(\ker \partial_k)}{F(\operatorname{im} \partial_{k+1})} \cong FH_k(C).$$

Када спојимо све резултате, добијамо

$$H_k(FC) = \frac{\ker F\partial_k}{\operatorname{im} F\partial_{k+1}} \cong \frac{F \ker \partial_k}{F \operatorname{im} \partial_{k+1}} \cong FH_k(C).$$

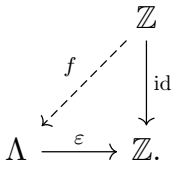
□

Како су код тачних низова све групе хомологије 0, ова лема показује да исто важи и за комплекс који се добија применом тачног функтора. Дакле, тачни функтори чувају тачне низове.

Ставови 21 и 22 показују да су Hom и тензорски производ функтори тачни у категорији пројективних модула. Међутим, раније смо рекли да ћемо дефинисати групе кохомологије и хомологије групе G као примене тих функтора редом на пројективно разрешење $\mathbb{Z}$ над Λ. Ово би могло довести до забуне, јер смо управо показали да, према ставу 23, тачни функтори чувају тачност низова, што би значило да су кохомологија и хомологија тривијалне. Међутим, кључна ствар је да $\mathbb{Z}$ *није* пројективан, као Λ-модул. Стога, кохомолошке и хомолошке групе не морају бити тривијалне.

Пример 4 *За нетривијалну G, Λ-модул $\mathbb{Z}$ са тривијалном G-структуром није пројективни Λ-модул.*

Размотримо следећи дијаграм:



Овде је ε пресликавање проширења. Претпоставимо да је $\mathbb{Z}$ пројективни Λ-модул. То би подразумевало постојање Λ-модул хомоморфизма $f : \mathbb{Z} \to \Lambda$ који чини горњи дијаграм комутативним, тј. $\varepsilon f = \mathrm{id}$. Нека означимо $a = f(1)$. Сада, за произвољни $g \in G$, имамо

$$g \cdot a = g \cdot f(1) = f(g \cdot 1) = f(1) = a,$$

чиме је $a \in \Lambda^G$. Ако напишемо $a = \sum_{i=1}^{n} k_i g_i$ за $n \geq 1$, $k_i \in \mathbb{Z}$, $g_i \in G$, онда како је $g \cdot a = a$ за све $g \in G$, то значи да су сви k_i, $i \leq n$ идентични. То такође значи да за сваки елемент $g \in G$ постоји неко $i \leq n$ такво да је $g = g_i$, стога G мора бити коначна и $n = |G|$. Дакле, имамо $a = k \sum_{g \in G} g$. Међутим, како је $\varepsilon f = \mathrm{id}$, то значи да је $\varepsilon a = 1$, тј. $k|G| = 1$. Значи, $k = |G| = 1$, што је контрадикција.

4.3 Кохомологија група са коефицијентима

Показали смо у леми 2 да је инваријантни функтор $(\_)^G$ лево тачан као функтор, али не да је тачан функтор. Конкретно, није доказано да је ψ^G епиморфизам попут ψ. Генерално, ово и не мора бити тачно. То је мотивација за дефинисање $H^1(G, A)$, прве кохомолошке групе G са коефицијентима у A, као мере неуспеха десне тачности функтора подмодула инваријанте. То се ради узимањем пројективног разрешења $\mathbb{Z}$ над Λ и применом функтора $\mathrm{Hom}(\_, A)$. Последњи (или, сада, први) ненула члан резултујућег комплекса ће бити $\mathrm{Hom}(\mathbb{Z}, A)$, што је, према једначини (1), A^G. Хомологија овог низа ће да прати следеће аксиоме, које јединствено одређују ово кохомолошко проширење:

Дефиниција 7 *Кохомолошке групе групе G са коефицијентима у A, означене са $H^k(G, A)$, $k \geq 0$, чине коваријантну фамилију функтора из $\mathcal{U}_G$, категорије G-модула, у категорији Абелових група, са следећим својствима:*

1. $H^0(G, A) = A^G$

2. *За сваки кратак тачан низ* $0 \to A \to B \to C \to 0$ *у* $\mathcal{U}_G$ *постоји природна трансформација* $\delta = \delta^k : H^k(G, C) \to H^{k+1}(G, A)$ *и дугачак тачан низ кохомолошких група*

$$\cdots \longrightarrow H^k(G, A) \xrightarrow{\phi^*} H^k(G, B) \xrightarrow{\psi^*} H^k(G, C) \xrightarrow{\delta} H^{k+1}(G, A) \longrightarrow \dots$$

3. *Ако је* A *коиндуковани модул, онда је* $H^k(G, A) = 0$ *за све* $k \geq 1$.

Фамилија $\{H^k(G, \cdot),\ k \geq 0\}$ се стога може сматрати кохомолошком проширењем функтора инваријантних елемената, које се поништи на коиндукованим модулима. Покажимо да ово проширење заиста постоји и да је јединствено.

Теорема 24 *Кохомолошко проширење* $H^k(G, *)$, $k \geq 0$ *постоји и јединствено је.*

Доказ: Нека је

$$\cdots \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow \dots \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

пројективно разрешење тривијалног G-модула $\mathbb{Z}$. За било који G-модул A, имамо коланчани комплекс

$$\cdots \leftarrow \mathrm{Hom}_G(P_k, A) \leftarrow \mathrm{Hom}_G(P_{k-1}, A) \leftarrow \dots \leftarrow \mathrm{Hom}_G(P_0, A) \leftarrow A^G \leftarrow 0.$$

где смо заменили $\mathrm{Hom}_G(\mathbb{Z}, A)$ са A^G, по једначини (1). Композиција два узастопна хомоморфизма у коланчаном комплексу је нула, и стога можемо дефинисати кохомолошке групе са

$$H^k(G, A) = H_k(\mathrm{Hom}_G(P_k, A)).$$

Функтор $\mathrm{Hom}_G(\_, A)$ је адитивни, и стога чува хомотопије ланца. Дакле, истим аргументом као и за интегралну кохомологију, кохомолошке групе не зависе од избора пројективног разрешења.

Постојање природних когранични хомоморфизама δ^k и дугог тачног низа из друге тачке дефиниције следи уобичајеном потером по дијаграму. Прво својство је задовољено прихватањем конвенције да су 0-димензионалне когранице тривијалне. Да бисмо ово утврдили, размотримо реп коланчаног комплекса

$$\cdots \longleftarrow \mathrm{Hom}_G(P_1, A) \xleftarrow{d^1} \mathrm{Hom}_G(P_0, A) \xleftarrow{d^0} A^G \longleftarrow 0.$$

Постављањем $d^0 = 0$, имамо $H^0(G, A) = \ker d^1$. Остатак овог прорачуна одлажемо за касније, где ћемо користити преградно разрешење. Уместо

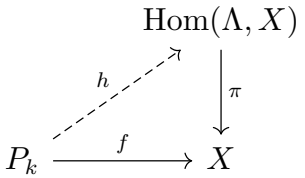
тога, прво ћемо показати треће својство, да кохомологија нестаје на коиндукованим модулима.

Нека је $A = \mathrm{Hom}(\Lambda, X)$ коиндуковани модул, где X има тривијално G-дејство. Прво ћемо показати да

$$\mathrm{Hom}_G(P_k, \mathrm{Hom}(\Lambda, X)) \cong \mathrm{Hom}_{\mathbb{Z}}(P_k, X).$$

Дефинишимо пресликавање $\pi : \mathrm{Hom}(\Lambda, X) \to X$ са $\pi(\varphi) = \varphi(1)$ за све $\varphi \in \mathrm{Hom}(\Lambda, X)$. Ово пресликавање је очигледно сурјекција.

Претпоставимо $f \in \mathrm{Hom}(P_k, X)$, тј. $f : P_k \to X$. Желимо да покажемо да за сваки такав f постоји јединствени Λ-модул хомоморфизам $h : P_k \to \mathrm{Hom}(\Lambda, X)$. Прецизније, показаћемо следеће универзално својство: у следећем проблему допуњавања дијаграма



увек постоји јединствени h тако да дијаграм комутира, тј. $\pi h = f$.

Претпоставимо да такав h постоји, који шаље елементе $z \in P_k$ у хомоморфизме $h_z : \Lambda \to X$. Пошто је у питању Λ-модул хомоморфизам, мора задовољити

$$g \cdot h_z = h_{g \cdot z}$$

за све $z \in P_k$. То су елементи $\mathrm{Hom}(\Lambda, X)$, тј. хомоморфизми од Λ до X, тако да можемо израчунати обе стране за вредност 1:

$$(g \cdot h_z)(1) = g \cdot h_z(g^{-1}) = h_z(g^{-1}),$$

и

$$h_{g \cdot z}(1) = \pi(h_{g \cdot z}) = f(g \cdot z).$$

Дакле, заменом g са g^{-1}, добијамо

$$h_z(g) = f(g^{-1} \cdot z).$$

Стога, такав h је јединствено дефинисан на целом P_k. Хомоморфизам h заиста и постоји по овој наведеној конструкцији, јер се та пресликавања линеарно проширују на цело Λ. Дакле, показали смо

$$\mathrm{Hom}_G(P_k, \mathrm{Hom}(\Lambda, X)) \cong \mathrm{Hom}(P_k, X).$$

Пројективни G-модул P_k је слободан, а самим тим и пројективан, над $\mathbb{Z}$. Дакле, разрешење се може третирати као тачан низ пројективних $\mathbb{Z}$-модула,

а према ставовима 21 и 23, примена $\mathrm{Hom}(\_, X)$ на пројективно разрешење чува тачност. Дакле, за $k \geq 1$, важи

$$H^k(G, \mathrm{Hom}(\Lambda, X)) = 0.$$

До сада смо имали за циљ да покажемо да постоји кохомолошко проширење које испуњава сва три својства. Да бисмо показали јединственост, да су било која два таква проширења изоморфна, користимо технику која се зове померање димензије (eng. dimension shifting), засновану на индукцији.

У димензији 0, имамо $H^0(G, A) \cong A^G$, па је јединственост у димензији 0 очигледна. Индуктивно претпоставимо да смо доказали јединственост до димензије $k-1$. Доказаћемо јединственост $H^k(G, A)$ тиме што ћемо да покажемо да је изоморфна некој $(k-1)$-димензионалној кохомолошкој групи $H^{k-1}(G, \bar{A})$, која је јединствена по индуктивној хипотези.

Размотримо $\bar{A}$ дефинисан кратким тачним низом

$$0 \longrightarrow A \longrightarrow \mathrm{Hom}(\Lambda, A_0) \longrightarrow \bar{A} \longrightarrow 0,$$

где је A_0 $\mathbb{Z}$-модул структура A у основи. По другом својству, изводимо следећи дугачак тачан низ:

$$\ldots \xrightarrow{\delta^{k-2}} H^k(G, A) \longrightarrow H^{k-1}(G, \mathrm{Hom}(\Lambda, A_0)) \longrightarrow H^{k-1}(G, \bar{A}) \xrightarrow{\delta^{k-1}}$$

$$\xrightarrow{\delta^{k-1}} H^k(G, A) \longrightarrow H^k(G, \mathrm{Hom}(\Lambda, A_0)) \longrightarrow H^k(G, \bar{A}) \xrightarrow{\delta^k} \ldots$$

Сада, користећи треће својство, да кохомолошко проширење нестаје на коиндукованим модулима, имамо $H^k(G, \mathrm{Hom}(\Lambda, A_0)) = H^{k-1}(G, \mathrm{Hom}(\Lambda, A_0)) = 0$. Стога нам остаје следећи кратак тачан низ:

$$0 \longrightarrow H^{k-1}(G, \bar{A}) \xrightarrow{\delta^{k-1}} H^k(G, A) \longrightarrow 0.$$

Дакле, $H^k(G, A) \cong H^{k-1}(G, \bar{A})$. Треба напоменути да се треће својство односи на димензије 1 и више, па је δ^0 само епиморфизам. Међутим, ово је довољно, јер ће $H^1(G, A)$ бити јединствено дефинисано којезгром од δ^0.

Стога је, индукцијом, кохомолошко проширење јединствено.

Завршимо сада прорачуне за прво својство које смо оставили за касније. Када смо дефинисали стандардно разрешење, увели смо појам преградне нотације и разрешења. Слична нотација се може увести за коланчани комплекс. Размотримо коланчани комплекс

$$\cdots \leftarrow \mathrm{Hom}_G(\bar{P}_k, A) \leftarrow \mathrm{Hom}_G(\bar{P}_{k-1}, A) \leftarrow \ldots \leftarrow \mathrm{Hom}_G(\bar{P}_0, A) \leftarrow A^G.$$

Како је $B_k = G \times \cdots \times G$ ($(k+1)$ копија од G) база за $\bar{P}_k$, можемо идентификовати коланац у $\mathrm{Hom}_\Lambda(\bar{P}_k, A)$ са функцијом

$$f : B_k \longrightarrow A,$$

која, да би правилно дефинисала G-хомоморфизам, мора да задовољи:

$$g \cdot f(g_0, \ldots, g_k) = f(g \cdot (g_0, \ldots, g_k)) = f(gg_0, \ldots, gg_k)$$

за све $g, g_0, \ldots, g_k \in G$. Ово називамо условом еквиваријантности. Као базне елементе у односу на Λ уместо $\mathbb{Z}$ можемо узети $(k+1)$-торке са $g_0 = 1$. У ствари, можемо ограничити нашу пажњу на базу од k-торки

$$\widetilde{B_k} = \big\{ [g_1|g_2|\ldots|g_k] \;\big|\; g_i \in G,\ 1 \leq i \leq k \big\},$$

где означавамо

$$[g_1|g_2|\ldots|g_k] = (1, g_1, g_1g_2, \ldots, g_1g_2\ldots g_k).$$

Функција дефинисана на B_k, тј. на елементима облика $(g_0, g_1, \ldots, g_k)$, јасно дефинише функцију на $\widetilde{B_k}$, подскупу B где је $g_0 = 1$. Показаћемо да је и обрнуто тачно, функција на $\widetilde{B}$ се проширује на функцију на B_k која задовољава услов еквиваријантности. Нека је $\widetilde{f} : \widetilde{B_k} \to A$. Сада покушавамо да дефинишемо одговарајућу функцију $f : B_k \to A$. Из G-дејства на B имамо

$$g \cdot (g_0, \ldots, g_k) = (gg_0, \ldots, gg_k),$$

где ако поставимо $g = g_0^{-1}$ имамо

$$g_0^{-1} \cdot (g_0, \ldots, g_k) = (1, g_0^{-1}g_1, \ldots, g_0^{-1}g_k).$$

Десна страна је елемент у $\widetilde{B_k}$:

$$\begin{aligned} (1, g_0^{-1}g_1, \ldots, g_0^{-1}g_k) &= [h_1|h_2|\cdots|h_k] \\ &= (1, h_1, h_1h_2, \ldots, h_1\ldots h_k). \end{aligned}$$

Одавде имамо систем од k једначина:

$$\begin{aligned} g_0^{-1}g_1 &= h_1 \\ g_0^{-1}g_2 &= h_1h_2 \\ \vdots &\quad \vdots \\ g_0^{-1}g_k &= h_1\ldots h_k. \end{aligned}$$

Заменом сваког реда у следећи имамо:

$$\begin{aligned} g_0^{-1}g_1 &= h_1 \\ g_0^{-1}g_2 &= g_0^{-1}g_1h_2 \\ \vdots &\quad \vdots \\ g_0^{-1}g_k &= g_0^{-1}g_{k-1}h_k. \end{aligned}$$

Значи,

$$\begin{aligned} h_1 &= g_0^{-1}g_1 \\ h_2 &= g_1^{-1}g_2 \\ \vdots &\quad \vdots \\ h_k &= g_{k-1}^{-1}g_k, \end{aligned}$$

а одавде добијамо

$$(g_0, \ldots, g_k) = g_0 \cdot [g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k].$$

Дакле, дефинишемо $f : B_k \to A$ тачка по тачка као

$$f(g_0, \ldots, g_k) := g_0 \cdot \widetilde{f}[g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k].$$

Узгред, напомињемо да имамо G-дејство дефинисано само на A, а не на B_k или $\widetilde{B_k}$. Можемо сада да видимо да такво пресликавање испуњава услов еквиваријантности:

$$\begin{aligned} g \cdot f(g_0, \ldots, g_k) &= g \cdot \left(g_0 \cdot \widetilde{f}[g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k]\right) \\ &= (gg_0) \cdot \widetilde{f}[g_0^{-1}g^{-1}gg_1|g_1^{-1}g^{-1}gg_2|\cdots|g_{k-1}^{-1}g^{-1}gg_k] \\ &= (gg_0) \cdot \widetilde{f}[(gg_0)^{-1}(gg_1)|(gg_1)^{-1}(gg_2)|\cdots|(gg_{k-1})^{-1}(gg_k)] \\ &= f(gg_0, gg_1, \ldots, gg_k) \end{aligned}$$

Дакле, показали смо да коланци у $\mathrm{Hom}_\Lambda(\bar{P}_k, A)$ одговарају функцијама које пресликавају k-торке $(g_1, \ldots, g_k)$ у A. Сада ћемо да видимо како гранични хомоморфизам d^* делује на такве функције, користећи граничну формулу за преградно разрешење.

$$\begin{aligned} d_*f[g_1|\ldots|g_{k+1}] &= fd[g_1|\ldots|g_k] \\ &= g_1 \cdot f[g_2|\ldots|g_{k+1}] \\ &\quad + \sum_{j=1}^{k}(-1)^j f[g_1|\ldots|g_jg_{j+1}|\ldots|g_{k+1}] \end{aligned}$$

$$
\begin{aligned}
& +(-1)^{k+1} f[g_1|\dots|g_k] \\
= \; & g_1 \cdot f[g_2|\dots|g_{k+1})] - f[g_1g_2|g_3|\dots|g_{k+1}] \\
& + f[g_1|g_2g_3|\dots|g_{k+1}] - \dots \\
& + (-1)^j f[g_1|\dots|g_jg_{j+1}|\dots|g_{k+1}] + \dots \\
& + (-1)^{k+1} f[g_1|\dots|g_k].
\end{aligned}
$$

У димензији 0 ово има облик

$$d^1 f[g_1] = g_1 \cdot f[\,] - f[g_1]$$

за све $g_1 \in G$, где је f тривијална константна функција, што значи да одговара елементу A. Дакле, језгро од d^1 одговара елементима A који су фиксирани свим елементима G, тј. A^G. Како је $\operatorname{im} d^0 = 0$, имамо

$$H^0(G, A) = \frac{\ker d^1}{\operatorname{im} d^0} \cong A^G,$$

задовољавајући својство 1. □

Користили смо стандардно разрешење да бисмо доказали постојање дотичног кохомолошког проширења. Међутим, није практично користити га за прорачуне. Уместо тога, покушавамо да пронађемо најбољи избор за групу која се проучава. Често је он повезан са тополошким просторима.

Нека сада користимо разрешења која смо израчунали у примеру 1 да израчунамо хомолошке групе.

Пример 5 *Кохомолошке групе за цикличне групе.*

Као и у примеру 1, означавамо са C_r^T нашу цикличну групу G реда $2 \le r \le \infty$, са генератором T, и поделићемо наш пример на случајеве када је ред бесконачан, односно коначан.

Случај 1: $r = \infty$. Користићемо слободно разрешење које смо конструисали у примеру 1:

$$0 \longrightarrow \mathbb{Z}C_\infty^S \longrightarrow \mathbb{Z}C_\infty^T \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

За произвољни G-модул A, имамо повезани низ

$$0 \xleftarrow{d^2} \operatorname{Hom}_G(\mathbb{Z}C_\infty^S, A) \xleftarrow{d^1} \operatorname{Hom}_G(\mathbb{Z}C_\infty^T, A) \longleftarrow 0.$$

Језгро $\ker d^1$ је скуп коланаца који задовољавају $d^1 f(S) = 0$. Међутим,

$$d^1 f_a(S) = f_a d_1(S) = f_a(T-1) = (T-1) \cdot a = T \cdot a - a.$$

Дакле, $T \cdot a = a$, и зато $a \in A^G$. Стога, $H^0(G, A) = A^G$, као и очекивано.

Идентификовањем a са $g_a : 1 \mapsto a$, видимо да је $\mathrm{Hom}_G(\mathbb{Z}C_\infty^T, A) = \mathrm{Hom}_G(\mathbb{Z}C_\infty^S, A) = A$. Према томе, $\ker d^2 = A$ и $\mathrm{im}\, d^1 = (T-1)A$, па је $H^1(G, A) = A/(T-1)A$. За $k \geq 2$, $H^2(G, A) = 0$. Дакле, кохомолошке групе су:

$$H^k(C_\infty^T, A) = \begin{cases} A^G, & k = 0, \\ \frac{A}{(T-1)A}, & k = 1, \\ 0, & k \geq 2. \end{cases}$$

Случај 2: $r < \infty$. Поново ћемо користити слободно разрешење које смо конструисали у примеру 1:

$$\ldots \xrightarrow{T-1} \Lambda_{(2k)} \xrightarrow{N} \Lambda_{(2k-1)} \xrightarrow{T-1} \ldots \xrightarrow{N} \Lambda_{(1)} \xrightarrow{T-1} \Lambda_{(0)} \longrightarrow \mathbb{Z}.$$

Одатле имамо коланчани комплекс:

$$\ldots \xleftarrow{T-1} \mathrm{Hom}_G(\Lambda_{(2k)}, A) \xleftarrow{N} \mathrm{Hom}_G(\Lambda_{2k-1}, A) \xleftarrow{T-1} \ldots$$

$$\ldots \xleftarrow{N} \mathrm{Hom}_G(\Lambda_{(1)}, A) \xleftarrow{T-1} \mathrm{Hom}_G(\Lambda_{(0)}, A) \xleftarrow{0} 0.$$

Као и у бесконачном случају, идентификовањем a са $g_a : 1 \mapsto a$, видимо да је $\mathrm{Hom}_G(\mathbb{Z}C_r^S, A) = A$. Коланчани комплекс записујемо у следећем облику:

$$\ldots \xleftarrow[d^{2k+1}]{T-1} A_{(2n)} \xleftarrow[d^{2k}]{N} A_{(2n-1)} \xleftarrow[d^{2k-1}]{T-1} \ldots \xleftarrow[d^2]{N} A_{(1)} \xleftarrow[d^1]{T-1} A_{(0)} \xleftarrow[d^0]{0} 0.$$

Сада само треба да израчунавамо кохомологију. Аналогно бесконачном случају, $H^0(G, A) = \ker d^1 = \ker(T-1)$ је скуп коланаца f_a који задовољавају $(T-1) \cdot a = 0$, или $T \cdot a = a$, стога $H^0(G, A) = A^G$. Користећи ово, такође имамо

$$H^{2k}(G, A) = \frac{\ker d^{2k+1}}{\mathrm{im}\, d^{2k}} = \frac{\ker T - 1}{\mathrm{im}\, N} = \frac{A^G}{NA}.$$

Коначно, израчунавамо

$$H^{2k-1}(G, A) = \frac{\ker d^{2k}}{\mathrm{im}\, d^{2k-1}} = \frac{\ker N}{(T-1)A}.$$

Дакле, кохомолошке групе су:

$$H_k(C_r^T, A) = \begin{cases} A^G, & k = 0, \\ \frac{A^G}{NA}, & 2 \mid k, \\ \frac{\ker N}{(T-1)A}, & 2 \nmid k. \end{cases}$$

4.4 Хомологија група са коефицијентима

Може да се прати сличан поступак као код кохомологије за дефинисање хомолошких група групе са коефицијентима. Сада, уместо да разматрамо инваријанте, користимо коинваријанте, уместо коиндукованих модула користимо индуковане модуле, а уместо Hom функтора $\mathrm{Hom}_G(\_, A)$ користимо функтор тензорског производа $\_ \otimes_\Lambda A$.

У леми 3, показано је да је функтор коинваријантних елемената $(\_)_G$ десно тачан, али не и тачан функтор. Конкретно, није доказано да је ϕ_G мономорфизам попут ϕ. Генерално, ово не мора бити тачно. То је мотивација за дефинисање $H_1(G, A)$, прве хомолошке групе од G са коефицијентима у A, као мера неуспеха леве тачности функтора коинваријанти.

Дефиниција 8 *Хомолошке групе групе G са коефицијентима у A, означене са $H_k(G, A)$, $k \geq 0$, формирају ковариjантну фамилију функтора из $\mathcal{U}_G$, категорије G-модула, у категорију Абелових група, са следећим својствима:*

1. $H_0(G, A) = A_G$
2. *За сваки кратак тачан низ $0 \to A \to B \to C \to 0$ у $\mathcal{U}_G$ постоји природна трансформација $\delta = \delta_k : H_k(G, C) \to H_{k-1}(G, A)$ и дугачак тачан низ кохомолошких група*

$$\cdots \longrightarrow H_k(G, A) \xrightarrow{\phi_*} H_k(G, B) \xrightarrow{\psi_*} H_k(G, C) \xrightarrow{\delta} H_{k-1}(G, A) \longrightarrow \ldots$$

3. *Ако је A индуковани модул, онда је $H_k(G, A) = 0$ за све $k \geq 1$.*

Фамилија $\{H_k(G, \cdot),\ k \geq 0\}$ се зато може сматрати као хомолошко проширење функтора коинваријанти, које нестаје на коиндукованим модулима.

Теорема 25 *Хомолошко проширење $H_k(G, *)$, $k \geq 0$ постоји и јединствено је.*

Доказ: Овај доказ је у великој мери аналоган доказу теореме 24. Нека

$$\cdots \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

буде пројективно разрешење тривијалног G-модула $\mathbb{Z}$. За било који G-модул A, формирамо ланчани комплекс

$$\cdots \to P_k \otimes_\Lambda A \longrightarrow P_{k-1} \otimes_\Lambda A \longrightarrow \ldots \longrightarrow P_0 \otimes_\Lambda A \longrightarrow A_G \longrightarrow 0.$$

где смо одмах заменили $\mathbb{Z} \otimes_\Lambda A$ са A_G, по једначини (2). Напоменимо да користимо десну структуру на P_k, тако да је $x \cdot g = g^{-1} \cdot x$ за све $g \in G$ и

$x \in P_k$. Композиција два узастопна хомоморфизма у ланчаном комплексу је нула, стога можемо дефинисати

$$H_k(G, A) = H_k(P_k \otimes_\Lambda A).$$

Функтор $\_ \otimes_\Lambda A$ је адитивни и стога чува ланчане хомотопије. Дакле, истим аргументом као и за интегралну хомологију, групе хомологија су независне од избора пројективног разрешења.

Постојање природних граничних хомоморфизама δ_k и дугог тачног низа из друге тачке дефиниције следи уобичајеном потером по дијаграму. Прво својство је задовољено конвенцијом да су 0-димензионалне границе тривијалне. Да бисмо ово утврдили, размотримо реп ланчаног комплекса

$$\cdots \to P_1 \otimes_\Lambda A \xrightarrow{d_1} P_0 \otimes_\Lambda A \xrightarrow{d_0} A_G \longrightarrow 0.$$

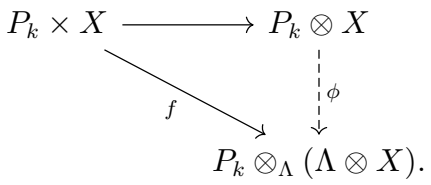
Постављањем $d_0 = 0$, имамо $H_0(G, A) = (P_0 \otimes_\Lambda A)/\operatorname{im} d_1$. Остатак овог прорачуна одлажемо за касније, где ћемо користити преградно разрешење. Покажимо треће својство, да хомологија нестаје на индукованим модулима.

Нека је $A = \Lambda \otimes X$ индуковани модул, где X има тривијално G-дејство. Прво ћемо показати да

$$P_k \otimes_\Lambda (\Lambda \otimes X) \cong P_k \otimes X.$$

Дефинишимо пресликавање $i : X \to \Lambda \otimes X$ са $i(x) = 1 \otimes x =$ за све $x \in X$. Ово пресликавање је очигледно инјекција.

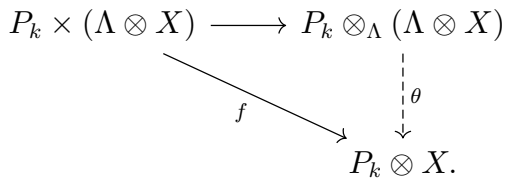
Користимо универзално својство тензорског производа $P_k \otimes_\Lambda (\Lambda \otimes X)$ на следећем дијаграму:



Према универзалном својству тензорског производа, ако је f билинеарно пресликавање, онда постоји пресликавање ϕ које чини дијаграм комутативним.

Дефинишимо f са $(z, x) \mapsto z \otimes_\Lambda (1 \otimes x)$, за све $z \in P_k$, $x \in X$. Ово пресликавање је очигледно билинеарно, стога је, према универзалном својству, пресликавање $\phi : z \otimes x \mapsto z \otimes_\Lambda (1 \otimes x)$ добро дефинисано на целом $P_k \otimes X$.

За обрнуто, употребимо универзално својство тензорског производа $P_k \otimes_\Lambda (\Lambda \otimes X)$ на следећем дијаграму:



На основу универзалног својства тензорског производа, ако је f билинеарно пресликавање, овог пута у односу на прстен Λ, онда постоји пресликавање θ које чини дијаграм комутативним.

Дефинишимо f са $(z, (\lambda \otimes x)) \mapsto z \cdot \lambda \otimes x$, за све $z \in P_k$, $\lambda \otimes \Lambda$, $x \in X$. Сада, покажимо да је f билинеарно. Нека је $z \otimes (\lambda \otimes x) \in P_k$ и $\mu \in \Lambda$ произвољно. Затим, имајући у виду да третирамо P_k као десни Λ-модул, имамо

$$f(z \cdot \mu, \lambda \otimes x) = (z \cdot \mu) \cdot \lambda \otimes x = z \cdot \mu\lambda \otimes x$$

и

$$f(z, \mu \cdot (\lambda \otimes x)) = f(z, \mu\lambda \otimes x) = z \cdot \mu\lambda \otimes x,$$

тј. $f(z \cdot \mu, \lambda \otimes x) = f(z, \mu \cdot (\lambda \otimes x))$.

Дакле, ово пресликавање је билинеарно, па је, према универзалном својству, пресликавање $\phi : z \otimes_\Lambda (\lambda \otimes x) \mapsto z \cdot \lambda \otimes x$ добро дефинисано на свим $P_k \otimes_\Lambda (\Lambda \otimes X)$.

Коначно, пресликавања ϕ и θ су инверзна. Заиста:

$$\theta \circ \phi(z \otimes x) = \theta(z \otimes_\Lambda (1 \otimes x)) = z \otimes x$$

и

$$\phi \circ \theta(z \otimes_\Lambda (\lambda \otimes x)) = \phi(z \cdot \lambda \otimes x) = z \cdot \lambda \otimes_\Lambda (1 \otimes x) = z \otimes_\Lambda \lambda \cdot (1 \otimes x) = z \otimes_\Lambda (\lambda \otimes x).$$

Дакле, $P_k \otimes_\Lambda (\Lambda \otimes X)$ и $P_k \otimes X$ су изоморфни.

Пројективни G-модул P_k је слободан, а самим тим и пројективан, над $\mathbb{Z}$. Дакле, према ставовима 22 и 23, примена $\_ \otimes X$ на пројективно разрешење чува тачност. Дакле, за $k \geq 1$,

$$H_k(G, \Lambda \otimes X) = 0.$$

До сада смо имали за циљ да покажемо да постоји хомолошко проширење које испуњава три својства. Да бисмо показали јединственост, да су било која два таква проширења изоморфна, поново ћемо користити померање димензија, као у случају кохомолошког проширења.

У димензији 0, имамо $H_0(G,A) \cong A_G$, па је јединственост у димензији 0 очигледна. Индуктивно претпоставимо да смо доказали јединственост до димензија $k-1$. Доказаћемо јединственост $H_k(G,A)$ тако што ћемо да покажемо да је изоморфна некој $(k-1)$-димензионалној хомолошкој групи $H_{k-1}(G,\bar{A})$, која је јединствена по индуктивној хипотези.

Размотримо $\bar{A}$ дефинисан кратким тачним низом

$$0 \longrightarrow \bar{A} \longrightarrow \Lambda \otimes A_0 \longrightarrow A \longrightarrow 0,$$

где је A_0 основна структура $\mathbb{Z}$-модула A. На основу другог својства, изводимо следећи дугачак тачан низ:

$$\ldots \xrightarrow{\delta_k} H_k(G,\bar{A}) \longrightarrow H_k(G,\Lambda\otimes A_0) \longrightarrow H_k(G,A) \xrightarrow{\delta_{k-1}}$$

$$\xrightarrow{\delta_{k-1}} H_{k-1}(G,\bar{A}) \longrightarrow H_{k-1}(G,\Lambda\otimes A_0) \longrightarrow H_{k-1}(G,A) \xrightarrow{\delta_{k-2}} \ldots$$

Сада, користећи треће својство, да хомолошко проширење нестаје на индукованим модулима, имамо $H_k(G,\Lambda\otimes A_0) = H_{k-1}(G,\Lambda\otimes A_0) = 0$. Стога нам остаје следећи кратак тачан низ:

$$0 \longrightarrow H_k(G,A) \xrightarrow{\delta_{k-1}} H_{k-1}(G,\bar{A}) \longrightarrow 0.$$

Дакле, $H_k(G,A) \cong H_{k-1}(G,\bar{A})$. Треба напоменути да се треће својство примењује на димензије 1 и више, па је δ_0 само мономорфизам. Међутим, ово је довољно, јер ће $H_1(G,A)$ бити јединствено дефинисано језгром од δ_0.

Стога је, индукцијом, хомолошко проширење јединствено.

Остало је од раније да завршимо прорачуне везане за прво својство које смо оставили за касније. Када смо дефинисали стандардно разрешење, увели смо појам преградне нотације и разрешења. Можемо сличну нотацију да уведемо за ланчани комплекс добијен тензорисањем. Размотримо ланчани комплекс

$$\cdots \to \bar{P}_k \otimes A \longrightarrow \bar{P}_{k-1} \otimes A \longrightarrow \ldots \longrightarrow \bar{P}_0 \otimes A \longrightarrow A_G.$$

Нека је $x \in \bar{P}_{k-1} \otimes A$. Тај елемент може да се представи на јединствен начин као збир елемената облика $[g_1|\otimes|g_{k-1}]\otimes a$. Означимо $\widetilde{B}_{k-1} = \{[g_1|\ldots|g_k - 1] : g_i \in G,\ 1 \le i \le k-1\}$, као и што смо урадили код кохомолошке групе. $\widetilde{B}_{k-1}$ је опет база за $\bar{P}_k$. Можемо идентификовати ланац $x \in \bar{P}_k \otimes A$ са функцијом $f_x : B_k \longrightarrow A$ која се слика у 0 скоро свуда, тј. на слика се у 0 осим за коначно много вредности. Формално, приметимо да се x може јединствено представити као линеарна комбинација елемената облика $b\otimes a$,

где је $b \in \widetilde{B}_{k-1}$ и $a \in A$. Дефинишемо $f_{b\otimes a}$ на елементу $[g_1|\dots|g_{k-1}] \in \widetilde{B}_{k-1}$ са

$$f_{b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} a, & [g_1|\dots|g_{k-1}] = b, \\ 0, & \text{иначе.} \end{cases}$$

и ово линеарно проширујемо на f_x за све $x \in \bar{P}_{k-1} \otimes A$. Заиста,

$$\begin{aligned} &f_{b_1\otimes a_1 + b_2 \otimes a_2}[g_1| \otimes |g_{k-1}] \\ &\qquad = f_{b_1\otimes a_1}[g_1| \otimes |g_{k-1}] + f_{b_2\otimes a_2}[g_1| \otimes |g_{k-1}] = \begin{cases} a_1, & [g_1| \otimes |g_{k-1}] = b_1, \\ a_2, & [g_1| \otimes |g_{k-1}] = b_2, \\ 0, & \text{иначе,} \end{cases} \end{aligned}$$

и

$$f_{g\cdot b\otimes a}[g_1|\dots|g_{k-1}] = g \cdot f_{b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} g\cdot a, & [g_1|\dots|g_{k-1}] = b, \\ 0, & \text{иначе.} \end{cases}$$

Пошто се x тако представља на јединствен начин, пресликавање $x \mapsto f_x$ је добро дефинисано. Инверзно пресликавање $f \mapsto x_f$ конструишемо као

$$x_f = \sum_{b \in \widetilde{B}_{k-1}} f(b).$$

Ово је добро дефинисано јер f нестаје скоро свуда. Дакле, имамо везу између елемената P_{k-1} и функције $\widetilde{B}_{k-1} \to A$ које нестају скоро свуда.

Сада тражимо како изгледа гранични хомоморфизам d_* у овој нотацији. У дефиницији стандардног разрешења смо имали

$$d_* x = dx = \sum_{j=0}^{k} (-1)^j \hat{r}_j x,$$

где са $\hat{r}_j$ означавамо оператор уклањања j-те координате, тј.

$$\hat{r}_j : (h_0, \dots, h_k) \mapsto (h_0, \dots, \hat{h}_j, \dots, h_k),$$

за било које $(h_0, \dots, h_k) \in \bar{P}_k$. Сада, за произвољне $b \in \widetilde{B}_{k-1}$ и $a \in A$, имамо

$$f_{\hat{r}_j b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} a, & [g_1|\dots|g_k] = \hat{r}_j b; \\ 0, & \text{иначе.} \end{cases}$$

Ако је $[g_1|\dots|g_k] = (h_0, \dots, h_{k-1})$, онда је $(h_0, \dots, h_{k-1}) = \hat{r}_j b$ еквивалентно са

$$(h_0, \dots, h_{j-1}, g, h_j, \dots, h_{k-1}) = b,$$

где је $g \in G$ j-та координата од b. Наравно, ако g није j-та координата од b, онда је вредност $f_{b\otimes a}$ на овоме 0. Дакле, можемо означити

$$f_{\hat{r}_j b\otimes a}[g_1| \otimes |g_{k-1}] = \sum_{g\in G} f_{b\otimes a}(h_0, \otimes, h_{j-1}, g, h_j, \otimes, h_{k-1}).$$

Ово се линеарно проширује на било који произвољни елемент $x \in \bar{P}_k$, и стога из $d_* x = dx$ што даје $d_* f_x = f_{dx}$ добијамо

$$\begin{aligned} d_* f_x[g_1|\ldots|g_{k-1}] &= f_{dx}(1, h_1, \ldots, h_{k-1}) \\ &= \sum_{j=0}^{k} (-1)^j f_{\hat{r}_j x}(h_0, h_1, \ldots, h_{k-1}) \\ &= \sum_{j=0}^{k} \sum_{g\in G} (-1)^j f_x(h_0, h_1, \ldots, h_{j-1}, g, h_j, \ldots, h_{k-1}), \end{aligned}$$

где је свако $h_i = g_1 \ldots g_i$ и узимајући $1 = h_0$. Сада, израчунајмо сваки сабирак.

За $j = 0$:

$$\begin{aligned} f_x(g, h_1, h_2, \ldots, h_{k-1}) &= f_x(g, g_1, g_1 g_2, \ldots, g_1 \ldots g_{k-1}) \\ &= g^{-1} \cdot f_x(g, g1, g_2, \ldots, g_2 \ldots g_{k-1}) \\ &= g^{-1} \cdot f_x[g_1|\ldots|g_{k-1}]. \end{aligned}$$

За $1 \leq j \leq k-1$:

$$\begin{aligned} & \sum_{g\in G} f_x(1, h_1, \ldots, g, \ldots, h_{k-1}) \\ = & \sum_{g\in G} f_x(1, g_1, \ldots, g_1 \ldots g_{j-1}, g, g_1 \ldots g_j, \ldots, g_1 \ldots g_{k-1}) \\ = & \sum_{g\in G} f_x(1, g_1, \ldots, g_1 \ldots g_{j-1}, g_1 \ldots g_j g, g_1 \ldots g_j, \ldots, g_1 \ldots g_{k-1}) \\ = & \sum_{g\in G} f_x[g_1|\ldots|g_{j-1}|g_j g|g^{-1}|g_{j+1}|\ldots|g_{k-1}]. \end{aligned}$$

Овде смо заменили g са $g_1 \ldots g_j g$ у другој једначини, јер је збир над свим елеменатима G.

За $j = k$:

$$\sum_{g\in G} f_x(1, h_1, \ldots, h_{k-1}, g) = \sum_{g\in G} f_x(1, g_1, \ldots, g_1 \ldots g_{k-1}, g)$$

$$\begin{aligned} &= \sum_{g\in G} f_x(1, g_1, \ldots, g_1 \ldots g_{k-1}, g_1 \ldots g_{k-1} g) \\ &= \sum_{g\in G} f_x[g_1|\ldots|g_{k-1}|g]. \end{aligned}$$

Слично, заменили смо g са $g_1 \ldots g_{k-1} g$ у другој једначини, јер се збир врши над свим елеменатима G.

Дакле, наша резултујућа формула за гранични хомоморфизам је:

$$\begin{aligned} d_* f_x[g_1|\ldots|g_{k-1}] &= \sum_{g\in G} g^{-1} \cdot f_x[g_1|\ldots|g_{k-1}] \\ &\quad + \sum_{j=1}^{k} \sum_{g\in G} (-1)^j f_x[g_1|\ldots|g_{j-1}|g_j g|g^{-1}|g_{j+1}|\ldots|g_{k-1}] \\ &\quad + (-1)^{k+1} \sum_{g\in G} f_x[g_1|\ldots|g_{k-1}|g]. \end{aligned}$$

У димензији 0 ово има облик

$$d_1 f_x[\,] = \sum_{g\in G} g^{-1} \cdot f_x[g] - f_x[g].$$

Дакле, $\operatorname{im} d_1$ је скуп формалних збира елемената облика $g \cdot a - a$. Како је $\ker d_0 = A$, то значи да је $H^0(G, A) = \ker d_0 / \operatorname{im} d_1$ група коинваријанти од A, тј.

$$H^0(G, A) = \frac{\ker d_0}{\operatorname{im} d_1} \cong A_G,$$

што задовољава својство 1. □

5 Нискодимензионална интерпретација

5.1 Укрштени хомоморфизми

Дефиниција 9 *Пресликавање $f : G \to A$ које задовољава услов $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$ за све $g_1, g_2 \in G$ назива се укрштени хомоморфизам. Пресликавање $f_a : G \to A$ које задовољава услов $f_a(g) = g \cdot a - a$ за све $g \in G$ назива се главни укрштени хомоморфизам.*

Када је G-дејство на A тривијално, укрштени хомоморфизам је хомоморфизам у уобичајеном смислу, а једини главни укрштени хомоморфизам је константно пресликавање у 0.

Једноставно је показати да су главни укрштени хомоморфизми заиста укрштени хомоморфизми. За било која два $g_1, g_2 \in G$, имамо

$$\begin{aligned} f_a(g_1g_2) &= (g_1g_2) \cdot a - a \\ &= g_1 \cdot (g_2 \cdot a) + g_1 \cdot a - g_1 \cdot a - a \\ &= g_1 \cdot (g_2 \cdot a - a) + (g_1 \cdot a - a) \\ &= g_1 \cdot f_a(g_2) + f_a(g_1) \end{aligned}$$

Видимо да су когранице у димензији 1 управо главни укрштени хомоморфизми. Нека је f укрштени хомоморфизам. Једначина $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$ се добија као резултат кограничне формуле за $d^k f$, за $k = 1$. Пошто формула за $d^k f$ гласи

$$\begin{aligned} d^k f(g_1, \ldots, g_{k+1}) &= g_1 \cdot f(g_2, \ldots, g_{k+1})) - f(g_1g_2, g_3, \ldots, g_{k+1}) \\ &\quad + f(g_1, g_2g_3, \ldots, g_{k+1}) - \ldots \\ &\quad + (-1)^{-1} f(g_1, \ldots, g_jg_{j+1}, \ldots, g_{k+1}) + \ldots \\ &\quad + (-1)^{k+1} f(g_1, \ldots, g_k), \end{aligned}$$

добија се

$$d^1 f(g_1, g_2) = g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1).$$

Пошто за 1-коцикле важи $d^1 f = 0$, имамо $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$. Другим речима, скуп укрштених хомоморфизама је тачно скуп 1-коциклуса.

Према томе, прва групна кохомологија $H^1(G, A)$ је изоморфна Абеловој групи укрштених хомоморфизама по модулу главних укрштених хомоморфизама.

5.2 Групна раширења

Сличну дискусију имамо и за другу кохомолошку групу. Применом кограничне формуле на $d^k f$ за $k = 2$ имамо

$$d^2 f(g_1, g_2) = g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2).$$

За 2-коцикле важи $d^2 f = 0$, па дајемо следећу дефиницију:

Дефиниција 10 *Пресликавање $f : G \times G \to A$ које задовољава услов*

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

назива се фактор систем.

Такво пресликавање се назива фактор систем због тога што такво пресликавање одређује закон композиције за одређено раширење E Абелове групе A са G, где G-структура на A одговара дејству конјугације G на A. Такво раширење E је дефинисано следећим кратким тачним низом;

$$0 \longrightarrow A \xrightarrow{\iota} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 0.$$

Поистовећујемо A са $\iota(A)$, што је подскуп од E. Штавише, биће нормална подгрупа, пошто је $\iota(A) = \ker \pi$. Имамо трансверзалу $s : G \to A \in E$, десни инверз за π одређен избором $s(g)$. То је функција између скупова, не нужно хомоморфизам, међутим, задовољава

$$s(g_1)s(g_2) = f(g_1, g_2)s(g_1 g_2).$$

за све $g_1, g_2 \in G$.

Формализујемо ово у следећем ставу:

Став 26 *Нека је дато је раширење E и трансверзала s као горе. Тада важе следећа својства:*

(i) Факторски систем f одређује закон композиције у E.

(ii) Горенаведена коциклична веза је еквивалентна асоцијативности у E.

(iii) Избор нове трансверзале $s' : G \to E$ мења f за кограницу.

Доказ: G дејствује на A конјугацијом, тј.

$$g \cdot a = gag^{-1}.$$

Посматрамо A као подскуп од E, али не и G, што избегавамо помоћу s:

$$g \cdot a = s(g)as(g)^{-1}$$

Користимо ову формулу током остатка доказа.

Пошто је s десни инверз од π, имамо

$$\pi(s(gh)) = gh$$

и

$$\pi(s(g)s(h)) = \pi(s(g))\pi(s(h)) = gh,$$

стога је $\pi(s(g)s(h)s(gh)^{-1}) = 1$. Дакле, $s(g)s(h)s(gh)^{-1} \in \ker\pi = \operatorname{im}\iota = A$ по тачности. Према томе, иако s не мора бити хомоморфизам и стога $s(g)s(h)s(gh)^{-1}$ није нужно 1, он је ипак елемент групе A. Зато можемо да дефинишемо функцију $f : G \times G \to A$ са $f(g,h) := s(g)s(h)s(gh)^{-1}$.

Применимо асоцијативност у E:

$$\begin{array}{rcll} (s(g)s(h))s(k) & = & f(g,h)s(gh)s(k) & = & f(g,h)f(gh,k)s(ghk), \\ s(g)(s(h)s(k)) & = & s(g)f(h,k)s(hk) & = & s(g)f(h,k)s(g)^{-1}s(g)s(hk) \\ & & & = & g\cdot f(h,k)f(g,hk)s(ghk) \end{array}$$

и онда, поништавањем члана $s(ghk)$ са обе стране, добијамо

$$g\cdot f(h,k)f(g,hk) = f(g,h)f(gh,k).$$

Међутим, пошто сви ови чланови леже у A, што је Абелова група, можемо да се пребацимо на адитивну нотацију:

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

Дакле,

$$g\cdot f(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0$$

што значи да је f факторски систем, чиме смо доказали особину (ii).

Враћамо се сада на (i). Фиксирамо елемент $x \in E$ и разматрамо следеће:

$$\pi(xs(\pi(x))^{-1}) = \pi(x)\big(\pi(s(\pi(x)))\big)^{-1} = \pi(x)\pi(x)^{-1} = 1_G.$$

Дакле, $xs(\pi(x))^{-1} \in \ker\pi = A$, па је $x = a_x s(\pi(x))$ за неко $a_x \in A$.

Нека су дата два елемента, $x, y \in E$. Тада је

$$\begin{array}{rcl} xy & = & a_x s(\pi(x))a_y s(\pi(y)) \\ & = & a_x s(\pi(x))a_y s(\pi(x))^{-1}s(\pi(x))s(\pi(y)) \\ & = & a_x\pi(x)\cdot a_y f(\pi(x),\pi(y))s(\pi(x)\pi(y)). \end{array}$$

Са друге стране, $xy = a_{xy}s(\pi(xy)) = a_{xy}s(\pi(x)\pi(y))$, и стога је

$$a_{xy} = a_x\pi(x)\cdot a_y f(\pi(x),\pi(y)).$$

Овиме смо показали својство (i).

Нека је $s' : G \to E$ други избор трансверзале. Показаћемо да се повезани факторски систем f' разликује од f за неки коциклус.

Прво, напоменимо да је $\pi(s'(g)) = g = \pi(s(g))$, и због тога је

$$\pi(s'(g)(s(g))^{-1}) = \pi(s'(g))(\pi(s(g)))^{-1} = 1_G,$$

па је $s'(g)(s(g))^{-1} \in \ker \pi = A$. Дефинишемо $F : G \to A$ овом вредношћу, $F(g) = s'(g)(s(g))^{-1}$, тј. $s'(g) = F(g)s(g)$.

Сада, примењујемо ово на

$$\begin{aligned}
s'(g)s'(h) &= f'(g,h)s'(gh) \\
F(g)s(g)F(h)s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)s(g)F(h)s(g)(s(g))^{-1}s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)s(g)s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)f(g,h)s(gh) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)f(g,h)s(gh) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)f(g,h) &= f'(g,h)F(gh).
\end{aligned}$$

Пошто сада радимо у A где је операција комутативна, можемо прећи на адитивну нотацију и рачунати

$$\begin{aligned}
F(g) + g \cdot F(h) + f(g,h) &= f'(g,h) + F(gh), \\
f'(g,h) - f(g,h) &= g \cdot F(h) - F(gh) + F(g), \\
f'(g,h) - f(g,h) &= d^1F(g,h).
\end{aligned}$$

Дакле, $f' - f = d^1F$, и тиме смо показали (iii). □

Овај став описује бијективну везу између друге кохомолошке групе $H^2(G,A)$ и фамилије раширења

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

за дато G-дејство на A. Другим речима, ако је дат пар (G,A), где је A абелова као нормална подгрупа, групе раширења су одређене до изоморфизма структуром модула у A, односно G дејством у A и другом кохомолошком класом.

Пошто за све $x \in E$ имамо $x = a_x s(\pi(x))$ за неко $a_x \in A$, имамо бијективну везу између скупова E и $A \times G$. Посматрајући E као такав, закон композиције $xy = a_x\pi(x) \cdot a_y f(\pi(x),\pi(y))s(\pi(x)\pi(y))$ постаје

$$(a,g)(b,h) = (a + g \cdot b + f(g,h), gh), \tag{3}$$

где f одговара елементу друге класе кохомологије. Ако је G-дејство тривијална, а систем фактора f одговара тривијалној класи кохомологије, што

значи да без губитка општости можемо узети да је f једнако 0 свуда, онда закон композиције постаје

$$(a, g)(b, h) = (a + b, gh).$$

Дакле, имамо следећи резултат:

Лема 27 *Нека је A Абелова група са тривијалним G-дејством. Раширење чији систем фактора одговара тривијалној класи кохомологије изоморфно је $A \times G$.*

Ако, у формули 3, посматрамо случај где f одговара тривијалној класи кохомологије, али дозволимо да G-дејство на A буде нетривијално, добијамо

$$(a, g)(b, h) = (a + g \cdot b, gh).$$

Ово одговара операцији на спољашњем полудиректном производу $A \rtimes_\varphi G$, где $\varphi : G \to \operatorname{Aut} A$ означава G-дејство на A.

Лема 28 *Нека је A Абелова група са G-дејством одређеном са $\varphi : G \to \operatorname{Aut} A$. Нека је E раширење дефинисано низом*

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

Ако факторски систем овог раширења одговара тривијалној класи кохомологије, онда се раширење цепа и E је изоморфно $A \rtimes_\varphi G$, где је композиција одређена G-дејством на A са

$$(a, g)(b, h) = (a + g \cdot b, gh).$$

за све $a, b \in A$ и $g, h \in G$.

Доказ: Нека је E такво раширење са тривијалним фактор системом f. Нека је $E = A \times G$ као скуп, са горе одређеном композицијом. Сада, A је изоморфна својој слици $\operatorname{im} \iota = \ker \pi$ која је нормална у E. То су елементи облика $(a, 1)$, за све $a \in A$. Слично, узимамо да је трансверзала $s : G \to E$ $s : g \mapsto (0, g)$ за све $g \in G$. Сада, за све $g, h \in G$ имамо

$$(0, g)(0, h) = (f(g, h), gh) = (0, gh),$$

јер f одговара тривијалној класи кохомологије и зато може без губитка општости да се сматра тривијалном. То значи да је s заправо хомоморфизам група, инверзан π, па се по леми 13 кратки тачан низ цепа. Дакле, G је изоморфна подгрупи $\operatorname{im} s$ у E, подгрупи свих елемената облика $(0, g)$. Подгрупе $\operatorname{im} \iota$ и $\operatorname{im} s$ очигледно имају тривијални пресек. За произвољни елемент $(a, g) \in E$, имамо

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

тј. $E = \operatorname{im} \iota \operatorname{im} s$. Dakle, $E = \operatorname{im} \iota \rtimes \operatorname{im} s \cong A \rtimes_\varphi G$. □

5.3 Абелизација

Лема 29 *Нека $\mathbb{Z}$ има тривијално структуру G-модула и нека $[G,G]$ означава комутаторску подгрупу од G. Тада*

$$H_1(G,\mathbb{Z}) \cong G/[G,G].$$

Доказ: Према леми 7, имамо $A_G = A/IA$, где је I иедал проширења. Наравно, како је $H_0(G,A) = A_G$, то значи $H_0(G,A) = A/IA$. Идеал проширења може да се дефинише кратким тачним низом

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

Применом другог својства хомологије групе, на кратким тачним низовима, добијамо дуги тачан низ

$$\ldots \longrightarrow H_1(G,I) \longrightarrow H_1(G,\Lambda) \longrightarrow H_1(G,\mathbb{Z}) \longrightarrow$$

$$\longrightarrow H_0(G,I) \longrightarrow H_0(G,\Lambda) \longrightarrow H_0(G,\mathbb{Z}) \longrightarrow 0.$$

Сада, како је Λ очигледно пројективни Λ-модул, он има тривијално разрешење, тако да је $H_1(G,\Lambda) = H_0(G,\Lambda) = 0$. Заменом A са I код тврђења на почетку доказа, имамо $H_0(G,I) = I/I^2$. Дакле, из дугог тачног низа добијамо следећи кратак тачан низ:

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

Дакле, $H_1(G,\mathbb{Z}) \cong I/I^2$. Сада желимо да покажемо $I/I^2 \cong G/[G,G]$, након чега смо завршили.

Нека је пресликавање $\phi : G \to I/I^2$ дефинисано са $g \mapsto [g-1]$. Два елемента у I су у истој класи у I/I^2 ако се разликују за елемент од I^2. Означимо ову релацију са $\equiv$. За произвољне $g,h \in G$ израчунавамо следеће:

$$\begin{aligned}
\phi(gh) &\equiv gh-1 \\
&\equiv gh-1-(g-1)(h-1) \\
&\equiv g-1+h-1 \\
&\equiv \phi(g)+\phi(h) \\
&\equiv \phi(h)+\phi(g) \\
&\equiv \phi(hg).
\end{aligned}$$

Дакле, $\phi(ghg^{-1}h^{-1}) \equiv 0$. Како је $[G,G]$ комутаторска подгрупа, она је генерисана свим елементима облика $ghg^{-1}h^{-1}$, па је стога $[G,G] \subseteq \ker\phi$. Дакле, можемо дефинисати $\bar{\phi} : G/[G,G] \to I/I^2$ са $[g] \mapsto [g-1]$.

Са друге стране, нека је пресликавање $\theta : I \to G/[G,G]$ дефинисано на генераторима I са $g-1 \mapsto [g]$ и линеарно се проширује до остатка I. Заиста, ако је $\lambda = \sum_i^k m_i g_i \in I$, онда је $\varepsilon(\lambda) = 0$, тј. $\sum_i^k m_i = 0$, а према томе је

$$\lambda = \sum_i^k m_i g_i = \sum_i^k m_i g_i - \sum_i^k m_i = \sum_i^k (m_i - 1) g_i.$$

Дакле, $\theta(\lambda) = \prod_i^k g_i^{m_i}$. Сада, I^2 је генерисано свим производима два генератора I, тј. елементима облика $(g-1)(h-1)$ за било која два $g, h \in G$. Опет означавајући са $\equiv$ релацију да се два елемента у G разликују за елемент од $[G,G]$, имамо

$$\begin{aligned}
\theta((g-1)(h-1)) &= \theta(gh - g - h + 1) \\
&= \theta((gh-1) - (g-1) - (h-1)) \\
&\equiv \theta(gh-1)\theta(g-1)^{-1}\theta(h-1)^{-1} \\
&\equiv ghg^{-1}h^{-1} \\
&\equiv 1.
\end{aligned}$$

Према томе, $ghg^{-1}h^{-1} \in [G,G]$. Дакле, $I^2 \subseteq \ker\theta$, и зато можемо дефинисати пресликавање $\bar{\theta} : I/I^2 \to G/[G,G]$ као $[g-1] \mapsto [g]$. Јасно је да је овај хомоморфизам инверзан хомоморфизму $\bar{\phi}$ од раније, па су оба заправо изоморфизми. Дакле, $I/I^2 \cong G/[G,G]$. $\square$

6 Примери

6.1 Основни примери

У овом одељку ћемо обрадити неке једноставне примере раширења група.

Пример 6 *Раширења $\mathbb{Z}$ помоћу $\mathbb{Z}_2$.*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} E \xrightarrow{\pi} C_2^T \longrightarrow 0.$$

Ради јасноће, третираћемо $\mathbb{Z}_2$ као цикличну групу реда 2 са генератором T, понекад означеним са C_2^T, при чему се за операцију у групи изима да је множење како бисмо остали у складу са до сада постављеном теоријом. Сада, применимо формулу за кохомологију цикличних група коју смо раније израчунали у примеру 5:

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}}.$$

Кохомолошке групе, наравно, зависе од структуре $\mathbb{Z}_2$-модула $\mathbb{Z}$, тј. од дејства $\mathbb{Z}_2$ на $\mathbb{Z}$. Ово одговара пресликавању $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$. Пошто $\mathrm{Aut}(\mathbb{Z})$ има два елемента, тривијални аутоморфизам и аутоморфизам који шаље 1 у -1, имамо два случаја за разматрање.

Нека је $T \cdot a = a$. Како је сваки елемент тада фиксиран, имамо

$$\mathbb{Z}^{\mathbb{Z}_2} = \mathbb{Z}$$

и

$$N\mathbb{Z} = (1+T)\mathbb{Z} = (1+1)\mathbb{Z} = 2\mathbb{Z},$$

и стога је

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2.$$

Дакле, имамо две могућности за наш факторски систем f који дефинише E. Подсетимо се да, ако је f факторски систем, он задовољава

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

за све $g_1, g_2, g_3 \in \mathbb{Z}_2$. Ако поставимо $g_1 = 1$, онда је

$$\begin{aligned} 0 &= 1 \cdot f(g_2, g_3) - f(1 g_2, g_3) + f(1, g_2 g_3) - f(1, g_2) \\ &= f(1, g_2 g_3) - f(1, g_2), \end{aligned}$$

што значи $f(1,T) = f(1,1) = 0$. Ако поставимо $g_1 = T$, онда је

$$\begin{aligned} 0 &= T \cdot f(g_2, g_3) - f(Tg_2, g_3) + f(T, g_2 g_3) - f(T, g_2) \\ &= f(g_2, g_3) - f(Tg_2, g_3) + f(T, g_2 g_3) - f(T, g_2). \end{aligned}$$

Ако је $g_2 = 1$, тада је $f(1, g_3) = f(T, 1)$, то је $f(T, 1) = 0$. Ако је $g_3 = T$, онда је $f(g_2, 1) = f(Tg_2, 1)$, што даје исти резултат. Ако је $g_2 = T$ и $g_3 = 1$, онда је $f(T, 1) = f(1, 1)$, што поново даје исти резултат. Дакле, вредност $f(T, T)$ нема ограничења и стога ће одговарати елементу друге класе кохомологије.

Ако је $f(T, T) = 0$, имамо

$$(a, g)(b, h) = (a + g \cdot b + f(g, h), gh) = (a + b, gh),$$

то јест, $E \cong \mathbb{Z} \times \mathbb{Z}_2$. Ово се поклапа са резултатом леме 27.

Ако је $f(T, T) = 1$, имамо

$$(a, g)(b, h) = (a + g \cdot b + f(g, h), gh) = (a + b + f(g, h), gh),$$

што, за сваку комбинацију вредности $g, h \in \{1, T\}$ даје

$$\begin{aligned} (a, 1)(b, 1) &= (a + b, 1), \\ (a, T)(b, 1) &= (a + b, T), \\ (a, 1)(b, T) &= (a + b, T), \\ (a, T)(b, T) &= (a + b + 1, 1). \end{aligned}$$

Пресликавањем $(a, g) \mapsto \begin{cases} 2a, & \text{if } g = 1; \\ 2a + 1, & \text{if } g = T; \end{cases}$ видимо да је E изоморфно $\mathbb{Z}$.

Нека је сада $T \cdot a = -a$. Тада је једини фиксирани елемент 0, па

$$\mathbb{Z}^{\mathbb{Z}_2} = \{0\}$$

и

$$N\mathbb{Z} = (1 + T)\mathbb{Z} = (1 - 1)\mathbb{Z} = \{0\},$$

и стога је

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}} = \frac{\{0\}}{\{0\}} \cong 0.$$

Дакле, имамо само једно раширење. Факторски систем у овом раширењу мора да одговара једином елементу кохомолошке класе, тривијалном елементу. Ово би нас интуитивно водило ка томе да је факторски систем константан на 0. То можемо видети из идентитета за факторски систем:

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0.$$

Имамо исти резултат као и раније за $g_1 = 1$, пошто 1 дејствује тривијално, па $f(1,T) = f(1,1) = 0$. Када $g_1 = T$, имамо

$$0 = -f(g_2, g_3) - f(Tg_2, g_3) + f(T, g_2g_3) - f(T, g_2).$$

Постављањем $g_3 = 1$ добија се $f(g_2,1) + f(Tg_2,1) = 0$ што за било коју вредност g_2 даје $f(T,1) = -f(1,1) = 0$. За $g_3 = T$ и $g_2 = 1$ имамо $f(T,1) = -f(1,T)$, тј. $0 = 0$. Коначно, постављањем $g_1 = g_2 = g_3 = T$ имамо $2f(T,T) = f(T,1) - f(1,T) = 0$, а како f слика у $\mathbb{Z}$, мора бити $f(T,T) = 0$. Дакле, f је константно пресликавање у 0.

Операција у E је сада дата са

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

Ово показује да је E изоморфна бесконачној диедарској групи

$$\mathbb{D}_\infty = \langle r, s \mid s^2 = 1,\ rsr = r^{-1}\rangle,$$

постављањем $r = (1,1)$, и $s = (0,T)$. Заиста, $s^2 = (0,T)(0,T) = (0,1)$ и

$$rsr^{-1} = (1,1)(0,T)(1,1)^{-1} = (1,T)(-1,1) = (0,1).$$

Дакле, сва могућа раширење $\mathbb{Z}$ са $\mathbb{Z}_2$ су $\mathbb{Z}\times\mathbb{Z}_2$, $\mathbb{Z}$ и $\mathbb{D}_\infty$, до на изоморфизам.

Пример 7 *Раширења $\mathbb{Z}_p$ са $\mathbb{Z}_2$, где је p прост број већи од 2.*

Овај пример је доста сличан претходном. Нека је раширење E дата са

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_2^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_2^T \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. Пошто T мора да се пресликава у неки елемент чији ред дели 2, мора важити или $T\cdot a = a$ или $T\cdot a = -a$.

Нека је $T\cdot a = a$. Сада,

$$\mathbb{Z}_p^{\mathbb{Z}_2} = \mathbb{Z}_p$$

и

$$N\mathbb{Z}_p = (1+T)\mathbb{Z}_p = (1+1)\mathbb{Z}_p = 2\mathbb{Z}_p = \mathbb{Z}_p,$$

па је

$$H^2(\mathbb{Z}_2, \mathbb{Z}_p) = \frac{\mathbb{Z}_p^{\mathbb{Z}_2}}{N\mathbb{Z}_p} = \frac{\mathbb{Z}_p}{\mathbb{Z}_p} \cong 0.$$

Дакле, наш факторски систем је тривијалан и стога, према леми 27, наше раширење је $E \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.

Нека је $T \cdot a = -a$. Сада, једини фиксни елемент је 0, па је према томе

$$\mathbb{Z}_p^{\mathbb{Z}_2} = \{0\}$$

и

$$N\mathbb{Z}_p = (1+T)\mathbb{Z}_p = (1-1)\mathbb{Z}_p = \{0\},$$

и стога је

$$H^2(\mathbb{Z}_2, \mathbb{Z}_p) = \frac{\mathbb{Z}_p^{\mathbb{Z}_2}}{N\mathbb{Z}_p} = \frac{\{0\}}{\{0\}} \cong 0.$$

Опет, наш факторски систем је тривијалан, па је операција у E дата следећим везама:

$$\begin{aligned}
(a,1)(b,1) &= (a+b,1),\\
(a,1)(b,T) &= (a+b,T),\\
(a,T)(b,1) &= (a-b,T),\\
(a,T)(b,T) &= (a-b+2,1).
\end{aligned}$$

Одавде добијамо да је E изоморфно диедарској групи

$$\mathbb{D}_p = \langle r, s \mid r^p = s^2 = 1,\ rsr = r^{-1} \rangle,$$

са $r = (1,1)$ и $s = (0,T)$.

Дакле, сва могућа раширења $\mathbb{Z}_p$ помоћу $\mathbb{Z}_2$ су $\mathbb{Z}_{2p}$ и $\mathbb{D}_p$.

Пример 8 *Раширења $\mathbb{Z}_4$ помоћу $\mathbb{Z}_2$.*

Нека је раширење E дата са

$$0 \longrightarrow \mathbb{Z}_4 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_2^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_2^T \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$. Пошто се T мора пресликати у елемент чији ред дели 2, поново имамо или $T \cdot a = a$ или $T \cdot a = -a$.

Нека је $T \cdot a = a$. Сада,

$$\mathbb{Z}_4^{\mathbb{Z}_2} = \mathbb{Z}_4$$

и

$$N\mathbb{Z}_4 = (1+T)\mathbb{Z}_4 = (1+1)\mathbb{Z}_4 = 2\mathbb{Z}_4,$$

па је

$$H^2(\mathbb{Z}_2, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_2}}{N\mathbb{Z}_4} = \frac{\mathbb{Z}_4}{2\mathbb{Z}_4} \cong 0.$$

Аналогно примеру 6, наша раширења су $\mathbb{Z}_4 \times \mathbb{Z}_2$ и $\mathbb{Z}_8$.

Нека је сада $T \cdot a = -a$. Супротно претходним примерима, имамо сада још један фиксни елемент, наиме 2. Значи,

$$\mathbb{Z}_4^{\mathbb{Z}_2} = \{0, 2\} = 2\mathbb{Z}_4$$

и

$$N\mathbb{Z}_4 = (1+T)\mathbb{Z}_4 = (1-1)\mathbb{Z}_4 = \{0\},$$

па је према томе

$$H^2(\mathbb{Z}_2, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_2}}{N\mathbb{Z}_4} = \frac{2\mathbb{Z}_4}{\{0\}} \cong \mathbb{Z}_2.$$

Приликом израчунавања факторског система, пратимо исти поступак као у примеру 6 да бисмо добили $f(1,T) = f(T,1) = f(1,1) = 0$ и $2f(T,T) = 0$. У том примеру, одмах смо закључили да је $f(T,T) = 0$, јер је слика f $\mathbb{Z}$, где нема делилаца нуле. То није случај у $\mathbb{Z}_4$, можемо имати $f(T,T) = 0$ или $f(T,T) = 2$, и у оба случаја $2f(T,T) = 0$. Ови случајеви одговарају двема различитим класама кохомологије.

У првом случају, када је $f(T,T) = 0$, што одговара тривијалној класи кохомологије, раширење је диедарска група $\mathbb{D}_4$, слично примеру 7.

У другом случају, када је $f(T,T) = 2$, што одговара нетривијалној класи кохомологије, операција у E је дата са

$$\begin{aligned}
(a,1)(b,1) &= (a+b,1),\\
(a,1)(b,T) &= (a+b,T),\\
(a,T)(b,1) &= (a-b,T),\\
(a,T)(b,T) &= (a-b+2,1).
\end{aligned}$$

Ово даје изоморфизам кватернионима

$$\mathbb{Q}_8 = \pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = ijk = -1\}$$

преко

$$\begin{aligned}
(2,1) &\mapsto -1,\\
(1,1) &\mapsto i,\\
(0,T) &\mapsto j,\\
(1,T) &\mapsto k.
\end{aligned}$$

6.2 Диедарска група $\mathbb{D}_3$

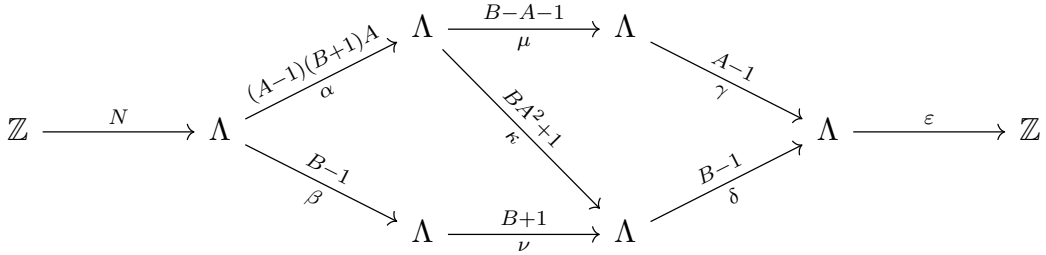
У овом одељку, означићемо са $G = \mathbb{D}_3$ диедарску групу са 6 елемената. G има репрезентацију

$$G = \langle A, B \mid A^3 = B^2 = 1,\ BAB = A^2 \rangle.$$

Циљ овог одељка је да се пронађе разрешење за ову групу и израчунају њене кохомолошке групе, у случају тривијалног дејства групе.

Пример 9 *Конструисање разрешења за диедарску групу* $\mathbb{D}_3$.

Посматраћемо следећи дијаграм:



Спајањем горњег и доњег реда у средини, као и спајањем главе са репом, формирамо следећи периодични ланчани комплекс, за који ћемо показати да је тачан:

$$\cdots \xrightarrow[\partial_4]{N\varepsilon} \Lambda \xrightarrow[\partial_3]{\begin{pmatrix}\alpha\\ \beta\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_2]{\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_1]{\begin{pmatrix}\gamma & \delta\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.$$

До краја овог одељка, елемент λ од Λ означавамо као

$$\lambda = x + yA + zA^2 + uB + vBA + wBA^2$$

са $\mathbb{Z}$-коефицијентима x, y, z, u, v и w.

Пресликавање $N\varepsilon : \Lambda \to \Lambda$ је композиција пресликавања $\varepsilon : \Lambda \to \mathbb{Z}$, која шаље елементе $\lambda \in \Lambda$ у збир њихових коефицијената $x + y + z + u + v + w = k \in \mathbb{Z}$, и $N : \mathbb{Z} \to \Lambda$, која шаље елементе $k \in \mathbb{Z}$ у kN, где је N збир свих елемената у G, тј. $N = 1 + A + A^2 + B + BA + BA^2$.

Множење са N шаље елемент $\lambda \in \Lambda$ у

$$N\lambda = (x + y + z + u + v + w)(1 + A + A^2 + B + BA + BA^2) = kN,$$

где је k збир коефицијената. Стога, пресликавање $N\varepsilon$ можемо гледати једноставно као множење са N.

Доказ тачности низа почињемо тако што прво показујемо да било која два узастопна пресликавања имају тривијалну композицију, тј. слике су садржане у језгрима. Након тога, показаћемо тежи део, да су језгра садржана у сликама.

Примећујемо да је

$$N = 1 + A + A^2 + B + BA + BA^2 = (1 + B)(1 + A + A^2),$$

и стога су композиције $\alpha N = \beta N = 0$ јер је $(1+B)(1-B) = 1-B^2 = 1-1 = 0$. Дакле, композиција $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} N = 0$.

За композицију $\begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \mu\alpha \\ \kappa\alpha + \nu\beta \end{pmatrix}$ израчунајмо сваки производ зацесебно:

$$\begin{aligned}
\mu\alpha &= (-1 - A + B)(A - 1)(B + 1)A \\
&= (-1 - A + B)(AB - B + A - 1)A \\
&= (-1 - A + B)(B - BA + A^2 - A) \\
&= -B + BA - A^2 + A - AB + ABA - A^3 \\
&\quad + A^2 + B^2 - B^2A + BA^2 - BA \\
&= -B + BA - A^2 + A - BA^2 + B - 1 \\
&\quad + A^2 + 1 - A + BA^2 - BA \\
&= 0; \\
\kappa\alpha &= (1 + BA^2)(A - 1)(B + 1)A \\
&= (1 + BA^2)(B + A^2 - BA - A) \\
&= B + A^2 - BA - A + A + BA - A^2 - B \\
&= 0; \\
\nu\beta &= (B + 1)(B - 1) \\
&= 0.
\end{aligned}$$

Дакле, композиција $\begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \mu\alpha \\ \kappa\alpha + \nu\beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ је тривијална.

За комопзицију $\begin{pmatrix} \gamma & \delta \end{pmatrix} \begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} = \begin{pmatrix} \gamma\mu + \delta\kappa & \delta\nu \end{pmatrix}$ ћемо опет да израчунамо сваки производ посебно:

$$\begin{aligned}
\gamma\mu &= (A - 1)(-1 - A + B) \\
&= -A - A^2 + AB + 1 + A - B \\
&= -B + 1 - BA^2 + A^2; \\
\delta\kappa &= (B - 1)(1 + BA^2) \\
&= B - 1 + BA^2 - A^2 \\
&= -\gamma\mu;
\end{aligned}$$

$$\begin{aligned}\delta\nu &= (B-1)(B+1)\\ &= 0.\end{aligned}$$

Одавде видимо да је композиција $\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix} = \begin{pmatrix}\gamma\mu+\delta\kappa & \delta\nu\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ тривијална.

Да бисмо израчунали композицију пресликавања $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ и $N\varepsilon$, прво посматрамо пресликавање $N\varepsilon$ као множење за N, па ће композиција да постане $N\begin{pmatrix}\gamma & \delta\end{pmatrix}$. Приметимо да пошто је

$$N = (1+B)(1+A+A^2) = (1+A+A^2)(1+B),$$

следеће композиције испадају тривијалне:

$$\begin{aligned}N\gamma &= (1+B)(1+A+A^2)(A-1)\\ &= (1+B)(A^3-1)\\ &= 0;\\ N\delta &= (1+A+A^2)(1+B)(1-B)\\ &= 0.\end{aligned}$$

Значи, комозиција $N\begin{pmatrix}\gamma & \delta\end{pmatrix} = \begin{pmatrix}N\gamma & N\delta\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ је тривијална.

Коначно, разматрамо композицију последња два пресликавања, $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ и ε. Показаћемо да се сваки произвољни елемент $\lambda \in \Lambda$ пресликава у 0. Прво проверавамо где γ и δ шаљу λ:

$$\begin{aligned}\gamma\lambda &= (A-1)(x+yA+zA^2+uB+vBA+wBA^2)\\ &= xA+yA^2+zA^3+uAB+vABA+wABA^2\\ &\quad -x-yA-zA^2-uB-vBA-wBA^2\\ &= (z-x)+(x-y)A+(y-x)A^2+(v-u)B\\ &\quad +(w-v)BA+(u-w)BA^2;\\ \delta\lambda &= (B-1)(x+yA+zA^2+uB+vBA+wBA^2)\\ &= xB+yBA+zBA^2+uB^2+vB^2A+wB^2A^2\\ &\quad -x-yA-zA^2-uB-vBA-wBA^2\\ &= (u-x)+(v-y)A+(w-z)A^2+(x-u)B\\ &\quad +(y-v)BA+(z-w)BA^2.\end{aligned}$$

Сада, када применимо ε, добијамо збир коефицијената:

$$\begin{aligned}\varepsilon\gamma\lambda &= (z-x)+(x-y)+(y-x)+(v-u)+(w-v)+(u-w)\\ &= 0;\end{aligned}$$

$$\begin{aligned}\varepsilon\delta\lambda &= (u-x)+(v-y)+(w-z)+(x-u)+(y-v)+(z-w)\\ &= 0.\end{aligned}$$

Дакле, композиција $\varepsilon\begin{pmatrix}\gamma & \delta\end{pmatrix} = \begin{pmatrix}\varepsilon\gamma & \varepsilon\delta\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ је тривијална.

До сада смо показали да било која два узастопна пресликавања имају тривијалну композицију. То значи да је слика било ког пресликавања садржана у језгру следећег. Следећи корак је да се покаже да је језгро било ког пресликавања садржано у слици претходног. Опет ћемо да радимо корак по корак.

Покажимо $\ker\varepsilon \subset \operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$. Пресликавање $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ шаље елемент $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \Lambda\oplus\Lambda$ у $\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} = \gamma\lambda_1+\delta\lambda_2$. Покажимо сада да је било који елемент у језгру ε овог облика. Приметимо да

$$\lambda_1 = x_1 + y_1A + z_1A^2 + u_1B + v_1BA + w_1BA^2$$

и

$$\lambda_2 = x_2 + y_2A + z_2A^2 + u_2B + v_2BA + w_2BA^2.$$

До краја доказа претпостављамо да су λ_1 и λ_2 елементи са овако означеним коефицијентима.

Нека је $\lambda\in\Lambda$ елемент језгра од ε. Елемент λ се налази у језгру од ε, то јест $\varepsilon\lambda = 0$, када је збир његових коефицијената 0. Другим речима,

$$x+y+z+u+v+w = 0.$$

Ово ћемо да искористимо тако што ћемо да заменимо $x = -y-z-u-v-w$ у λ и затим да пронађемо λ_1 и λ_2 такве да је $\lambda = \gamma\lambda_1+\delta\lambda_2 = (A-1)\lambda_1+(B-1)\lambda_2$. Дакле,

$$\begin{aligned}\lambda &= (-y-z-u-v-w)+yA+zA^2+uB+vBA+wBA^2\\ &= y(A-1)+z(A^2-1)+u(B-1)+v(BA-1)+w(BA^2-1)\\ &= y(A-1)+z(A-1)(A+1)+u(B-1)\\ &\quad +v(BA-A+A-1)+w(BA^2-A^2+A^2-1)\\ &= (A-1)(y+z(A+1))+u(B-1)+v(B-1)A+v(A-1)\\ &\quad +w(B-1)A^2+w(A-1)(A+1)\\ &= (A-1)(y+z(A+1)+v+w(A+1))+(B-1)(u+vA+wA^2).\end{aligned}$$

Ово значи да за $\lambda_1 = (y+z+v+w)+(z+w)A$ и $\lambda_2 = u+vA+wA^2$ имамо $\lambda = \gamma\lambda_1+\delta\lambda_2$, и стога је $\ker\varepsilon\subset\operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$.

Овај резултат је био за крај низа, тј. $\ker\varepsilon = \operatorname{im}\partial_1$. Код $\ker\partial_{4k} = \operatorname{im}\partial_{4k+1}$ за $k\geq 1$ је слично, јер су $\partial_{4k} = N\varepsilon$ и $\partial_{4k+1} = \partial_1$. Тачније, како је $\ker N = 0$,

значи да је $\ker N\varepsilon = \ker\varepsilon$, па, по управо доказаном тврђењу $\ker\varepsilon = \operatorname{im}\partial_1$, добијамо $\ker N\varepsilon \in \operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$.

Покажимо сада да је $\ker\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \subset \operatorname{im} N\varepsilon$. Раније смо показали $\operatorname{im} N\varepsilon = N\mathbb{Z}$. Нека је λ елемент језгра $\ker\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Тада је $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\lambda = 0$, that is $\begin{pmatrix}\alpha\lambda\\ \beta\lambda\end{pmatrix} = \begin{pmatrix}0\\ 0\end{pmatrix}$, Дакле, имамо $\alpha\lambda = \beta\lambda = 0$, тј. $\lambda \in \ker\alpha \cap \ker\beta$. Наш циљ је сада да покажемо да је $\ker\alpha \cap \ker\beta = N\mathbb{Z}$, тј. да је $\lambda = kN$ за неки цео број k.

Почећемо са разматрањем једноставнијег од та два пресликавања, $\beta = B - 1$. Пошто је δ истог облика, значи да смо већ израчунали

$$\beta\lambda = (u-x) + (v-y)A + (w-z)A^2 + (x-u)B + (y-v)BA + (z-w)BA^2.$$

Ако је $\beta\lambda = 0$, онда то значи да су сви ови коефицијенти 0, па је $u = x$, $v = y$ и $w = z$. Дакле, сада имамо нови облик за λ:

$$\begin{aligned}\lambda &= x + yA + zA^2 + xB + yBA + zBA^2\\ &= x(1+B) + y(A+BA) + z(A^2+BA^2)\\ &= x(1+B) + y(1+B)A + z(1+B)A^2\\ &= (1+B)(x + yA + zA^2)\end{aligned}$$

Ово вуче на неку везу између пресликавања $B+1$ и $B-1$. Израчунајмо $(B+1)\lambda'$, за неки други елемент λ' у Λ облика $\lambda = x' + y'A + z'A^2 + u'B + v'BA + w'BA^2$:

$$\begin{aligned}(B+1)\lambda' &= (B+1)(x' + y'A + z'A^2 + u'B + v'BA + w'BA^2)\\ &= (x'+u') + (y'+v')A + (z'+w')A^2\\ &\quad +(u'+x')B + (v'+y')BA + (w'+z')BA^2\\ &= (x'+u')(1+B) + (y'+v')(A+BA) + (z'+w')(A^2+BA^2)\\ &= (1+B)((x'+u') + (y'+v')A + (z'+w')A^2).\end{aligned}$$

Ово је у $\ker(B-1)$ пошто је $(B-1)(B+1) = B^2 - 1 = 0$. Постављањем $x = x' + u'$, $y = y' + v'$, и $z = z' + w'$, видимо да је $\lambda = (B+1)\lambda'$. Дакле $\ker(B-1) = \operatorname{im}(B+1)$. Аналогно се добија $\ker(B+1) = \operatorname{im}(B-1)$.

Окренимо пажњу назад на $\ker\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Погледајмо како $\alpha\lambda = 0$ утиче на коефицијенте од λ:

$$\begin{aligned}\alpha\lambda &= (A-1)(B+1)A\lambda\\ &= (B + A^2 - BA - A)(x + yA + zA^2 + uB + vBA + wBA^2)\\ &= (u + y - v - z) + (v + z - w - x)A + (w + x - u - y)A^2\end{aligned}$$

$$
\begin{aligned}
&+(x+w-z-v)B+(y+u-x-w)BA+(z+v-y-u)BA^2\\
=\;& (BA^2-1)((z-y+v-u)+(x-z+w-v)A+(y-x+u-w)A^2).
\end{aligned}
$$

Пошто је вредност овога 0, значи да су сви коефицијенти 0, из чега следи услов $u+y=v+z=w+x$.

Заменом онога што смо добили из $\beta\lambda=0$, тј. $u=x$, $v=y$ и $w=z$, добијамо $x+y=y+z=z+x$, из чега одмах добијамо $x=y=z$. Дакле, сви коефицијенти λ морају бити једнаки, рецимо, неком целом броју k. Другим речима,

$$
\begin{aligned}
\lambda &= k+kA+kA^2+kB+kBA+kBA^2\\
&= k(1+A+A^2+B+BA+BA^2)\\
&= kN,
\end{aligned}
$$

и следи да смо нашли то што смо желели, да је $\ker\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ садржано у $\operatorname{im} N\varepsilon$.

Остаје да се покаже тачност средња два дела низа. Нека почнемо са $\ker\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}\subseteq\operatorname{im}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Претпоставимо да је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\ker\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$. Желимо да нађемо $\lambda\in\Lambda$ такав да је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\lambda=\begin{pmatrix}\alpha\lambda\\ \beta\lambda.\end{pmatrix}$.

Из $\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}=\begin{pmatrix}0\\ 0\end{pmatrix}$ добијамо две једначине, $\mu\lambda_1=0$ и $\kappa\lambda_1+\nu\lambda_2=0$. Израчунајмо $\mu\lambda_1$:

$$
\begin{aligned}
\mu\lambda_1 &= (-1-A+B)(x_1+y_1A+z_1A^2+_1\,uB+v_1BA+w_1BA^2)\\
&= (u_1-x_1-z_1)+(v_1-y_1-x_1)A+(w_1-z_1-y_1)A^2\\
&\quad +(x_1-u_1-v_1)B+(y_1-v_1-w_1)BA+(z_1-w_1-u_1)BA^2.
\end{aligned}
$$

Пошто су сви ти коефицијенти једнаки 0, из прва три добијамо везе $u_1=x_1+z_1$, $v_1=y_1+x_1$ и $w_1=z_1+y_1$. Заменом ових у следеће три везе, $x_1=u_1+v_1$, $y_1=v_1+w_1$ и $z_1=w_1+u_1$, добијамо исти услов, $x_1+y_1+z_1=0$. Заменом $x_1=-y_1-z_1$ назад у λ_1, добијамо

$$
\begin{aligned}
\lambda_1 &= (-y_1-z_1)+y_1A+z_1A^2-z_1B-y_1BA+(z_1+y_1)BA^2\\
&= y_1(-1+A-B+BA^2)+z_1(-1+A^2-BA+BA^2).
\end{aligned}
$$

Сада, пошто је $(BA^2+1)(BA^2-1)=0$, важи

$$
\begin{aligned}
\kappa\lambda_1 &= (BA^2+1)\lambda_1\\
&= y_1(BA^2+1)(A-B+BA^2-1)\\
&\quad +z_1(BA^2+1)(A^2-BA+BA^2-1)
\end{aligned}
$$

$$\begin{aligned} &= y_1(B-A+A-B)+z_1(BA-A^2+A^2-BA)\\ &= 0. \end{aligned}$$

Значи, аналогно како смо показали $\ker(B+1)=\mathrm{im}(B-1)$, следи $\ker(BA^2+1)=\mathrm{im}(BA^2-1)$, ра је $\lambda_1\in\mathrm{im}(BA^2-1)$. Заправо, можемо израчунати

$$\begin{aligned} \lambda_1 &= y_1(-1+A-B+BA^2)+z_1(-1+A^2-BA+BA^2)\\ &= (BA^2-1)(y_1+z_1)-y_1(B-A)-z_1(BA-A^2)\\ &= (BA^2-1)(y_1+z_1)-y_1A(BA^2-1)-z_1A^2(BA^2-1)\\ &= (BA^2-1)(y_1+z_1-y_1A-z_1A^2). \end{aligned}$$

Пошто је $\kappa\lambda_1=0$, $\kappa\lambda_1+\nu\lambda_2=0$ се сведе на $\nu\lambda_2=0$, тј. $\lambda_2\in\ker\nu$. Као што смо раније показали, $\ker(B-1)=\mathrm{im}(B+1)$, па је

$$\lambda_2=(B-1)(x_2+y_2A+z_2A^2).$$

Сада, пошто је

$$\lambda_2=\beta\lambda=(B-1)((u-x)+(v-y)A+(w-z)A^2,$$

следи $u=x+x_2$, $v=y+y_2$ и $w=z+z_2$. Заменом ових у $\lambda_1=\alpha\lambda$ имамо

$$\begin{aligned} \lambda_1 &= (BA^2-1)((z-y+v-u)+(x-z+w-v)A+(y-x+u-w)A^2)\\ &= (BA^2-1)((z-x+y_2-x_2)+(x-y+z_2-y_2)A+(y-z+x_2-z_2)A^2. \end{aligned}$$

Сада, пошто је

$$\lambda_1=(BA^2-1)(y_1+z_1-y_1A-z_1A^2)$$

изједначавањем коефицијената добијамо систем једначина

$$\begin{aligned} z-x+y_2-x_2 &= y_1+z_1\\ x-y+z_2-y_2 &= -y_1\\ y-z+x_2-z_2 &= -z_1. \end{aligned}$$

Како је прва једначина очигледно линеарна комбинација следеће две, систем заправо даје два услова, рецимо $y=z-z_1+z_2-x_2$ и $x=z-z_1+y_2-x_2$, а z остаје слободан. Према томе, за λ са таквим коефицијентима, заиста добијамо $\alpha\lambda=\lambda_1$ и $\beta\lambda=\lambda_2$, тј. $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\mathrm{im}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, што смо и желели.

Коначно, треба да покажемо $\ker\begin{pmatrix}\gamma & \delta\end{pmatrix}\subseteq\mathrm{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$. Нека је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\ker\begin{pmatrix}\gamma & \delta\end{pmatrix}$. Желимо да покажемо да је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\mathrm{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$, што значи да треба да нађемо $\lambda_1',\lambda_2'\in\Lambda$ тако да је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}=\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}\begin{pmatrix}\lambda_1'\\ \lambda_2'\end{pmatrix}$, тј.

$$\lambda_1 = \mu\lambda_1',$$

$$\lambda_2 \;=\; \kappa\lambda_1' + \nu\lambda_2'.$$

Пошто је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \ker\begin{pmatrix}\gamma & \delta\end{pmatrix}$, имамо

$$\begin{aligned}\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} &= 0\\ \gamma\lambda_1 + \delta\lambda_2 &= 0\\ \gamma\lambda_1 &= -\delta\lambda_2.\end{aligned}$$

Како су $\gamma = A - 1$ и $\delta = B - 1$, можемо да искористимо рачунице од раније да бисмо добили

$$\begin{aligned}\gamma\lambda_1 &= (z_1 - x_1) + (x_1 - y_1)A + (y_1 - x_1)A^2\\ &\quad +(v_1 - u_1)B + (w_1 - v_1)BA + (u_1 - w_1)BA^2;\\ \delta\lambda_2 &= (u_2 - x_2) + (v_2 - y_2)A + (w_2 - z_2)A^2\\ &\quad +(x_2 - u_2)B + (y_2 - v_2)BA + (z_2 - w_2)BA^2;\\ -\delta\lambda_2 &= (B-1)((u_2 - x_2) + (y_2 - v_2)A + (z_2 - w_2)A^2).\end{aligned}$$

Сада, пошто важи $\gamma\lambda_1 = -\delta\lambda_2$, можемо да изједначимо коефицијенете да добијемо следеће везе:

$$\begin{aligned}z_1 - x_1 &= -(u_2 - x_2) = -(v_1 - u_1),\\ x_1 - y_1 &= -(v_2 - y_2) = -(w_1 - v_1),\\ y_1 - z_1 &= -(w_2 - z_2) = -(u_1 - w_1).\end{aligned} \tag{4}$$

Када средимо овај систем, добијамо

$$x_1 - v_1 = y_1 - w_1 = z_1 - u_1.$$

Нека је вредност ових једнаких израза t. Сада, важи

$$\begin{aligned}\lambda_1 &= x_1 + y_1A + z_1A^2 + (t + z_1)B + (t_1 + x_1)BA + (t + y_1)BA^2\\ &= x_1(1 + BA) + y_1(A + BA^2) + z_1(A^2 + B) + t(B + BA + BA^2)\\ &= (1 + BA)(x_1 + y_1A + z_1A^2) + t(B + BA + BA^2).\end{aligned}$$

Треба да нађемо λ_1' тако да је $\lambda_1 = \mu\lambda_1'$. Довољно је наћи предслике од $1 + BA$ и $B + BA + BA^2$.

Од раније смо имали да за произвољно $\lambda \in \Lambda$ важи

$$\begin{aligned}\mu\lambda &= (u - x - z) + (v - y - x)A + (w - z - y)A^2\\ &\quad +(x - u - v)B + (y - v - w)BA + (z - w - u)BA^2.\end{aligned}$$

Изједначавањем коефицијената код овог елемента и $1 + BA$, добијамо

$$\begin{aligned} u - x - z &= 1, \\ v - y - x &= 0, \\ w - z - y &= 0, \\ x - u - v &= 0, \\ y - v - w &= 1, \\ z - w - u &= 0, \end{aligned}$$

што има као једно решење $x = v = -1$, $y = z = u = w = 0$. То значи да важи

$$\mu(-1 - BA) = 1 + BA.$$

Слично за $B + BA + BA^2$ добијамо систем једначина

$$\begin{aligned} u - x - z &= 0, \\ v - y - x &= 0, \\ w - z - y &= 0, \\ x - u - v &= 1, \\ y - v - w &= 1, \\ z - w - u &= 1, \end{aligned}$$

а једно решење овог система је $x = u = v = -1$, $y = z = w = 0$. То значи да важи

$$\mu(-1 - B - BA) = B + BA + BA^2.$$

Дакле,

$$\begin{aligned} \lambda_1 &= (1 + BA)(x_1 + y_1A + z_1A^2) + t(B + BA + BA^2) \\ &= \mu(-1 - BA)(x_1 + y_1A + z_1A^2) + \mu t(-1 - B - BA) \\ &= -\mu((1 + BA)(x_1 + y_1A + z_1A^2) + t(1 + B + BA)), \end{aligned}$$

и према томе је $\lambda_1 = \mu\lambda_1'$ за

$$\lambda_1' = (1 + BA)(x_1 + y_1A + z_1A^2) + t(1 + B + BA).$$

Сада, треба да нађемо λ_2' тако да је $\lambda_2 = \kappa\lambda_1' + \nu\lambda_2'$, тј. желимо да покажемо да је $\lambda_2 - \kappa\lambda_1' \in \operatorname{im}\nu$.

У систему (4), када саберемо сва три реда, добијамо

$$0 = x_2 + y_2 + z_2 - u_2 - v_2 - w_2 = 0$$

тј. $x_2 = -y_2 - z_2 + u_2 + v_2 + w_2$. Такође можемо из система (4) да извучемо услове $v_2 = y_2 + y_1 - x_1$ и $w_2 = z_2 + z_1 - y_1$. Сада, важи

$$\begin{aligned}\lambda_2 &= y_2(A-1) + z_2(A^2-1) + u_2(B+1) + v_2(BA+1) + w_2(BA^2+1)\\ &= y_2(A-1) + z_2(A^2-1) + u_2(B+1)\\ &\quad +(y_2+y_1-x_1)(BA+1) + (z_2+z_1-y_1)(BA^2+1)\\ &= (B+1)(u_2 + y_2A + z_2A^2) - x_1(BA+1)\\ &\quad +y_1(BA - BA^2) + z_2(BA^2+1).\end{aligned}$$

Издвојили смо део који је у $\operatorname{im}\nu$ испред, тј. $(B+1)(u_2 + y_2A + z_2A^2)$. Сада, слично за $\kappa\lambda_1'$,

$$\begin{aligned}-\kappa\lambda_1' &= (1+BA^2)((1+BA)(x_1 + y_1A + z_1A^2) + t(1+B+BA))\\ &= (1+BA+BA^2+A^2)(x_1 + y_1A + z_1A^2)\\ &\quad +t(1+BA^2+B+A+BA+A^2)\\ &= (1+B)(A^2(x_1 + y_1A + z_1A^2) + t(1+A+A^2))\\ &\quad +(1+BA)(x_1 + y_1A + z_1A^2).\end{aligned}$$

Опет смо издвојили на почетку израза део који је очигледно у $\operatorname{im}\nu$. Показаћемо сада да је $\lambda_2 - \kappa\lambda_1'$ садржан у $\operatorname{im}\nu$. Инспирисани рачунањем по модулу неког целог броја, користимо нотацију за конгруенцију по модуло уместо једнакости у првом реду, јер занемарујемо делове за које смо већ показали да су леви умножак $\nu = B+1$.

$$\begin{aligned}\lambda_2 - \kappa\lambda_1' &\equiv -x_1(BA+1) + y_1(BA - BA^2) + z_2(BA^2+1)\\ &\quad +(1+BA)(x_1 + y_1A + z_1A^2)\\ &= x_1(-BA - 1 + 1 + BA) + y_1(BA - BA^2 + A + BA^2)\\ &\quad +z_1(BA^2 + 1 + A^2 + B)\\ &= (B+1)(y_1A + z_1(1+A^2)).\end{aligned}$$

Значи, заиста $\lambda_2 - \kappa\lambda_1' \in \operatorname{im}\nu$. Дакле, показали смо да је $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \operatorname{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$.

Коначно смо завршили доказ тачности низа

$$\cdots \xrightarrow{N\varepsilon} \Lambda \xrightarrow{\begin{pmatrix}\alpha\\ \beta\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow{\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow{\begin{pmatrix}\gamma & \delta\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.$$

Дакле, он је слободно разрешење за $\mathbb{D}_3$. □

Пример 10 *Кохомолошке групе од $\mathbb{D}_3$ за тривијално дејство.*

Нека је $G = \mathbb{D}_3$ и нека је M G-модул са тривијалном G-дејством. Дакле, наше разрешење постаје

$$\cdots \xrightarrow[\partial_4]{6\varepsilon} \Lambda \xrightarrow[\partial_3]{\begin{pmatrix}0\\0\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_2]{\begin{pmatrix}-1 & 0\\ 2 & 2\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_1]{\begin{pmatrix}0 & 0\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.$$

Одавде добијамо периодични коланчани комплекс

$$\cdots \xleftarrow[d_4]{(6\varepsilon)^*} M \xleftarrow[d_3]{\begin{pmatrix}0\\0\end{pmatrix}} M \oplus M \xleftarrow[d_2]{\begin{pmatrix}-1 & 2\\ 0 & 2\end{pmatrix}} M \oplus M \xleftarrow[d_1]{\begin{pmatrix}0 & 0\end{pmatrix}} M \xleftarrow[d^0]{0} 0.$$

Напоменимо да смо модуле $\mathrm{Hom}_G(\Lambda, M)$ и $\mathrm{Hom}_G(\Lambda \oplus \Lambda, M)$ заменили изоморфним модулима M и $M \oplus M$ редом.

Сада, $H^0(G, M) = \ker d^1 = M$, а за $k \geq 1$ кохомолошке групе су следеће:

$$H^k(G, M) = \begin{cases} \ker d^2, & k \equiv 1 \mod 4, \\ \operatorname{coker} d^2, & k \equiv 2 \mod 4, \\ \ker d^4, & k \equiv 3 \mod 4, \\ \operatorname{coker} d^4, & k \equiv 0 \mod 4. \end{cases}$$

Израчунаћемо ова језгра и којезгра. Прво, као резултат d^2 на произвољни вектор $\bar{a} = \begin{pmatrix}a\\b\end{pmatrix} \in M \oplus M$ добијамо

$$\begin{pmatrix}-1 & 2\\ 0 & 2\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}2b - a\\ 2b\end{pmatrix}.$$

Према томе, ако је $\bar{a} \in \ker d^2$, онда је $a = 2b$ и $2b = 0$, тј. $a = 0$ и b је реда највише 2 у M. Означимо подмодул елемената чији редови деле $t \in \mathbb{Z}$ у M на следећи начин:

$$\mathrm{T}_M(t) = \{m \in M : \ tm = 0\}.$$

Са оваквом нотацијом, важи $b \in \mathrm{T}_M(2)$. Дакле,

$$H^{4k+1}(G, A) = \ker d^2 = 0 \oplus \mathrm{T}_M(2) \cong \mathrm{T}_M(2).$$

Пошто скуп свих комбинација облика $2a - b$ обухвата цео M, имамо да је $\operatorname{im} d^2 = M \oplus 2M$, па је

$$H^{4k+2}(G, A) = \operatorname{coker} d^2 = \frac{M \oplus M}{M \oplus 2M} \cong 0 \oplus \frac{M}{2M} \cong \frac{M}{2M}.$$

Посматрамо сада $d^4 = (6\varepsilon)^*$. Пошто је дејство групе тривијално, за било које $\lambda = \Sigma_i n_i g_i \in \Lambda$ и $m \in M$ имамо

$$\lambda \cdot m = \sum_i n_i g_i \cdot m = \sum_i n_i m = \varepsilon(\lambda) m,$$

тј. λ дејствује као множење елементом $\varepsilon(\lambda)$. Сада, нека је $f_m \in \mathrm{Hom}_G(\Lambda, M)$ коланац дефинисан са $f : 1 \mapsto m$. Ово значи да за све $\lambda \in \Lambda$, важи $f_m(\lambda) = \lambda \cdot m = \varepsilon(\lambda)m$. Проверимо сада куда d^4 пресликава овакав елемент:

$$d^4 f_m(\lambda) = f_m(\partial_4 \lambda) = f_m(6\varepsilon(\lambda)) = 6\varepsilon(\lambda) f_m(1) = 6\varepsilon(\lambda)m = 6 f_m(\lambda).$$

Значи, d^4 је једноставно множење бројем 6. Стога је једноставно рачунати кохомолошке групе: $H^{4k+3}(G, A) = \ker d^4 = \mathrm{T}_M(6)$ и $H^{4k}(G, A) = \mathrm{coker}\, d^4 = M/6M$.

Када сакупимо све ове резултате заједно, добијамо

$$H^k(G, M) = \begin{cases} M, & k = 0 \\ \mathrm{T}_M(2), & k \equiv 1 \mod 4, \\ \frac{M}{2M}, & k \equiv 2 \mod 4, \\ \mathrm{T}_M(6), & k \equiv 3 \mod 4, \\ \frac{M}{6M}, & k \equiv 0 \mod 4,\ k \geq 4. \end{cases}$$

6.3 Клајнова 4-група

У овом одељку ћемо израчунати разрешење за групу G једнаку Клајновој 4-групи $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. То ћемо учинити уз помоћ следеће тополошке чињенице:

Лема 30 *Нека је X простор типа $K(G_1, 1)$ и Y простор типа $K(G_2, 1)$. Тада је $X \times Y$ простор типа $K(G_1 \times G_2, 1)$.*

Доказ: Нека су p и q канонске пројекције из $X \times Y$ у X и Y редом. За произвољно непрекидно пресликавање $\gamma : S^k \to X \times Y$, добијамо непрекидна пресликавања $p\gamma : S^k \to X$ и $q\gamma : S^k \to Y$. Дакле, класа $[\gamma] \in \pi_k(X \times Y)$ одговара елементу $([p\gamma], [q\gamma]) \in \pi_k(X) \times \pi_k(Y)$. Са друге стране, нека су i и j канонске инклузије X и Y у $X \times Y$. За два пресликавања $\gamma_1 : S^k \to X$ и $\gamma_2 : S^k \to Y$ имамо пресликавање $\gamma : S^k \to X \times Y$ дато са $\gamma(t) = (\gamma_1(t), \gamma_2(t))$. Дакле, класа $([\gamma_1], [\gamma_2]) \in \pi_k(X) \times \pi_k(Y)$ одговара класи $[\gamma] \in \pi_k(X \times Y)$. Ове везе су добро дефинисане и инверзне једна другој, стога је $\pi_k(X \times Y) \cong \pi_k(X) \times \pi_k(Y)$, у свакој димензији $k \geq 1$.

Дакле, $\pi_1(X \times Y) \cong G_1 \times G_2$ и $\pi_k(X \times Y) = 0$ за $k > 1$, па је $X \times Y$ простор типа $K(G_1 \times G_2)$. □

Сада се фокусирамо на групу $G = V$.

Пример 11 *Конструикција разрешења за Клајнову 4-групу.*

У примеру 3 смо израчунали разрешење за $\mathbb{Z}_2$ тако што смо уочили да је $\mathbb{R}P^\infty$ простор типа $K(\mathbb{Z}_2, 1)$, па смо употребили став 10, из чега је следило да проширени ћелијски ланчани комплекс од S^∞, универзално наткривање за $\mathbb{R}P^\infty$, чини слободно разрешење $\mathbb{Z}$ над $\mathbb{Z}C_2^T$. Према леми 30, $\mathbb{R}P^\infty \times \mathbb{R}P^\infty$ је $K(G, 1)$ комплекс, а како је $S^\infty \times S^\infty$ контрактибилно универзално наткривање $\mathbb{R}P^\infty \times \mathbb{R}P^\infty$, можемо поново видети према ставу 10 да је ћелијски ланчани комплекс од $S^\infty \times S^\infty$ слободно разрешење од $\mathbb{Z}$ над $\mathbb{Z}G$.

Нека је $G = V = \{1, T, S, TS\}$ са $T^2 = S^2 = (TS)^2 = 1$. Имамо C_2^T и C_2^S као подгрупе у G, генерисане са T и S редом. Наравно, $G \cong C_2^T \times C_2^S$. Сада, означимо $X = S^\infty \times S^\infty$. Из Примера 3, имамо следећа два разрешења за C_2^T и C_2^S редом, дата ћелијским ланчаним комплексом за S^∞:

$$\ldots \xrightarrow[1+T]{\partial'_4} \Lambda' \xrightarrow[1-T]{\partial'_3} \Lambda' \xrightarrow[1+T]{\partial'_2} \Lambda' \xrightarrow[1-T]{\partial'_1} \Lambda' \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

$$\ldots \xrightarrow[1+S]{\partial''_4} \Lambda'' \xrightarrow[1-S]{\partial''_3} \Lambda'' \xrightarrow[1+S]{\partial''_2} \Lambda'' \xrightarrow[1-S]{\partial''_1} \Lambda'' \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

где је сваки $\Lambda' = \mathbb{Z}C_2^T$ и $\Lambda'' = \mathbb{Z}C_2^S$. Приметимо да важи

$$\Lambda = \mathbb{Z}G = \mathbb{Z}[C_2^T \times C_2^S] \cong \mathbb{Z}C_2^T \otimes \mathbb{Z}C_2^S = \Lambda' \otimes \Lambda''.$$

Свака k-ћелија у X је производ i-ћелије у првом S^∞ и j-ћелије у другом S^∞, где је $i + j = k$ и $i, j \geq 0$. Оне генеришу модул $\Lambda'_i \otimes \Lambda''_j$, према билинеарности. Зато, у димензији k, модул P_k је директна сума свих производа $\Lambda'_i \otimes \Lambda''_j$, тј.

$$P_k = \bigoplus_{i+j=k} \Lambda'_i \otimes \Lambda''_j \cong \bigoplus_{i=0}^{k} \Lambda.$$

Наравно, ово тачно одговара тензорском производу ланчаних комплекса. Гранично пресликавање у тензорском производу ланчаних комплекса је дато на елементу $c' \otimes c'' \in P_k$, где су $c' \in \Lambda'_i$ и $c'' \in \Lambda''_j$, са:

$$\partial_k(c' \otimes c'') = \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c''.$$

Заиста,

$$\begin{aligned} \partial\partial(c' \otimes c'') &= \partial(\partial' c' \otimes c'') + (-1)^{\deg c'} \partial(c' \otimes \partial'' c'') \\ &= \partial'\partial' c' \otimes c'' + (-1)^{\deg \partial' c'} \partial' c' \otimes c'' + (-1)^{\deg c'} \partial' c' \otimes \partial'' c'' \\ &\quad + (-1)^{\deg c' + \deg \partial' c'} c' \otimes \partial''\partial'' c''. \end{aligned}$$

Први и последњи сабирак нестају јер $\partial'\partial' = 0$ и $\partial''\partial'' = 0$. Средња два сабирка се поништавају јер $\deg \partial' c' = \deg c' + 1$. Дакле, $\partial\partial = 0$.

Затим проверавамо да је $\ker \partial_k = \operatorname{im} \partial_{k+1}$. У ту сврху, посматрамо ∂_k као линеарно пресликавање од $P_k = \bigoplus_{i+j=k} \Lambda'_i \otimes \Lambda''_j$ до P_{k-1}, чиме га можемо представити као матрицу са k врста и $k+1$ колона.

За елемент $c' \otimes c'' \in \Lambda'_i \otimes \Lambda''_j$, имамо

$$\partial_k(c' \otimes c'') = \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c'',$$

уз напомену да је $\partial'_i c' \otimes c'' \in \Lambda'_{i-1} \otimes \Lambda''_j$ и $c' \otimes \partial''_j c'' \in \Lambda'_i \otimes \Lambda''_j$. То значи да добијамо факторе из $\Lambda'_i \otimes \Lambda''_j$ у резултујућем елементу P_{k-1} од сабирака из $\Lambda'_i \otimes \Lambda''_{j+1}$ и $\Lambda'_{i+1} \otimes \Lambda''_j$. Дакле, у i-том реду матрице ∂_k, где бројимо врсте и колоне од 0, имамо ненула чланове на позицијама i и $i+1$, и нуле на другим местима. Да бисмо одредили вредност ових чланова користимо чињеницу да је $\partial'_i = T + (-1)^i$ и $\partial''_j = S + (-1)^j$, и замењујемо ове чланове у формулу за ∂_k, поново примењена на неком елементу $c' \otimes c'' \in \Lambda'_i \otimes \Lambda''_j$:

$$\begin{aligned}
\partial_k(c' \otimes c'') &= \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c'' \\
&= (T + (-1)^i) c' \otimes c'' + (-1)^i 1 \otimes (S + (-1)^j) c'' \\
&= (T + (-1)^i) c' \otimes c'' + \otimes((-1)^{k-j} S + (-1)^k) c''.
\end{aligned}$$

Дакле, имамо $1 \otimes ((-1)^{k-j} S + (-1)^k)$ на позицији (i, i) и $(T + (-1)^{i+1}) \otimes 1$ на позицији $(i, i+1)$. Међутим, пре него што прикажемо матрицу, подсетимо се да елемент $T \otimes 1$ у $\Lambda' \otimes \Lambda''$ одговара елементу T у $\Lambda = \mathbb{Z}G$, и слично, $1 \otimes S$ одговара S. Стога, након ових измена, у матричном облику имамо:

$$\partial_k = \begin{pmatrix}
S + (-1)^k & T - 1 & 0 & \cdots & 0 & 0 \\
0 & -S + (-1)^k & T + 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \ddots & T + (-1)^{k-1} & 0 \\
0 & 0 & \cdots & \cdots & (-1)^{k-1} S + (-1)^k & T + (-1)^k
\end{pmatrix}.$$

Показаћемо сада да је $\ker \partial_k = \operatorname{im} \partial_{k+1}$. Претпоставимо да је $\bar{\lambda} \in \ker \partial_k$, тј. $\bar{\lambda} \in P_k$ и $\partial_k \bar{\lambda} = 0$. Означимо вектор $\bar{\lambda}$ са $\bar{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_k)$. Сада, из $\partial_k \bar{\lambda} = 0$ добијамо систем од $k-1$ једначина:

$$\begin{aligned}
(S + (-1)^k)\lambda_0 + (T - 1)\lambda_1 &= 0, \\
(-S + (-1)^k)\lambda_1 + (T + 1)\lambda_2 &= 0, \\
&\vdots \\
((-1)^{k-1} S + (-1)^k)\lambda_{k-1} + (T + (-1)^k)\lambda_k &= 0.
\end{aligned}$$

Проверимо прву једначину:

$$(S + (-1)^k)\lambda_0 = -(T-1)\lambda_1. \tag{5}$$

Можемо да поништимо десну страну једначине множењем обе стране с лева са $(T+1)$, чиме следи

$$(T+1)(S + (-1)^k)\lambda_0 = 0.$$

Дакле, $\lambda_0 \in \ker(T+1)(S+(-1)^k)$. Успут, израчунајмо $\ker(T-1)$. Претпоставимо да је $\lambda = x + yT + zS + wTS \in \Lambda$. Имамо

$$\begin{aligned}(T-1)\lambda &= (T-1)(x+yT+zS+wTS)\\ &= (y-x)+(w-z)T+(x-y)S+(z-w)TS\\ &= (T-1)((y-x)+(w-z)S),\end{aligned}$$

па ако је $(T-1)\lambda = 0$, онда је $x = y$ и $z = w$, и стога је

$$\lambda = x + xT + zS + zTS = (1+T)(x+zS).$$

Међутим, слично имамо за $\lambda' \in \Lambda$:

$$\begin{aligned}(T+1)\lambda' &= (T+1)(x'+y'T+z'S+w'TS)\\ &= (y'+x')+(w'+z')T+(x'+y')S+(z'+w')TS\\ &= (T+1)((y'+x')+(w'+z')S).\end{aligned}$$

Дакле, за $y' + x' = x$ и $w' + z' = z$, имамо $(T+1)\lambda' = \lambda$. Према томе, $\ker(T-1) = \mathrm{im}(T+1) = (T+1)\Lambda = \{(T+1)(a+bS) : \ a, b \in \mathbb{Z}\}$. Слично, $\ker(T+1) = (T-1)\Lambda$, и аналогно важи за $S+1$ и $S-1$.

Вратимо се на наш рачун за $\lambda_0 \in \ker(T+1)(S+(-1)^k)$. Елементи у $\ker(T+1)$ су облика $(T-1)(a+bS)$, а елементи у $\mathrm{im}(S+(-1)^k)$ су облика $(S+(-1)^k(c+dT)$. Како је λ_0 у оба, имамо

$$(S + (-1)^k)\lambda_0 = (T-1)(a+bS) = (S+(-1)^k)(c+dT),$$

дакле,

$$\begin{aligned}(T-1)(a+bS) &= (S+(-1)^k)(c+dT)\\ -a + aT - bS + bTS &= (-1)^k c + (-1)^k dT + cS + dTS,\end{aligned}$$

из чега следи $a = (-1)^{k+1}c$, $a = (-1)^k d$, $-b = c$ и $b = d$. Дакле, $b = (-1)^k a$, тј.

$$(S + (-1)^k)\lambda_0 = (T-1)(S+(-1)^k)a. \tag{6}$$

Преуређујући ово, имамо

$$(S + (-1)^k)(\lambda_0 - (T-1)a) = 0,$$

што значи да је $\lambda_0 - (T-1)a \in \ker S + (-1)^k$, тј.

$$\lambda_0 = (S + (-1)^{k+1})\mu_0 + (T-1)\mu_1,$$

за $\mu_0 \in \Lambda$ и $\mu_1 = a \in \Lambda$. Сада, враћајући се на једначину (5) и замењујући (6), имамо

$$(T-1)\lambda_1 = -(T-1)(S + (-1)^k)\mu_1,$$

по чему се λ_1 разликује од $(S + (-1)^k)\mu_1$ за елемент од $\ker T - 1$, рецимо $(T+1)\mu_2$. Дакле,

$$\lambda_1 = (-S + (-1)^{k+1})\mu_1 + (T+1)\mu_2.$$

Сада, заменом овога у другу једначину из система,

$$(T+1)\lambda_2 + -(-S + (-1)^k)\lambda_1 = 0,$$

добијамо

$$(T+1)\lambda_2 = -(-S + (-1)^k)\mu_1,$$

и тако, опет, λ_2 се разликује од $(S+(-1)^k)\mu_1$ за елемент од $\ker T - 1$, рецимо $(T+1)\mu_2$, и стога важи

$$\lambda_2 = (S + (-1)^{k+1})\mu_2 + (T-1)\mu_3.$$

Ако наставимо овај процес индуктивно, добијамо да је вектор

$$\begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix}^T = \begin{pmatrix} (S + (-1)^{k+1})\mu_0 + (T-1)\mu_1 \\ (-S + (-1)^{k+1})\mu_1 + (T+1)\mu_2 \\ (S + (-1)^{k+1})\mu_2 + (T-1)\mu_3 \\ \vdots \\ ((-1)^k S + (-1)^{k+1})\mu_k + (T + (-1)^k)\mu_{k+1} \end{pmatrix}^T = \partial_{k+1} \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \mu_{k+1} \end{pmatrix},$$

тј. $\bar{\lambda}^T = \partial_k \bar{\mu}$, за неко $\bar{\mu} \in P_{k+1}$. Дакле, $\ker \partial_k = \operatorname{im} \partial_{k+1}$.

Тако смо конструисали разрешење за $\mathbb{Z}$ над Λ:

$$\cdots \longrightarrow P_3 \xrightarrow{\partial_3} P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \longrightarrow 0.$$

Пример 12 *Кохомолошке групе Клајнове 4-групе за тривијално дејство групе.*

Да бисмо израчунали кохомолошке групе Клајнове 4-групе $G = V$, морамо да посматрамо коланчани комплекс

$$\cdots \leftarrow \mathrm{Hom}_G(P_k, A) \xleftarrow[d^k]{} \mathrm{Hom}_G(P_{k-1}, A) \xleftarrow[d^{k-1}]{} \ldots \xleftarrow[d^1]{} \mathrm{Hom}_G(P_0, A) \leftarrow 0.$$

Како је сваки P_k директна сума $k+1$ копија од Λ, значи да је

$$\mathrm{Hom}_G(P_k, A) \cong \mathrm{Hom}_G(\bigoplus_{i=0}^{k} \Lambda, A) \cong \bigoplus_{i=0}^{k} \mathrm{Hom}_G(\Lambda, A) \cong \bigoplus_{i=0}^{k} A.$$

Гранично пресликавање d^k је стога представљено у матричном облику као транспозиција од матрице за ∂_k:

$$\begin{pmatrix} S+(-1)^k & 0 & \cdots & \cdots & 0 & 0 \\ T-1 & -S+(-1)^k & \cdots & \cdots & 0 & 0 \\ 0 & T+1 & \ddots & & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & & \ddots & (-1)^{k-2}S+(-1)^k & 0 \\ 0 & 0 & \cdots & \cdots & T+(-1)^{k-1} & (-1)^{k-1}S+(-1)^k \\ 0 & 0 & \cdots & \cdots & 0 & T+(-1)^k \end{pmatrix}.$$

Да бисмо израчунали кохомолошку групу димензије k, морамо пронаћи $\ker d_{k+1}$ и $\mathrm{im}\, d_k$. У димензији 0, имамо $\mathrm{im}\, d_0 = 0$ и $d^1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, тј. $\ker d^1 = A$, па је $H^0(G, A) = A$.

Израчунајмо елементе у вектору $\bar{b} = d^k \bar{a} \in P_k$ за произвољно $\bar{a} \in P_{k-1}$. Делимо резултате на два случаја, када је $k = 2n$ парно (лево) и када је $k = 2n+1$ непарно (десно):

$$\begin{aligned} b_0 &= 2a_0 \\ b_1 &= 0a_0 + 0a_1 \\ b_2 &= 2a_1 + 2a_2 \\ &\vdots \\ b_{k-1} &= 0a_{k-2} + 0a_{k-1} \\ b_k &= 2a_{k-1} \end{aligned} \qquad \begin{aligned} b_0 &= 0a_0 \\ b_1 &= 0a_0 - 2a_1 \\ b_2 &= 2a_1 + 0a_2 \\ &\vdots \\ b_{k-1} &= 2a_{k-2} + 0a_{k-1} \\ b_k &= 0a_{k-1} \end{aligned}$$

Прво, израчунајмо $H^{2n}(G, A) = \ker d^{2n+1} / \mathrm{im}\, d^{2n}$. Имамо

$$\ker d^{2n+1} = A \oplus \mathrm{T}_A(2) \oplus A \oplus \ldots \mathrm{T}_A(2) \oplus A,$$

где је $\mathrm{T}_A(2) = \{a \in A : \ 2a = 0\}$, подмодул од A сачињен елементима реда највише 2. Напоменимо да је ово исто као и група елемената фиксираних дејством $-1 \in \Lambda$ на A, јер је $2a = 0 \Leftrightarrow (-1) \cdot a = a$. Имамо $2n$ фактора у директној суми, јер се d^{2n+1} пресликава из $\mathrm{Hom}_g(P_{2n}, A) \cong \bigoplus_{i=0}^{2n} A$, директне суме $2n$ копија A. Затим имамо

$$\operatorname{im} d^{2n} = 2A \oplus 0 \oplus 2A \oplus \cdots \oplus 0 \oplus 2A.$$

Дакле:

$$\begin{aligned} H^{2n}(G, A) &= \frac{\ker d^{2n+1}}{\operatorname{im} d^{2n}} \\ &= \frac{A \oplus \mathrm{T}_A(2) \oplus A \oplus \ldots \mathrm{T}_A(2) \oplus A}{2A \oplus 0 \oplus 2A \oplus \cdots \oplus 0 \oplus 2A} \\ &= \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \frac{A}{2A} \oplus \cdots \oplus \frac{A}{2A} \oplus \mathrm{T}_A(2) \\ &= \big(\mathrm{T}_A(2)\big)^n \oplus \big(\frac{A}{2A}\big)^{n+1}. \end{aligned}$$

Затим, израчунајмо $H^{2n-1}(G, A) = \ker d^{2n} / \operatorname{im} d^{2n-1}$. Имамо

$$\ker d^{2n} = \mathrm{T}_A(2) \oplus B \oplus \cdots \oplus B \oplus \mathrm{T}_A(2),$$

где је $B = \{(a, b) \in A \oplus A : \ 2a + 2b = 0\}$. Ово можемо протумачити као „дат је елемент $a \in A$, пронаћи $b \in A$ тако да је $a + b \in \mathrm{T}_A(2)$“. Ова логика нас води до везе $\varphi : B \to A \oplus \mathrm{T}_A(2)$ дате са $(a, b) \mapsto (a, a + b)$. Тривијално се види да је ово изоморфизам, па је $B \cong A \oplus \mathrm{T}_A(2)$. Затим,

$$\operatorname{im} d^{2n-1} = 0 \oplus (-2, 2)A \oplus \cdots \oplus (-2, 2)A \oplus 0,$$

где је $(-2, 2)A$ подмодул модула $A \oplus A$ генерисан са $(-2, 2)$. Како је $(-2, 2) \in B$, то значи $(-2, 2)A \subseteq B$. Слика овог подмодула под изоморфизмом φ је $2A \oplus 0$, па је

$$\frac{B}{(-2, 2)A} \cong \frac{A \oplus \mathrm{T}_A(2)}{2A \oplus 0} \cong \frac{A}{2A} \oplus \mathrm{T}_A(2).$$

Коначно, израчунавамо

$$\begin{aligned} H^{2n-1}(G, A) &= \frac{\ker d^2 n}{\operatorname{im} d^{2n-1}} \\ &= \frac{\mathrm{T}_A(2) \oplus B \oplus \ldots B \oplus \mathrm{T}_A(2)}{0 \oplus (-2, 2)A \oplus \cdots \oplus (-2, 2)A \oplus 0} \\ &= \mathrm{T}_A(2) \oplus \frac{B}{(-2, 2)A} \oplus \ldots \frac{B}{(-2, 2)A} \oplus \mathrm{T}_A(2) \end{aligned}$$

$$
\begin{aligned}
&= \mathrm{T}_A(2) \oplus \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \dots \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \mathrm{T}_A(2) \\
&= \big(\mathrm{T}_A(2)\big)^{n+1} \oplus \big(\frac{A}{2A}\big)^{n-1}.
\end{aligned}
$$

Дакле, израчунали смо кохомолошке групе групе $G = V$ над групом A са тривијалним G-дејством:

$$
H^k(G, A) = \begin{cases} A & k = 0 \\ \big(\mathrm{T}_A(2)\big)^{n+1} \oplus \big(\frac{A}{2A}\big)^{n-1} & k = 2n-1,\ n \geq 1 \\ \big(\mathrm{T}_A(2)\big)^{n} \oplus \big(\frac{A}{2A}\big)^{n+1} & k = 2n,\ n \geq 1. \end{cases}
$$

6.4 Раширења реда 12

Наш циљ у овом одељку је да користимо теорију раширења група како бисмо лакше класификовали све групе реда 12. Према Силовљевој теорији, свака група реда 12 се заиста факторише као раширење једне од својих подгрупа другом.

Претпоставимо да је G група реда 12. Нека је $s_3 = |\mathrm{Syl}_3(G)|$ број Силовљевих 3-подгрупа од G. Према трећој Силовљевој теореми, морамо имати $s_3 | 4$ и $s_3 \equiv 1 \mod 3$. То значи $s_3 = 1$ или $s_3 = 4$. Претпоставимо да је $s_3 = 4$. Онда, то значи да имамо 4 Силовљеве 3-подгрупе у G. Пошто су ове подгрупе све реда 3, оне су генерисане било којим њиховим нетривијалним елементом. Дакле, пресек било које две различите 3-подгрупе мора бити тривијалан. Набрајањем различитих елемената у свакој подгрупи, имамо $4 \cdot 2 = 8$ елемената реда 3, што нам заједно са неутралним елементом даје укупно 9 елемената. Преостала 3 елемента, заједно са неутралним елементом, морају формирати једину Силовљеву 2-групу. Дакле, $s_2 = 1$.

Када је $s_p = 1$, то значи да имамо једну Силовљеву p-групу, што значи да је та подгрупа нормална. Стога је за нашу групу G гарантовано да има нормалну подгрупу реда 3 или 4. Назовимо је A, напомињући да мора бити Абелова. Претпоставимо да је A реда 3. У G постоји барем једна 2-подгрупа, тј. подгрупа реда 4. Пошто ниједан њен елемент не може бити реда 3, то значи да има тривијални пресек са нормалном Абеловом подгрупом A. Дакле, G је заправо еквивалентно раширењу A овом подгрупом. Обрнуто, ако је A реда 4, онда је G еквивалентно раширењу A Силовљевом 3-групом. Да бисмо остали доследни са нашом досадашњом нотацијом, преименоваћемо G у E и назваћемо подгрупу којом проширујемо A са G .

Ми смо сада дошли до закључка да свака група реда 12 може да се представи раширењем групе

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

где је A група реда 3 или 4, а G је група реда $12/|A|$. Пошто постоји само једна група реда 3, $\mathbb{Z}_3 \cong C_3^T$, и две групе реда 4, наиме $\mathbb{Z}_4 \cong C_T^4$ и $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$, покривамо све случајеве у следећа четири примера.

Пример 13 *Раширења $\mathbb{Z}_3$ са $\mathbb{Z}_4$.*

$$0 \longrightarrow \mathbb{Z}_3 \xrightarrow{\iota} E \xrightarrow{\pi} C_4^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_4^T \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$, па, пошто се T пресликава у елемент чији ред дели 2, мора да важи или $T \cdot a = a$ или $T \cdot a = -a$.

Нека је $T \cdot a = a$. Сада,

$$\mathbb{Z}_3^{\mathbb{Z}_4} = \mathbb{Z}_3$$

и

$$N\mathbb{Z}_3 = (1 + T + T^2 + T^3)\mathbb{Z}_3 = (1 + 1 + 1 + 1)\mathbb{Z}_3 = 4\mathbb{Z}_3 = \mathbb{Z}_3,$$

и стога је

$$H^2(\mathbb{Z}_4, \mathbb{Z}_3) = \frac{\mathbb{Z}_3^{\mathbb{Z}_4}}{N\mathbb{Z}_3} = \frac{\mathbb{Z}_3}{\mathbb{Z}_3} \cong 0.$$

Јединствено раширење у овом случају одговара $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$, по леми 27.

Нека је $T \cdot a = -a$. Једини фиксни елемент је 0, па важи

$$\mathbb{Z}_3^{\mathbb{Z}_4} = 0$$

и

$$N\mathbb{Z}_3 = (1 + T + T^2 + T^3)\mathbb{Z}_3 = (1 - 1 + 1 - 1)\mathbb{Z}_4 = \{0\},$$

и стога је

$$H^2(\mathbb{Z}_4, \mathbb{Z}_3) = \frac{\mathbb{Z}_3^{\mathbb{Z}_4}}{N\mathbb{Z}_3} = \frac{\{0\}}{\{0\}} \cong 0.$$

Факторски систем одговара тривијалној кохомолошкој класи, па операција у E постаје

$$(a, T^k)(b, T^l) = (a + T^k \cdot b, T^{k+l}) = (a + (-1)^k b, T^{k+l}).$$

Ова група је изоморфна дициклична група

$$\mathrm{Dic}_3 = \langle x, y \mid x^6 = y^4 = 1,\ y^2 = x^3,\ yxy^{-1} = x^{-1} \rangle$$

где су $x = (1, T^2)$ и $y = (0, T)$. Заиста, $y^2 = x^3 = (0, T^2) = (0, T^2)$, а пошто $(0, T^2)(0, T^2) = (0, 1)$, значи да је $x^6 = y^4 = 1$. Такође, важи

$$yxy^{-1} = (0, T)(1, T^2)(0, T)^{-1} = (0 - 1, T^3)(0, T^3) = (-1, T^2) = x^{-1}.$$

Пример 14 *Раширења $\mathbb{Z}_3$ са $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Заменимо $\mathbb{Z}_2 \times \mathbb{Z}_2$ изоморфном групом V, генерисаном са T и S, као у примеру 11. Посматрамо раширење дефинисано са

$$0 \longrightarrow \mathbb{Z}_3 \xrightarrow{\iota} E \xrightarrow{\pi} V \longrightarrow 0.$$

Дејство групе је одређено хомоморфизмом $\varphi : V \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$. Нетривијални аутоморфизам одговара множењу са -1 (или 2, еквивалентно), што има ред 2. Оба генератора T и S су реда 2, тако да оба могу дејствовати као множење са 1 или -1, независно један од другог. То значи да имамо следећа четири случаја:

1. $T \mapsto 1$, $S \mapsto 1$;
2. $T \mapsto 1$, $S \mapsto -1$;
3. $T \mapsto -1$, $S \mapsto 1$;
4. $T \mapsto -1$, $S \mapsto -1$.

По симетрији, трећи случај је еквивалентан другом једноставном заменом генератора. Мање очигледно, четврти случај је такође еквивалентан претходна два, пошто је $TS \mapsto (-1)(-1) = 1$, тј. TS делује тривијално. Дакле, ако једноставно узмемо за генераторе од V уствари TS и S, овај случај је такође еквивалентан другом. Дакле, имамо два нееквивалентна случаја: када је дејство V на $\mathbb{Z}_3$ тривијално, и када један нетривијални елемент делује тривијално, док друга два делују као множење са -1.

Први случај: V дејство на $\mathbb{Z}_3$ је тривијално, тј. $T \cdot a = S \cdot a = a$, за све $a \in \mathbb{Z}_3$. Раширења су сада одређена са $H^2(V, \mathbb{Z}_3)$, што смо израчунали у примеру 12:

$$H^2(V, \mathbb{Z}_3) = \mathrm{T}_{\mathbb{Z}_3}(2) \oplus \left(\frac{\mathbb{Z}_3}{2\mathbb{Z}_3}\right)^2 \cong 0 \oplus 0^2 \cong 0.$$

Према томе, постоји само једно раширење у овом случају, а оно је $E = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$ по леми 27.

Други случај: $T \cdot a = a$ и $S \cdot a = -a$, за све $a \in \mathbb{Z}_3$. У примеру 12 смо приказали разрешење и гранична пресликавања d^* у генералном случају. Заменимо T и S у d^2 и d^3 да бисмо израчунали $H^2(V, \mathbb{Z}_3)$ за овај случај:

$$d^2 = \begin{pmatrix} S+1 & 0 \\ T-1 & -S+1 \\ 0 & T+1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -2 \\ 0 & 2 \end{pmatrix},$$

$$d^2 = \begin{pmatrix} S-1 & 0 & 0 \\ T-1 & -S-1 & 0 \\ 0 & T+1 & S-1 \\ 0 & 0 & T-1 \end{pmatrix} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Сада, израчунамо

$$\begin{aligned} \ker d^3 &= \{(x,y,z) \in \mathbb{Z}_3^3 \mid -2x = 0,\ 2y - 2z = 0\} \\ &= \{(x,y,z) \in \mathbb{Z}_3^3 \mid 2x = 0,\ y = z\} \\ &= \mathrm{T}_{\mathbb{Z}_3}(2) \oplus (1,1)\mathbb{Z}_3, \end{aligned}$$

$$\begin{aligned} \operatorname{im} d^2 &= \{d^2(a,b) \mid a,b \in \mathbb{Z}_3\} \\ &= \{(0,2b,2b) \mid b \in \mathbb{Z}_3\} \\ &= 0 \oplus (1,1)\mathbb{Z}_3. \end{aligned}$$

Стога, добијамо

$$H^2(\mathbb{Z}_3, V) = \frac{\ker d^3}{\operatorname{im} d^2} \cong \frac{0 \oplus (1,1)\mathbb{Z}_3}{0 \oplus (1,1)\mathbb{Z}_3} \cong 0,$$

па опет постоји само једно могуће раширење, који одговара тривијалној кохомолошкој класи.

Операција у E за тривијални факторски систем је дата за све $a, b \in \mathbb{Z}_3$ и $g, h \in V$ са

$$(a,g)(b,h) = (a + g \cdot b, gh).$$

Видимо да је елемент $(1,S)$ реда 6, па генерише подгрупу реда 6. Елемент $(0,T)$ је реда 2, и делује на $(1,S)$ конјугацијом као

$$(0,T)(1,S)(0,T) = (0,T)(1,TS) = (2,S) = (1,S)^{-1}.$$

Ово значи да елементи $(1,S)$ и $(0,T)$ чине генераторе за диедарску групу од 12 елемената. Дакле, $E \cong \mathbb{D}_6$.

Пример 15 *Раширења $\mathbb{Z}_4$ са $\mathbb{Z}_3$.*

$$0 \longrightarrow \mathbb{Z}_4 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_3^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_3^T \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, па пошто се T пресликава у елемент чији ред дели 3, дејство мора бити тривијално. Према томе, $\mathbb{Z}_4^{\mathbb{Z}_3} = \mathbb{Z}_4$, и

$$N\mathbb{Z}_4 = (1 + T + T^2)\mathbb{Z}_4 = (1+1+1)\mathbb{Z}_4 = 3\mathbb{Z}_4 = \mathbb{Z}_4,$$

па важи

$$H^2(\mathbb{Z}_3, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_3}}{N\mathbb{Z}_4} = \frac{\mathbb{Z}_4}{\mathbb{Z}_4} \cong 0.$$

Раширење је $\mathbb{Z}_4 \times \mathbb{Z}_3$.

Пример 16 *Раширења* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *са* $\mathbb{Z}_3$.

$$0 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} C_3^T \longrightarrow 0.$$

Означимо $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$ где је $V = \{1, R, S, RS\}$ опет Клајнову 4-групу генерисану са T и S. Дејство је одређено пресликавањем $C_3^T \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$, а како T мора да се пресликава у елемент чији ред дели 3, одговарајуће дејство мора бити тривијално или 3-циклус.

Нека је ово дејство тривијално. Сада, $A^{\mathbb{Z}_3} = A$, и

$$NA = (1 + T + T^2)A = (1 + 1 + 1)A = 3A = A,$$

па важи

$$H^2(\mathbb{Z}_3, A) = \frac{A^{\mathbb{Z}_3}}{NA} = \frac{A}{A} \cong 0.$$

Раширење је стога $A \times \mathbb{Z}_3$.

Сада, размотримо нетривијално дејство C_3^T на $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Означимо елементе A: $e = (0, 0)$, $a = (0, 1)$, $b = (1, 0)$ и $c = (1, 1)$, и користимо мултипликативну нотацију за операцију у A. Како T делује на A као 3-циклус, можемо без губитка општости да претпоставимо да се T слика у 3-циклус $(a\ b\ c)$, тј. $T \cdot a = b$, $T \cdot b = c$ и $T \cdot c = a$. Сада можемо израчунати $A^G = \{e\}$, и

$$NA = (1 + T + T^2)A = \{eee,\ abc\} = \{e\}.$$

Дакле,

$$H^2(A, G) = \frac{A^G}{NA} = \frac{0}{0} \cong 0,$$

што значи да имамо јединствено раширење. Операција у E је сада дефинисана са

$$(x, g)(y, h) = (x(g \cdot h), gh),$$

за све $x, y \in A$ и $g, h \in G$. Приметимо да је

$$(e, g)(x, 1)(e, g)^{-1} = (e, g)(x, g^2) = (g \cdot x, 1),$$

за све $x \in A$ и $g \in G$. Дакле, (e, T) и $(a, 1)$ генеришу цело E.

Група A може дејствовати сама на себе множењем с лева. Ово нам даје утапање $A \hookrightarrow \mathrm{Sym}(A)$ дато са $a \mapsto \sigma_a = (e\ a)(b\ c)$, $b \mapsto \sigma_b = (e\ b)(a\ c)$ и

$c \mapsto \sigma_c = (e\ c)(a\ b)$. Слично, дејство G на A може да се схвата као утапање $G \hookrightarrow \mathrm{Sym}(A)$ дато са $T \mapsto \tau = (a\ b\ c)$. То значи да можемо утапати и E, третирајући елемент (x, g) као композицију x и g. Заиста, како се при томе $(e, T)(a, 1)(e, T)^{-1}$ пресликава у

$$\tau(e\ a)(b\ c)\tau^{-1} = (e\ \tau(a))(\tau(b)\ \tau(c)) = \sigma_{\tau(a)} = \sigma_{T\cdot a} = \sigma_b,$$

имамо да је $(e, T)(a, 1)(e, T)^{-1} = (b, 1)$. Дакле, утапање је добро дефинисано. Слика утапања је генерисана двоструком транспозицијом σ_a и 3-циклусом τ, па је изоморфна алтернирајућој групи $\mathbb{A}_4$.

Значи, показали смо да раширење у овом случају одговара алтернирајућој групи $\mathbb{A}_4$.

Пронашли смо сада све групе реда 12, наравно до на изоморфизам. Оне су:

$$\mathbb{Z}_{12},\ \mathbb{Z}_2 \otimes \mathbb{Z}_6,\ \mathbb{D}_6,\ \mathbb{A}_4,\ \mathrm{Dic}_3.$$

Међутим, групе реда 12 могу да се посматрају као раширења група на друге начине, не само као раширење $\mathbb{Z}_3$ групом реда 4 и обрнуто. Ради комплетирања, покрићемо преостале такве примере. Група реда 12 може имати подгрупе реда 2, 3, 4 и 6. Дакле, група реда 12 може се приказати као раширење Абелове групе A групом G на следеће начине:

- $\mathbb{Z}_2$ за $\mathbb{Z}_6$ или $\mathbb{D}_3$;
- $\mathbb{Z}_3$ за $\mathbb{Z}_4$ или $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- $\mathbb{Z}_4$ или $\mathbb{Z}_2 \times \mathbb{Z}_2$ за $\mathbb{Z}_3$;
- $\mathbb{Z}_6$ за $\mathbb{Z}_2$.

Преостале случајеве ћемо обрадити у примерима који следе.

Пример 17 *Раширења $\mathbb{Z}_6$ са $\mathbb{Z}_2$.*

$$0 \longrightarrow \mathbb{Z}_6 \xrightarrow{\iota} E \xrightarrow{\pi} C_2^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_2^T \to \mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$, па пошто се T пресликава у елемент чији ред дели 2, мора важити или $T \cdot a = a$ или $T \cdot a = -a$.

Нека је $T \cdot a = a$. Сада,

$$\mathbb{Z}_6^{\mathbb{Z}_2} = \mathbb{Z}_6$$

и

$$N\mathbb{Z}_6 = (1 + T)\mathbb{Z}_6 = (1 + 1)\mathbb{Z}_6 = 2\mathbb{Z}_6$$

па

$$H^2(\mathbb{Z}_2, \mathbb{Z}_6) = \frac{\mathbb{Z}_6^{\mathbb{Z}_2}}{N\mathbb{Z}_6} = \frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \cong \mathbb{Z}_2.$$

Раширења су $\mathbb{Z}_6 \times \mathbb{Z}_2$ и $\mathbb{Z}_{12}$, аналогно примеру 7, рецимо.

Нека је $T \cdot a = -a$. Сада, фиксирани елементи су 0 и 3. Значи,

$$\mathbb{Z}_6^{\mathbb{Z}_2} = \{0, 3\}$$

а

$$N\mathbb{Z}_3 = (1 - T)\mathbb{Z}_6 = (1 - 1)\mathbb{Z}_6 = \{0\}$$

па је

$$H^2(\mathbb{Z}_2, \mathbb{Z}_6) = \frac{\mathbb{Z}_6^{\mathbb{Z}_2}}{N\mathbb{Z}_6} = \frac{\{0, 3\}}{\{0\}} \cong \mathbb{Z}_2.$$

Као што смо израчунали у примерима 7 и 8, факторски систем је 0 свуда осим у $f(T, T)$, где имамо $2f(T, T) = 0$, па је $f(T, T) = 0$, што одговара раширењу $\mathbb{D}_6$, или $f(T, T) = 3$. Овде имамо операцију одређену следећим једначинама:

$$\begin{aligned}
(a, 1)(b, 1) &= (a + b, 1) \\
(a, 1)(b, T) &= (a + b, T) \\
(a, T)(b, 1) &= (a - b, T) \\
(a, T)(b, T) &= (a - b + 3, 1).
\end{aligned}$$

Елементи облика $(a, 1)$ генеришу нормалну подгрупу изоморфну са $\mathbb{Z}_6$. Елементи облика (a, T) су реда 4, јер је $(a, T)(a, T) = (3, 1)$. Показујемо да је ова група изоморфна дицикличној групи

$$\mathrm{Dic}_3 = \langle a, b \mid a^6 = b^4 = 1,\ b^2 = a^3,\ bab^{-1} = a^{-1} \rangle.$$

Постављањем $a = (1, 1)$ и $b = (0, T)$ видимо да заиста $a^6 = b^4 = (0, 1)$ и $b^2 = a^3 = (3, 1)$. Све што је преостало је да се покаже последњи услов:

$$bab^{-1} = (0, T)(1, 1)(0, T)^{-1} = (-1, T)(3, T) = (-1 - 3 + 3, 1) = (5, 1) = a^{-1}.$$

Значи, коначно, сва могућа раширења су $\mathbb{Z}_6 \times \mathbb{Z}_2$, $\mathbb{Z}_{12}$, $\mathbb{D}_6$ и Dic_3.

Пример 18 *Раширења $\mathbb{Z}_2$ са $\mathbb{Z}_6$.*

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_6^T \longrightarrow 0.$$

Дејство је одређено пресликавањем $C_6^T \to \mathrm{Aut}(\mathbb{Z}_2) \cong 0$, па је G-дејство тривијално, тј. $T \cdot a = a$. Дакле, $\mathbb{Z}_2^{\mathbb{Z}_6} = \mathbb{Z}_2$, и

$$N\mathbb{Z}_2 = (1 + T + T^2 + T^3 + T^4 + T^5)\mathbb{Z}_2 = 6\mathbb{Z}_2 = 0,$$

и стога је

$$H^2(\mathbb{Z}_6, \mathbb{Z}_2) = \frac{\mathbb{Z}_2^{\mathbb{Z}_6}}{N\mathbb{Z}_2} = \frac{\mathbb{Z}_2}{0} \cong \mathbb{Z}_2.$$

Као и раније, ова два раширења одговарају групама $\mathbb{Z}_2 \times \mathbb{Z}_6$ и $\mathbb{Z}_{12}$.

Пример 19 *Раширења $\mathbb{Z}_2$ са $\mathbb{D}_3$.*

Нека је $\mathbb{D}_3 = \langle T, S \mid T^3 = S^2 = 1,\ STS = T^{-1} \rangle$.

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } \mathbb{D}_3 \longrightarrow 0.$$

Дејство је одређено пресликавањем $\mathbb{D}_3 \to \mathrm{Aut}(\mathbb{Z}_2) \cong 0$, па је G-дејство тривијално, тј. $T \cdot a = S \cdot a = a$.

По примеру 10, можемо израчунати другу кохомолошку групу:

$$H^2(\mathbb{Z}_2, \mathbb{D}_3) = \frac{\mathbb{Z}_2}{2\mathbb{Z}_2} = \frac{\mathbb{Z}_2}{0} \cong \mathbb{Z}_2.$$

Дакле, имамо два случаја. Према леми 27, раширење које одговара класи тривијалне кохомологије је $\mathbb{Z}_2 \times \mathbb{D}_3 \cong \mathbb{D}_6$. Размотримо нетривијални случај. Овде је формула за факторски систем дата са

$$f(h, k) + f(gh, k) + f(g, hk) + f(g, h) = 0. \tag{7}$$

Дефинишимо нетривијални факторски систем на следећи начин: $f(s^i r^a, s^j r^b) = ij$, за све $s^i r^a, s^j r^b \in \mathbb{D}_3$. Заиста, (7) постаје $jk + (i + j)k + i(j + k) + ij = 0$, што важи за све $i, j, k \in \mathbb{Z}_2$.

Ова група је изоморфна дицикличној групи

$$\mathrm{Dic}_3 = \langle x, y \mid x^6 = y^4 = 1,\ y^2 = x^3,\ yxy^{-1} = x^{-1} \rangle$$

где је $x = (1, r)$ и $y = (0, s)$. Заиста, $y^2 = x^3 = (1, 1)$, и како је $(1, 1)(1, 1) = (0, 1)$, то значи $x^6 = y^4 = 1$. Коначно,

$$yxy^{-1} = (0, s)(1, r)(0, s)^{-1} = (1, sr)(1, s) = (1, srs) = (1, r^{-1}) = x^{-1}.$$

Дакле, раширења у овом случају су $\mathbb{D}_6$ и Dic_3.

6.5 Примена кохомологија група на p-групе са цикличном подгрупом индекса p

Циљ овог одељка је да се искористи примена кохомологије група на раширења група како би се одредила класификација p-група које садрже цикличну подгрупу индекса p, где је p прост број. Наравно, класичан је резултат да је таква подгрупа нормална. Поделићемо анализу на случајеве када је $p > 2$ и када је $p = 2$.

Теорема 31 *Нека је p прост број већи од 2. Све коначне p-групе са цикличном подгрупом индекса p спадају у једну од следећих категорија:*

(A) $\mathbb{Z}_q$, *где је* $q = p^n$ *и* $n \geq 1$,

(B) $\mathbb{Z}_q \times \mathbb{Z}_p$, *где је* $q = p^n$ *и* $n \geq 1$,

(C) $\mathbb{Z}_q \rtimes \mathbb{Z}_p$, *где је* $q = p^n$ *и* $n \geq 2$, *где генератор* $\mathbb{Z}_p$ *дејствује на* $\mathbb{Z}_q$ *као множење са* $1 + p^{n-1}$.

Треба напоменути да трећа категорија има смисла јер је $(1 + p^{n-1})^p \equiv 1 \mod p^n$ према биномној теореми. Прво ћемо доказати лему која ће нам помоћи у доказу.

Лема 32 *Нека је p прост број и a цео број такав да је $a^p \equiv 1 \mod p^n$ за неко $n \geq 2$. Ако је $p \geq 3$, онда је $a \equiv 1 \mod p^{n-1}$. Ако је $p = 2$, онда је $a \equiv \pm 1 \mod 2^{n-1}$.*

Доказ: Претпоставимо да је $a \neq 1$, и означимо са $d(a)$ највећи цео број такав да је $a^p \equiv 1 \mod p^{d(a)}$. Према малој Фермаовој теореми, $a \equiv a^p \equiv 1 \mod p$, па је $d(a) \geq 1$. Можемо написати $a = 1 + bp^{d(a)}$. Сада, применимо биномну теорему на a^p,

$$\begin{aligned} a^p &= (1 + bp^{d(a)})^p \\ &= \sum_{k=0}^{p} \binom{p}{k} b^k p^{d(a)k} \\ &\equiv 1 \mod p^{d(a)+1}, \end{aligned}$$

како $p | \binom{p}{k}$ за $k \geq 1$. Дакле, $d(a^p) = d(a) + 1$, међутим, претпоставили смо да је $a^p \equiv 1 \mod p^n$, па је $d(a^p) \geq n$. Дакле, $d(a) \geq n-1$, тј. $a \equiv 1 \mod p^{n-1}$. □

Доказ теореме 31:

Претпоставимо да је циклична подгрупа групе G реда $q = p^n$. Дакле, G је раширење групе $\mathbb{Z}_q$ за $H = C_p^T$:

$$0 \longrightarrow \mathbb{Z}_q \longrightarrow G \longrightarrow H \longrightarrow 1.$$

Претпоставимо да H дејствује тривијално на $\mathbb{Z}_q$. Према томе, за фактор систем f, имамо

$$f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0.$$

Заменом $g_1 = g_2 = g_3 = g$ добијамо $f(g, g^2) = f(g^2, g)$. Дакле, индукцијом (заменом $g_1 = g_3 = g$ и $g_2 = g^{k-1}$) добијамо да је $f(g, g^k) = f(g^k, g)$. За произвољне $g = T^a$ и $h = T^b$ у H, нека је $k = a^{-1}b$, где је a^{-1} мултипликативни инверз од a у пољу p елемената. Сада, $h = g^k$, и стога $f(g, h) = f(h, g)$, што можемо користити у закону композиције:

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

Дакле, G је Абелова група. Оваква група може бити само $\mathbb{Z}_{p^{n+1}}$ или $\mathbb{Z}_q \times \mathbb{Z}_p$, тако да је G типа (A) или (B).

Размотримо сада случај када је дејство групе H на $\mathbb{Z}_q$ нетривијално и користимо пример 5 да израчунамо $H^2(H, \mathbb{Z}_q)$. Дејство елемента $h \in \mathbb{Z}_q$ је одређено тиме како он делује на генератор $1 \in \mathbb{Z}_q$, делујући као множење резултата овог дејства, тј. $h \cdot a = (h \cdot 1)a$ за све $a \in \mathbb{Z}_q$. Пошто се генератор шаље у други генератор, то значи да је дејство елемента H на $\mathbb{Z}_q$ дато утапањем $\varphi : H \hookrightarrow \mathbb{Z}_q^*$, где је $\mathbb{Z}_q^*$ група јединица прстена $\mathbb{Z}_q = \mathbb{Z}/p^n\mathbb{Z}$. Пошто је сваки нетривијални елемент H реда p, слика овог утапања мора бити подскуп елемената облика

$$\operatorname{im}\varphi = \{1 + kp^{n-1} :\ 1 \leq k \leq p-1\} = \{1 + b :\ b \in p^{n-1}\mathbb{Z}_q\} \subseteq \mathbb{Z}_q.$$

Дакле, један од елемената у H, рецимо h, се понаша као $1 + p^{n-1}$, што одговара случају (C). Како је сваки елемент од H генератор од H, то значи $\mathbb{Z}_q^H = \mathbb{Z}_q^h$, дакле, елемент x се фиксира ако је $h \cdot x = x$, тј. $(1 + p^{n-1})h \cdot x = x$, тј.

$$\mathbb{Z}_q^H = \{x \in \mathbb{Z}_q :\ p^{n-1} \cdot x = 0\} = p\mathbb{Z}_q.$$

С друге стране, оператор норме делује као множење са

$$N = \sum_{i \in \operatorname{im}\varphi} i = \sum_{k=0}^{p-1}(1 + kp^{n-1}) = p + p^{n-1}\sum_{k=0}^{p-1} k = p + p^{n-1}\frac{p(p-1)}{2} = p + \frac{p-1}{2}p^n.$$

Међутим, $\sum_{k=0}^{p-1} 1 = p$, и

$$\sum_{k=0}^{p-1} kp^{n-1} = p^{n-1} \sum_{k=0}^{p-1} k = p^{n-1} \frac{p(p-1)}{2} = \frac{p-1}{2} p^n,$$

што је подударно са 0, јер је p непаран, што значи да $p|\frac{p(p-1)}{2}$. Дакле, оператор норме делује као множење са $N = p$, и стога $N\mathbb{Z}_q = p\mathbb{Z}_q$. Дакле,

$$H^2(H, \mathbb{Z}_q) = \frac{\mathbb{Z}_q^H}{N\mathbb{Z}_q} = \frac{p\mathbb{Z}_q}{p\mathbb{Z}_q} = 0.$$

Према леми 28, имамо да је раширење изоморфно $\mathbb{Z}_q \rtimes_\varphi H$, са операцијом одређеном дејством генератора на H, за који смо утврдили да делује множењем са $1 + p^{n-1}$. Овај случај одговара категорији (C). □

Када је у питању случај за $p = 2$, имамо још неколико категорија могућих 2-група са цикличном подгрупом индекса 2, поред већ наведених категорија (A), (B) и (C). Оне су следеће:

(D) Диедарске 2-групе: $D_{2m} = \mathbb{Z}_m \rtimes \mathbb{Z}_2$, где генератор од $\mathbb{Z}_2$ делује на $\mathbb{Z}_m$ као множење са -1. Сматрамо да је $m = q = 2^n$ за неко $n \geq 2$.

(E) Генерализоване кватернионске 2-групе: Q_{4m} је дефинисана као мултипликативна подгрупа кватернионске алгебре $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ генерисане са $x = e^{\pi i/m}$ и $y = j$. Видимо да је x реда $2m$ и $yxy^{-1} = x^{-1}$, па је циклична подгрупа генерисана са x нормална и индекса 2. То значи да је Q_{4m} реда $4m$, па узимамо да је m степен броја 2 тако да је Q_{4m} заиста 2-група са цикличном подгрупом индекса 2.

(F) $\mathbb{Z}_q \rtimes \mathbb{Z}_2$, где је $q = 2^n$ и $n \geq 2$, где генератор $\mathbb{Z}_2$ делује на $\mathbb{Z}_q$ као множење са $-1 + p^{n-1}$.

Показујемо да ова листа обухвата све могућности.

Теорема 33 *Ако је G 2-група са цикличном подгрупом индекса 2, онда је G изоморфна једној од група горе наведених категорија (A)-(F).*

Доказ: Наш доказ почиње исто као и у доказу теореме 31. Посматрајмо раширење

$$0 \longrightarrow \mathbb{Z}_q \longrightarrow G \longrightarrow H \longrightarrow 1.$$

где је $q = 2^n$ за неко n и $H = C_2^T$. Ако је H-дејство тривијално на $\mathbb{Z}_q$, онда је G типа (A) или (B). Ако је H-дејство нетривијално, онда израчунавамо

$H^2(H, \mathbb{Z}_q)$. Дејство H на $\mathbb{Z}_q$ је дато утапањем $\varphi : H \hookrightarrow \mathbb{Z}_q^*$, из H у групу јединица од $\mathbb{Z}_q$. Сада, као у претходној теореми, користићемо Лему 32, међутим, резултат је другачији за $p = 2$ у поређењу са непарним p. Овде имамо да је слика утапања $\{\pm 1 + b : \ b \in 2^{n-1}\mathbb{Z}_q\} = \{1, 1+2^{n-1}, -1, -1+2^{n-1}\}$. Дакле, имамо три нетривијалне могућности за слику $a \in \mathbb{Z}_q^*$ генератора H:

Случај 1: $a = 1 + 2^{n-1}$. Слично претходном доказу, $\mathbb{Z}_q^H = 2\mathbb{Z}_q$ и оператор норме је множење са $N = 1 + a = 2 + 2^{n-1} = 2(1 + 2^{n-2})$. Ако је $n = 2$, онда је $q = 4$ и $a = 1 + 2 = 3 \equiv -1$, што је еквивалентно следећем случају који ћемо ускоро обрадити. Претпоставимо $n \geq 3$. Сада, $1 + 2^{n-2} \in \mathbb{Z}_q^*$, и зато је $N\mathbb{Z}_q = 2\mathbb{Z}_q$. Стога, имамо

$$H^2(H, \mathbb{Z}_q) = \frac{2\mathbb{Z}_q}{2\mathbb{Z}_q} \cong 0,$$

и дакле, по леми 28, раширење се цепа и она је типа (C).

Случај 2: $a = -1$. У овом случају је $\mathbb{Z}_q^H = 2^{n-1}\mathbb{Z}_q$ и оператор норме је $N = 1 + a = 1 - 1 = 0$, тако да

$$H^2(H, \mathbb{Z}_q) = \frac{\mathbb{Z}_q^H}{N\mathbb{Z}_q} = \frac{2^{n-1}\mathbb{Z}_{2^n}}{0} \cong \mathbb{Z}_2.$$

Дакле, постоје тачно два нееквивалентна раширења која одговарају овом дејству H на $\mathbb{Z}_q$, тако да морају бити типа (D), што одговара тривијалној класи кохомологије, и (E) за нетривијалну класу (приметите да y заиста делује на x као -1).

Случај 3: $a = -1 + 2^{n-1}$. Разматрамо $n \geq 3$, јер за $n = 2$ имамо $a = -1+2 = 1$. Овде имамо $\mathbb{Z}_q^H = 2^{n-1}\mathbb{Z}_q$ и да оператор норме одговара множењу са $N = 1 + a = 2^{n-1}$. Стога,

$$H^2(H, \mathbb{Z}_q) = \frac{2^{n-1}\mathbb{Z}_q}{2^{n-1}\mathbb{Z}_q} \cong 0,$$

и дакле, према леми 28, раширење се цепа и мора да је типа (F). □

Биографија

Александар Шон Колинс (енг. Alexander Sean Collins) је рођен у Даблину, у Ирској, 25. јануара 1999. године. Када је имао две године, са породицом се преселио у Бризбејн, у Аустралији, где је и одрастао. 2012. године, одмах након што је завршио основну школу, поново су се преселили у Београд, у Србији, где је похађао Математичку гимназију. Након завршетка средње школе, отишао је на Универзитет у Кембрицу да студира математику, где је стекао диплому основних студија. Похађао је колеџ Корпус Кристи (енг. Corpus Christi College), где му је руководилац био др Кристофер Брукс (енг. Dr Christopher Brookes). Током Ковида-19, вратио се у Београд да би наставио мастер студије. Овде је такође радио као асистент у настави. Током последње године у Кембрицу, а такође и током мастер програма у Београду, под менторством др Зорана Петровића, развио је интересовање за предмете као што су алгебарска топологија, диференцијална геометрија, хомолошка алгебра и друге сличне, чисто математичке теме. Жели да настави да ради у овим областима.

7 Библиографија

1. K. S. Brown *Cohomology of Groups* - Springer-Verlag 1982;

2. Henri Cartan and Samuel Eilenberg *Homological Algebra* - Princeton University Press, 1956;

3. George E. Cooke and Ross L. Finney *Homology of Cell Complexes* - Princeton University Press, 1967;

4. Samuel Eilenberg and Saunders Maclane *Eilenberg-Mac Lane: Collected Works* - Academic Press Inc, 1986;

5. Serge Lang *Algebra* - Springer-Verlag 2002;

6. Saunders Maclane *Homology* - Springer-Verlag 1963;

7. C. B. Thomas *Characteristic Classes and the Cohomology of Finite Groups* - Cambridge University Press 1986;

8. Charles A. Weibel, *An Introduction to Homological Algebra* - Cambridge University Press 1994;

9. Charles A. Weibel, *History of Topology* - Cambridge University Press 1999.

University of Belgrade
Department of Mathematics

Master's Thesis

GROUP COHOMOLOGY
BASIC CONCEPTS AND EXAMPLES

Alexander Sean Collins

Supervisor:

Prof. Dr Zoran Petrović

Belgrade - 2025

Supervisor

Prof. Dr Zoran Petrović
University of Belgrade, Faculty of Mathematics

Committee members

Dr Maja Roslavcev University of Belgrade, Faculty of Mathematics

Dr Aleksandra Kostić University of Belgrade, Faculty of Mathematics

Acknowledgments

I would like to extend my sincerest gratitude to my supervisor, Professor Zoran Petrović, for the immense support and patience from the time we chose the topic, to the final edits. From the very start he's helped to motivate me and make sure I'm on the right path. I would also like to thank the other members of the committee, assistant professors Dr Maja Roslavcev and Dr Aleksandra Kostić Matijević for their time and effort spent reading this work. Finally, I would like to thank my family, especially my parents.

Contents

1 Introduction

1.1 Foreword

The aim of this thesis is to introduce the cohomology of groups and some simple applications. I closely follow two sources to set up the framework – "Cohomology of Groups" by Kenneth S. Brown 1982, a text based on a graduate course he held at Cornell University; and "Characteristic Classes and the Cohomology of Finite Groups" by C.B. Thomas 1986. Afterwards, I work through several examples, mostly taken from the problems and exercises listed in those books.

1.2 History

The seed for modern day homological algebra was planted by Riemann in the second half of the 19th century, when he was studying closed curves on surfaces. This line of thought was continued by Betti, and then Poincare in his 1895 paper "Analysis Situs". There he introduced a relation called a "homology", based on formal sums of submanifolds. He also introduced the Betti numbers of a manifold, as well as his eponymous theorem, the Poincare Duality Theorem. In his follow-up papers in 1899 and 1900, there appeared a concept that would later be known as a chain complex, along with boundary maps, which he introduced through linear algebra and the notion of torsion coefficients.

At the start of the 20th century, mathematicians such as O. Veblen, J. W. Alexander and H. Kuneth worked on understanding and clarifying Poincare's breakthrough ideas. However, the field remained a discipline for topologists, who manipulated incidence matrices to determine Betti numbers and torsion coefficients. It wasn't until 1925, where Emmy Noether reported that homology was in fact an abelian group, rather than just Betti numbers and torsion coefficients. Slowly, perceptions began to shift towards a more algebraic approach. In 1929 L. Mayer introduced chain complexes and the homology groups of a complex purely algebraically. During the decade 1925-1935, several mathematicians created their own versions of homology. Among these mathematicians are Alexander, Alexandrov, Čech, Lefschetz, Kolmogorov, Vietoris, de Rham. Each case was similar, a recipe was given to construct a chain complex and their homology groups would be defined as the homology of that complex. Then, they would show that the result is independent of choices, and would yield the usual Betti numbers for compact manifolds.

In 1935, there were several major breakthroughs in the development of homology theory. Pontrjagin and Brauer calculated the homology of the classical Lie groups, results which Hopf used in what would later become the theory of Hopf algebras. Čech developed the Universal Coefficient Theorem. The last great result

we'll mention for now was the discovery of cohomology theory and cup products. This was developed independently by Alexander and Kolmogorov, who presented their results back-to-back at the Moscow International Conference on Topology in September 1935.

Also in 1935, Hurewicz defined the higher homotopy groups $\pi_n(X)$ of a space X. He constructed the Hurewicz maps $h : \pi_n(X) \to H_n(X; \mathbb{Z})$. He then focused on aspherical spaces, those spaces whose higher homotopy groups ($n \geq 2$) are all trivial, but whose fundamental group $\pi_1(X)$ need not be trivial. He proved, among other things, that the homology groups of X depend only on the fundamental group of X. In particular, this means that given a group π, the homology groups of an aspherical space X with fundamental group π are in fact independent of the choice of space X.

For the next period, up to 1950, topologists started realising the implications that homological theory of topological spaces had in algebraic systems. Certain cohomologies were discovered to rely solely on algebraic data, such as the cohomology of an aspherical space depending only on its fundamental group, or the cohomology of a Lie group depending only on its associated Lie algebra. This led to thinking in more algebraically defineable terms, without reliance on topology. The former example is what led to the creation of the cohomology of groups.

The lower dimension cohomology groups of a group G had been interpreted before in different ways, yielding classical results. For example, in dimension zero, $H^0(G; A) = A^G$, the group of invariant elements. In dimension 1, the homology group $H_1(G; \mathbb{Z}) = G/[G, G]$, the abelianisation of the group. The cohomology group $H^1(G; A)$ was an already studied classical object, the group of crossed homomorphisms of G into a representation A. Hilbert's "Theorem 90" from 1897 is a calculation that $H^1(G; L^\times) = 0$ when G is the Galois group of a cyclic field extension L/K, and the name comes from its role in the study of crossed product algebras. In dimension 2, the group $H^2(G; A)$ is in fact a classification of the extensions over G with normal subgroup A via factor sets. Factor sets appear in concept as early as 1893 in a paper by Hölder, a 1904 study by Schur, or in 1906 by Dickinson. In 1926, Schreier gave the first systematic approach to factor sets, which Brauer continued in 1928. In 1934, Baer noticed that when A was abelian, these factor sets could be added termwise, such that the extensions formed an abelian group. This lead to the first treatment of extensions without using factor sets.

In 1941, Heinz Hopf submitted a paper in which he showed that the fundamental group $\pi = \pi_1(X)$ of a space X determined the cokernel of the Hurewicz map $h : \pi_2(X) \to H_2(X; \mathbb{Z})$. Presenting π as the quotient F/R of a free group F by the subgroup R of relations, Hopf gave the explicit formula:

$$\frac{H_2(X; \mathbb{Z})}{h(\pi_2(X))} \cong \frac{R \cap [F, F]}{[F, R]},$$

where $[A, B]$ for $A, B \subseteq F$ denotes the subgroup generated by commutators $[a, b] = aba^{-1}b^{-1}$ ($a \in A, b \in B$). In particular, if $\pi_2(X) = 0$ (as is in the case of aspherical spaces) this shows that $H_2(X; \mathbb{Z})$ depends only on $\pi_1(X)$. In that case, this formula is called Hopf's formula for $H_2(\pi; \mathbb{Z})$.

Hopf's paper, and the work of Hurewicz, inspired many mathematicians to study the homology and cohomology of aspherical spaces, and to express the results in terms of the fundamental group. In MacLane's words: "This line of investigation provided the justification for the study of cohomology of groups in **all** dimensions and was the starting point of homological algebra". Thus, Eilenberg together with MacLane, Freudenthal, and Hopf, followed up by Eckmann, all simultaneously, yet independently defined the homology and/or cohomology of a group.

Eilenberg and MacLane had worked together to discover what is now known as the Universal Coefficient Theorem for singular cohomology in 1942, specifically that cohomology was determined by homology. Hopf's work that year had left a big impression on them, and they then worked together to study aspherical spaces. Using Hurewicz' result, that given a group π, the homology and cohomology groups of an aspherical space Y were independent of the choice of Y, as long as $\pi_1(Y) = \pi$, they took these definitions to be $H_n(\pi; A)$ and $H^n(\pi; A)$. For computations, they created a specific abstract simplicial complex $K(\pi)$ for the choice of aspherical space Y. Its n-cells are ordered arrays $[x_1, \ldots, x_n]$ of elements in the group. Thus, they calculated the cohomology groups of π as the cohomology groups of the cellular cochain complex of $K(\pi)$. Eckmann's paper also defined a cohomology ring in a similar way, defining the cohomology cup product in terms of this complex. Both papers showed that $H^2(G; A)$ classifies group extensions.

Concurrently, Hopf created a completely different definition. This definition was much closer to the modern definition. He considered a module M over a ring R, then constructed a free resolution F of M by R-modules. For I an ideal of R, he considered the homology of the kernel of $F \to F \otimes (R/I)$ and showed it is independent of the choice of resolution. In fact, he specialised to the case of the group ring $R = \mathbb{Z}\pi$, the augmentation ideal I, and $M = \mathbb{Z}$. Here he showed that if Y is an aspherical cell space with fundamental group π, then $H_n(Y; \mathbb{Z}) = H_n(\pi; \mathbb{Z})$. Freudenthal's method was similar, but less general.

At first, calculations were restricted to groups that were fundamental groups of familiar topological spaces, using the bar complex. Later, in 1946, another method was found by Lyndon, which Serre realised in 1950 by using a spectral sequence. He finished this description with Hochschild in 1953, and it is now known as the Lyndon-Hochschild-Serre spectral sequence.

Hochschild applied the new definitions of cohomology of groups in his study of local class field theory, to create Galois cohomology. Studying this Galois cohomology, Tate was lead to define the Tate cohomology, indexed by all integers,

by splicing together the cohomology and homology of a group.

In 1950, in the Seminaire Cartan, Eilenberg gave an axiomatic characterisation of homology and cohomology theories for a group, and established the existence of said theories using a fixed free resolution, and Cartan proved the Comparison Theorem for chain complexes. This lead to their collaboration, with the goal of rewriting the foundations of all the ad hoc algebraic homology and cohomology theories that had arisen so far. It is here they introduced the term "Homological Algebra", using it for the title of their 1956 textbook. This book denotes the first occurrence of the notation Tor_n and Ext^n, as well as the concept of a projective module. In his review of their book, Hochschild stated that "The appearance of this book must mean that the experimental phase of homological algebra is now surpassed".

The book made use of the notion of chain complexes and resolutions, which had also been developing over time. Chain complexes were first formally introduced by Mayer in 1929, inspired by Noether's report from 1925. In 1947 Kelley and Pitcher coined the term "exact sequence". Chain complexes were further developed by Eilenberg and Steenrod in their 1945 book, which saw the first occurrence of the five-lemma and Mayer-Vietoris sequence. The snake lemma first occured in Cartan and Eilenberg's 1950 book. Free resolutions had been used for a long time in algebra, starting with Hilbert in his 1890 paper. Baer implicitly used free resolutions in his 1934 study of group extensions. Similarly, as mentioned before, Hopf used them in his description of the homology of a group. Injective modules and resolutions had been implicitly used by Baer, in his characterisation of semisimple rings, and MacLane, in a 1948 paper on group extensions.

It was based on the work of Hopf that Cartan and Eilenberg used free $\mathbb{Z}G$-resolutions of a G-module A in order to give an axiomatic description for the group homology $H_*(G; A)$. However, they went on to define the concept of a projective module. Then, they defined projective and injective resolutions. They use these definitions in their definitions of $Tor_n^R(M, N)$ and $Ext_R^n(M, N)$ as the derived functors of $M \otimes_R N$ and $\mathrm{Hom}_R(M, N)$. This lead to the unification of many previously studied homology and cohomology theories. The homology and cohomology groups of a group G were shown to be the Tor and Ext groups over the group ring $\mathbb{Z}G$. Similarly, Hochschild's homology and cohomology of an associative algebra Λ were shown to be the Tor and Ext groups over the enveloping algebra $\Lambda \otimes \Lambda^{\mathrm{op}}$, and the homology and cohomology of a Lie algebra $\mathfrak{g}$ were shown to be the Tor and Ext groups over the enveloping algebra $U_{\mathfrak{g}}$.

The publication of Cartan and Eilenberg's "Homological Algebra" lead to an incredible amount of research inspired by the work. In fact, many new fields of study emerged and flourished as a result. Some of these fields include areas in projective modules; theories in ring theory such as regular local rings, local rings, Matlis duality, and local cohomology and duality; theories in algebraic geometry

such as Galois cohomology and Étale cohomology; areas in derived categories; and many more. This book remained popular until the 1970s, and along with MacLane's 1963 book "Homology", helped the subject become standard course material.

2 G-modules

2.1 Group rings and G-modules

Let G be a group, not necessarily finite. We define the integral group ring of G as $\Lambda = \mathbb{Z}G$, consisting of formal sums $\Sigma_i n_i g_i$ where $n_i \in \mathbb{Z}$, $g_i \in G$, and i are elements of a finite index set, with the operations

$$\Sigma_i n_i g_i + \Sigma_i m_i g_i = \Sigma_i (n_i + m_i) g_i$$

and

$$(\Sigma_i n_i g_i)(\Sigma_i m_j g'_j) = \Sigma_{i,j} (n_i m_j)(g_i g'_j).$$

The left G-module A is defined as an abelian group A together with a G-action on A which respects addition in A: $g \cdot (a+b) = g \cdot a + g \cdot b$. As A is an abelian group, we may consider it as a $\mathbb{Z}$-module. We shall sometimes denote that underlying $\mathbb{Z}$-module by A_0.

As the G-action on A respects addition, we may linearly extend the G-action to a Λ-action on A: for an element $\lambda = \Sigma_i n_i g_i \in \Lambda$, $\lambda \cdot a = (\Sigma n_i g_i) \cdot a = \Sigma n_i (g_i \cdot a)$. Let $a \in A$. Clearly $1 \cdot a = a$. For λ and $\mu = \Sigma_j m_j g'_j$ we have

$$(\lambda\mu) \cdot a = \big((\Sigma_i n_i g_i)(\Sigma_j m_j g'_j)\big) \cdot a = \big(\Sigma_{i,j} (n_i m_j)(g_i g'_j)\big) \cdot a =$$
$$\Sigma_{i,j} (n_i m_j)(g_i g'_j) \cdot a = \Sigma_{i,j} (n_i m_j) g_i \cdot (g'_j \cdot a) = \Sigma_{i,j} n_i g_i \cdot (m_j g'_j \cdot a) =$$
$$\Sigma_i n_i g_i \cdot (\Sigma_j m_j g'_j \cdot a) = (\Sigma_{i,j} n_i g_i) \cdot \big((\Sigma_j m_j g'_j) \cdot a\big) = \lambda \cdot (\mu \cdot a)$$

This action also respects addition:

$$\begin{aligned} \lambda \cdot (a+b) &= (\Sigma_i n_i g_i) \cdot (a+b) \\ &= \Sigma_i n_i g_i \cdot (a+b) \\ &= \Sigma_i n_i (g_i \cdot a + g_i \cdot b) \\ &= (\Sigma_i n_i g_i \cdot a) + (\Sigma_i n_i g_i \cdot b) \\ &= \lambda \cdot a + \lambda \cdot b. \end{aligned}$$

Hence, A, together with the G-action, is a Λ-module, in the classic sense. The converse is also obviously true. Thus, from here on forth we use the terms G-module and Λ-module interchangeably.

Throughout this text, G, Λ and A shall be as above, unless stated otherwise. We typically denote the neutral element of G as 1, so that in Λ we can simply write 2 instead of $2e_g$, or something similar. We denote by $\mathcal{U}_G$ the category of left Λ-modules and Λ-homomorphisms. We will also often treat $\mathbb{Z}$ as a G-module with trivial G-action.

We can create a G-module out of any arbitrary set with a G-action. We call such a set X with a G-action a G-set. From X we form the free abelian group (or, equivalently, $\mathbb{Z}$-module) $\mathbb{Z}X$, sometimes denoted $\mathbb{Z}[X]$, and we extend the G-action on X to a $\mathbb{Z}$-linear action of G on $\mathbb{Z}X$. We call the resulting G-module a permutation module.

Furthermore, as the orbits X_i of the G-action on X are disjoint G-sets themselves, we have the following decomposition:

$$\mathbb{Z}[\bigsqcup X_i] = \bigoplus \mathbb{Z}X_i.$$

Of course, using the orbit stabilizer theorem we have

$$\mathbb{Z}X \cong \bigoplus \mathbb{Z}[G/G_{x_i}]$$

where the $x_i \in X_i$ are representatives for the G-orbits in X, and G_x is the stabilizer subgroup of G with respect to x. Thus, the representatives x_i form a generating set for $\mathbb{Z}X$ as a Λ-module.

In particular, for a free G-set, i.e. when the G-action on X is free, the stabilizer subgroups are trivial. This means each $\mathbb{Z}[G/G_{x_i}] \cong \mathbb{Z}G$, from which we obtain the following proposition:

Proposition 1 *Let X be a free G-set and let E be a set of representatives for the G-orbits in X. Then $\mathbb{Z}X$ is a free $\mathbb{Z}G$-module with basis E.*

2.2 Invariants and coinvariants

The subset of invariant elements in the G-module A is defined as

$$A^G = \{a \in A : g \cdot a = a \text{ for all } g \in G\}.$$

This submodule is the largest submodule of A on which G acts trivially.

Let A and A' be two G-modules. We can define a G-action on the $\mathbb{Z}$-homomorphisms $\mathrm{Hom}(A, A')$ by the rule

$$(g \cdot f)(a) = g \cdot f(g^{-1} \cdot a)$$

for all $g \in G$, $f \in \mathrm{Hom}(A, A')$ and $a \in A$. Here we used the G-actions on A and A'.

To verify that this action is well defined, we check the following hold for all $g, h \in G$, $f \in \mathrm{Hom}(A, A')$ and $a \in A$:

1. $(1 \cdot f)(a) = 1 \cdot f(1^{-1} \cdot a) = f(a)$
2. $(g \cdot (h \cdot f))(a) = g \cdot (h \cdot f)(g^{-1} \cdot a) = g \cdot (h \cdot f(h^{-1} \cdot (g^{-1} \cdot a))) = (gh) \cdot f((gh)^{-1} \cdot a) = ((gh) \cdot f)(a)$ for all $g, h \in G$.

An invariant element of $\mathrm{Hom}(A, A')$ is an element f which satisfies $(g \cdot f)(a) = f(a)$ for all $g \in G$ and $a \in A$, that is $g \cdot f(g^{-1} \cdot a) = f(a)$, for all $g \in G$ and $a \in A$. By replacing a with $g \cdot a$ (which spans all of A) we get the equivalent condition $g \cdot f(a) = f(g \cdot a)$, for all $g \in G$ and $a \in A$. Thus, f is an invariant element if and only if it is a module homomorphism between G-modules A and A'. Hence,

$$\mathrm{Hom}_G(A, A') = \mathrm{Hom}(A, A')^G.$$

This formula gives rise to another description of A^G, given by the following property:

$$A^G \cong \mathrm{Hom}_G(\mathbb{Z}, A), \tag{1}$$

where we consider $\mathbb{Z}$ as a G-module with trivial G-action. Indeed, as $\mathrm{Hom}_G(\mathbb{Z}, A) = \mathrm{Hom}(\mathbb{Z}, A)^G$, it is enough to show $\mathrm{Hom}(\mathbb{Z}, A) \cong A$. Each homomorphism is determined by the image of $1 \in \mathbb{Z}$ by linearity, so let us map homomorphisms f to $f(1)$. This mapping is clearly an isomorphism, all that is left is to check that the G-structures correspond. This is easily checked: $(g \cdot f)(1) = g \cdot f(g^{-1} \cdot 1) = g \cdot f(1)$, noting that the G-action on $\mathbb{Z}$ is trivial.

The following lemma displays a useful property of the invariants functor:

Lemma 2 *The functor $A \to A^G$ is left exact on the category of left Λ-modules, i.e. if*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

is a short exact sequence of left Λ-modules, the sequence

$$0 \longrightarrow A^G \xrightarrow{\phi^G} B^G \xrightarrow{\psi^G} C^G$$

is exact in the category of abelian groups.

Proof: If $\ker \phi = 0$ then $\ker \phi^G = 0$ as it is a subset of $\ker \phi$.

Let us show that $\ker \psi = \mathrm{im}\, \phi$. Of course, $\mathrm{im}\, \phi^G \subseteq \ker \psi^G$, as their composition is 0. Now, let $b \in \ker \psi^G$, so $b \in B^G$ and $\psi^G b = 0$, which means $\psi b = 0$, as ψ^G is the restriction of ψ to B^G. As $\ker \psi = \mathrm{im}\, \phi$ we have $b = \phi a$ for some $a \in A$. Now, as ϕ is a module homomorphism, for arbitrary $g \in G$ we have

$$\phi(g \cdot a) = g \cdot (\phi a) = g \cdot b = b$$

as b is an invariant element of B. Thus, $\phi(g \cdot a)$ has the same image as $\phi(a)$. However, ϕ is a monomorphism, which means $g \cdot a = a$. Since g was arbitrary, this means a is an invariant element of A, or $a \in A^G$. Thus, $b \in \mathrm{im}\, \phi^G$. Hence, $\ker \psi = \mathrm{im}\, \phi$. $\square$

The subset of coinvariant elements in A is defined as the quotient of A by the submodule generated by elements of the form $g \cdot a - a$ for all $g \in G$ and $a \in A$. This quotient is denoted by A_G. Where A^G was the largest submodule of A on which G acts trivially, A_G is the largest quotient of A on which G acts trivially.

An equivalent definition of A_G may be given by:

$$A_G \cong \mathbb{Z} \otimes_\Lambda A. \tag{2}$$

Note that for the tensor product to make sense, we regard $\mathbb{Z}$ as a right Λ-module, with trivial G-action. Let us prove the above identity is equivalent to the original definition. By the universal property of tensor products, there is a unique map $\varphi : \mathbb{Z} \otimes_\Lambda A \to A_G$ given by $n \otimes a \mapsto n\bar{a}$, where $\bar{a}$ denotes the image of a in the quotient A_G. Conversely, Let us consider the map $\theta : A_G \to \mathbb{Z} \otimes_\Lambda A$ given by $\bar{a} \mapsto 1 \otimes a$ We check that θ is a well-defined map of Λ-modules. As the G-action on $\mathbb{Z}$ is trivial, we have

$$1 \otimes (g \cdot a) = (1 \cdot g) \otimes a = 1 \otimes a,$$

which means we have $1 \otimes (g \cdot a - a) = 0$. Thus the map θ is well defined, as if two elements $\bar{a_1}, \bar{a_2}$, are the same, they differ by a sum of elements of the form $g \cdot a - a$, and so $1 \otimes a_1 = 1 \otimes a_2$. The maps φ and θ are inverses of each other, and thus A_G and $\mathbb{Z} \otimes_\Lambda A$ are isomorphic as Λ-modules, noting that the G-action is trivial in both cases.

Note that, by bilinearity, every element of $\mathbb{Z} \otimes_\Lambda A$ may be expressed as $1 \otimes a$, for some $a \in A$. This expression need not be unique.

In general, we are able to work with the tensor product $A \otimes_\Lambda A'$ of two left G-modules A and A'. We do this by regarding A as a right G-module with the right G-action defined as $a \cdot g = g^{-1} \cdot a$, for all $a \in A$ and $g \in G$. In this case, $A \otimes_\Lambda N$ is obtained from $A \otimes A'$ by quotienting out the relations $g^{-1} \cdot a \otimes a' = a \otimes g \cdot a'$ (instead of the usual $a \cdot g \otimes a' = a \otimes g \cdot a'$). By replacing a with $g \cdot a$, these relations take the form $a \otimes a' = g \cdot a \otimes g \cdot a'$.

Inspired by this, can give $A \otimes A'$ a G structure. We define the G-action on $A \otimes A'$ by $g(a \otimes a') = ga \otimes ga'$ for all $a \otimes a' \in A \otimes A'$. Thus, we have

$$A \otimes_\Lambda A' = (A \otimes A')_G.$$

Similar to Lemma 2, we have the following property of the co-invariants functor:

Lemma 3 *The functor $A \to A_G$ is right exact on the category of left Λ-modules, i.e. if*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

is a short exact sequence of left Λ-modules, the sequence

$$A_G \xrightarrow{\phi_G} B_G \xrightarrow{\psi_G} C_G \longrightarrow 0$$

is exact in the category of abelian groups.

Proof: The maps ϕ_G and ψ_G are the maps that make the following diagram commute:

$$\begin{array}{ccccc} A & \xrightarrow{\phi} & B & \xrightarrow{\psi} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle r} \\ A_G & \xrightarrow{\phi_G} & B_G & \xrightarrow{\psi_G} & C_G, \end{array}$$

where p, q and r are the quotients from the definition of the coinvariants. In other words, we have $\phi_G p = q\phi$ and $\psi_G q = r\psi$. We see that for any $a \in A$ and $g \in G$ we have

$$\phi(g \cdot a - a) = g \cdot \phi(a) - \phi(a),$$

i.e. ϕ sends elements in $\ker p$ to $\ker q$. This allows us to define ϕ_G in the natural way, sending elements of the form $p(a) \in A_G$ to $q\phi(a) \in B_G$. Similarly for ψ.

First we will show $\operatorname{im} \psi_G = C_G$. Suppose we are given an arbitrary element of C_G. It is of the form $r(c)$, for some $c \in C$. As ψ is surjective, this means there exists some $b \in B$ such that $\psi b = c$. Thus, $r(c) = r(\psi b) = \psi_G q(b) \in \operatorname{im} \psi_G$, hence $\operatorname{im} \psi_G = C_G$.

Now, let us show $\ker \psi_G = \operatorname{im} \phi_G$. First of all, we have that their composition is 0: Given an arbitrary element $p(a) \in A_G$, we have

$$\psi_G \phi_G p(a) = \psi_G q(\phi a) = r(\psi\phi(a)) = r(0) = 0.$$

Thus, $\operatorname{im} \phi_G \subseteq \ker \psi_G$. Let us show the converse.

Suppose we have an arbitrary element $q(b) \in \ker \psi_G$. This means $\psi_G q(b) = 0$, i.e. $r(\psi b) = 0$, by which we have $\psi b \in \ker r$. From the definition of the quotient map r, this means that ψb is in the subgroup of C generated by elements or the form $g \cdot c - c$, where $g \in G$ and $c \in C$. Hence, for some $g_i \in G$, $c_i \in C$ and $n \geq 1$, we have

$$\psi b = \sum_{i=1}^{n} (g_i \cdot c_i - c_i).$$

As each $c_i \in C$ for all $1 \leq i \leq n$, and ψ is surjective, this means there exist $b_i \in B$ such that $c_i = \psi b_i$ for all $1 \leq i \leq n$. Thus,

$$\psi b = \sum_{i=1}^{n} (g_i \cdot \psi b_i - \psi b_i) = \psi(\sum_{i=1}^{n} (g_i \cdot b_i - b_i)) = \psi m,$$

i.e. $\psi(b-m) = 0$, where we denote $m = (\sum_{i=1}^{n}(g_i \cdot b_i - b_i))$. Thus, $b-m \in \ker\psi = \operatorname{im}\phi$ by the exactness of the starting sequence. So, we now have $b - m = \phi a$ for some $a \in A$. As m is in the subgroup outlined in the definition of B_G, it follows $m \in \ker q$. Now, we have

$$q(b) = q(b-m) = q(\phi a) = \phi_G p(a) \in \operatorname{im}\phi_G.$$

Thus, we have shown $\ker\psi_G \in \ker\phi_G$. □

2.3 Coinduced and Induced Λ-Modules

The G-structures obtained from the above defined G-actions on resulting objects of the $\mathrm{Hom}(\_,\_)$ and $\_ \otimes \_$ functors give rise to the concepts of induced and coinduced Λ-modules.

Definition 1 *A Λ-module A is considered coinduced if there exists an abelian group X with trivial G-action such that $A = \mathrm{Hom}(\Lambda, X)$, and induced if $A = \Lambda \otimes X$.*

Proposition 4 *If G is finite, the definitions of coinduced and induced modules coincide.*

Proof: Let X be an abelian group with trivial G-action. Let A and A' be the modules from the definitions of induced and coinduced modules respectively, that is $A = \Lambda \otimes X$ and $A' = \mathrm{Hom}(\Lambda, X)$.

Let n be the number of elements in G, and denote the elements of G as $\{g_1, g_2, \ldots, g_n\}$. As $\Lambda = \mathbb{Z}G$ is the set of formal sums over elements in G, of which there are $n < \infty$, it is clearly isomorphic to $\mathbb{Z}^n$. As such, we have

$$A = \Lambda \otimes X \cong \mathbb{Z}^n \otimes X \cong (\mathbb{Z} \otimes X)^n \cong X^n$$

The resulting isomorphism $A = \Lambda \otimes X \to X^n$ is given on an arbitrary element $\sum_{g\in G} g \otimes x_g \in \Lambda$ by

$$\sum_{g\in G} g \otimes x_g \mapsto (x_{g_1}, x_{g_2}, \ldots, x_{g_n}).$$

It follows that any element in A can be uniquely represented as $\sum_{g\in G} g \otimes x_g$ for appropriate $x_g \in X$.

On the other hand, as a homomorphism from $\mathbb{Z}^n$ to a group is uniquely determined by the images of the n basis elements of $\mathbb{Z}^n$, we have

$$A' = \mathrm{Hom}(\Lambda, X) \cong \mathrm{Hom}(\mathbb{Z}^n, X) \cong (\mathrm{Hom}(\mathbb{Z}, X))^n \cong X^n$$

where the last isomorphism arises as each homomorphism from $\mathbb{Z}$ to X is uniquely determined by where 1 maps to.

Hence, as $\mathbb{Z}$ modules, we see that A' and A are isomorphic. All that is left is to show that there is an isomorphism between them which respects their G-actions. To do this, we shall construct an isomorphism between A' and A, and directly show that it preserves the G-action.

As G is finite, we may write an arbitrary element $\lambda \in \Lambda$ as a sum over all elements of G, i.e. $\lambda = \sum_{g \in G} k_g g$, with $k_g \in \mathbb{Z}$. Let us consider the mapping $\varphi \colon A \to A'$ that sends an element $g \otimes x$ to the homomorphism $x\chi_g$, where χ_g is the indicator homomorphism for g, i.e. if $\lambda = \sum_{h \in G} k_h h$, then $\chi_g(\lambda) = k_g$. We extend φ additively to the rest of A.

If $a = \sum_{g \in G} g \otimes x_g \in A$, and $\lambda = \sum_{g \in G} k_g g$ then

$$f_a(\lambda) = f_{\sum_{g \in G} g \otimes x_g}(\lambda) = \sum_{g \in G} f_{g \otimes x_g}(\lambda) = \sum_{g \in G} x_g \chi_g(\lambda) = \sum_{g \in G} k_g x_g.$$

As every element in A can be uniquely represented in the form $\sum_{g \in G} g \otimes x_g$, the mapping φ is well defined.

To show it is injective, let us suppose φ has the same image on elements $a = \sum_{g \in G} g \otimes x_g$ and $b = \sum_{g \in G} g \otimes y_g$, i.e. $f_a = f_b$. That means they have the same image on any arbitrary element $g \in G$, i.e. $f_a(g) = f_b(g)$. Hence, $x_g = y_g$ for all $g \in G$. Thus, $a = b$ and φ is injective.

Let us now check that the mapping is also surjective. Suppose $f \in A' = \mathrm{Hom}(\Lambda, X)$. For each $g \in G$, let $f(g) = x_g$. Let $a = \sum_{g \in G} g \otimes x_g \in X$. Now, $f = f_a$ on G, so by linearity, they also concur on Λ.

All that is left is to check that the G actions on A' and A match, that is $h \cdot f_a = f_{h \cdot a}$ for all $h \in G$. As before, any arbitrary element $a \in A$ can be written simply as $a = \sum_{g \in G} g \otimes x_g$. Let $h \in G$. Keeping in mind the G-action is trivial on X, we calculate:

$$h \cdot a = h \cdot (\sum_{g \in G} g \otimes x_g) = \sum_{g \in G} h \cdot (g \otimes x_g) = \sum_{g \in G} h \cdot g \otimes h \cdot x_g = \sum_{g \in G} h \cdot g \otimes x_g.$$

As G acts on Λ by left multiplication, and as G is finite, we may identify the action of multiplying from the left with an element h of G with a permutation $\sigma \in \mathrm{Aut}(G)$.

$$h \cdot a = \sum_{g \in G} hg \otimes x_g = \sum_{g \in G} \sigma(g) \otimes x_g = \sum_{g \in G} g \otimes x_{\sigma^{-1}(g)}.$$

Now we calculate how h acts on f_a for any arbitrary $\mu \in \Lambda$:

$$(h \cdot f_a)(\mu) = h \cdot f(h^{-1} \cdot \mu) = f(h^{-1} \cdot \mu)$$

as $f(g^{-1} \cdot \mu) \in X$. Restricting to the images of elements of G, we have

$$(h \cdot f_a)(g) = f_a(h^{-1} \cdot g) = f_a(\sigma^{-1}(g)) = x_{\sigma^{-1}(g)} = f_{h \cdot a}(g)$$

where we conclude the final equality from the calculations of $h \cdot a$ above. Therefore, as both sides agree on G they must agree on their extensions to Λ. $\square$

Lemma 5 *Every G-module embeds in a coinduced module.*

Proof: Let A be a G-module. We will show A embeds in $\mathrm{Hom}(\Lambda, A_0)$, where A_0 is the underlying $\mathbb{Z}$-module of A, meaning it has trivial G-action. Consider the map $A \to \mathrm{Hom}(\Lambda, A_0)$ given by $a \mapsto f_a$ where $f_a(g) = g^{-1} \cdot a$ for all $g \in G$ as a subset of Λ (as the G action on A_0 is trivial we consider the result of g^{-1} acting on a in A, which is an element of A_0), and f_a extends to the rest of Λ by linearity, that is, $f_a(\lambda) = f_a(\sum_{i=1}^n k_i g_i) = \sum_{i=1}^n k_i g_i^{-1} \cdot a$. This mapping is injective, as, if $f_a = f_b$, then $f_a(1) = f_b(1)$, which means $a = b$. We must also show that the G-actions agree, that is, $g \cdot f_a = f_{g \cdot a}$. We thus must have $(g \cdot f_a)(\lambda) = f_{g \cdot a}(\lambda)$ for all λ.

$$(g \cdot f_a)(\lambda) = g \cdot f_a(g^{-1} \cdot \lambda) = f_a(g^{-1} \cdot \lambda) = f_a(g^{-1} \cdot \sum_{i=1}^n k_i g_i) = f_a(\sum_{i=1}^n k_i g^{-1} g_i)$$

$$= \sum_{i=1}^n k_i (g^{-1} g_i)^{-1} \cdot a = \sum_{i=1}^n k_i (g_i^{-1} g) \cdot a = \sum_{i=1}^n k_i g_i^{-1} \cdot (g \cdot a) = f_{g \cdot a}(\lambda).$$

The second equality holds, as, in $g \cdot f_a(g^{-1} \cdot \lambda)$, the outer action is the G-action on A_0, which is trivial. $\square$

Lemma 6 *Every G-module is the homomorphic image of a projection of an induced G-module.*

Proof: Let A be a G-module and denote by A_0 its underlying $\mathbb{Z}$-module. Consider the map from $\Lambda \otimes A_0$ to A mapping $g \otimes a$ to $g \cdot a$ and extending to all of $\Lambda \otimes A_0$ by linearity. We shall show it is an epimorphism. It is surjective, as every $a \in A$ is the image of $1 \otimes a$. To show the G-actions agree, we show that $g' \cdot (g \otimes a)$ maps to $g' \cdot (g \cdot a)$. Thus,

$$g' \cdot (g \otimes a) = (g'g \otimes g' \cdot a) = (g'g \otimes a)$$

as G acts on A_0 trivially. This result maps to $(g'g) \cdot a = g' \cdot (g \cdot a)$. $\square$

3 Resolutions

3.1 Free Resolutions

Other than G-modules, the other core structure in the theory of group cohomology is the projective resolution. For now we will start with resolutions of free modules, and properly define projective modules later.

Definition 2 *Let R be a ring and M an R-module. The set E is a basis for M if it generates M and if it is linearly independent. If such a set exists, then we say M is a free module.*

Definition 3 *Let R be a ring and M be a left R-module. A resolution of M is an exact sequence of R-modules*

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

If each F_i is free, then this is called a free resolution of M over R.

We can show that a free resolution exists for any arbitrary module M, by simple construction: Let F_0 be the free module generated by the elements of M as generators, and $\varepsilon : F_0 \to M$ be the obvious surjection. Next, repeat the process to create the free module F_1 generated by the elements of $\ker \varepsilon$ as generators and a surjection $F_1 \to \ker \varepsilon$. This process can then be repeated indefinitely to create a free resolution for M.

We will mostly be concerned with the case where M is $\mathbb{Z}$ and R is $\Lambda = \mathbb{Z}G$ for a given group G.

3.2 The Augmentation Map

We define the augmentation map to be the ring homomorphism $\varepsilon : \Lambda \to \mathbb{Z}$ such that $\varepsilon(g) = 1$ for all $g \in G$. The kernel of ε is called the augmentation ideal of λ and is denoted I.

Let $\lambda = \sum_i^n k_i g_i$ be an arbitrary element in Λ. We compute

$$\varepsilon(\lambda) = \varepsilon(\sum_i^n k_i g_i) = \sum_i^n k_i \varepsilon(g_i) = \sum_i^n k_i.$$

Hence, if $\lambda \in I$, then $\sum_i^n k_i = 0$, which means

$$\lambda = \lambda - \sum_i^n k_i = \sum_i^n k_i g_i - \sum_i^n k_i = \sum_i^n k_i (g_i - 1).$$

Thus, every element of I is generated by elements of the form $g-1$, i.e. the elements $\{g-1|\ g\in G,\ g\neq 1\}$ form a basis for I as a $\mathbb{Z}$-module.

Now, suppose S is a set of generators for G. We shall show that the elements $\{s-1|\ s\in S\}$ generate I as a left ideal. As the elements $\{g-1|\ g\in G,\ g\neq 1\}$ generate I, it suffices to show that these elements are generated by $\{s-1|\ s\in S\}$. An element $g\in G$ is of the form $g=s_1s_2\cdots s_k$ where $s_1,\ldots,s_k\in S$ are not necessarily distinct. Now, we create the telescoping sum

$$\begin{aligned} g-1 &= s_1s_2\cdots s_k-1 \\ &= s_1s_2\cdots s_k-\sum_{i=1}^{k-1}s_1\cdots s_i+\sum_{i=1}^{k-1}s_1\cdots s_i-1 \\ &= \sum_{i=1}^{k}(s_1\cdots s_i-s_1\cdots s_{i-1}) \\ &= \sum_{i=1}^{k}(s_1\cdots s_{i-1})\cdot(s_i-1). \end{aligned}$$

Hence, the elements $\{s-1|\ s\in S\}$ generate I as a left ideal.

The converse is also true, if the elements $\{s-1|\ s\in S\}$ generate I as a left ideal, then S is a set of generators for G. Indeed, suppose H is the subgroup of G generated by S. Consider the permutation module $\mathbb{Z}[G/H]$. The neutral element $\bar{1}\in G/H$ is fixed by H. Thus, as S generates H, as a subgroup, and the elements $\{s-1|\ s\in S\}$ generate I, $\bar{1}$ is annihilated by I. Hence, for all elements $g\in G$, $(g-1)\bar{1}=0$ i.e. $gH=H$ i.e. $g\in H$. Thus $G\subset H$, which means $G=H$. In other words, S generates G.

We defined the group of coinvariant elements A_G of A as the quotient of A by the additive subgroup generated by elements of the form $ga-a$ for all $g\in G$, $a\in A$. These elements are in fact the product of an element $g-1\in I$ and $a\in A$. These elements thus generate the ideal $IA=\{\sum_i^n a_ib_i\mid n\geq 1,\ a_i\in I,\ b_i\in A\}$, and thus we have another form for the coinvariant group.

Lemma 7 $A_G=A/IA$.

3.3 Example: Free Resolution of $\mathbb{Z}$ over a Cyclic Group

Let us now construct a basic example of a free resolution:

Example 1 *A free resolution of $\mathbb{Z}$ over a cyclic group.*

Note: Let us denote by C_r^T a cyclic group of order r generated by T, for integer r, $2\leq r\leq\infty$.

Proof: We shall divide our proof into the two cases when the order of the cyclic group, r, is infinite or finite.

Case 1: $r = \infty$. The tail end of our resolution must be the augmentation map $\varepsilon : \mathbb{Z}C_\infty^T \longrightarrow \mathbb{Z}$, where the generator T maps to 1. This means $T-1$ maps to 0, so we construct the preceding free module to be $\mathbb{Z}C_\infty^S \cong \mathbb{Z}C_\infty^T \cong \Lambda$, with boundary map $d : S \mapsto T-1$, where we renamed the generator as S simply for clarity's sake.

It is simple to show d is injective: let $a+bS, c+dS \in \mathbb{Z}C_\infty^S$ with $d(a+bS) = d(c+ds)$. Thus,

$$a + bT - b = c + dT - d,$$

and so

$$(a-c) + (d-b) = (d-b)T.$$

By linear independence, we get that $d = b$ and $c = a$, i.e. $a + bS = c + dS$.

Thus, the sequence

$$0 \longrightarrow \mathbb{Z}C_\infty^S \xrightarrow{d} \mathbb{Z}C_\infty^T \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

is exact, and so this is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}C_\infty^T$.

Case 2: $r < \infty$. Consider $N = 1 + T + T^2 + \cdots + T^r$ We will show that the following is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}C_r^T$:

$$\ldots \xrightarrow{T-1} \Lambda_{(2k)} \xrightarrow{N} \Lambda_{(2k-1)} \xrightarrow{T-1} \ldots \xrightarrow{N} \Lambda_{(1)} \xrightarrow{T-1} \Lambda_{(0)} \longrightarrow \mathbb{Z}.$$

Each $\Lambda_{(i)}$ is a copy of the free module Λ. We check that the sequence is exact, that the kernels and images of the maps $N : \Lambda_{(2k)} \longrightarrow \Lambda_{(2k-1)}$ and $T-1 : \Lambda_{(2k+1)} \longrightarrow \Lambda_{(2k)}$ coincide. $N(T-1) = (T-1)N = T^r - 1 = 0$, so the image of each map lies within the kernel of the next. We show the converse is also true.

For the odd case, let $\lambda = \sum_{i=0}^{r-1} a_i T^i \in \Lambda_{(2k+1)}$. As λ is in $\ker(T-1)$, we have

$$\begin{aligned}
(T-1)\cdot\lambda &= 0 \\
(T-1)\cdot\sum_{i=0}^{r-1} a_i T^i &= 0 \\
T\cdot\sum_{i=0}^{r-1} a_i T^i - 1\cdot\sum_{i=0}^{r-1} a_i T^i &= 0 \\
\sum_{i=0}^{r-1} a_i T^{i+1} - \sum_{i=0}^{r-1} a_i T^i &= 0 \\
a_{r-1}T^r + \sum_{i=1}^{r-1}(a_{i-1} - a_i)T^i - a_0 &= 0
\end{aligned}$$

which, noting $T^r = 1$, implies $a_0 = a_1 = \cdots = a_{r-1} = a_0$ by linear independence. Thus, λ is of the form $\sum_{i=0}^{r-1} a_0 T^i = a_0 N$ and so $\lambda \in \operatorname{im} N$.

For the even case, again let $\lambda = \sum_{i=0}^{r-1} a_i T^i$, this time, however, in $\Lambda_{(2k)}$. Suppose $\lambda \in \ker N$. Then,

$$\begin{aligned} N \cdot \lambda &= 0 \\ N \cdot \sum_{i=0}^{r-1} a_i T^i &= 0 \\ \sum_{j=0}^{r-1} \big(T^j \cdot \sum_{i=0}^{r-1} a_i T^i\big) &= 0 \\ \sum_{j=0}^{r-1} \sum_{i=0}^{r-1} a_i T^{i+j} &= 0 \\ \sum_{i=0}^{r-1} \big(a_i \sum_{j=0}^{r-1} T^{i+j}\big) &= 0 \\ \big(\sum_{i=0}^{r-1} a_i\big)\big(\sum_{i=0}^{r-1} T^i\big) &= 0. \end{aligned}$$

By linear independence, this results in r identical equations: $a_0 + \cdots + a_{r-1} = 0$, or $a_0 = -a_1 - \cdots - a_{r-1}$. Putting this back into λ, we get

$$\lambda = \sum_{i=0}^{r-1} a_i T^i = a_0 + \sum_{i=1}^{r-1} a_i T^i = \sum_{i=1}^{r-1} a_i (T^i - 1) = \sum_{i=1}^{r-1} a_i (T-1)(1 + \cdots + T^{i-1}).$$

Hence, $\lambda = (T-1) \cdot \mu$ for some $\mu \in \Lambda$ (or rather $\Lambda_{(2k+1)}$), and so $\lambda \in \operatorname{im}(T-1)$.

Therefore, our sequence is exact, and as such is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}C_r^T$. □

3.4 The Standard Resolution

While we have already shown that a free resolution exists in general, for the case where our module is over the group ring $\Lambda = \mathbb{Z}G$, we have a more convenient construction: the standard resolution. Let $\bar{P}_k$ be the free $\mathbb{Z}$-module with basis given by $(k+1)$-tuples $(g_0, \ldots, g_k)$ of elements from G, and let G act via

$$g \cdot (g_0, \ldots, g_k) = (gg_0, \ldots, gg_k).$$

Note that $\bar{P}_0$ is in fact $\mathbb{Z}G$, i.e. Λ.

The boundary homomorphism $d : \bar{P}_k \to \bar{P}_{k-1}$ is defined on the basis as:

$$d(g_0, \ldots, g_k) = \sum_{j=0}^{k} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_k),$$

where we read $\hat{g_j}$ as "omit the element g_j". In dimension zero we use the augmentation map $\epsilon : \bar{P}_0 \to \mathbb{Z}$ given by $\varepsilon(g_0) = 1$. This definition of d is analogous to the definition of the simplicial boundary of a simplex with vertices $g_0, \ldots, g_k$. Hence the sequence

$$\cdots \longrightarrow \bar{P}_k \xrightarrow{d_k} \bar{P}_{k-1} \xrightarrow{d_{k-1}} \cdots \xrightarrow{d_1} \bar{P}_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is exact, and so constitutes a free resolution of $\mathbb{Z}$ over Λ. We can also verify this directly by writing down a contracting homotopy $h : \bar{P}_k \to \bar{P}_{k+1}$ for the underlying augmented complex of $\mathbb{Z}$-modules. We define h by $h(g_0, \ldots, g_k) = (1, g_0, \ldots, g_k)$ if $n \geq 0$ and $h(1) = (1)$ for $k = -1$. Indeed, we have

$$\begin{aligned} d_{k+1}h(g_0, \ldots, g_k) &= d_{k+1}(1, g_0, \ldots, g_k) \\ &= (g_0, \ldots, g_k) + \sum_{j=1}^{k+1} (-1)^j (1, g_0, \ldots, g_j \hat{-} 1, \ldots, g_k) \\ &= (g_0, \ldots, g_k) + \sum_{j=0}^{k+1} (-1)^{j+1} (1, g_0, \ldots, \hat{g_j}, \ldots, g_k) \end{aligned}$$

and

$$\begin{aligned} hd_k(g_0, \ldots, g_k) &= h \sum_{j=0}^{k} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_k) \\ &= \sum_{j=0}^{k} (-1)^j (1, g_0, \ldots, \hat{g_j}, \ldots, g_k), \end{aligned}$$

hence $(d_{k+1}h + hd_k)(1, g_0, \ldots, g_k) = (g_0, \ldots, g_k)$, i.e. $dh + hd = id_C$, and thus h is in fact a contracting homotopy.

As a basis for the free Λ-module $\bar{P}_k$ we may take the $(n+1)$-tuples whose first element is 1, since these represent the G-orbits of $(n+1)$-tuples. It is often useful to write such an $(n+1)$-tuple in the form $(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n)$ and to introduce the bar notation

$$[g_1|g_2|\ldots|g_n] = (1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n).$$

For $k = 0$, there is only one such basis element, denoted $[\,]$. As we already identify $\bar{P}_0$ with Λ, then $[\,] = 1$ under this identification.

Now let us find out how the boundary homomorphism ∂_* looks with this notation.

$$\begin{aligned}\partial_*[g_1|\dots|g_k] &= d(1,h_1,\dots,h_k)\\ &= \sum_{j=0}^{k}(-1)^j(1,h_1,\dots,\hat{h}_j,\dots,h_k)\end{aligned}$$

where each $h_i = g_1 \dots g_i$ and taking $1 = h_0$. Now, let us calculate each summand.

For $j = 0$:

$$\begin{aligned}(h_1,h_2,\dots,h_k) &= (g_1,g_1g_2,\dots,g_1\dots g_k)\\ &= g_1\cdot(1,g_2,\dots,g_2\dots g_k)\\ &= g_1\cdot[g_2|\dots|g_k].\end{aligned}$$

For $1 \le j \le k-1$:

$$\begin{aligned}(1,h_1,\dots,\hat{h}_j,\dots,h_k) &= (1,g_1,\dots,g_1\dots g_{j-1},g_1\dots g_jg_{j+1},\dots,g_1\dots g_k)\\ &= [g_1|\dots|g_{j-1}|g_jg_{j+1}|g_{j+2}|\dots|g_k].\end{aligned}$$

We get the second equality through forming a $(k-1)$-tuple out of $g_1,\dots,g_k$ by "sticking" together g_j and g_{j+1}.

For $j = k$:

$$\begin{aligned}(1,h_1,\dots,h_{k-1}) &= (1,g_1,\dots,g_1\dots g_{k-1})\\ &= [g_1|\dots|g_{k-1}].\end{aligned}$$

Thus, our resulting formula for the boundary homomorphism is:

$$\begin{aligned}d_*[g_1|\dots|g_{k+1}] &= g_1\cdot[g_2|\dots|g_{k+1}]\\ &\quad+\sum_{j=1}^{k}(-1)^j[g_1|\dots|g_jg_{j+1}|\dots|g_{k+1}]\\ &\quad+(-1)^{k+1}[g_1|\dots|g_k]\\ &= g_1\cdot[g_2|\dots|g_{k+1})]-[g_1g_2|g_3|\dots|g_{k+1}]\\ &\quad+[g_1|g_2g_3|\dots|g_{k+1}]-\dots\\ &\quad+(-1)^j[g_1|\dots|g_jg_{j+1}|\dots|g_{k+1}]+\dots\\ &\quad+(-1)^{k+1}[g_1|\dots|g_k].\end{aligned}$$

This standard resolution is often taken to be bar resolution. In low dimensions it has the form

$$\dots\to\bar{P}_2\xrightarrow{d_2}\bar{P}_1\xrightarrow{d_1}\bar{P}_0\xrightarrow{\epsilon}\mathbb{Z}\longrightarrow 0$$

where $d_2([g|h]) = g \cdot [h] - [gh] + [g]$, $d_1([g]) = g[\,] - [\,] = g - 1$, and $\varepsilon([\,]) = 1$.

Another version of the standard resolution is the normalised standard (or bar) resolution $\bar{F}_* = F_*/D_*$, where D_* is the degenerate subcomplex of $\bar{P}_*$, the subcomplex generated by the elements $(g_0, \cdots, g_n)$ such that $g_i = g_{i+1}$ for some i. In terms of the bar notation, D_* can be described as the G-subcomplex of F_* generated by the elements $[g_1|\ldots|g_n]$ such that $g_i = 1$ for some i. Thus $\bar{F}_*$ is a free Λ module with one basis element (still denoted $[g_1|\ldots|g_n]$) for every n-tuple of non-trivial elements of G. The chain complex $\bar{F}_*$ is exact as it is contractible by using the same contracting homotopy h from before, as it carries $\bar{F}_*$ onto itself.

3.5 From a Topological Perspective

Definition 4 *A G-complex is a CW-complex together with an action of G on X which permutes the cells. Thus, for each $g \in G$, we have a homeomorphism $x \mapsto g \cdot x$ of X for which the image $g \cdot \sigma$ of any cell σ in X is also a cell. If the G action on X is free, then we say X is a free G-complex.*

If X is a G-complex then the action of G on X induces an action of G on the cellular chain complex $C_*(X)$, through which it becomes a chain complex of G-modules.

If X is a free G-complex then each module $C_n(X)$ in the associated chain complex has a $\mathbb{Z}$-basis which is freely permuted by G. In other words, X is a G-set, and we can determine a specific Λ-basis using Proposition 1. We get that each module C_n of the associated chain complex is a Λ-module with a basis element for each G-orbit of cells. To obtain a specific basis we would have to choose a representative cell from each orbit and an orientation for each one.

For a G-complex X, the orbit complex Y is the quotient space X/G. The points in Y correspond to the orbits of points in X. Thus, if X is a free G complex, $C_*(Y)$ has a $\mathbb{Z}$-basis with a basis element for each G-orbit of cells of X. However, $C_*(X)$ is a complex of free Λ-modules with a basis element for each G-orbit of cells. Thus, $C_*(Y)$ is equivalent to the image of $C_*(X)$ after quotienting out the G-action, i.e. the groups of coinvariants. To summarise:

Proposition 8 *Let X be a free G-complex and let Y be the orbit complex X/G. Then $C_*(Y) \cong C_*(X)_G$.*

If X is contractible, then $H_*(X) \cong H_*(pt.)$. That is, the sequence

$$\cdots \longrightarrow C_k \xrightarrow{\partial} C_{k-1} \longrightarrow \cdots \longrightarrow C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is exact. Thus, we have the following proposition:

Proposition 9 *Let X be a contractible free G-complex. Then the augmented cellular chain complex of X is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$.*

Example 2 *A topological way of viewing the standard resolution.*

Consider the space X to be the simplex spanned by G (assuming G is finite), where the vertices of X are the elements of G, with G acting by left translation, and every (finite) subset of G is a simplex of X. For infinite G, consider the infinite dimensional analogue. The group G acts on X simplicially, sending simplices to other simplices of the same dimension, and the action is clearly free. We see that in both cases, the resulting simplicial chain complex, and hence boundary operator, coincide with the definitions of the standard resolution as given above.

In both cases, X is contractible by a straight-line contracting homotopy. Hence, by Proposition 9, the augmented cellular chain complex of X is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$. This is a topological way of showing the exactness of the standard resolution.

The standard resolution is a useful theoretical tool. For example, we will use it to prove the existence of the cohomological extension for groups. However, is not often practical to use for calculations. Instead, we try to find the best option for whatever group is being studied. Often, these are related to topological spaces. For example, in Example 1, there is a topological motivation by considering the action of C_∞^T on $\mathbb{R}$ by the rule $T \cdot x = x + 1$. Similarly, for the finite cyclic group C_r^T, we consider the action of T on a circle $S^1 = \{e^{i\varphi} : \phi \in \mathbb{R}\}$ by mapping $T : e^{i\varphi} \mapsto e^{i(\varphi + 2\pi/r)}$. Or, equivalently, we could consider a regular r-gon acted upon by its group of rotations.

3.6 Eilenberg-MacLane Spaces

A natural way to construct a G-complex is to take the group of deck transformations of a normal covering space. Let $p : \tilde{X} \to X$ be a normal covering space of a CW-complex X and G the group of deck transformations of $\tilde{X}$. The space $\tilde{X}$ inherits a CW-structure from X, where G freely and transitively permutes the set $p^{-1}\sigma$ for any cell $\sigma \in X$, i.e. the cells of the preimage of σ. Thus, $\tilde{X}$ is a free G-complex. The orbits of the G-action are the preimage sets $p^{-1}\sigma$, so by Proposition 1, $C_*\tilde{X}$ is a complex of free $\mathbb{Z}G$-modules with one basis element for each cell of X. The boundary maps are then derived from the boundary maps in the cellular chain complex of X.

It is now only natural to consider the effects of Proposition 9, when applicable. To do so, we consider a connected space Y with fundamental group $\pi_1 Y \cong G$ with a contractible universal cover X. Such a space is called an Eilenberg-Maclane space $K(G, 1)$. We thus obtain from 9 the following:

Proposition 10 *Let Y be a $K(G,1)$. Then, the augmented cellular chain complex of the universal cover X of Y is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$.*

In general, an Eilenberg-Maclane space $K(G,n)$ is a connected space with $\pi_n K(G,n) = G$ and all other homotopy groups trivial. For dimension 1, this definition is equivalent to our definition above. This is due to the following lemma:

Lemma 11 *For a connected space X, the following are equivalent:*

1. *the universal cover of X is contractible,*
2. *$H_i(X) = 0$ for $i \geq 2$,*
3. *$\pi_i(X) = 0$ for $i \geq 2$.*

This lemma, is due to results from basic homotopy theory. Similarly, the existence of a space $K(G,n)$ can be proven by construction, another famous result from homotopy theory.

Let us now cover a basic example:

Example 3 *A resolution of $\mathbb{Z}$ over $\mathbb{Z}G$ for $G = \mathbb{Z}_2$.*

The infinite dimensional real projective space $\mathbb{R}\mathrm{P}^\infty$ is a well-known example of a $K(G,1)$, as it has $\pi(\mathbb{R}\mathrm{P}^\infty) = \mathbb{Z}_2$ and all other homotopy groups trivial. The universal cover of the real projective space $\mathbb{R}\mathrm{P}^\infty$ is the infinite sphere S^∞, where the covering map identifies two opposite points. This means the non-trivial element of G acts as the antipodal map. By Proposition 10, the cellular chain complex of S^∞ together with the G action forms a resolution for $\Lambda = \mathbb{Z}G$ over $\mathbb{Z}$.

We construct the CW-complex for S^∞ inductively. Each X_k skeleton is homeomorphic to an k-sphere, where the $(k-1)$-sphere X_{k-1} is the equator, and the hemispheres are formed by two k-cells a_k and b_k attached along said equator. Thus, in $\mathbb{Z}$ coefficients we have the following cellular chain complex:

$$\cdots \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\partial_k} \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\partial_{k-1}} \ldots \xrightarrow{\partial_1} \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

The boundary maps ∂_k are determined by the degrees of the attaching maps of the k-cells. As each k-cell b_k is the antipodal image of a_k, the degree of its attaching map is $(-1)^k$ times that of a_k. Hence, we have

$$\begin{aligned} \partial_1 a_1 &= a_0 - b_0, & \partial_1 b_1 &= b_0 - a_0, \\ \partial_2 a_2 &= a_1 + b_1, & \partial_2 b_2 &= b_1 + a_1, \\ \partial_3 a_3 &= a_2 - b_2, & \partial_3 b_3 &= b_2 - a_2. \\ \vdots & & \vdots & \end{aligned}$$

In general form, we have

$$\partial_k a_k = a_{k-1} + (-1)^k b_{k-1}$$
$$\partial_k b_k = b_{k-1} + (-1)^k a_{k-1}$$

In every dimension k, a_k and b_k are antipodal images of each other, meaning the non-trivial element T in G acts by swapping them. Hence, we may write $b_k = Ta_k$. This way, the $\mathbb{Z}$-module in dimension k, $\mathbb{Z} \oplus \mathbb{Z}$ generated by a_k and b_k, becomes the G-module $\mathbb{Z} \oplus T\mathbb{Z} = \Lambda$ generated by a_k. Here, the boundary map becomes

$$\partial_k a_k = (1 + (-1)^k T)a_{k-1} = \begin{cases} 1+T, & 2 \mid k, \\ 1-T, & 2 \nmid k. \end{cases}$$

Thus, we have the following resolution of $\mathbb{Z}G$ over $\mathbb{Z}$:

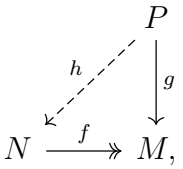
$$\ldots \xrightarrow[1+T]{\partial_4} \Lambda \xrightarrow[1-T]{\partial_3} \Lambda \xrightarrow[1+T]{\partial_2} \Lambda \xrightarrow[1-T]{\partial_1} \Lambda \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

This resolution coincides with the resolution calculated in Example 1, taking order $r = 2$.

3.7 Projective Modules and Uniqueness of Resolutions

Let us return to the more general case, resolutions of an R-module M where R is an arbitrary ring. An R-module M admits many free resolutions, our goal in this section is to show that all such resolutions are homotopy equivalent. In fact, this is true more generally, for projective resolutions.

Definition 5 *Consider the mapping problem*

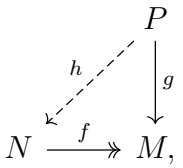


where f is a surjection, and we wish to construct h such that the diagram commutes, i.e. $fh = g$. A module P is called projective if a solution exists for every mapping problem of this form.

Let us show why this generalises the concept of free modules:

Lemma 12 *Free modules are projective.*

Proof: Let F be free with basis (e_γ) and consider a mapping problem



where f is a surjection. Then $g(e_\gamma) \in M = \operatorname{im} f$, so we can choose $x_\gamma \in N$ with $f(x_\gamma) = g(e_\gamma)$. Now let h be the unique R-module map with $g(e_\gamma) = x_\gamma$. $\square$

In Definition 3, by replacing each instance of "free" with "projective, we have the definition of a projective resolution; a resolution where all the modules are projective. Therefore, any free resolution is also a projective resolution.

There are other, equivalent, ways to define projective modules. One that will be useful for us later is using split sequences.

Definition 6 *Consider the short exact sequence of R-modules:*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0.$$

We define the following:

a) the sequence is right split if there exists a homomorphism $s : C \to B$ such that $\beta s = id_C$;

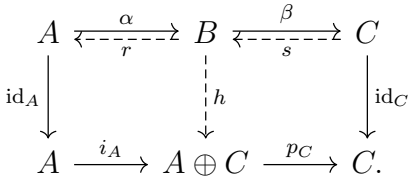
b) the sequence is left split if there exists a homomorphism $r : B \to A$ such that $r\alpha = id_A$;

c) the sequence is split exact if there exists an isomorphism $h : B \to A \oplus C$ such that $h\alpha = i_A$ and $hp_C = \beta$, where $i_A : A \to A \oplus C$ is the natural inclusion and $p_C : A \oplus C$ is the natural projection.

In fact, these definitions are all equivalent. So, if any of these hold true, we say the sequence splits. This is shown in what is commonly known as the Splitting Lemma:

Lemma 13 *The cases in Definition 6 are equivalent.*

Proof: Throughout the proof, we will be referring to the maps given by the following diagram:



The solid arrows denote α and β, from the starting short exact sequence, the identity maps on A and C, and the natural inclusion $i_A : A \to A \oplus C$ and projection $p_C : A \oplus C \to C$. The dotted arrows are the maps from the cases (a), (b), and (c). Let us to proceed to show how each case implies the other.

(a) $\Rightarrow$ (b): Suppose there is an injection $s : C \to B$ such that $\beta s = \mathrm{id}_C$. Let $b \in B$ and consider $b' = b - s\beta b$. Now, we have

$$\beta b' = \beta b - \beta s \beta b = \beta b - \mathrm{id}_C \beta b = \beta b - \beta b = 0.$$

Thus, $b' \in \ker \beta$. However, by the exactness of the starting sequence, $\ker \beta = \operatorname{im} \alpha$. As α is an injection, we can define α^{-1} on $\operatorname{im} \alpha$. Thus, we may define the map $r : B \to A$ on an arbitrary element $b \in B$ by

$$r(b) = \alpha^{-1}(b - s\beta b).$$

Clearly, we have $r\alpha = \mathrm{id}_A$. As r has a right inverse, it must be a surjection. Note that

$$rsc = \alpha^{-1}(sc - s\beta sc) = \alpha^{-1}(sc - sc) = 0,$$

for all $c \in C$, hence $rs = 0$.

(b) $\Rightarrow$ (a): Suppose there is a surjection $r : B \to A$ such that $r\alpha = \mathrm{id}_A$. Let $c \in C$. As β is a surjection, there is some $b \in B$ such that $c = \beta b$. Define $s : C \to B$ on c as

$$s(c) = b - \alpha r b.$$

Thus, $\beta sc = \beta b - \beta \alpha r b = c - 0 = c$, i.e. $\beta s = \mathrm{id}_C$. As s has a left inverse, it must be an injection. Again, note that

$$rsc = rb - r\alpha rb = rb - rb = 0,$$

i.e. $rs = 0$.

We have thus far shown that (a) and (b) are equivalent. Let us now show the following.

(a) $\Rightarrow$ (c): Suppose there is a map $s : C \to B$ such that $\beta s = \mathrm{id}_C$. Immediately, it follows that s is injective, and hence $\operatorname{im} s \cong C$. Also, as $\beta s = \mathrm{id}_C$, this means $\ker \beta \cap \operatorname{im} s = 0$, i.e. $\operatorname{im} \alpha \cap \operatorname{im} s = 0$.

Consider an arbitrary element $b \in B$. Let $b' = b - s\beta b$. We showed in the proof of (a) $\Rightarrow$ (b) that $b' \in \operatorname{im} \alpha$. Also, by taking r defined from our proof of (a) $\Rightarrow$ (b), we have $b' = \alpha r b$. Clearly, we have $b'' = s\beta b \in \operatorname{im} s$. Thus, we have written b as the sum $b' + b''$ for some $b' \in \operatorname{im} \alpha$ and $b'' \in \operatorname{im} s$.

Suppose we have another way to write b as a sum of two elements from $\operatorname{im} \alpha$ and $\operatorname{im} s$, say $b = c' + c''$, where $c' \in \operatorname{im} \alpha$ and $c'' \in \operatorname{im} s$. Thus, $b' + b'' = c' + c''$, i.e. $b' - c' = c'' - b''$. The left side is in $\operatorname{im} \alpha = \ker \beta$, and the right side is in

$\operatorname{im} s$. However, $\ker \beta \cap \operatorname{im} s = 0$, and so $c' = b'$ and $c'' = b''$. Therefore, the decomposition of b as a sum of elements from $\operatorname{im} \alpha$ and $\operatorname{im} s$ is unique.

We have thus shown that $B = \operatorname{im} \alpha \oplus \operatorname{im} s \cong A \oplus C$. The isomorphism $h : B \to A \oplus C$ is given on an element $b \in B$ with unique composition $b = b' + b''$, for $b' \in \operatorname{im} \alpha$ and $b'' \in \operatorname{im} s$, as $h(b) = i_A r(b') + i_C \beta(b'')$. As $\operatorname{im} \beta = \ker \alpha$, we have $b' \in \operatorname{im} \beta = \ker \alpha$, and, as we noted earlier $rs = 0$, so $b'' \in \operatorname{im} s \subseteq \ker r$. This means the homomorphism h is defined as $h = i_A r + i_C \beta$. To see that h indeed fulfils the requirements in (c), we calculate as follows:

$$h\alpha = i_A r\alpha + i_C \beta\alpha = i_A \mathrm{id}_A + i_C \circ 0 = i_A,$$

and

$$p_C h = p_C i_A r + p_C i_C \beta = 0r + \mathrm{id}_C \beta = \beta.$$

Finally, let us show **(c) ⇒ (a)**. Suppose we have an isomorphism $h : B \to A \oplus C$ such that $h\alpha = i_A$ and $p_C h = \beta$. We can define $s : C \to B$ as $s = h^{-1} i_C$. Now, from $p_C h = \beta$, we have $p_C = \beta h^{-1}$. Hence,

$$\beta s = \beta h^{-1} i_C = p_C i_C = \mathrm{id}_C.$$

Thus, we have shown that (a), (b), and (c) are equivalent. □

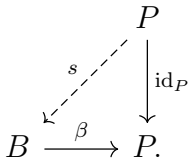
For projective modules, we have the following property.

Lemma 14 *If P is a projective module, then any short exact sequence ending in P splits. That is to say, given R-modules A and B, such that the following is an exact sequence:*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} P \longrightarrow 0,$$

then this sequence necessarily splits.

Proof: Given such a sequence, let us consider the following diagram:

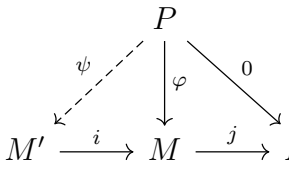


As P is projective, there must exist an R-homomorphism $s : P \to B$ such that the diagram commutes. Hence $\beta s = \mathrm{id}_P$. □

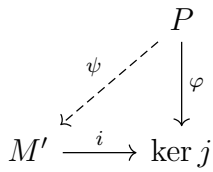
In fact, the converse is also true, and this may be taken as an alternative definition of projective modules. However, we will only be using the implication in

the above lemma, so we will skip the proof of the converse.

We now move on to showing the uniqueness of projective (and thus free) resolutions. We will be using a modified definition of a projective module: consider the mapping problem



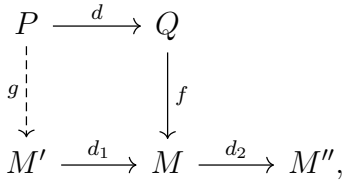
where $j\varphi = 0$. A module P is called projective if a solution exists for every such mapping problem in which the row is exact. This is equivalent to the previous definition simply by restricting to



as $j\varphi = 0$ implies $\operatorname{im}\varphi \in \ker j$.

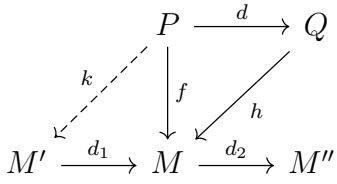
Now let us prove the following lemma which will assist us later:

Lemma 15 *(a) Suppose given a diagram*



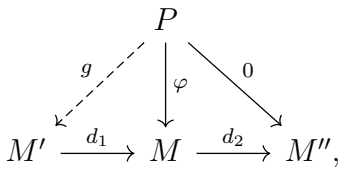
where $d_2fd = 0$ and it is desired to find a g such that $d_1g = fd$. If P is projective and the bottom row is exact, then such a g exists.

(b) Suppose given a diagram (not necessarily commutative)



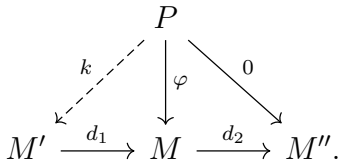
where $d_2hd = d_2f$ and it is desired to find a k such that $d_1k + hd = f$. If P is projective and the bottom row is exact, then such a k exists.

Proof: (a) By setting $\varphi = fd$ we transform the problem into



where $d_2\varphi = 0$ as $d_2\varphi = d_2fd = 0$. Hence for projective P, there exists g such that $d_1g = \varphi$ i.e. $d_1g = fd$.

(b) This time, set $\varphi = f - hd$. Now, as $d_2\varphi = d_2(f - hd) = 0$, we have

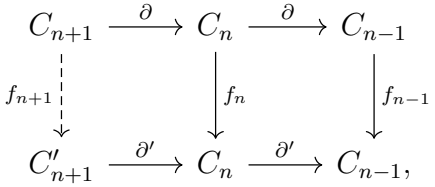


Thus for projective P, there exists k such that $\varphi = d_1k$ i.e. $d_1k = f - hd$. Thus $d_1k + hd = f$. □

The next lemma is about chain maps and homotopies from a projective complex to an exact one.

Lemma 16 *Let (C, ∂) and (C', ∂') be chain complexes and let r be an integer. Let $(f_i : C_i \to C'_i)_{i\le r}$ be a family of maps such that $\partial'_i f_i = f_{i-1}\partial_i$ for $i \le r$. If C_i is projective for $i > r$ and $H_i(C') = 0$ for $i \ge r$, then $(f_i)_{i\le r}$ extends to a chain map $f : C \to C'$, and f is unique up to homotopy. More precisely, any two extensions are homotopic by a homotopy h such that $h_i = 0$ for $i \le r$.*

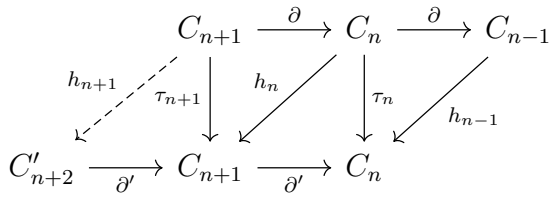
Proof: Assume inductively that f_i has been defined for $i \le n$, where $n \ge r$, and that $\partial'_i f_i = f_{i-1}\partial_i$ for $i \le n$. We then have a mapping problem



where $\partial' f_n \partial = f_{n-1}\partial\partial = 0$. The desired f_{n+1} therefore exists by Lemma 15a.

Suppose now that g is a second extension of $(f_i)_{i\le r}$. We wish to find a homotopy h between f and g. Let us proceed inductively. We start the induction by setting $h_i = 0$ for $i \le r$. Now, assume that $h_i : C_i \to C''_{i+1}$ has been defined for

$i \leq n$, where $n \geq r$, and that $\partial' h_i + h_{i-1}\partial = f_i - g_i$. Setting $\tau = f_i - g_i$, we have the mapping problem

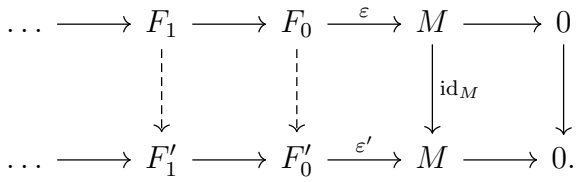


with $\partial' h_n \partial = (\tau_n - h_{n-1}\partial)\partial$ by the inductive hypothesis. Since $\partial^2 = 0$, this is equal to $\tau_n \partial$. As τ is a chain map, we thus have $\partial' h_n \partial = \partial' \tau_{n+1}$. Now, as C_{n+1} is projective, we may apply Lemma 15b, by which the desired h_{n+1} with $\partial' h_{n+1} + h_n \partial = \tau_{n+1}$ exists. □

This lemma is the core that is used to reach our goal of finding the uniqueness of projective resolutions, which we shall wrap up in the following theorem:

Theorem 17 *Given projective resolutions F and F' of a module M, there is a augmentation-preserving (i.e. it satisfies $\varepsilon' f_0 = \varepsilon$) chain map $f : F \to F'$, unique up to homotopy, and f is a homotopy equivalence.*

Proof: Let us consider the following diagram:



We apply Lemma 16 to the augmented resolutions F and F' with $r = -1$ and the map $f_{-1} = \mathrm{id}_M$. We conclude that there is a (unique up to homotopy) chain map $f : F \to F'$ which is augmentation-preserving because $\varepsilon' f_0 = \mathrm{id}_M \varepsilon = \varepsilon$. Moreover, we conclude that f is unique up to homotopy. Analogously, we have an augmentation-preserving map $f' : F' \to F$. Now, as $f'f$ and id_F are both extensions of id_M between two copies of F, by the second part of Lemma 16, we have $f'f \simeq \mathrm{id}_F$. Similarly, we have $ff' \simeq \mathrm{id}_{F'}$. Hence, f is a homotopy equivalence. □

4 The Cohomology of Groups

4.1 The Cohomology and Homology Groups of a Group

Let G be a group and let $\varepsilon : F \to \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ over Λ. We define the cohomology and homology groups of G respectively by

$$H^iG = H^i(F^G),\ H_iG = H_i(F_G).$$

The invariants and coinvariants functors $(\_)^G$ and $(\_)_G$ are additive, i.e. for any $\psi, \phi : A \to A'$, we have $(\psi + \phi)^G = \psi^G + \phi^G$ and $(\psi + \phi)_G = \psi_G + \phi_G$. This follows from the alternative definitions using the Hom and tensor functors respectively, i.e. $(\_)^G = \mathrm{Hom}_\Lambda(\mathbb{Z}, \_)$ and $(\_)_G = \mathbb{Z} \otimes_\Lambda \_$. Thus, these functors preserve chain homotopies. Indeed, suppose $\varphi : F \to F'$ is a chain homotopy from ψ to ϕ, i.e. $d'\varphi + \varphi d = \psi - \phi$. Then, when applying the functor to both sides of this equation, we have

$$\begin{aligned} (d'\varphi + \varphi d)^G &= (\psi - \phi)^G \\ (d'\varphi)^G + (\varphi d)^G &= \psi^G - \phi^G \\ d'^G\varphi^G + \varphi^G d^G &= \psi^G - \phi^G. \end{aligned}$$

Hence, φ^G is a chain homotopy from ψ^G to ϕ^G. Analogously, φ_G is a chain homotopy from ψ_G to ϕ_G.

Suppose we have a second free resolution $\varepsilon' : F' \to \mathbb{Z}$ of $\mathbb{Z}$ over Λ. By Theorem 17, there exists an augmentation preserving homotopy equivalence $f : F \to F'$. By the above reasoning, $f^G : F^G \to F'^G$ and $f_G : F_G \to F'_G$ are both also homotopy equivalences. Therefore, our definitions of H^iG and H_iG don't depend on the choice of projective resolution $\varepsilon : F \to \mathbb{Z}$.

The cohomology and homology groups of G always exist, by the existence of a free resolution. Specifically, we may take the standard resolution, or the bar resolution, or a resolution found via topology, etc.

For a topological perspective, consider a $K(G,1)$-complex Y with universal cover X. By Proposition 10, $C_*(X)$ is a free resolution of $\mathbb{Z}$ over Λ. The space Y is the orbit complex of X, hence $C_*(X)_G \cong C_*(Y)$ by Proposition 8. Thus, by taking homologies of both sides, we obtain:

Proposition 18 *If Y is a $K(G,1)$-complex, then $H_*G \cong H_*Y$.*

4.2 Exactness of the Hom and Tensor Product Functors

To compute the cohomology and homology with coefficients in a Λ-module A instead of $\mathbb{Z}$ we will be applying the functors $\mathrm{Hom}_\Lambda(\_, A)$ and $\_ \otimes_\Lambda A$ to the

projective resolution respectively, and computing the homology of these chain complexes. This section is dedicated to covering a few preliminary properties about these functors.

As we saw in the previous section, these functors are additive and preserve chain homotopies. We now inspect how they behave on short exact sequences. Suppose, throughout the rest of this section, that A is a given left R-module.

Lemma 19 *The contravariant functor* $\mathrm{Hom}_R(\_, A)$ *is left exact on the category of left* R*-modules. That is to say, if*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

is a short exact sequence of left R *modules, the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(N, A) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, A) \xrightarrow{\phi^*} \mathrm{Hom}_R(L, A)$$

is exact in the category of abelian groups.

Proof: For an element $f \in \mathrm{Hom}_R(M, A)$, the image of f under ϕ^* is defined pointwise as $(\phi^* f)(a) = f(\phi(a))$ for all $a \in A$, i.e. $\phi^* f = f\phi$. Similarly for ψ^*.

Let us start by showing $\ker \psi^* = 0$. Suppose $f \in \ker \psi^*$, i.e. $\psi^* f = 0$. Thus $f\psi = 0$. Hence $\mathrm{im}\, \psi \subseteq \ker f$. As $\mathrm{im}\, \psi = N$ by the exactness of the first sequence, this means $f(n) = 0$ for all $n \in N$, i.e. $f = 0$.

Let us now show that $\ker \phi^* = \mathrm{im}\, \psi^*$. First, for an element $f \in \mathrm{Hom}_R(M, A)$, $\phi^*\psi^* f = \phi^* f\psi = f\psi\phi = 0$, i.e. $\mathrm{im}\, \psi^* \subseteq \ker \phi^*$. Now let us show the opposite inclusion. Suppose $f \in \ker \phi^*$, i.e. $\phi^* f = 0$. This means $f\phi = 0$, by which $\mathrm{im}\, \phi \subseteq \ker f$. As $\mathrm{im}\, \phi = \ker \psi$ by the exactness of the first sequence, this means $\ker \psi \subseteq \ker f$. Thus, we can treat f as the composition of the quotient map $q : M \to M/\ker \psi$, defined by ψ, and $f' : M/\ker \psi \to A$. As $M/\ker \psi \cong N$, we may replace $M/\ker \psi$ with N in the above maps, resulting in the maps $\psi : M \to N$ and $g : N \to A$, by which we have $f = g\psi = \psi^* g$. Thus, $f \in \mathrm{im}\, \psi^*$. Hence, $\ker \phi^* = \mathrm{im}\, \psi^*$.

$$\begin{array}{ccc} M & \xrightarrow{\psi} & N \\ \downarrow{\scriptstyle q} & \searrow^{f} & \downarrow{\scriptstyle g} \\ M/\ker \psi & \xrightarrow{f'} & A. \end{array}$$

□

We have a similar story for the tensor product functors, except they are right exact instead of left exact. The arguments are all very similar as with the Hom functors, although slightly more involved.

Lemma 20 *The covariant functor* $\_ \otimes_R A$ *is right exact on the category of right* R*-modules. That is to say, if*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

is a short exact sequence of right R *modules, the sequence*

$$L \otimes_R A \xrightarrow{\phi_*} M \otimes_R A \xrightarrow{\psi_*} N \otimes_R A \longrightarrow 0$$

is exact in the category of abelian groups.

Proof: The induced homomorphisms are defined as $\phi_* = \phi \otimes \mathrm{id}_A$ and $\psi_* = \psi \otimes \mathrm{id}_A$. This is clearly well-defined.

Let us start by showing $\operatorname{im} \psi_* = N \otimes_R A$. A simple tensor $m \otimes_R a \in M \otimes_R A$ maps to $\psi_*(m \otimes_R a) = \psi(m) \otimes_R a$. Thus, by the linearity of ψ_*, $\operatorname{im} \psi_*$ is generated by all such elements, i.e. $\operatorname{im} \psi_* = \operatorname{im} \psi \otimes_R A$. As ψ is surjective, i.e. $\operatorname{im} \psi = N$, this means $\operatorname{im} \psi_* = N \otimes_R A$.

Now, let us show $\ker \psi_* = \operatorname{im} \phi_*$. First of all, their composition is 0: for any simple tensor $l \otimes_R a \in L \otimes_R A$,

$$\psi_* \phi_* (l \otimes_R a) = \psi(\phi(l) \otimes_R a) = \psi\phi(l) \otimes_R a = 0.$$

This extends to all of $L \otimes_R A$, and so $\psi_* \phi_* = 0$, i.e. $\operatorname{im} \phi_* \subseteq \ker \psi_*$.

Next, let us consider $(M \otimes_R A)/\ker \psi_*$ and $(M \otimes_R A)/\operatorname{im} \phi_*$. As $\operatorname{im} \phi_* \subseteq \ker \psi_*$, we have a natural homomorphism from $(M \otimes_R A)/\operatorname{im} \phi_*$ to $(M \otimes_R A)/\ker \psi_*$. This homomorphism is an isomorphism if and only if $\operatorname{im} \phi_* = \ker \psi_*$. Hence, we will proceed to show that this homomorphism is indeed an isomorphism.

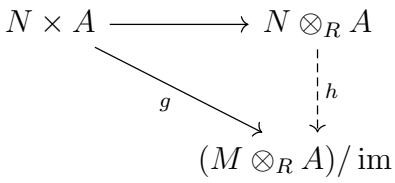
By the first isomorphism theorem, we have $(M \otimes_R A)/\ker \psi_* \cong \operatorname{im} \psi_* = N \otimes_R A$. Now, analogously to the first part of the proof, we have $\operatorname{im} \phi_* = \operatorname{im} \phi \otimes_R A$. By the exactness of the first sequence, $\operatorname{im} \phi = \ker \psi$, so $(M \otimes_R A)/\operatorname{im} \phi_* = (M \otimes_R A)/(\ker \phi \otimes_R A)$.

As $\operatorname{im} \phi_* \subseteq \ker \psi_*$, we can factor ψ_* as

$$M \otimes_R A \xrightarrow{q} (M \otimes_R A)/\operatorname{im} \phi_* \xrightarrow{f} N \otimes_R A$$

where q is the quotient map and f is defined as follows: as any element in $(M \otimes_R A)/\operatorname{im} \phi_*$ is of the form $q(t)$ for some $t \in M \otimes_R A$, we define f on $q(t)$ as $\psi_*(t)$. Indeed, if $q(t') = q(t)$ for some $t \in M \otimes_R A$, then $q(t' - t) = 0$ i.e. $t' - t \in \ker q = \operatorname{im} \phi_*$. However, $\operatorname{im} \phi_* \subseteq \ker \psi_*$, so $\psi_*(t' - t) = 0$, and so $f(t) = f(t')$, therefore f is well-defined. If we can show f is an isomorphism, then we will have $(M \otimes_R A)/\operatorname{im} \phi_* \cong N \otimes_R A \cong (M \otimes_R A)/\ker \psi_*$, as desired.

Let us find an inverse of f. We shall do this using the universal property of the tensor product. Consider the following diagram:



By the universal property of the tensor product, if g is a bilinear map, then there exists a map h making the diagram commute.

Let us define g by $(n, a) \mapsto q(m \otimes_R a)$, for all $(n, a) \in N \times A$, where m is some element of M such that $\psi(m) = n$. First let us check that this map is well-defined: suppose for some other $m' \in M$ we also have $\psi(m') = n$. This means $\psi(m') = \psi(m)$, hence $m' - m \in \ker\psi$. Thus, $(m' - m) \otimes_R a \in \ker\psi \otimes_R A$. Now, analogously to the very first part of the proof, we have $\operatorname{im}\phi_* = \operatorname{im}\phi \otimes_R A$. By the exactness of the first sequence, $\operatorname{im}\phi = \ker\psi$, and thus $(m' - m) \otimes_R a \in \operatorname{im}\psi_*$. Consequently, this means that $q(m' \otimes_R a) = q(m \otimes_R a)$. Therefore, $g(n)$ has a unique image, hence g is well-defined.

To use the universal property, we must also show that g is bilinear. Suppose $n, n' \in N$ and $a, a' \in A$. Let $m, m' \in M$ be some elements of M such that $\psi(m) = n$ and $\psi(m') = n'$. This means $\psi(m + m') = n + n'$. Thus, we have

$$g(n + n', a) = q((m + m') \otimes_R a) = q(m \otimes_R a) + q(m' \otimes_R a) = g(n, a) + g(n', a)$$

and

$$g(n, a + b) = q(m \otimes_R (a + b)) = q(m \otimes_R a) + q(m \otimes_R b) = g(n, a) + g(n, b).$$

Also, for any $r \in R$,

$$g(n \cdot r, a) = q(m \cdot r \otimes_R a) = q(m \otimes_R r \cdot a) = g(n, r \cdot a).$$

Therefore, g is bilinear, and so, by the universal property, we have a well-defined map $h : N \otimes_R A \to (M \otimes_R A)/\operatorname{im}\phi_*$ defined by $h : n \otimes_R a \mapsto q(m \otimes a)$ on all simple tensors $n \otimes_R a \in N \otimes_R A$ with $m \in M$ such that $\psi(m) = n$.

Let us now show that this map, h, and f are inverses. Suppose $n \otimes_R a \in N \otimes_R A$, and $m \in M$ such that $\psi(m) = n$. Then,

$$f \circ h(n \otimes_R a) = f(q(m \otimes_R a)) = \psi_*(m \otimes a) = \psi(m) \otimes a = n \otimes a$$

Conversely, consider an element $q(m \otimes_R a) \in M \otimes_R A/\operatorname{im}\phi_*$. Now,

$$h \circ f(q(m \otimes_R a)) = h(\psi_*(m \otimes_R a)) = h(\psi_*(m) \otimes_R a) = q(m \otimes_R a).$$

Thus, f and h are inverses, and are therefore isomorphisms, and so we are done. $\square$

It is also true that for a right R-module A, the functor $\mathrm{Hom}_R(\_, A)$ is left exact on the category of right R-modules, and $A \otimes_R \_$ is right exact on the category of left R-modules. The proofs of these statements are entirely analogous to the previous proofs.

Lemma 2 is a direct result of Lemma 19, as $A^G \cong \mathrm{Hom}_\Lambda(\mathbb{Z}, A)$. Similarly, Lemma 3 is a direct result of Lemma 20, as $A_G \cong \mathbb{Z} \otimes_\Lambda A$.

On projective modules, the results of the previous two lemmas can be refined further.

Proposition 21 *The functor* $\mathrm{Hom}_R(\_, A)$ *is exact on the category of projective modules. That is to say, if*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

is a short exact sequence of projective left R modules, then the sequence

$$0 \longrightarrow \mathrm{Hom}_R(N, A) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, A) \xrightarrow{\phi^*} \mathrm{Hom}_R(L, A) \longrightarrow 0$$

is exact in the category of abelian groups.

Proof: By Lemma 19 we have that the derived sequence is left exact, so all that's left to prove is that ϕ^* is a surjection.

By Lemma 14, as N is projective, we have that the original sequence splits. Hence, there is a surjection $r : M \to L$ such that $r\phi = \mathrm{id}_L$. Thus, for any $f \in \mathrm{Hom}_R(L, A)$, let $g = fr$. Then, we get

$$\phi^*(fr) = fr\phi = f\mathrm{id}_L = f.$$

Therefore, $f \in \mathrm{im}\, \phi^*$, and hence ϕ^* is a surjection. $\square$

Proposition 22 *The functor* $\_ \otimes_R A$ *is exact in the category of projective modules. That is to say, if*

$$0 \longrightarrow L \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

is a short exact sequence of projective left R modules, the sequence

$$0 \longrightarrow L \otimes_R A \xrightarrow{\psi_*} M \otimes_R A \xrightarrow{\phi_*} N \otimes_R A \longrightarrow 0$$

is exact in the category of abelian groups.

Proof: By Lemma 20 we have that the sequence is right exact, so all that's left to prove is that ϕ_* is injective.

By Lemma 14, as N is projective, we have that the original sequence splits. Thus, there is a surjection $r : M \to L$ such that $r\phi = \mathrm{id}_L$. Now, we have

$$r_*\phi_* = (r \otimes_R \mathrm{id}_A) \circ (\phi \otimes_R \mathrm{id}_A) = r\phi \otimes_R \mathrm{id}_A = \mathrm{id}_L \otimes_R \mathrm{id}_A = \mathrm{id}_{L \otimes_R A}$$

Thus, r_* is a left inverse of ϕ_*, hence ϕ_* is an injection. □

When an additive functor is exact, it doesn't just preserve the exactness of short sequences, it also preserves exact sequences, as the name implies. Moreover, it in fact commutes with the homology functor on any chain complex.

Proposition 23 *Suppose we have a chain complex* (C_*, ∂_*)*:*

$$\cdots \to C_{k+1} \xrightarrow{\partial_{k+1}} C_k \xrightarrow{\partial_k} C_{k-1} \to \dots$$

Then, for the chain complex

$$\cdots \to FC_{k+1} \xrightarrow{F\partial_{k+1}} FC_k \xrightarrow{F\partial_k} FC_{k-1} \to \dots$$

we have

$$H_k(FC) = FH_k(C).$$

Proof: Let F and C be as above. First of all, we have

$$\mathrm{im}\, F\partial_{k+1} = F \,\mathrm{im}\, \partial_{k+1}.$$

Next, consider the short exact sequence

$$0 \to \ker \partial_k \xrightarrow{i_k} C_k \xrightarrow{\partial_k} \mathrm{im}\, \partial_k \to 0.$$

As F is exact, then the following sequence is also short exact:

$$0 \to F \ker \partial_k \xrightarrow{Fi_k} FC_k \xrightarrow{F\partial_k} F \,\mathrm{im}\, \partial_k \to 0.$$

Thus,

$$\ker F\partial_k = F \ker \partial_k.$$

Now, let us consider the short exact sequence defining the k-th homology group:

$$0 \to \mathrm{im}\, \partial_{k+1} \xrightarrow{j_k} \ker \partial_k \xrightarrow{\pi_k} H_k(C) \to 0.$$

Again, as F is exact, then the following sequence is also short exact:

$$0 \to F \operatorname{im} \partial_{k+1} \xrightarrow{Fj_k} F \ker \partial_k \xrightarrow{F\pi_k} FH_k(C) \to 0.$$

Thus, by exactness, we have

$$\frac{F(\ker \partial_k)}{F(\operatorname{im} \partial_{k+1})} \cong FH_k(C).$$

hence $a \in \Lambda^G$. If we write $a = \sum_{i=1}^{n} k_i g_i$ for $n \geq 1$, $k_i \in \mathbb{Z}$, $g_i \in G$, then as $g \cdot a = a$ for all $g \in G$, this means all the k_i, $i \leq n$ are identical. It also means that for every element $g \in G$ there exists some $i \leq n$ such that $g = g_i$, hence G must be finite and $n = |G|$. Thus, we have $a = k \sum_{g \in G} g$. However, as $\varepsilon f = \mathrm{id}$, this means $\varepsilon a = 1$, i.e. $k|G| = 1$. Hence, $k = |G| = 1$, which is a contradiction.

4.3 The Cohomology of Groups with Coefficients

In Lemma 2, the invariants functor $(\_)^G$ was shown to be left exact, but not an exact functor. Specifically, ψ^G was not proven to be an epimorphism like ψ. In general, this need not be true. This is the motive for defining $H^1(G, A)$, the first cohomology group of G with coefficients in A, as a measure of the failure of the right exactness of the invariants functor. This is done by taking a projective resolution of $\mathbb{Z}$ over Λ and applying the functor $\mathrm{Hom}(\_, A)$. The final (or, now, first) non-zero element of the resulting complex will be $\mathrm{Hom}(\mathbb{Z}, A)$, which, by equation (1), is A^G. The homology of this sequence will obey the following axioms, which uniquely determine the cohomology extension:

Definition 7 *The cohomology groups of a group G with coefficients in A, denoted $H^k(G, A)$, $k \geq 0$, form a covariant family of functors from $\mathcal{U}_G$, the category of G-modules, to abelian groups, which have the following properties:*

1. $H^0(G, A) = A^G$
2. *For each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{U}_G$ there exists a natural transformation $\delta = \delta^k : H^k(G, C) \to H^{k+1}(G, A)$ and a long exact sequence of cohomology groups*

$$\cdots \longrightarrow H^k(G, A) \xrightarrow{\phi^*} H^k(G, B) \xrightarrow{\psi^*} H^k(G, C) \xrightarrow{\delta} H^{k+1}(G, A) \longrightarrow \ldots$$

3. *If A is a coinduced module, then $H^k(G, A) = 0$ for all $k \geq 1$.*

The family $\{H^k(G, \cdot), k \geq 0\}$ can thus be viewed as a cohomological extension of the invariant elements functor, which vanishes on coinduced modules. Let us show this extension indeed exists, and is unique.

Theorem 24 *The cohomological extension $H^k(G, *)$, $k \geq 0$ exists and is unique.*

Proof: Let

$$\cdots \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

be a projective resolution of the trivial G-module $\mathbb{Z}$. For any G-module A, we have the related cochain complex

$$\cdots \leftarrow \mathrm{Hom}_G(P_k, A) \leftarrow \mathrm{Hom}_G(P_{k-1}, A) \leftarrow \ldots \leftarrow \mathrm{Hom}_G(P_0, A) \leftarrow A^G \leftarrow 0.$$

where we replaced $\mathrm{Hom}_G(\mathbb{Z}, A)$ with A^G, by equation (1). The composition of two successive homomorphisms in the cochain complex is zero, thus, we may define the cohomology groups as

$$H^k(G, A) = H_k(\mathrm{Hom}_G(P_k, A)).$$

The functor $\mathrm{Hom}_G(\_, A)$ is additive, and so preserves chain homotopies. Thus, by the same argument as for the integral cohomology, the cohomology groups are independent of the choice of projective resolution.

The existence of the natural coboundary homomorphisms δ^k and the long exact sequence from the second point of the definition follow by the usual diagram chase. The first property is satisfied by making the convention that 0-dimensional coboundaries are trivial. Consider the tail of the cochain complex

$$\cdots \longleftarrow \mathrm{Hom}_G(P_1, A) \xleftarrow{d^1} \mathrm{Hom}_G(P_0, A) \xleftarrow{d^0} A^G \longleftarrow 0.$$

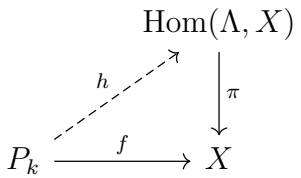
By setting $d^0 = 0$, we have $H^0(G, A) = \ker d^1$. We defer the rest of this calculation to later, where we will use the bar resolution. Let us instead first show the third property, that the cohomology disappears on coinduced modules.

Let $A = \mathrm{Hom}(\Lambda, X)$ be a coinduced module, where X has trivial G-action. We will first show that

$$\mathrm{Hom}_G(P_k, \mathrm{Hom}(\Lambda, X)) \cong \mathrm{Hom}_{\mathbb{Z}}(P_k, X).$$

Let us define the map $\pi : \mathrm{Hom}(\Lambda, X) \to X$ with $\pi(\varphi) = \varphi(1)$ for all $\varphi \in \mathrm{Hom}(\Lambda, X)$. This map is clearly a surjection.

Suppose $f \in \mathrm{Hom}(P_k, X)$, i.e. $f : P_k \to X$. We wish to show there exists for each such f a unique Λ-module homomorphism $h : P_k \to \mathrm{Hom}(\Lambda, X)$. More specifically, we will show the following universal property: in the following mapping problem



there always exists a unique h so that the diagram commutes, i.e. $\pi h = f$.

Suppose such a h exists, sending elements $z \in P_k$ to homomorphisms $h_z : \Lambda \to X$. As it is a Λ-module homomorphism, it must satisfy

$$g \cdot h_z = h_{g \cdot z}$$

for all $z \in P_k$. These are elements of $\mathrm{Hom}(\Lambda, X)$, i.e. homomorphisms from Λ to X, so we can evaluate both sides at 1:

$$(g \cdot h_z)(1) = g \cdot h_z(g^{-1}) = h_z(g^{-1}),$$

and

$$h_{g \cdot z}(1) = \pi(h_{g \cdot z}) = f(g \cdot z).$$

Hence, by replacing g with g^{-1}, we have

$$h_z(g) = f(g^{-1} \cdot z).$$

Thus, such a h is uniquely defined on all of P_k. Its existence follows by the above construction, since the maps constructed as above extend to all of Λ by linearity. Thus, we have shown

$$\mathrm{Hom}_G(P_k, \mathrm{Hom}(\Lambda, X)) \cong \mathrm{Hom}(P_k, X).$$

The projective G-module P_k is free, and hence projective, over $\mathbb{Z}$. Thus, the resolution can be treated as an exact sequence of projective $\mathbb{Z}$-modules, and so by Propositions 21 and 23, applying $\mathrm{Hom}(\_, X)$ to the projective resolution preserves exactness. Hence, for $k \geq 1$,

$$H^k(G, \mathrm{Hom}(\Lambda, X)) = 0.$$

So far we have aimed to show that a cohomological extension fulfilling the three properties exists. To show uniqueness, that any two such extensions are isomorphic, we use a technique called dimension shifting, based on induction.

In dimension 0, we have $H^0(G, A) \cong A^G$, hence uniqueness in dimension 0 is obvious. Inductively assume that we have proven uniqueness up to dimensions $k - 1$. We will prove uniqueness of $H^k(G, A)$ by showing it is isomorphic to some $(k-1)$-dimensional cohomology group $H^{k-1}(G, \bar{A})$, which is unique by the inductive hypothesis.

Consider $\bar{A}$ defined by the short exact sequence

$$0 \longrightarrow A \longrightarrow \mathrm{Hom}(\Lambda, A_0) \longrightarrow \bar{A} \longrightarrow 0,$$

where A_0 is the underlying $\mathbb{Z}$-module structure of A. By the second property, we derive the following long exact sequence:

$$\ldots \xrightarrow{\delta^{k-2}} H^k(G, A) \longrightarrow H^{k-1}(G, \mathrm{Hom}(\Lambda, A_0)) \longrightarrow H^{k-1}(G, \bar{A}) \xrightarrow{\delta^{k-1}}$$

$$\xrightarrow{\delta^{k-1}} H^k(G, A) \longrightarrow H^k(G, \mathrm{Hom}(\Lambda, A_0)) \longrightarrow H^k(G, \bar{A}) \xrightarrow{\delta^k} \ldots$$

Now, using the third property, that the cohomology extension disappears on coinduced modules, we have $H^k(G, \mathrm{Hom}(\Lambda, A_0)) = H^{k-1}(G, \mathrm{Hom}(\Lambda, A_0)) = 0$. We are thus left with the following short exact sequence:

$$0 \longrightarrow H^{k-1}(G, \bar{A}) \xrightarrow{\delta^{k-1}} H^k(G, A) \longrightarrow 0.$$

Hence, $H^k(G, A) \cong H^{k-1}(G, \bar{A})$. Note that the third property applies to dimensions 1 and above, hence δ^0 is merely an epimorphism. However, this is sufficient, as $H^1(G, A)$ will be uniquely defined by the cokernel of δ^0.

Therefore, by induction, the cohomology extension is unique.

Now let us complete the calculations for the first property that we had left for later. When we defined the standard resolution we introduced the notion of bar notation, and the bar resolution. Similar notation can be introduced for the cochain complex. Consider the cochain complex

$$\cdots \leftarrow \mathrm{Hom}_G(\bar{P}_k, A) \leftarrow \mathrm{Hom}_G(\bar{P}_{k-1}, A) \leftarrow \ldots \leftarrow \mathrm{Hom}_G(\bar{P}_0, A) \leftarrow A^G.$$

As $B_k = G \times \cdots \times G$ ($(k+1)$ copies of G) is a basis for $\bar{P}_k$, we may identify a cochain in $\mathrm{Hom}_\Lambda(\bar{P}_k, A)$ with a function

$$f : B_k \longrightarrow A,$$

which, to properly define a G-homomorphism, must satisfy:

$$g \cdot f(g_0, \ldots, g_k) = f(g \cdot (g_0, \ldots, g_k)) = f(gg_0, \ldots, gg_k)$$

for all $g, g_0, \ldots, g_k \in G$. We call this the equivariance condition. As basis elements with respect to Λ instead of $\mathbb{Z}$ we may take $(k+1)$-tuples with $g_0 = 1$. In fact, we may confine our attention to a basis of k-tuples

$$\tilde{B}_k = \big\{ [g_1|g_2|\ldots|g_k] \;\big|\; g_i \in G,\ 1 \le i \le k \big\},$$

where we denote

$$[g_1|g_2|\ldots|g_k] = (1, g_1, g_1g_2, \ldots, g_1g_2\ldots g_k).$$

A function defined on B_k, i.e. on elements of the form $(g_0, g_1, \ldots, g_k)$, clearly defines a function on $\tilde{B}_k$, the subset of B where $g_0 = 1$. We shall show that the converse is also true, a function on $\tilde{B}$ extends to a function on B_k which satisfies the equivariance condition. Let $\tilde{f} : \tilde{B}_k \to A$. Now, we try to define the desired function $f : B_k \to A$. From the G-action on B we have

$$g \cdot (g_0, \ldots, g_k) = (gg_0, \ldots, gg_k),$$

where if we set $g = g_0^{-1}$ we have

$$g_0^{-1} \cdot (g_0, \ldots, g_k) = (1, g_0^{-1}g_1, \ldots, g_0^{-1}g_k).$$

The right-hand side is an element in $\tilde{B}_k$:

$$\begin{aligned}(1, g_0^{-1}g_1, \ldots, g_0^{-1}g_k) &= [h_1|h_2|\cdots|h_k] \\ &= (1, h_1, h_1h_2, \ldots, h_1 \ldots h_k).\end{aligned}$$

From here we have a system of k equations:

$$\begin{aligned}g_0^{-1}g_1 &= h_1 \\ g_0^{-1}g_2 &= h_1h_2 \\ \vdots &\quad \vdots \\ g_0^{-1}g_k &= h_1 \ldots h_k.\end{aligned}$$

Substituting each line into the next we have:

$$\begin{aligned}g_0^{-1}g_1 &= h_1 \\ g_0^{-1}g_2 &= g_0^{-1}g_1h_2 \\ \vdots &\quad \vdots \\ g_0^{-1}g_k &= g_0^{-1}g_{k-1}h_k.\end{aligned}$$

Thus,

$$\begin{aligned}h_1 &= g_0^{-1}g_1 \\ h_2 &= g_1^{-1}g_2 \\ \vdots &\quad \vdots \\ h_k &= g_{k-1}^{-1}g_k,\end{aligned}$$

and so we have

$$(g_0, \ldots, g_k) = g_0 \cdot [g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k].$$

Thus, we define $f : B_k \to A$ point-wise as

$$f(g_0, \ldots, g_k) := g_0 \cdot \tilde{f}[g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k].$$

Note in passing that we only have a G-action defined on A, not on B_k or $\tilde{B}_k$. We can see now that such a mapping holds the equivariance condition:

$$\begin{aligned} g \cdot f(g_0, \ldots, g_k) &= g \cdot \left(g_0 \cdot \tilde{f}[g_0^{-1}g_1|g_1^{-1}g_2|\cdots|g_{k-1}^{-1}g_k]\right) \\ &= (gg_0) \cdot \tilde{f}[g_0^{-1}g^{-1}gg_1|g_1^{-1}g^{-1}gg_2|\cdots|g_{k-1}^{-1}g^{-1}gg_k] \\ &= (gg_0) \cdot \tilde{f}[(gg_0)^{-1}(gg_1)|(gg_1)^{-1}(gg_2)|\cdots|(gg_{k-1})^{-1}(gg_k)] \\ &= f(gg_0, gg_1, \ldots, gg_k) \end{aligned}$$

Thus we have shown that cochains in $\mathrm{Hom}_\Lambda(\bar{P}_k, A)$ correspond to functions mapping k-tuples $(g_1, \ldots, g_k)$ to A. Now let us consider how the boundary homomorphism d^* acts on such functions, using the boundary formula for the bar resolution.

$$\begin{aligned} d_* f[g_1|\ldots|g_{k+1}] &= fd[g_1|\ldots|g_k] \\ &= g_1 \cdot f[g_2|\ldots|g_{k+1}] \\ &\quad + \sum_{j=1}^{k} (-1)^j f[g_1|\ldots|g_jg_{j+1}|\ldots|g_{k+1}] \\ &\quad + (-1)^{k+1} f[g_1|\ldots|g_k] \\ &= g_1 \cdot f[g_2|\ldots|g_{k+1})] - f[g_1g_2|g_3|\ldots|g_{k+1}] \\ &\quad + f[g_1|g_2g_3|\ldots|g_{k+1}] - \ldots \\ &\quad + (-1)^j f[g_1|\ldots|g_jg_{j+1}|\ldots|g_{k+1}] + \ldots \\ &\quad + (-1)^{k+1} f[g_1|\ldots|g_k]. \end{aligned}$$

In dimension 0 this has the form

$$d^1 f[g_1] = g_1 \cdot f[\,] - f[g_1]$$

for all $g_1 \in G$, where f is a trivial constant function, meaning it corresponds to an element of A. Thus, the kernel of d^1 corresponds to the elements of A which are fixed by all elements of G, i.e. A^G. As $\operatorname{im} d^0 = 0$, we have

$$H^0(G, A) = \frac{\ker d^1}{\operatorname{im} d^0} \cong A^G,$$

satisfying property 1. □

We used the standard resolution to prove the existence of the cohomological extension in question, however, it is not practical to use for calculations. Instead, we try to find the best option for whatever group is being studied. Often, these are related to topological spaces.

Let us use the resolutions we calculated in Example 1 and calculate the cohomology groups.

Example 5 *The cohomology groups for cyclic groups.*

As with Example 1, we denote by C_r^T our cyclic group G of order $2 \leq r \leq \infty$, with generator T, and we will divide our example into the infinite and finite cases.

Case 1: $r = \infty$. We will use the free resolution we constructed in Example 1:

$$0 \longrightarrow \mathbb{Z}C_\infty^S \longrightarrow \mathbb{Z}C_\infty^T \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

For an arbitrary G-module A, we have the related sequence

$$0 \xleftarrow{d^2} \mathrm{Hom}_G(\mathbb{Z}C_\infty^S, A) \xleftarrow{d^1} \mathrm{Hom}_G(\mathbb{Z}C_\infty^T, A) \longleftarrow 0.$$

The kernel $\ker d^1$ is the set of cochains that satisfy $d^1 f(S) = 0$. However,

$$d^1 f_a(S) = f_a d_1(S) = f_a(T-1) = (T-1) \cdot a = T \cdot a - a.$$

Thus, $T \cdot a = a$, and so $a \in A^G$. Therefore, $H^0(G, A) = A^G$, as expected.

By identifying a with $g_a : 1 \mapsto a$, we see that $\mathrm{Hom}_G(\mathbb{Z}C_\infty^T, A) = \mathrm{Hom}_G(\mathbb{Z}C_\infty^S, A) = A$. Hence, $\ker d^2 = A$ and $\mathrm{im}\, d^1 = (T-1)A$, so $H^1(G, A) = A/(T-1)A$. For $k \geq 2$, $H^2(G, A) = 0$. Thus, the cohomology groups are:

$$H^k(C_\infty^T$$

Now, we simply compute the cohomology. Analogue to the infinite case, $H^0(G,A) = \ker d^1 = \ker(T-1)$ is the set of cochains f_a that satisfy $(T-1)\cdot a = 0$, or $T \cdot a = a$, hence $H^0(G,A) = A^G$. Using this, we also have

$$H^{2k}(G,A) = \frac{\ker d^{2k+1}}{\operatorname{im} d^{2k}} = \frac{\ker T - 1}{\operatorname{im} N} = \frac{A^G}{NA}.$$

Finally, we compute

$$H^{2k-1}(G,A) = \frac{\ker d^{2k}}{\operatorname{im} d^{2k-1}} = \frac{\ker N}{(T-1)A}.$$

Thus, the cohomology groups are:

$$H_k(C_r^T, A) = \begin{cases} A^G, & k = 0, \\ \frac{A^G}{NA}, & 2 \mid k, \\ \frac{\ker N}{(T-1)A}, & 2 \nmid k. \end{cases}$$

4.4 The Homology of Groups with Coefficients

A similar process as with the cohomology can be applied to define the homology groups of a group with coefficients. This time, instead of considering invariants, we use coinvariants, instead of coinduced modules we use induced modules, and instead of the Hom functor $\operatorname{Hom}_G(\_, A)$ we use the Tensor functor $\_ \otimes_\Lambda A$.

In the Lemma 3, the coinvariants functor $(\_)_G$ was shown to be right exact, but not an exact functor. Specifically, ϕ_G was not proven to be a monomorphism like ϕ. In general, this need not be true. This is the motive for defining $H_1(G,A)$, the first cohomology group of G with coefficients in A, as a measure of the failure of the left exactness of the coinvariants functor.

Definition 8 *The homology groups of a group G with coefficients in A, denoted $H_k(G,A)$, $k \geq 0$, form a covariant family of functors from $\mathcal{U}_G$ to abelian groups, which have the following properties:*

1. $H_0(G,A) = A_G$
2. *For each short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{U}_G$ there exists a natural transformation $\delta = \delta_k : H_k(G,C) \to H_{k-1}(G,A)$ and a long exact sequence of cohomology groups*

$$\cdots \longrightarrow H_k(G,A) \xrightarrow{\phi_*} H_k(G,B) \xrightarrow{\psi_*} H_k(G,C) \xrightarrow{\delta} H_{k-1}(G,A) \longrightarrow \ldots$$

3. *If A is an induced module, then $H_k(G,A) = 0$ for all $k \geq 1$.*

The family $\{H_k(G,\cdot),\, k \geq 0\}$ can thus be viewed as a homological extension of the coinvariants functor, which vanishes on coinduced modules.

Theorem 25 *The homological extension $H_k(G,*)$, $k \geq 0$ exists and is unique.*

Proof: This proof is largely analogue to the proof of Theorem 24. Let

$$\cdots \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

be a projective resolution of the trivial G-module $\mathbb{Z}$. For any G-module A, we form the related chain complex

$$\cdots \to P_k \otimes_\Lambda A \longrightarrow P_{k-1} \otimes_\Lambda A \longrightarrow \ldots \longrightarrow P_0 \otimes_\Lambda A \longrightarrow A_G \longrightarrow 0.$$

where we replaced $\mathbb{Z} \otimes_\Lambda A$ with A_G, by equation (2). Note that we are using the right structure on P_k, so $x \cdot g = g^{-1} \cdot x$ for all $g \in G$ and $x \in P_k$. The composition of two successive homomorphisms in the chain complex is zero, thus, we may define

$$H_k(G,A) = H_k(P_k \otimes_\Lambda A).$$

The functor $\_ \otimes_\Lambda A$ is additive, and thus preserves chain homotopies. So, by the same argument as for the integral homology, the homology groups are independent of the choice of projective resolution.

The existence of the natural boundary homomorphisms δ_k and the long exact sequence from the second point of the definition follow by the usual diagram chase. The first property is satisfied by making the convention that 0-dimensional boundaries are trivial. Consider the tail of the chain complex

$$\cdots \to P_1 \otimes_\Lambda A \xrightarrow{d_1} P_0 \otimes_\Lambda A \xrightarrow{d_0} A_G \longrightarrow 0.$$

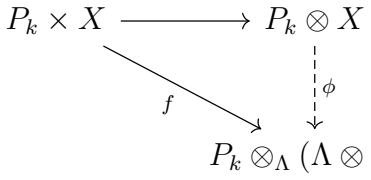
By setting $d_0 = 0$, we have $H_0(G,A) = (P_0 \otimes_\Lambda A)/\operatorname{im} d_1$. We defer the rest of this calculation, to later, where we will use the bar resolution. Let us show the third property, that the homology disappears on induced modules.

Let $A = \Lambda \otimes X$ be an induced module, where X has trivial G-action. We will first show that

$$P_k \otimes_\Lambda (\Lambda \otimes X) \cong P_k \otimes X.$$

Let us define the map $i : X \to \Lambda \otimes X$ with $i(x) = 1 \otimes x =$ for all $x \in X$. This map is clearly an injection.

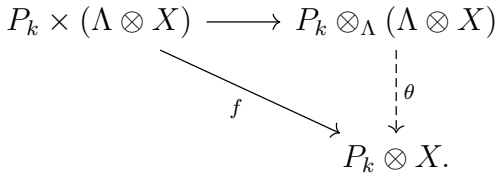
Let us use the universal property of the tensor product $P_k \otimes_\Lambda (\Lambda \otimes X)$ in the following diagram:



By the universal property of the tensor product, if f is a bilinear map, then there exists a map ϕ making the diagram commute.

Let us define f by $(z, x) \mapsto z \otimes_\Lambda (1 \otimes x)$, for all $z \in P_k$, $x \in X$. This map is clearly bilinear, thus by the universal property, the map $\phi : z \otimes x \mapsto z \otimes_\Lambda (1 \otimes x)$ is well-defined on all of $P_k \otimes X$.

Conversely, let us use the universal property of the tensor product $P_k \otimes_\Lambda (\Lambda \otimes X)$ in the following diagram:



By the universal property of the tensor product, if f is a bilinear map, this time with respect to the ring Λ, then there exists a map θ making the diagram commute.

Let us define f by $(z, (\lambda \otimes x)) \mapsto z \cdot \lambda \otimes x$, for all $z \in P_k$, $\lambda \in \Lambda$, $x \in X$. Now, let us show f is bilinear. Let $z \times (\lambda \otimes x) \in P_k$, and $\mu \in \Lambda$ arbitrary. Then, noting that we are treating P_k as a right Λ-module, we have

$$f(z \cdot \mu, \lambda \otimes x) = (z \cdot \mu) \cdot \lambda \otimes x = z \cdot \mu\lambda \otimes x$$

and

$$f(z, \mu \cdot (\lambda \otimes x)) = f(z, \mu\lambda \otimes x) = z \cdot \mu\lambda \otimes x,$$

i.e. $f(z \cdot \mu, \lambda \otimes x) = f(z, \mu \cdot (\lambda \otimes x))$.

Thus, this map is bilinear, so by the universal property, the map $\phi : z \otimes_\Lambda (\lambda \otimes x) \mapsto z \cdot \lambda \otimes x$ is well-defined on all of $P_k \otimes_\Lambda (\Lambda \otimes X)$.

Finally, the maps ϕ and θ are inverses. Indeed:

$$\theta \circ \phi(z \otimes x) = \theta(z \otimes_\Lambda (1 \otimes x)) = z \otimes x$$

and

$$\phi \circ \theta(z \otimes_\Lambda (\lambda \otimes x)) = \phi(z \cdot \lambda \otimes x) = z \cdot \lambda \otimes_\Lambda (1 \otimes x) = z \otimes_\Lambda \lambda \cdot (1 \otimes x) = z \otimes_\Lambda (\lambda \otimes x).$$

Thus, $P_k \otimes_\Lambda (\Lambda \otimes X)$ and $P_k \otimes X$ are isomorphic.

The projective G-module P_k is free, and hence projective, over $\mathbb{Z}$. Thus, by Propositions 22 and 23, applying $\_ \otimes X$ to the projective resolution preserves exactness. Hence, for $k \geq 1$,

$$H_k(G, \Lambda \otimes X) = 0.$$

So far we have aimed to show that a homological extension fulfilling the three properties exists. To show uniqueness, that any two such extensions are isomorphic, we will again use dimension shifting, as in the case for the cohomological extension.

In dimension 0, we have $H_0(G, A) \cong A_G$, hence uniqueness in dimension 0 is obvious. Inductively assume that we have proven uniqueness up to dimensions $k-1$. We will prove uniqueness of $H_k(G, A)$ by showing it is isomorphic to some $(k-1)$-dimensional homology group $H_{k-1}(G, \bar{A})$, which is unique by the inductive hypothesis.

Consider $\bar{A}$ defined by the short exact sequence

$$0 \longrightarrow \bar{A} \longrightarrow \Lambda \otimes A_0 \longrightarrow A \longrightarrow 0,$$

where A_0 is the underlying $\mathbb{Z}$-module structure of A. By the second property, we derive the following long exact sequence:

$$\ldots \xrightarrow{\delta_k} H_k(G, \bar{A}) \longrightarrow H_k(G, \Lambda \otimes A_0) \longrightarrow H_k(G, A) \xrightarrow{\delta_{k-1}}$$

$$\xrightarrow{\delta_{k-1}} H_{k-1}(G, \bar{A}) \longrightarrow H_{k-1}(G, \Lambda \otimes A_0) \longrightarrow H_{k-1}(G, A) \xrightarrow{\delta_{k-2}} \ldots$$

Now, using the third property, that the homology extension disappears on induced modules, we have $H_k(G, \Lambda \otimes A_0) = H_{k-1}(G, \Lambda \otimes A_0) = 0$. We are thus left with the following short exact sequence:

$$0 \longrightarrow H_k(G, A) \xrightarrow{\delta_{k-1}} H_{k-1}(G, \bar{A}) \longrightarrow 0.$$

Hence, $H_k(G, A) \cong H_{k-1}(G, \bar{A})$. Note that the third property applies to dimensions 1 and above, hence δ_0 is merely an monomorphism. However, this is sufficient, as $H_1(G, A)$ will be uniquely defined by the kernel of δ_0.

Therefore, by induction, the homology extension is unique.

Now let us complete the calculations that we had left for later. When we defined the standard resolution we introduced the notion of bar notation, and the bar resolution. Similar notation can be introduced for the chain complex. Consider the chain complex

$$\cdots \to \bar{P}_k \otimes A \longrightarrow \bar{P}_{k-1} \otimes A \longrightarrow \ldots \longrightarrow \bar{P}_0 \otimes A \longrightarrow A_G.$$

Consider an element $x \in \bar{P}_{k-1} \otimes A$. It may be uniquely represented as a sum of elements of the form $[g_1|\ldots|g_{k-1}] \otimes a$. Let us denote $\tilde{B}_{k-1} = \{[g_1|\ldots|g_k - 1] : g_i \in G,\ 1 \leq i \leq k-1\}$, like we did for cohomology groups. $\tilde{B}_{k-1}$ is a basis for $\bar{P}_k$. we may identify a chain $x \in \bar{P}_k \otimes A$ with a function $f_x : B_k \longrightarrow A$ which

vanishes almost everywhere, i.e. it is non-zero for only a finite number of values. Formally, let us note that x can be uniquely represented as a linear combination of elements of the form $b \otimes a$, where $b \in \tilde{B}_{k-1}$ and $a \in A$. We define $f_{b\otimes a}$ on an element $[g_1|\dots|g_{k-1}] \in \tilde{B}_{k-1}$ as

$$f_{b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} a, & [g_1|\dots|g_{k-1}] = b, \\ 0, & \text{otherwise.} \end{cases}$$

and extend this linearly to f_x for all $x \in \bar{P}_{k-1} \otimes A$. Indeed,

$$\begin{aligned} &f_{b_1\otimes a_1 + b_2 \otimes a_2}[g_1|\dots|g_{k-1}] \\ &\quad = f_{b_1\otimes a_1}[g_1|\dots|g_{k-1}] + f_{b_2\otimes a_2}[g_1|\dots|g_{k-1}] = \begin{cases} a_1, & [g_1|\dots|g_{k-1}] = b_1, \\ a_2, & [g_1|\dots|g_{k-1}] = b_2, \\ 0, & \text{otherwise,} \end{cases} \end{aligned}$$

and

$$f_{g\cdot b\otimes a}[g_1|\dots|g_{k-1}] = g \cdot f_{b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} g\cdot a, & [g_1|\dots|g_{k-1}] = b, \\ 0, & \text{otherwise.} \end{cases}$$

Thus, as x has a unique such representation, the mapping $x \mapsto f_x$ is well defined. We construct the inverse map $f \mapsto x_f$ as

$$x_f = \sum_{b \in \tilde{B}_{k-1}} f(b).$$

This is well defined as f vanishes almost everywhere. Hence, we have a correspondence between P_{k-1} and functions $\tilde{B}_{k-1} \to A$ which vanish almost everywhere.

Now let us find the form of the boundary homomorphism d_* in this notation. First, as in the definition of the standard resolution, we have

$$d_* x = dx = \sum_{j=0}^{k} (-1)^j \hat{r}_j x,$$

where we denote by $\hat{r}_j$ the operator of removing the j-th coordinate i.e.

$$\hat{r}_j : (h_0, \dots, h_k) \mapsto (h_0, \dots, \hat{h}_j, \dots, h_k),$$

for any $(h_0, \dots, h_k) \in \bar{P}_k$. Now, for arbitrary $b \in \tilde{B}_{k-1}$ and $a \in A$, we have

$$f_{\hat{r}_j b\otimes a}[g_1|\dots|g_{k-1}] = \begin{cases} a, & [g_1|\dots|g_k] = \hat{r}_j b; \\ 0, & \text{otherwise.} \end{cases}$$

If $[g_1|\dots|g_k] = (h_0,\dots,h_{k-1})$, then $(h_0,\dots,h_{k-1}) = \hat{r}_j b$ is equivalent to

$$(h_0,\dots,h_{j-1},g,h_j,\dots,h_{k-1}) = b,$$

where $g \in G$ is the j-th coordinate of b. Of course, if g isn't the j-th coordinate of b, then the value of $f_{b\otimes a}$ on this is 0. Thus, we can simply denote

$$f_{\hat{r}_j b\otimes a}[g_1|\dots|g_{k-1}] = \sum_{g\in G} f_{b\otimes a}(h_0,\dots,h_{j-1},g,h_j,\dots,h_{k-1}).$$

This extends linearly to any arbitrary $x \in \bar{P}_k$, and thus from $d_* x = dx$ implying $d_* f_x = f_{dx}$ we get

$$\begin{aligned} d_* f_x[g_1|\dots|g_{k-1}] &= f_{dx}(1,h_1,\dots,h_{k-1}) \\ &= \sum_{j=0}^{k}(-1)^j f_{\hat{r}_j x}(h_0,h_1,\dots,h_{k-1}) \\ &= \sum_{j=0}^{k}\sum_{g\in G}(-1)^j f_x(h_0,h_1,\dots,h_{j-1},g,h_j,\dots,h_{k-1}), \end{aligned}$$

where each $h_i = g_1\dots g_i$ and taking $1 = h_0$. Now, let us calculate each summand.

For $j = 0$:

$$\begin{aligned} f_x(g,h_1,h_2,\dots,h_{k-1}) &= f_x(g,g_1,g_1g_2,\dots,g_1\dots g_{k-1}) \\ &= g^{-1}\cdot f_x(g,g1,g_2,\dots,g_2\dots g_{k-1}) \\ &= g^{-1}\cdot f_x[g_1|\dots|g_{k-1}]. \end{aligned}$$

For $1 \le j \le k-1$:

$$\begin{aligned} &\sum_{g\in G} f_x(1,h_1,\dots,g,\dots,h_{k-1}) \\ =\ &\sum_{g\in G} f_x(1,g_1,\dots,g_1\dots g_{j-1},g,g_1\dots g_j,\dots,g_1\dots g_{k-1}) \\ =\ &\sum_{g\in G} f_x(1,g_1,\dots,g_1\dots g_{j-1},g_1\dots g_j g,g_1\dots g_j,\dots,g_1\dots g_{k-1}) \\ =\ &\sum_{g\in G} f_x[g_1|\dots|g_{j-1}|g_j g|g^{-1}|g_{j+1}|\dots|g_{k-1}]. \end{aligned}$$

7.3 1 q Tf 5 51.9552 Tf 6.725 1.794 Td (

5 Low-dimensional interpretation

5.1 Crossed Homomorphisms

Definition 9 *A map $f : G \to A$ which satisfies the condition $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$ for all $g_1, g_2 \in G$ is called a crossed homomorphism. A map $f_a : G \to A$ which satisfies the condition $f_a(g) = g \cdot a - a$ for all $g \in G$ is called a principal crossed homomorphism.*

When the G-action on A is trivial, a crossed homomorphism is a homomorphism in the usual sense, and the only principal crossed homomorphism is the constant 0-map.

It is simple to show that principal crossed homomorphisms are in fact crossed homomorphisms. For any two $g_1, g_2 \in G$, we have

$$\begin{aligned} f_a(g_1g_2) &= (g_1g_2) \cdot a - a \\ &= g_1 \cdot (g_2 \cdot a) + g_1 \cdot a - g_1 \cdot a - a \\ &= g_1 \cdot (g_2 \cdot a - a) + (g_1 \cdot a - a) \\ &= g_1 \cdot f_a(g_2) + f_a(g_1) \end{aligned}$$

We see that the coboundaries in dimension 1 are exactly the principal crossed homomorphisms. Let f be a crossed homomorphism. The equation $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$ is the result of the coboundary formula for $d^k f$, for $k = 1$. From the formula for $d^k f$

$$\begin{aligned} d^k f(g_1, \cdots, g_{k+1}) &= g_1 \cdot f(g_2, \cdots, g_{k+1})) - f(g_1g_2, g_3, \ldots, g_{k+1}) \\ &\quad + f(g_1, g_2g_3, \ldots, g_{k+1}) - \ldots \\ &\quad + (-1)^{-1} f(g_1, \ldots, g_jg_{j+1}, \ldots, g_{k+1}) + \ldots \\ &\quad + (-1)^{k+1} f(g_1, \ldots, g_k), \end{aligned}$$

we get

$$d^1 f(g_1, g_2) = g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1).$$

and since for 1-cocycles $d^1 f = 0$, we have $f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1)$. In other words, the set of crossed homomorphisms is exactly the set of 1-cocycles.

Hence, the first group cohomology $H^1(G, A)$ is isomorphic to the abelian group of crossed homomorphisms modulo principal crossed homomorphisms.

5.2 Group Extensions

We have a similar discussion for the second cohomology group. Applying the coboundary formula on $d^k f$ for $k = 2$ we have

$$d^2 f(g_1, g_2) = g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2).$$

For a 2-cocycle, $d^2 f = 0$, so we give the following definition:

Definition 10 *A map $f : G \times G \to A$ which satisfies the condition*

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

is called a factor system.

The reason such a map is called a factor system is because such a map determines the composition law for a specific extension E of the abelian group A by G, where the G-structure on A corresponds to the conjugation G-action on A. Such an extension E is defined by the following short exact sequence:

$$0 \longrightarrow A \xrightarrow{\iota} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 0.$$

We view $A = \iota(A)$ as a subset of E, and, in fact, a normal subgroup, as $A = \ker \pi$. We have a transversal $s : G \to A \in E$, a right inverse to π determined by a choice of $s(g)$. It is a set function, not necessarily a homomorphism, however, it satisfies the property

$$s(g_1)s(g_2) = f(g_1, g_2)s(g_1 g_2).$$

for all $g_1, g_2 \in G$.

We formalise this in the following proposition:

Proposition 26 *Given an extension E and transversal s as above, the following hold:*

(i) The factor system f determines the composition law in E.

(ii) The cocycle identity above is equivalent to associativity in E.

(iii) Choice of a new transversal $s' : G \to E$ changes f by a coboundary.

Proof: G acts on A by conjugation, i.e.

$$g \cdot a = gag^{-1}.$$

We view A as a subset of E, but not G, which we circumvent by utilising s:

$$g \cdot a = s(g)as(g)^{-1}$$

We use this formula throughout the rest of the proof.

As s is a right inverse to π, we have

$$\pi(s(gh)) = gh$$

and

$$\pi(s(g)s(h)) = \pi(s(g))\pi(s(h)) = gh,$$

hence $\pi(s(g)s(h)s(gh)^{-1}) = 1$. Thus, $s(g)s(h)s(gh)^{-1} \in \ker\pi = \operatorname{im}\iota = A$ by exactness. As such, even though s need not be a homomorphism, and so $s(g)s(h)s(gh)^{-1}$ isn't necessarily 1, it is however an element of A. Hence, we may form a function $f : G \times G \to A$ with $f(g,h) := s(g)s(h)s(gh)^{-1}$.

Applying associativity in E:

$$\begin{array}{rclcl} (s(g)s(h))s(k) & = & f(g,h)s(gh)s(k) & = & f(g,h)f(gh,k)s(ghk), \\ s(g)(s(h)s(k)) & = & s(g)f(h,k)s(hk) & = & s(g)f(h,k)s(g)^{-1}s(g)s(hk) \\ & & & = & g \cdot f(h,k)f(g,hk)s(ghk) \end{array}$$

and then, cancelling out the $s(ghk)$ term on both sides, we have

$$g \cdot f(h,k)f(g,hk) = f(g,h)f(gh,k).$$

However, as all these terms lie in A, which is abelian, we may use additive notation:

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

Thus,

$$g \cdot f(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0$$

which means f is a factor system, thus proving (ii).

Let us now returning to (i). We shall fix an element $x \in E$, and consider the following:

$$\pi(xs(\pi(x))^{-1}) = \pi(x)\big(\pi(s(\pi(x)))\big)^{-1} = \pi(x)\pi(x)^{-1} = 1_G.$$

Thus, $xs(\pi(x))^{-1} \in \ker\pi = A$, and so $x = a_x s(\pi(x))$ for some $a_x \in A$.

Given two elements, $x, y \in E$, we have

$$\begin{array}{rcl} xy & = & a_x s(\pi(x))a_y s(\pi(y)) \\ & = & a_x s(\pi(x))a_y s(\pi(x))^{-1}s(\pi(x))s(\pi(y)) \\ & = & a_x \pi(x) \cdot a_y f(\pi(x),\pi(y))s(\pi(x)\pi(y)). \end{array}$$

On the other hand, $xy = a_{xy}s(\pi(xy)) = a_{xy}s(\pi(x)\pi(y))$, and so

$$a_{xy} = a_x \pi(x) \cdot a_y f(\pi(x),\pi(y)).$$

This shows (i).

Let $s' : G \to E$ be another choice of transversal. We will show that the related factor system f' differs from f by a cocycle.

First, note that $\pi(s'(g)) = g = \pi(s(g))$, hence

$$\pi(s'(g)(s(g))^{-1}) = \pi(s'(g))(\pi(s(g)))^{-1} = 1_G$$

and so $s'(g)(s(g))^{-1} \in \ker \pi = A$. Define $F : G \to A$ to be this value, $F(g) = s'(g)(s(g))^{-1}$, i.e. $s'(g) = F(g)s(g)$.

Now, we apply this to

$$\begin{aligned}
s'(g)s'(h) &= f'(g,h)s'(gh) \\
F(g)s(g)F(h)s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)s(g)F(h)s(g)(s(g))^{-1}s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)s(g)s(h) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)f(g,h)s(gh) &= f'(g,h)F(gh)s(gh) \\
F(g)g \cdot F(h)f(g,h) &= f'(g,h)F(gh).
\end{aligned}$$

As we now work in A where the operation is commutative, we may switch to additive notation

$$\begin{aligned}
F(g) + g \cdot F(h) + f(g,h) &= f'(g,h) + F(gh) \\
f'(g,h) - f(g,h) &= g \cdot F(h) - F(gh) + F(g) \\
f'(g,h) - f(g,h) &= d^1F(g,h).
\end{aligned}$$

Hence, $f' - f = d^1F$, and so we have shown (iii). □

This proposition outlines the correspondence between the second cohomology group $H^2(G, A)$ and the family of extensions

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

for a given G-action on A. In other words, given a pair (G, A), where A is abelian as a normal subgroup, the extension groups are determined up to isomorphism by the module structure in A, i.e. the G action in A, and the second cohomology class.

Since for all $x \in E$ we have $x = a_x s(\pi(x))$ for some $a_x \in A$, we have a correspondence between the sets E and $A \times G$. Viewing E as such, the composition law $xy = a_x\pi(x) \cdot a_y f(\pi(x), \pi(y))s(\pi(x)\pi(y))$ becomes

$$(a, g)(b, h) = (a + g \cdot b + f(g, h), gh), \tag{3}$$

where f corresponds to an element of the second cohomology class. If the G-action is trivial, and the factor system f corresponds to the trivial cohomology class, meaning without loss of generality we may take f to be 0 everywhere, then the composition law becomes

$$(a, g)(b, h) = (a + b, gh).$$

Hence, we have the following result:

Lemma 27 *Let A be abelian with trivial G-action. The extension whose factor system corresponds to the trivial cohomology class is isomorphic to $A \times G$.*

If, in the formula 3, we consider the case where f corresponds to the trivial cohomology class, but allow the G-action on A to be non-trivial, we get

$$(a, g)(b, h) = (a + g \cdot b, gh).$$

This corresponds to the operation on the outer semidirect product $A \rtimes_\varphi G$, where $\varphi : G \to \operatorname{Aut} A$ denotes the G-action on A.

Lemma 28 *Let A be an abelian group with a G-action determined by $\varphi : G \to \operatorname{Aut} A$. Consider the extension*

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

If the factor system of this extension corresponds to the trivial cohomology class, then the extension splits and E is isomorphic to $A \rtimes_\varphi G$, where composition is determined by the G-action on A with

$$(a, g)(b, h) = (a + g \cdot b, gh).$$

for all $a, b \in A$ and $g, h \in G$.

Proof: Let us consider such an extension E with a trivial factor system f. Let $E = A \times G$ as a set, with composition determined as above. Now, A is isomorphic to its image $\operatorname{im} \iota = \ker \pi$ which is normal in E. These are the elements of the form $(a, 1)$, for all $a \in A$. Similarly, we take the transversal $s : G \to E$ to be $s : g \mapsto (0, g)$ for all $g \in G$. Now, for all $g, h \in G$ we have

$$(0, g)(0, h) = (f(g, h), gh) = (0, gh)$$

as f corresponds to the trivial cohomology class and as such may be taken without loss of generality to be trivial. This means s is in fact a group homomorphism, inverse to π, hence the short exact sequence splits by Lemma 13. Thus G is isomorphic to the subgroup $\operatorname{im} s$ in E, the subgroup of all the elements of the form $(0, g)$. The subgroups $\operatorname{im} \iota$ and $\operatorname{im} s$ clearly have trivial intersection. For an arbitrary element $(a, g) \in E$, we have

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

i.e. $E = \operatorname{im} \iota \operatorname{im} s$. Therefore, we have $E = \operatorname{im} \iota \rtimes \operatorname{im} s \cong A \rtimes_\varphi G$.

5.3 Abelianisation

Lemma 29 *Let $\mathbb{Z}$ have the trivial G-module structure and $[G,G]$ denote the commutator subgroup of G. Then,*

$$H_1(G,\mathbb{Z}) \cong G/[G,G].$$

Proof: By Lemma 7, we have $A_G = A/IA$, where I is the augmentation ideal. Of course, as $H_0(G,A) = A_G$, this means $H_0(G,A) = A/IA$. The augmentation ideal can be defined by the short exact sequence

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

By applying the second property of group homology, on short exact sequences, we have the long exact sequence

$$\ldots \longrightarrow H_1(G,I) \longrightarrow H_1(G,\Lambda) \longrightarrow H_1(G,\mathbb{Z}) \longrightarrow$$

$$\longrightarrow H_0(G,I) \longrightarrow H_0(G,\Lambda) \longrightarrow H_0(G,\mathbb{Z}) \longrightarrow 0.$$

Now, as Λ is obviously a projective Λ-module, it has trivial resolution, so $H_1(G,\Lambda) = H_0(G,\Lambda) = 0$. By substituting I for A in the statement at the start of the proof, we have $H_0(G,I) = I/I^2$. Thus, the long exact sequence leads to the following short exact sequence:

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

Thus, $H_1(G,\mathbb{Z}) \cong I/I^2$. Now, we wish to show $I/I^2 \cong G/[G,G]$, after which we are done.

Let us consider the map $\phi : G \to I/I^2$ defined by $g \mapsto [g-1]$. Two elements of I are in the same class in I/I^2 if they differ by an element of I^2. Let us denote this relation by $\equiv$. For arbitrary $g,h \in G$ we calculate the following:

$$\begin{aligned}
\phi(gh) &\equiv gh-1 \\
&\equiv gh-1-(g-1)(h-1) \\
&\equiv g-1+h-1 \\
&\equiv \phi(g)+\phi(h) \\
&\equiv \phi(h)+\phi(g) \\
&\equiv \phi(hg).
\end{aligned}$$

Thus, $\phi(ghg^{-1}h^{-1}) \equiv 0$. As $[G,G]$ is the commutator subgroup, it is generated by all elements of the form $ghg^{-1}h^{-1}$, hence $[G,G] \subseteq \ker\phi$. Thus, we may define $\bar{\phi} : G/[G,G] \to I/I^2$ as $[g] \mapsto [g-1]$.

Conversely, let us consider the map $\theta : I \to G/[G,G]$ defined on the generating elements of I as $g-1 \mapsto [g]$ and extending linearly to the rest of I. Indeed, if $\lambda = \sum_i^k m_i g_i \in I$, then $\varepsilon(\lambda) = 0$, i.e. $\sum_i^k m_i = 0$, hence

$$\lambda = \sum_i^k m_i g_i = \sum_i^k m_i g_i - \sum_i^k m_i = \sum_i^k (m_i - 1) g_i.$$

Thus, $\theta(\lambda) = \prod_i^k g_i^{m_i}$. Now, I^2 is generated by the products of two generators of I, i.e. elements of the form $(g-1)(h-1)$ for any two $g, h \in G$. Again, denoting by $\equiv$ the relation of two elements in G that differ by an element of $[G,G]$, we have

$$\begin{aligned}
\theta((g-1)(h-1)) &= \theta(gh - g - h + 1) \\
&= \theta((gh-1) - (g-1) - (h-1)) \\
&\equiv \theta(gh-1)\theta(g-1)^{-1}\theta(h-1)^{-1} \\
&\equiv ghg^{-1}h^{-1} \\
&\equiv 1,
\end{aligned}$$

as $ghg^{-1}h^{-1} \in [G,G]$. Thus, $I^2 \subseteq \ker\theta$, and so we may define the map $\bar{\theta} : I/I^2 \to G/[G,G]$ as $[g-1] \mapsto [g]$. Clearly, this function is the inverse of $\bar{\phi}$ from before, hence both are in fact isomorphisms. Therefore, $I/I^2 \cong G/[G,G]$. $\square$

6 Examples

6.1 Basic examples

In this section we will cover some simple examples of group extensions:

Example 6 *Extensions of* $\mathbb{Z}$ *by* $\mathbb{Z}_2$.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} E \xrightarrow{\pi} C_2^T \longrightarrow 0.$$

For the sake of clarity, we will be treating $\mathbb{Z}_2$ as a cyclic group of order 2 with generator T, sometimes denoted by C_2^T, with the group operation taken to be multiplication so as to keep consistent with the theory set up thus far. Now, let us apply the formula for the cohomology for cyclic groups, which we computed earlier in Example 5:

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}}.$$

The cohomology groups, of course, depend on the module structure of $\mathbb{Z}$ as a $\mathbb{Z}_2$-module, i.e. the $\mathbb{Z}_2$-action on $\mathbb{Z}$. This corresponds to a mapping $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$. As $\mathrm{Aut}(\mathbb{Z})$ has two elements, the trivial automorphism and the automorphism sending 1 to -1, we have two cases to consider.

Consider $T \cdot a = a$. Then, as every element is fixed, we have

$$\mathbb{Z}^{\mathbb{Z}_2} = \mathbb{Z}$$

and

$$N\mathbb{Z} = (1+T)\mathbb{Z} = (1+1)\mathbb{Z} = 2\mathbb{Z},$$

and so

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2.$$

Thus, we have two possibilities for our factor system f which defines E. Recall that if f is a factor system, it satisfies

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

for all $g_1, g_2, g_3 \in \mathbb{Z}_2$. If we set $g_1 = 1$, then

$$\begin{aligned} 0 &= 1 \cdot f(g_2, g_3) - f(1 g_2, g_3) + f(1, g_2 g_3) - f(1, g_2) \\ &= f(1, g_2 g_3) - f(1, g_2), \end{aligned}$$

which means $f(1, T) = f(1, 1) = 0$. If we set $g_1 = T$, then

$$0 = T \cdot f(g_2, g_3) - f(T g_2, g_3) + f(T, g_2 g_3) - f(T, g_2)$$

$$= \quad f(g_2, g_3) - f(Tg_2, g_3) + f(T, g_2g_3) - f(T, g_2).$$

If $g_2 = 1$, then $f(1, g_3) = f(T, 1)$, that is $f(T, 1) = 0$. If $g_3 = T$, then $f(g_2, 1) = f(Tg_2, 1)$, which yields the same result. If $g_2 = T$ and $g_3 = 1$, then $f(T, 1) = f(1, 1)$, which again yields the same result. The value of $f(T, T)$ has no constraints, and thus it will correspond to the element of the second cohomology class.

If $f(T, T) = 0$, we have

$$(a, g)(b, h) = (a + g \cdot b + f(g, h), gh) = (a + b, gh),$$

that is, $E \cong \mathbb{Z} \times \mathbb{Z}_2$. This coincides with the result of Lemma 27.

If $f(T, T) = 1$, we have

$$(a, g)(b, h) = (a + g \cdot b + f(g, h), gh) = (a + b + f(g, h), gh),$$

which, for each combination of $g, h \in \{1, T\}$ yields

$$\begin{aligned}
(a, 1)(b, 1) &= (a + b, 1), \\
(a, T)(b, 1) &= (a + b, T), \\
(a, 1)(b, T) &= (a + b, T), \\
(a, T)(b, T) &= (a + b + 1, 1).
\end{aligned}$$

By mapping $(a, g) \mapsto \begin{cases} 2a, & \text{if } g = 1; \\ 2a + 1, & \text{if } g = T; \end{cases}$ we see that E is isomorphic to $\mathbb{Z}$.

Consider $T \cdot a = -a$. Then, the only fixed element is 0, so

$$\mathbb{Z}^{\mathbb{Z}_2} = \{0\}$$

and

$$N\mathbb{Z} = (1 + T)\mathbb{Z} = (1 - 1)\mathbb{Z} = \{0\},$$

and so

$$H^2(\mathbb{Z}_2, \mathbb{Z}) = \frac{\mathbb{Z}^{\mathbb{Z}_2}}{N\mathbb{Z}} = \frac{\{0\}}{\{0\}} \cong 0.$$

Thus, we only have one extension. In this extension the factor system corresponds to the only element of the cohomology class, the trivial element. This would intuitively lead us to believe that the factor system is then constant at 0. We can see this from the factor system identity:

$$g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0.$$

We have the same result as before for $g_1 = 1$, as 1 acts trivially, so $f(1,T) = f(1,1) = 0$. When $g_1 = T$, we have

$$0 = -f(g_2, g_3) - f(Tg_2, g_3) + f(T, g_2g_3) - f(T, g_2).$$

Setting $g_3 = 1$ yields $f(g_2, 1) + f(Tg_2, 1) = 0$ which for either value of g_2 gives $f(T,1) = -f(1,1) = 0$. For $g_3 = T$ and $g_2 = 1$ we have $f(T,1) = -f(1,T)$, i.e. $0 = 0$. Finally, setting $g_1 = g_2 = g_3 = T$ we have $2f(T,T) = f(T,1) - f(1,T) = 0$, and as the image of f is in $\mathbb{Z}$, we must have $f(T,T) = 0$. Thus, f is a constant mapping to 0.

Our composition law in E is now

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

This shows that E is isomorphic to the infinite dihedral group

$$\mathbb{D}_\infty = \langle r, s \mid s^2 = 1,\ rsr = r^{-1} \rangle,$$

where $r = (1,1)$, and $s = (0,T)$. Indeed, $s^2 = (0,T)(0,T) = (0,1)$ and

$$rsr^{-1} = (1,1)(0,T)(1,1)^{-1} = (1,T)(-1,1) = (0,1).$$

Hence our extensions of $\mathbb{Z}$ by $\mathbb{Z}_2$, up to isomorphism, are $\mathbb{Z} \times \mathbb{Z}_2$, $\mathbb{Z}$, and $\mathbb{D}_\infty$.

Example 7 *Extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_2$, where p is a prime number greater than 2.*

This example is done quite similarly to the previous one. Consider the extension E given by

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_2^T \longrightarrow 0.$$

The action is determined by a mapping $C_2^T \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, so as T must map to an element of order dividing 2, we have either $T \cdot a = a$ or $T \cdot a = -a$.

Let $T \cdot a = a$. Now,

$$\mathbb{Z}_p^{\mathbb{Z}_2} = \mathbb{Z}_p$$

and

$$N\mathbb{Z}_p = (1+T)\mathbb{Z}_p = (1+1)\mathbb{Z}_p = 2\mathbb{Z}_p = \mathbb{Z}_p,$$

hence

$$H^2(\mathbb{Z}_2, \mathbb{Z}_p) = \frac{\mathbb{Z}_p^{\mathbb{Z}_2}}{N\mathbb{Z}_p} = \frac{\mathbb{Z}_p}{\mathbb{Z}_p} \cong 0.$$

Thus, our factor system is trivial and so, by Lemma 27, our extension is $E \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.

Let $T \cdot a = -a$. Now, the only fixed element is 0, so

$$\mathbb{Z}_p^{\mathbb{Z}_2} = \{0\}$$

and

$$N\mathbb{Z}_p = (1+T)\mathbb{Z}_p = (1-1)\mathbb{Z}_p = \{0\},$$

thus

$$H^2(\mathbb{Z}_2, \mathbb{Z}_p) = \frac{\mathbb{Z}_p^{\mathbb{Z}_2}}{N\mathbb{Z}_p} = \frac{\{0\}}{\{0\}} \cong 0.$$

Again, our factor system is trivial, and so our composition law becomes

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

which shows that E is isomorphic to the dihedral group

$$\mathbb{D}_p = \langle r, s \mid r^p = s^2 = 1,\ rsr = r^{-1} \rangle,$$

with $r = (1,1)$ and $s = (0,T)$.

Hence our extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_2$ are $\mathbb{Z}_{2p}$ and $\mathbb{D}_p$.

Example 8 *Extensions of* $\mathbb{Z}_4$ *by* $\mathbb{Z}_2$.

Consider the extension E given by

$$0 \longrightarrow \mathbb{Z}_4 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_2^T \longrightarrow 0.$$

The action is determined by a mapping $C_2^T \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, so as T must map to an element of order dividing 2, we have once again either $T \cdot a = a$ or $T \cdot a = -a$.

Let $T \cdot a = a$. Now,

$$\mathbb{Z}_4^{\mathbb{Z}_2} = \mathbb{Z}_4$$

and

$$N\mathbb{Z}_4 = (1+T)\mathbb{Z}_4 = (1+1)\mathbb{Z}_4 = 2\mathbb{Z}_4,$$

thus

$$H^2(\mathbb{Z}_2, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_2}}{N\mathbb{Z}_4} = \frac{\mathbb{Z}_4}{2\mathbb{Z}_4} \cong 0.$$

Analogously to the first example, our extensions are $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_8$.

Let $T \cdot a = -a$. Now, contrary to the previous examples, we have another fixed element, namely 2.

$$\mathbb{Z}_4^{\mathbb{Z}_2} = \{0, 2\} = 2\mathbb{Z}_4$$

and

$$N\mathbb{Z}_4 = (1+T)\mathbb{Z}_4 = (1-1)\mathbb{Z}_4 = \{0\},$$

thus

$$H^2(\mathbb{Z}_2, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_2}}{N\mathbb{Z}_4} = \frac{2\mathbb{Z}_4}{\{0\}} \cong \mathbb{Z}_2.$$

When calculating the factor system, we follow the same procedure as in Example 6 to get $f(1,T) = f(T,1) = f(1,1) = 0$ and $2f(T,T) = 0$. In this example, we immediately deduced that $f(T,T) = 0$, as the codomain of f is $\mathbb{Z}$, where there are no divisors of zero. This is not the case in $\mathbb{Z}_4$. We may have $f(T,T) = 0$ or $f(T,T) = 2$, and in both cases $2f(T,T) = 0$. These cases correspond to the two distinct cohomology classes.

In the first case, when $f(T,T) = 0$, corresponding to the trivial cohomology class, the extension is, similar to Example 7, the dihedral group $\mathbb{D}_4$.

In the second case, when $f(T,T) = 2$, corresponding to the non-trivial cohomology class, we have the composition law

$$\begin{aligned}
(a,1)(b,1) &= (a+b,1),\\
(a,1)(b,T) &= (a+b,T),\\
(a,T)(b,1) &= (a-b,T),\\
(a,T)(b,T) &= (a-b+2,1).
\end{aligned}$$

This yields an isomorphism to the quaternions

$$\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = ijk = -1\}$$

via

$$\begin{aligned}
(2,1) &\mapsto -1,\\
(1,1) &\mapsto i,\\
(0,T) &\mapsto j,\\
(1,T) &\mapsto k.
\end{aligned}$$

Thus, the possible group extensions of $\mathbb{Z}_4$ by $\mathbb{Z}_2$ are $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, $\mathbb{D}_4$, and $\mathbb{Q}_8$.

6.2 The Dihedral Group $\mathbb{D}_3$

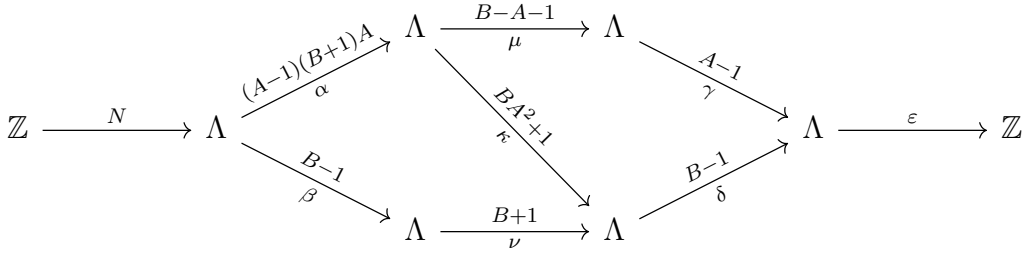
In this section, we will denote by $G = \mathbb{D}_3$ be the dihedral group with 6 elements. G has a presentation

$$G = \langle A, B \mid A^3 = B^2 = 1,\ BAB = A^2 \rangle.$$

The goal of this section is to find a resolution for this group, and calculate its cohomology groups, in the case of trivial group action.

Example 9 *Constructing a resolution for the dihedral group* $\mathbb{D}_3$.

Let us consider the following diagram:



By joining the upper and lower rows in the middle, as well as joining the head to the tail, we form the following periodic chain complex, which we will show is exact:

$$\cdots \xrightarrow[\partial_4]{N\varepsilon} \Lambda \xrightarrow[\partial_3]{\begin{pmatrix}\alpha\\ \beta\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_2]{\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}} \Lambda \oplus \Lambda \xrightarrow[\partial_1]{\begin{pmatrix}\gamma & \delta\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.$$

For the remainder of this section, we denote an element λ of Λ as

$$\lambda = x + yA + zA^2 + uB + vBA + wBA^2$$

with $\mathbb{Z}$-coefficients x, y, z, u, v, and w.

The map $N\varepsilon : \Lambda \to \Lambda$ is the composition of the maps $\varepsilon : \Lambda \to \mathbb{Z}$ sending elements $\lambda \in \Lambda$ to the sum of their coefficients $x + y + z + u + v + w = k \in \mathbb{Z}$, and $N : \mathbb{Z} \to \Lambda$, sending elements $k \in \mathbb{Z}$ to kN, where N is the sum of all the elements in G, i.e. $N = 1 + A + A^2 + B + BA + BA^2$.

Multiplying by N sends an element $\lambda \in \Lambda$ to

$$N\lambda = (x + y + z + u + v + w)(1 + A + A^2 + B + BA + BA^2) = kN,$$

where k is the sum of the coefficients. Hence, we may simply view the map $N\varepsilon$ as multiplication by N.

We start the proof of exactness by first showing that any two consecutive maps have trivial composition, i.e. images are contained in kernels. Afterwards, we will show the trickier part, that the kernels are contained in the images.

We notice that

$$N = 1 + A + A^2 + B + BA + BA^2 = (1 + B)(1 + A + A^2)$$

and hence the compositions $\alpha N = \beta N = 0$ as $(1+B)(1-B) = 1-B^2 = 1-1 = 0$. Thus, the composition $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} N = 0$.

For the composition $\begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \mu\alpha \\ \kappa\alpha + \nu\beta \end{pmatrix}$ we shall compute each product piecewise:

$$\begin{aligned}
\mu\alpha &= (-1 - A + B)(A - 1)(B + 1)A \\
&= (-1 - A + B)(AB - B + A - 1)A \\
&= (-1 - A + B)(B - BA + A^2 - A) \\
&= -B + BA - A^2 + A - AB + ABA - A^3 \\
&\quad + A^2 + B^2 - B^2A + BA^2 - BA \\
&= -B + BA - A^2 + A - BA^2 + B - 1 \\
&\quad + A^2 + 1 - A + BA^2 - BA \\
&= 0; \\
\kappa\alpha &= (1 + BA^2)(A - 1)(B + 1)A \\
&= (1 + BA^2)(B + A^2 - BA - A) \\
&= B + A^2 - BA - A + A + BA - A^2 - B \\
&= 0; \\
\nu\beta &= (B + 1)(B - 1) \\
&= 0.
\end{aligned}$$

Thus, the composition $\begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \mu\alpha \\ \kappa\alpha + \nu\beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is trivial.

For the composition $\begin{pmatrix} \gamma & \delta \end{pmatrix} \begin{pmatrix} \mu & 0 \\ \kappa & \nu \end{pmatrix} = \begin{pmatrix} \gamma\mu + \delta\kappa & \delta\nu \end{pmatrix}$ we shall again compute each product piecewise:

$$\begin{aligned}
\gamma\mu &= (A - 1)(-1 - A + B) \\
&= -A - A^2 + AB + 1 + A - B \\
&= -B + 1 - BA^2 + A^2; \\
\delta\kappa &= (B - 1)(1 + BA^2) \\
&= B - 1 + BA^2 - A^2 \\
&= -\gamma\mu;
\end{aligned}$$

$$\begin{aligned}\delta\nu &= (B-1)(B+1)\\ &= 0.\end{aligned}$$

From here we see the composition $\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix} = \begin{pmatrix}\gamma\mu+\delta\kappa & \delta\nu\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ is trivial.

To calculate the composition of maps $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ and $N\varepsilon$, we shall first view $N\varepsilon$ as the map of multiplication by N, through which the composition becomes the map $N\begin{pmatrix}\gamma & \delta\end{pmatrix}$. We notice that as

$$N = (1+B)(1+A+A^2) = (1+A+A^2)(1+B),$$

the following compositions are trivial:

$$\begin{aligned}N\gamma &= (1+B)(1+A+A^2)(A-1)\\ &= (1+B)(A^3-1)\\ &= 0;\\ N\delta &= (1+A+A^2)(1+B)(1-B)\\ &= 0.\end{aligned}$$

Thus, the composition of maps $N\begin{pmatrix}\gamma & \delta\end{pmatrix} = \begin{pmatrix}N\gamma & N\delta\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ is trivial.

Finally, we consider the composition of the final two maps, $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ and ε. Let us show that any arbitrary element $\lambda \in \Lambda$ is mapped to 0. First, we check where γ and δ send λ:

$$\begin{aligned}\gamma\lambda &= (A-1)(x+yA+zA^2+uB+vBA+wBA^2)\\ &= xA+yA^2+zA^3+uAB+vABA+wABA^2\\ &\quad -x-yA-zA^2-uB-vBA-wBA^2\\ &= (z-x)+(x-y)A+(y-x)A^2+(v-u)B\\ &\quad +(w-v)BA+(u-w)BA^2;\\ \delta\lambda &= (B-1)(x+yA+zA^2+uB+vBA+wBA^2)\\ &= xB+yBA+zBA^2+uB^2+vB^2A+wB^2A^2\\ &\quad -x-yA-zA^2-uB-vBA-wBA^2\\ &= (u-x)+(v-y)A+(w-z)A^2+(x-u)B\\ &\quad +(y-v)BA+(z-w)BA^2.\end{aligned}$$

Now, when we apply ε, we get the sum of the coefficients:

$$\begin{aligned}\varepsilon\gamma\lambda &= (z-x)+(x-y)+(y-x)+(v-u)+(w-v)+(u-w)\\ &= 0;\end{aligned}$$

$$\begin{aligned}\varepsilon\delta\lambda &= (u-x)+(v-y)+(w-z)+(x-u)+(y-v)+(z-w)\\ &= 0.\end{aligned}$$

Thus, the composition $\varepsilon\begin{pmatrix}\gamma & \delta\end{pmatrix} = \begin{pmatrix}\varepsilon\gamma & \varepsilon\delta\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$ is trivial.

We have so far shown that any two consecutive maps have trivial composition. This means that the image of any map is contained in the kernel of the next one. The next step is to show that the kernel of any map is contained in the image of the previous map. Again, we do this step by step.

Let us show $\ker\varepsilon \subset \operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$. The map $\begin{pmatrix}\gamma & \delta\end{pmatrix}$ sends an element $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \Lambda\oplus\Lambda$ to $\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} = \gamma\lambda_1 + \delta\lambda_2$. Let us now show that any element in the kernel of ε is of this form. Note that

$$\lambda_1 = x_1 + y_1A + z_1A^2 + u_1B + v_1BA + w_1BA^2$$

and

$$\lambda_2 = x_2 + y_2A + z_2A^2 + u_2B + v_2BA + w_2BA^2.$$

Throughout the rest of the proof, λ_1 and λ_2 will be assumed to have coefficients denoted as such.

Let λ be an element of the kernel of ε. An element $\lambda \in \Lambda$ is contained in the kernel of ε, that is $\varepsilon\lambda = 0$, when the sum of its coefficients is 0. Thus

$$x + y + z + u + v + w = 0.$$

We may then use this to replace $x = -y - z - u - v - w$ in λ, and try to find λ_1 and λ_2 such that $\lambda = \gamma\lambda_1 + \delta\lambda_2 = (A-1)\lambda_1 + (B-1)\lambda_2$. Indeed,

$$\begin{aligned}\lambda &= (-y-z-u-v-w) + yA + zA^2 + uB + vBA + wBA^2\\ &= y(A-1) + z(A^2-1) + u(B-1) + v(BA-1) + w(BA^2-1)\\ &= y(A-1) + z(A-1)(A+1) + u(B-1)\\ &\quad + v(BA - A + A - 1) + w(BA^2 - A^2 + A^2 - 1)\\ &= (A-1)(y + z(A+1)) + u(B-1) + v(B-1)A + v(A-1)\\ &\quad + w(B-1)A^2 + w(A-1)(A+1)\\ &= (A-1)(y + z(A+1) + v + w(A+1)) + (B-1)(u + vA + wA^2).\end{aligned}$$

Hence, for $\lambda_1 = (y + z + v + w) + (z + w)A$ and $\lambda_2 = u + vA + wA^2$ we have $\lambda = \gamma\lambda_1 + \delta\lambda_2$, and so $\ker\varepsilon \subset \operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$.

This result refers to the end of the sequence, i.e. $\ker\varepsilon = \operatorname{im}\partial_1$. The fact that $\ker\partial_{4k} = \operatorname{im}\partial_{4k+1}$ for $k \geq 1$ follows quickly, because $\partial_{4k} = N\varepsilon$ and $\partial_{4k+1} = \partial_1$. More precisely, as $\ker N = 0$, it means $\ker N\varepsilon = \ker\varepsilon$, and so, by what we have just shown above, we immediately have $\ker N\varepsilon \in \operatorname{im}\begin{pmatrix}\gamma & \delta\end{pmatrix}$.

Let us move on to showing $\ker \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \subset \operatorname{im} N\varepsilon$. We showed earlier that $\operatorname{im} N\varepsilon = N\mathbb{Z}$. Let λ be an element of $\ker \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Then $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \lambda = 0$, that is $\begin{pmatrix} \alpha\lambda \\ \beta\lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, hence, we have $\alpha\lambda = \beta\lambda = 0$, i.e. $\lambda \in \ker\alpha \cap \ker\beta$. Our goal is now thus to show that $\ker\alpha \cap \ker\beta = N\mathbb{Z}$, or that $\lambda = kN$ for some integer k.

We shall start by considering the simpler of the two maps, $\beta = B - 1$. As δ was of the same form, we have then already computed

$$\beta\lambda = (u-x) + (v-y)A + (w-z)A^2 + (x-u)B + (y-v)BA + (z-w)BA^2.$$

If $\beta\lambda = 0$, then that means that these coefficients are all 0, hence $u = x$, $v = y$, and $w = z$. Thus, we now have a new form for λ:

$$\begin{aligned} \lambda &= x + yA + zA^2 + xB + yBA + zBA^2 \\ &= x(1+B) + y(A+BA) + z(A^2 + BA^2) \\ &= x(1+B) + y(1+B)A + z(1+B)A^2 \\ &= (1+B)(x + yA + zA^2) \end{aligned}$$

This seems to imply a connection between the maps $B+1$ and $B-1$. Let us calculate $(B+1)\lambda'$, for some other element λ' in Λ of the form $\lambda = x' + y'A + z'A^2 + u'B + v'BA + w'BA^2$:

$$\begin{aligned} (B+1)\lambda' &= (B+1)(x' + y'A + z'A^2 + u'B + v'BA + w'BA^2) \\ &= (x'+u') + (y'+v')A + (z'+w')A^2 \\ &\quad + (u'+x')B + (v'+y')BA + (w'+z')BA^2 \\ &= (x'+u')(1+B) + (y'+v')(A+BA) + (z'+w')(A^2+BA^2) \\ &= (1+B)((x'+u') + (y'+v')A + (z'+w')A^2). \end{aligned}$$

This is in $\ker(B-1)$ as $(B-1)(B+1) = B^2 - 1 = 0$. Also, by setting $x = x'+u'$, $y = y'+v'$, and $z = z'+w'$, we see that $\lambda = (B+1)\lambda'$. Thus $\ker(B-1) = \operatorname{im}(B+1)$. Analogously, we can deduce $\ker(B+1) = \operatorname{im}(B-1)$.

Now, returning our attention back to $\ker \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, we inspect how $\alpha\lambda = 0$ affects the coefficients of λ:

$$\begin{aligned} \alpha\lambda &= (A-1)(B+1)A\lambda \\ &= (B + A^2 - BA - A)(x + yA + zA^2 + uB + vBA + wBA^2) \\ &= (u + y - v - z) + (v + z - w - x)A + (w + x - u - y)A^2 \\ &\quad + (x + w - z - v)B + (y + u - x - w)BA + (z + v - y - u)BA^2 \\ &= (BA^2 - 1)((z - y + v - u) + (x - z + w - v)A + (y - x + u - w)A^2). \end{aligned}$$

As this value is 0, all the coefficients must be 0, which leaves us with the condition $u + y = v + z = w + x$.

Substituting what we have found out from $\beta\lambda = 0$, that is $u = x$, $v = y$, and $w = z$, we get $x + y = y + z = z + x$, which immediately yields $x = y = z$. Thus, all the coefficients of λ must be equal, say to some integer k. In other words,

$$\begin{aligned}\lambda &= k + kA + kA^2 + kB + kBA + kBA^2 \\ &= k(1 + A + A^2 + B + BA + BA^2) \\ &= kN,\end{aligned}$$

and thus we have found what we were searching for, that $\ker \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$ is contained in $\operatorname{im} N\varepsilon$.

What is left is to finish showing exactness for the middle two parts. Let us start with showing $\ker \begin{pmatrix}\mu & 0 \\ \kappa & \nu\end{pmatrix} \subseteq \operatorname{im} \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$. Suppose $\begin{pmatrix}\lambda_1 \\ \lambda_2\end{pmatrix} \in \ker \begin{pmatrix}\mu & 0 \\ \kappa & \nu\end{pmatrix}$. We wish to find $\lambda \in \Lambda$ such that $\begin{pmatrix}\lambda_1 \\ \lambda_2\end{pmatrix} = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \lambda = \begin{pmatrix}\alpha\lambda \\ \beta\lambda.\end{pmatrix}$.

From $\begin{pmatrix}\mu & 0 \\ \kappa & \nu\end{pmatrix} \begin{pmatrix}\lambda_1 \\ \lambda_2\end{pmatrix} = \begin{pmatrix}0 \\ 0\end{pmatrix}$ we derive two equations, $\mu\lambda_1 = 0$ and $\kappa\lambda_1 + \nu\lambda_2 = 0$. Let us compute $\mu\lambda_1$:

$$\begin{aligned}\mu\lambda_1 &= (-1 - A + B)(x_1 + y_1A + z_1A^2 +_1 uB + v_1BA + w_1BA^2) \\ &= (u_1 - x_1 - z_1) + (v_1 - y_1 - x_1)A + (w_1 - z_1 - y_1)A^2 \\ &\quad +(x_1 - u_1 - v_1)B + (y_1 - v_1 - w_1)BA + (z_1 - w_1 - u_1)BA^2.\end{aligned}$$

As those coefficients are all 0, from the first three we gain the conditions $u_1 = x_1 + z_1$, $v_1 = y_1 + x_1$, and $w_1 = z_1 + y_1$. By substituting these into the next three conditions, $x_1 = u_1 + v_1$, $y_1 = v_1 + w_1$, and $z_1 = w_1 + u_1$, we gain the same condition, $x_1 + y_1 + z_1 = 0$. Substituting $x_1 = -y_1 - z_1$ back into λ_1, we get

$$\begin{aligned}\lambda_1 &= (-y_1 - z_1) + y_1A + z_1A^2 - z_1B - y_1BA + (z_1 + y_1)BA^2 \\ &= y_1(-1 + A - B + BA^2) + z_1(-1 + A^2 - BA + BA^2).\end{aligned}$$

Now, utilizing $(BA^2 + 1)(BA^2 - 1) = 0$, we have

$$\begin{aligned}\kappa\lambda_1 &= (BA^2 + 1)\lambda_1 \\ &= y_1(BA^2 + 1)(A - B + BA^2 - 1) \\ &\quad +z_1(BA^2 + 1)(A^2 - BA + BA^2 - 1) \\ &= y_1(B - A + A - B) + z_1(BA - A^2 + A^2 - BA) \\ &= 0.\end{aligned}$$

Note, analogously to how we achieved $\ker(B+1) = \mathrm{im}(B-1)$, we have $\ker(BA^2+1) = \mathrm{im}(BA^2-1)$. Thus, $\lambda_1 \in \mathrm{im}(BA^2-1)$. In fact, we can calculate

$$\begin{aligned}\lambda_1 &= y_1(-1+A-B+BA^2) + z_1(-1+A^2-BA+BA^2)\\ &= (BA^2-1)(y_1+z_1) - y_1(B-A) - z_1(BA-A^2)\\ &= (BA^2-1)(y_1+z_1) - y_1A(BA^2-1) - z_1A^2(BA^2-1)\\ &= (BA^2-1)(y_1+z_1-y_1A-z_1A^2).\end{aligned}$$

As $\kappa\lambda_1 = 0$, $\kappa\lambda_1 + \nu\lambda_2 = 0$ becomes just $\nu\lambda_2 = 0$, i.e. $\lambda_2 \in \ker\nu$. As shown earlier, $\ker(B-1) = \mathrm{im}(B+1)$, hence

$$\lambda_2 = (B-1)(x_2 + y_2A + z_2A^2).$$

Now, as

$$\lambda_2 = \beta\lambda = (B-1)((u-x) + (v-y)A + (w-z)A^2,$$

we have $u = x + x_2$, $v = y + y_2$, and $w = z + z_2$. Substituting these into $\lambda_1 = \alpha\lambda$ we have

$$\begin{aligned}\lambda_1 &= (BA^2-1)((z-y+v-u) + (x-z+w-v)A + (y-x+u-w)A^2)\\ &= (BA^2-1)((z-x+y_2-x_2) + (x-y+z_2-y_2)A + (y-z+x_2-z_2)A^2.\end{aligned}$$

Thus, using

$$\lambda_1 = (BA^2-1)(y_1+z_1-y_1A-z_1A^2)$$

by comparing coefficients we get a system of equations

$$\begin{aligned}z-x+y_2-x_2 &= y_1+z_1\\ x-y+z_2-y_2 &= -y_1\\ y-z+x_2-z_2 &= -z_1.\end{aligned}$$

As the first equation is the negative sum of the next two, the system yields two relations, say $y = z - z_1 + z_2 - x_2$ and $x = z - z_1 + y_2 - x_2$, and z may remain free. Thus, for λ with such coefficients, we indeed gain $\alpha\lambda = \lambda_1$ and $\beta\lambda = \lambda_2$, i.e. $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \mathrm{im}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, as we desired.

Lastly, we need to show that $\ker\begin{pmatrix}\gamma & \delta\end{pmatrix} \subseteq \mathrm{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$. Let $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \ker\begin{pmatrix}\gamma & \delta\end{pmatrix}$. We aim to show $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \mathrm{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$, which means we want to find $\lambda_1', \lambda_2' \in \Lambda$ such that $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} = \begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}\begin{pmatrix}\lambda_1'\\ \lambda_2'\end{pmatrix}$, i.e.

$$\lambda_1 = \mu\lambda_1'$$

$$\lambda_2 \;=\; \kappa\lambda_1' + \nu\lambda_2'.$$

Since $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \ker\begin{pmatrix}\gamma & \delta\end{pmatrix}$, we have

$$\begin{aligned}\begin{pmatrix}\gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} &= 0\\ \gamma\lambda_1 + \delta\lambda_2 &= 0\\ \gamma\lambda_1 &= -\delta\lambda_2.\end{aligned}$$

As $\gamma = A - 1$ and $\delta = B - 1$, we may use our calculations from earlier to get

$$\begin{aligned}\gamma\lambda_1 &= (z_1 - x_1) + (x_1 - y_1)A + (y_1 - x_1)A^2\\ &\quad +(v_1 - u_1)B + (w_1 - v_1)BA + (u_1 - w_1)BA^2;\\ \delta\lambda_2 &= (u_2 - x_2) + (v_2 - y_2)A + (w_2 - z_2)A^2\\ &\quad +(x_2 - u_2)B + (y_2 - v_2)BA + (z_2 - w_2)BA^2;\\ -\delta\lambda_2 &= (B-1)((u_2 - x_2) + (y_2 - v_2)A + (z_2 - w_2)A^2).\end{aligned}$$

As $\gamma\lambda_1 = -\delta\lambda_2$, we can identify their coefficients:

$$\begin{aligned}z_1 - x_1 &= -(u_2 - x_2) = -(v_1 - u_1),\\ x_1 - y_1 &= -(v_2 - y_2) = -(w_1 - v_1),\\ y_1 - z_1 &= -(w_2 - z_2) = -(u_1 - w_1).\end{aligned} \tag{4}$$

Manipulating this further, we have

$$x_1 - v_1 = y_1 - w_1 = z_1 - u_1.$$

Let us set this value to be t. Now,

$$\begin{aligned}\lambda_1 &= x_1 + y_1A + z_1A^2 + (t + z_1)B + (t_1 + x_1)BA + (t + y_1)BA^2\\ &= x_1(1 + BA) + y_1(A + BA^2) + z_1(A^2 + B) + t(B + BA + BA^2)\\ &= (1 + BA)(x_1 + y_1A + z_1A^2) + t(B + BA + BA^2).\end{aligned}$$

We are trying to find λ_1' such that $\lambda_1 = \mu\lambda_1'$. It suffices to find the preimages of $1 + BA$ and $B + BA + BA^2$.

From before, for any arbitrary $\lambda \in \Lambda$, we have

$$\begin{aligned}\mu\lambda &= (u - x - z) + (v - y - x)A + (w - z - y)A^2\\ &\quad +(x - u - v)B + (y - v - w)BA + (z - w - u)BA^2.\end{aligned}$$

By identifying the coefficients with the coefficients of $1 + BA$, we get

$$u - x - z \;=\; 1,$$

$$\begin{aligned} v - y - x &= 0, \\ w - z - y &= 0, \\ x - u - v &= 0, \\ y - v - w &= 1, \\ z - w - u &= 0, \end{aligned}$$

which has a solution $x = v = -1$, $y = z = u = w = 0$. This means

$$\mu(-1 - BA) = 1 + BA.$$

Similarly for $B + BA + BA^2$ we have the system of equations

$$\begin{aligned} u - x - z &= 0, \\ v - y - x &= 0, \\ w - z - y &= 0, \\ x - u - v &= 1, \\ y - v - w &= 1, \\ z - w - u &= 1, \end{aligned}$$

which has a solution $x = u = v = -1$, $y = z = w = 0$. This means

$$\mu(-1 - B - BA) = B + BA + BA^2.$$

Hence,

$$\begin{aligned} \lambda_1 &= (1 + BA)(x_1 + y_1A + z_1A^2) + t(B + BA + BA^2) \\ &= \mu(-1 - BA)(x_1 + y_1A + z_1A^2) + \mu t(-1 - B - BA) \\ &= -\mu((1 + BA)(x_1 + y_1A + z_1A^2) + t(1 + B + BA)), \end{aligned}$$

and thus $\lambda_1 = \mu\lambda_1'$ for

$$\lambda_1' = (1 + BA)(x_1 + y_1A + z_1A^2) + t(1 + B + BA).$$

Now, we want to find λ_2' such that $\lambda_2 = \kappa\lambda_1' + \nu\lambda_2'$, i.e. we want to show $\lambda_2 - \kappa\lambda_1' \in \operatorname{im}\nu$.

In (4), if we add up the three lines, we have

$$0 = x_2 + y_2 + z_2 - u_2 - v_2 - w_2 = 0$$

i.e. $x_2 = -y_2 - z_2 + u_2 + v_2 + w_2$. We also have $v_2 = y_2 + y_1 - x_1$ and $w_2 = z_2 + z_1 - y_1$. Now,

$$\lambda_2 = y_2(A - 1) + z_2(A^2 - 1) + u_2(B + 1) + v_2(BA + 1) + w_2(BA^2 + 1)$$

$$
\begin{aligned}
&= y_2(A-1)+z_2(A^2-1)+u_2(B+1)\\
&\quad +(y_2+y_1-x_1)(BA+1)+(z_2+z_1-y_1)(BA^2+1)\\
&= (B+1)(u_2+y_2A+z_2A^2)-x_1(BA+1)\\
&\quad +y_1(BA-BA^2)+z_2(BA^2+1).
\end{aligned}
$$

We have grouped the part that is in $\operatorname{im}\nu$ in front, $(B+1)(u_2+y_2A+z_2A^2)$. Now, similarly for $\kappa\lambda_1'$,

$$
\begin{aligned}
-\kappa\lambda_1' &= (1+BA^2)((1+BA)(x_1+y_1A+z_1A^2)+t(1+B+BA))\\
&= (1+BA+BA^2+A^2)(x_1+y_1A+z_1A^2)\\
&\quad +t(1+BA^2+B+A+BA+A^2)\\
&= (1+B)(A^2(x_1+y_1A+z_1A^2)+t(1+A+A^2))\\
&\quad +(1+BA)(x_1+y_1A+z_1A^2).
\end{aligned}
$$

Again, we have grouped at the front of the expression the part that is clearly in $\operatorname{im}\nu$. Now, we show that the rest of $\lambda_2-\kappa\lambda_1'$ also lies in $\operatorname{im}\nu$. Inspired by modular arithmetic, we use the notation for congruence instead of equality in the first line as we are disregarding the parts that we have already shown to be a left multiple of $\nu = B+1$.

$$
\begin{aligned}
\lambda_2-\kappa\lambda_1' &\equiv -x_1(BA+1)+y_1(BA-BA^2)+z_2(BA^2+1)\\
&\quad +(1+BA)(x_1+y_1A+z_1A^2)\\
&= x_1(-BA-1+1+BA)+y_1(BA-BA^2+A+BA^2)\\
&\quad +z_1(BA^2+1+A^2+B)\\
&= (B+1)(y_1A+z_1(1+A^2)).
\end{aligned}
$$

Hence, $\lambda_2-\kappa\lambda_1'\in\operatorname{im}\nu$. Thus, we have shown $\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\operatorname{im}\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}$.

We have now finally finished the proof of exactness of the sequence

$$
\cdots \xrightarrow{N\varepsilon} \Lambda \xrightarrow{\begin{pmatrix}\alpha\\ \beta\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow{\begin{pmatrix}\mu & 0\\ \kappa & \nu\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow{\begin{pmatrix}\gamma & \delta\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.
$$

Thus, it is a free resolution of $\mathbb{D}_3$. □

Example 10 *The cohomology groups of $\mathbb{D}_3$ for trivial group action.*

Let $G=\mathbb{D}_3$ and let M be a G-module with trivial G-action. Thus, our resolution becomes

$$
\cdots \xrightarrow[\partial_4]{6\varepsilon} \Lambda \xrightarrow[\partial_3]{\begin{pmatrix}0\\ 0\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow[\partial_2]{\begin{pmatrix}-1 & 0\\ 2 & 2\end{pmatrix}} \Lambda\oplus\Lambda \xrightarrow[\partial_1]{\begin{pmatrix}0 & 0\end{pmatrix}} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}.
$$

Let us then consider the periodic cochain complex

$$\cdots \xleftarrow[d^4]{(6\varepsilon)^*} M \xleftarrow[d^3]{\begin{pmatrix}0\\0\end{pmatrix}} M\oplus M \xleftarrow[d^2]{\begin{pmatrix}-1 & 2\\ 0 & 2\end{pmatrix}} M\oplus M \xleftarrow[d^1]{\begin{pmatrix}0 & 0\end{pmatrix}} M \xleftarrow[d^0]{0} 0.$$

Note that we replaced the modules $\mathrm{Hom}_G(\Lambda, M)$ and $\mathrm{Hom}_G(\Lambda\oplus\Lambda, M)$ with isomorphic modules M and $M\oplus M$ respectively.

Now, $H^0(G,M) = \ker d^1 = M$, and for $k \geq 1$ the cohomology groups are as follows:

$$H^k(G,M) = \begin{cases} \ker d^2, & k \equiv 1 \mod 4,\\ \operatorname{coker} d^2, & k \equiv 2 \mod 4,\\ \ker d^4, & k \equiv 3 \mod 4,\\ \operatorname{coker} d^4, & k \equiv 0 \mod 4. \end{cases}$$

Let us calculate these kernels and cokernels. First, we see that the result of d^2 applied to an arbitrary vector $\bar{a} = \begin{pmatrix}a\\b\end{pmatrix} \in M\oplus M$ is

$$\begin{pmatrix}-1 & 2\\ 0 & 2\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}2b-a\\ 2b\end{pmatrix}.$$

Hence, if $\bar{a} \in \ker d^2$, then $a = 2b$ and $2b = 0$, i.e. $a = 0$ and b is of order at most 2 in M. Let us denote the submodule of elements whose orders divide $t \in \mathbb{Z}$ in M as follows:

$$\mathrm{T}_M(t) = \{m \in M :\ tm = 0\}.$$

With this notation, we have $b \in \mathrm{T}_M(2)$. Thus,

$$H^{4k+1}(G,A) = \ker d^2 = 0 \oplus \mathrm{T}_M(2) \cong \mathrm{T}_M(2).$$

As $2a - b$ spans all of M, we have $\operatorname{im} d^2 = M \oplus 2M$, and hence

$$H^{4k+2}(G,A) = \operatorname{coker} d^2 = \frac{M\oplus M}{M\oplus 2M} \cong 0 \oplus \frac{M}{2M} \cong \frac{M}{2M}.$$

Let us consider $d^4 = (6\varepsilon)^*$. As the group action is trivial, for any $\lambda = \Sigma_i n_i g_i \in \Lambda$ and $m \in M$ we have

$$\lambda \cdot m = \sum_i n_i g_i \cdot m = \sum_i n_i m = \varepsilon(\lambda) m,$$

i.e. λ acts by multiplying by $\varepsilon(\lambda)$. Now, let $f_m \in \mathrm{Hom}_G(\Lambda, M)$ be the cochain defined by $f : 1 \mapsto m$. This means, for all $\lambda \in \Lambda$, $f_m(\lambda) = \lambda \cdot m = \varepsilon(\lambda)m$. Next, we check how d^4 maps this element:

$$d^4 f_m(\lambda) = f_m(\partial_4 \lambda) = f_m(6\varepsilon(\lambda)) = 6\varepsilon(\lambda) f_m(1) = 6\varepsilon(\lambda)m = 6 f_m(\lambda).$$

Thus, d^4 is is simply multiplication by 6. This makes calculating the cohomology groups very simple: $H^{4k+3}(G,A) = \ker d^4 = \mathrm{T}_M(6)$ and $H^{4k}(G,A) = \operatorname{coker} d^4 = M/6M$.

Putting all these results together, we get

$$H^k(G,M) = \begin{cases} M, & k = 0 \\ \mathrm{T}_M(2), & k \equiv 1 \mod 4, \\ \frac{M}{2M}, & k \equiv 2 \mod 4, \\ \mathrm{T}_M(6), & k \equiv 3 \mod 4, \\ \frac{M}{6M}, & k \equiv 0 \mod 4,\ k \geq 4. \end{cases}$$

6.3 The Klein 4-Group

In this section we will calculate a resolution for G equal to the Klein 4-group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. We will do so with the help of a topological fact:

Lemma 30 *Let X be a $K(G_1,1)$ space and Y a $K(G_2,1)$ space. Then, $X \times Y$ is a $K(G_1 \times G_2, 1)$ space.*

Proof: Let p and q be the canonical projections from $X \times Y$ to X and Y respectively. For an arbitrary continuous map $\gamma : S^k \to X \times Y$, we get the continuous maps $p\gamma : S^k \to X$ and $q\gamma : S^k \to Y$. Thus, a class $[\gamma] \in \pi_k(X \times Y)$ corresponds to the element $([p\gamma],[q\gamma]) \in \pi_k(X) \times \pi_k(Y)$. Conversely, let i and j be the canonical inclusions of X and Y in $X \times Y$. For two maps $\gamma_1 : S^k \to X$ and $\gamma_2 : S^k \to Y$ we have a map $\gamma : S^k \to X \times Y$ given by $\gamma(t) = (\gamma_1(t), \gamma_2(t))$. Thus, a class $([\gamma_1],[\gamma_2]) \in \pi_k(X) \times \pi_k(Y)$ corresponds to the class $[\gamma] \in \pi_k(X \times Y)$. These correspondences are well-defined and inverse to each other, hence $\pi_k(X \times Y) \cong \pi_k(X) \times \pi_k(Y)$, in every dimension $k \geq 1$.

Thus, $\pi_1(X \times Y) \cong G_1 \times G_2$ and $\pi_k(X \times Y) = 0$ for $k > 1$, and so $X \times Y$ is a $K(G_1 \times G_2)$ space. □

Now, let us focus on the group $G = V$.

Example 11 *Constructing a resolution for the Klein 4-group.*

In Example 3, we calculated the resolution of $\mathbb{Z}_2$ by noting that $\mathbb{R}P^\infty$ is a $K(\mathbb{Z}_2,1)$ space, and by using Proposition 10, which meant the augmented cellular chain complex of S^∞, the universal cover of $\mathbb{R}P^\infty$, gave a free resolution of $\mathbb{Z}$ over $\mathbb{Z}C_2^T$. By Lemma 30, $\mathbb{R}P^\infty \times \mathbb{R}P^\infty$ is a $K(G,1)$ complex, and so as $S^\infty \times S^\infty$ is a contractible universal cover of $\mathbb{R}P^\infty \times \mathbb{R}P^\infty$, we can see again by Proposition 10 that the cellular chain complex of $S^\infty \times S^\infty$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$.

Let $G = V = \{1, T, S, TS\}$ with $T^2 = S^2 = (TS)^2 = 1$. We have the C_2^T and C_2^S as subgroups in G, generated by T and S respectively. As such, $G \cong C_2^T \times C_2^S$. Now, denote $X = S^\infty \times S^\infty$. From Example 3, we have the following two resolutions for C_2^T and C_2^S given by the cellular chain complex for S^∞:

$$\ldots \xrightarrow[1+T]{\partial'_4} \Lambda' \xrightarrow[1-T]{\partial'_3} \Lambda' \xrightarrow[1+T]{\partial'_2} \Lambda' \xrightarrow[1-T]{\partial'_1} \Lambda' \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

$$\ldots \xrightarrow[1+S]{\partial''_4} \Lambda'' \xrightarrow[1-S]{\partial''_3} \Lambda'' \xrightarrow[1+S]{\partial''_2} \Lambda'' \xrightarrow[1-S]{\partial''_1} \Lambda'' \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

where each $\Lambda' = \mathbb{Z}C_2^T$ and $\Lambda'' = \mathbb{Z}C_2^S$. Let us note that

$$\Lambda = \mathbb{Z}G = \mathbb{Z}[C_2^T \times C_2^S] \cong \mathbb{Z}C_2^T \otimes \mathbb{Z}C_2^S = \Lambda' \otimes \Lambda''.$$

A k-cell in X is the product of an i-cell in the first S^∞ and a j-cell in the second S^∞, where $i + j = k$ and $i, j \geq 0$. These generate the module $\Lambda'_i \otimes \Lambda''_j$, by bilinearity. Thus, in dimension k, the module P_k is the direct sum of all the products $\Lambda'_i \otimes \Lambda''_j$, i.e.

$$P_k = \bigoplus_{i+j=k} \Lambda'_i \otimes \Lambda''_j \cong \bigoplus_{i=0}^{k} \Lambda.$$

Of course, this corresponds exactly to the tensor product of chain complexes. The differential map in the tensor product of chain complexes is given on an element $c' \otimes c'' \in P_k$, where $c' \in \Lambda'_i$ and $c'' \in \Lambda''_j$, by:

$$\partial_k(c' \otimes c'') = \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c''.$$

Indeed,

$$\begin{aligned} \partial\partial(c' \otimes c'') &= \partial(\partial' c' \otimes c'') + (-1)^{\deg c'} \partial(c' \otimes \partial'' c'') \\ &= \partial'\partial' c' \otimes c'' + (-1)^{\deg \partial' c'} \partial' c' \otimes c'' + (-1)^{\deg c'} \partial' c' \otimes \partial'' c'' \\ &\quad + (-1)^{\deg c' + \deg \partial' c'} c' \otimes \partial''\partial'' c''. \end{aligned}$$

The first and last summands disappear as $\partial'\partial' = 0$ and $\partial''\partial'' = 0$. The middle two summands cancel out as $\deg \partial' c' = \deg c' + 1$. Hence, $\partial\partial = 0$.

We next verify that $\ker \partial_k = \operatorname{im} \partial_{k+1}$. To do so, we will treat ∂_k as a linear map from $P_k = \bigoplus_{i+j=k} \Lambda'_i \otimes \Lambda''_j$ to P_{k-1}, by which we may represent it as a matrix with k rows and $k + 1$ columns.

For an element $c' \otimes c'' \in \Lambda'_i \otimes \Lambda''_j$, we have

$$\partial_k(c' \otimes c'') = \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c'',$$

noting that $\partial'_i c' \otimes c'' \in \Lambda'_{i-1} \otimes \Lambda''_j$ and $c' \otimes \partial''_j c'' \in \Lambda'_i \otimes \Lambda''_j$. This means we get factors in $\Lambda'_i \otimes \Lambda''_j$ in the resulting element of P_{k-1} from the summands in $\Lambda'_i \otimes \Lambda''_{j+1}$ and $\Lambda'_{i+1} \otimes \Lambda''_j$. Thus, in the i-th row of the matrix ∂_k, indexing the rows and columns from 0, we have a non-zero entry in positions i and $i+1$, and zeroes elsewhere. We see what these entries are by using the fact that $\partial'_i = T + (-1)^i$ and $\partial''_j = S + (-1)^j$, and substituting these into the formula for ∂_k, again on an element $c' \otimes c'' \in \Lambda'_i \otimes \Lambda''_j$:

$$\begin{aligned}
\partial_k(c' \otimes c'') &= \partial'_i c' \otimes c'' + (-1)^{\deg c'} c \otimes \partial''_j c'' \\
&= (T + (-1)^i)c' \otimes c'' + (-1)^i 1 \otimes (S + (-1)^j)c'' \\
&= (T + (-1)^i)c' \otimes c'' + \otimes((-1)^{k-j} S + (-1)^k)c''.
\end{aligned}$$

Hence, we have $1 \otimes ((-1)^{k-j} S + (-1)^k)$ in position (i,i) and $(T + (-1)^{i+1}) \otimes 1$ in position $(i, i+1)$. However, before we display the matrix, let us remember that the element $T \otimes 1$ in $\Lambda' \otimes \Lambda''$ corresponds to the element T in $\Lambda = \mathbb{Z}G$, and similarly, $1 \otimes S$ corresponds to S. Therefore, after making these conversions, in matrix form we have:

$$\partial_k = \begin{pmatrix}
S + (-1)^k & T - 1 & 0 & \cdots & 0 & 0 \\
0 & -S + (-1)^k & T + 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \ddots & T + (-1)^{k-1} & 0 \\
0 & 0 & \cdots & \cdots & (-1)^{k-1} S + (-1)^k & T + (-1)^k
\end{pmatrix}.$$

Now, let us show that $\ker \partial_k = \operatorname{im} \partial_{k+1}$. Suppose $\bar{\lambda} \in \ker \partial_k$, i.e. $\bar{\lambda} \in P_k$ and $\partial_k \bar{\lambda} = 0$. Denote the vector $\bar{\lambda}$ by $\bar{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_k)$. Now, from $\partial_k \bar{\lambda} = 0$ we get the system of $k-1$ equations:

$$\begin{aligned}
(S + (-1)^k)\lambda_0 + (T-1)\lambda_1 &= 0, \\
(-S + (-1)^k)\lambda_1 + (T+1)\lambda_2 &= 0, \\
&\vdots \\
((-1)^{k-1} S + (-1)^k)\lambda_{k-1} + (T + (-1)^k)\lambda_k &= 0.
\end{aligned}$$

Let us inspect the first equation:

$$(S + (-1)^k)\lambda_0 = -(T-1)\lambda_1 = . \tag{5}$$

If we cancel out the right side of the equation by multiplying both sides by $(T+1)$ on the left, we get

$$(T+1)(S + (-1)^k)\lambda_0 = 0.$$

Thus, $\lambda_0 \in \ker(T+1)(S+(-1)^k)$. As an aside, let us compute $\ker(T-1)$. Suppose $\lambda = x + yT + zS + wTS \in \Lambda$. We have

$$\begin{aligned}(T-1)\lambda &= (T-1)(x+yT+zS+wTS)\\ &= (y-x)+(w-z)T+(x-y)S+(z-w)TS\\ &= (T-1)((y-x)+(w-z)S),\end{aligned}$$

so if $(T-1)\lambda = 0$, then $x = y$ and $z = w$, and so

$$\lambda = x + xT + zS + zTS = (1+T)(x+zS).$$

However, we similarly have for $\lambda' \in \Lambda$:

$$\begin{aligned}(T+1)\lambda' &= (T+1)(x'+y'T+z'S+w'TS)\\ &= (y'+x')+(w'+z')T+(x'+y')S+(z'+w')TS\\ &= (T+1)((y'+x')+(w'+z')S).\end{aligned}$$

So, for $y'+x' = x$ and $w'+z' = z$, we have $(T+1)\lambda' = \lambda$. Thus, $\ker(T-1) = \mathrm{im}(T+1) = (T+1)\Lambda = \{(T+1)(a+bS) : \ a, b \in \mathbb{Z}\}$. Similarly, $\ker(T+1) = (T-1)\Lambda$, and we have analogues for $S+1$ and $S-1$.

Let us return to our calculation of $\lambda_0 \in \ker(T+1)(S+(-1)^k)$. Elements in $\ker(T+1)$ are of the form $(T-1)(a+bS)$, and elements in $\mathrm{im}(S+(-1)^k)$ are of the form $(S+(-1)^k(c+dT)$. As λ_0 is in both, we have

$$(S+(-1)^k)\lambda_0 = (T-1)(a+bS) = (S+(-1)^k)(c+dT),$$

hence,

$$\begin{aligned}(T-1)(a+bS) &= (S+(-1)^k)(c+dT)\\ -a+aT-bS+bTS &= (-1)^k c + (-1)^k dT + cS + dTS,\end{aligned}$$

by which $a = (-1)^{k+1}c$, $a = (-1)^k d$, $-b = c$ and $b = d$. Thus, $b = (-1)^k a$, i.e.

$$(S+(-1)^k)\lambda_0 = (T-1)(S+(-1)^k)a. \tag{6}$$

Rearranging this, we have

$$(S+(-1)^k)(\lambda_0 - (T-1)a) = 0,$$

which means $\lambda_0 - (T-1)a \in \ker S + (-1)^k$, i.e.

$$\lambda_0 = (S+(-1)^{k+1})\mu_0 + (T-1)\mu_1,$$

for $\mu_0 \in \Lambda$ and $\mu_1 = a \in \Lambda$. Now, returning to equation (5) and substituting (6), we have

$$(T-1)\lambda_1 = -(T-1)(S+(-1)^k)\mu_1,$$

by which λ_1 differs from $(S+(-1)^k)\mu_1$ by an element of $\ker T - 1$, say $(T+1)\mu_2$. Thus,

$$\lambda_1 = (-S+(-1)^{k+1})\mu_1 + (T+1)\mu_2.$$

Now, substituting this into the second equation from the system,

$$(T+1)\lambda_2 + -(-S+(-1)^k)\lambda_1 = 0,$$

we get

$$(T+1)\lambda_2 = -(-S+(-1)^k)\mu_1,$$

and so, once again, λ_2 differs from $(S+(-1)^k)\mu_1$ by an element of $\ker T - 1$, say $(T+1)\mu_2$, and hence,

$$\lambda_2 = (S+(-1)^{k+1})\mu_2 + (T-1)\mu_3.$$

Continuing this process inductively, we get that the vector

$$\begin{pmatrix}\lambda_0\\ \lambda_1\\ \lambda_2\\ \vdots\\ \lambda_k\end{pmatrix}^T = \begin{pmatrix}(S+(-1)^{k+1})\mu_0 + (T-1)\mu_1\\ (-S+(-1)^{k+1})\mu_1 + (T+1)\mu_2\\ (S+(-1)^{k+1})\mu_2 + (T-1)\mu_3\\ \vdots\\ ((-1)^k S+(-1)^{k+1})\mu_k + (T+(-1)^k)\mu_{k+1}\end{pmatrix}^T = \partial_{k+1}\begin{pmatrix}\mu_0\\ \mu_1\\ \mu_2\\ \vdots\\ \mu_{k+1}\end{pmatrix},$$

i.e. $\bar{\lambda}^T = \partial_k \bar{\mu}$, for some $\bar{\mu} \in P_{k+1}$. Therefore, $\ker \partial_k = \operatorname{im} \partial_{k+1}$.

We have thus constructed the resolution for $\mathbb{Z}$ over Λ:

$$\cdots \longrightarrow P_3 \xrightarrow{\partial_3} P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \longrightarrow 0.$$

Example 12 *The cohomology groups of the Klein 4-group for trivial group action.*

To calculate the cohomology groups of the Klein 4-group $G = V$, we must consider the cochain complex

$$\cdots \leftarrow \operatorname{Hom}_G(P_k, A) \xleftarrow[d^k]{} \operatorname{Hom}_G(P_{k-1}, A) \xleftarrow[d^{k-1}]{} \ldots \xleftarrow[d^1]{} \operatorname{Hom}_G(P_0, A) \leftarrow 0.$$

As each P_k is the direct sum of $k+1$ copies of Λ,

$$\operatorname{Hom}_G(P_k, A) \cong \operatorname{Hom}_G(\bigoplus_{i=0}^{k} \Lambda, A) \cong \bigoplus_{i=0}^{k} \operatorname{Hom}_G(\Lambda, A) \cong \bigoplus_{i=0}^{k} A.$$

The boundary map d^k is thus represented in matrix form the same as the transposition of ∂_k:

$$\begin{pmatrix} S+(-1)^k & 0 & \cdots & \cdots & 0 & 0 \\ T-1 & -S+(-1)^k & \cdots & \cdots & 0 & 0 \\ 0 & T+1 & \ddots & & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & & \ddots & (-1)^{k-2}S+(-1)^k & 0 \\ 0 & 0 & \cdots & \cdots & T+(-1)^{k-1} & (-1)^{k-1}S+(-1)^k \\ 0 & 0 & \cdots & \cdots & 0 & T+(-1)^k \end{pmatrix}.$$

To calculate the cohomology groups, we must find $\ker d_{k+1}$ and $\operatorname{im} d_k$. In dimension 0, we have $\operatorname{im} d_0 = 0$ and $d^1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, i.e. $\ker d^1 = A$, hence $H^0(G, A) = A$.

Let us calculate the entries in the vector $\bar{b} = d^k \bar{a} \in P_k$ for arbitrary $\bar{a} \in P_{k-1}$, dividing the results into two cases, when $k = 2n$ is even (left) and when $k = 2n+1$ is odd (right):

$$\begin{aligned} b_0 &= 2a_0 & b_0 &= 0a_0 \\ b_1 &= 0a_0 + 0a_1 & b_1 &= 0a_0 - 2a_1 \\ b_2 &= 2a_1 + 2a_2 & b_2 &= 2a_1 + 0a_2 \\ &\vdots & &\vdots \\ b_{k-1} &= 0a_{k-2} + 0a_{k-1} & b_{k-1} &= 2a_{k-2} + 0a_{k-1} \\ b_k &= 2a_{k-1} & b_k &= 0a_{k-1} \end{aligned}$$

First, let us calculate $H^{2n}(G, A) = \ker d^{2n+1} / \operatorname{im} d^{2n}$. We have

$$\ker d^{2n+1} = A \oplus \mathrm{T}_A(2) \oplus A \oplus \ldots \mathrm{T}_A(2) \oplus A,$$

where $\mathrm{T}_A(2) = \{a \in A : \ 2a = 0\}$, the submodule of A of elements order at most 2. Note that this is the same as the group of elements fixed by the action of $-1 \in \Lambda$ on A, as $2a = 0 \Leftrightarrow (-1) \cdot a = a$. We have $2n$ factors in the direct sum, as d^{2n+1} maps from $\mathrm{Hom}_g(P_{2n}, A) \cong \bigoplus_{i=0}^{2n} A$, a direct sum of $2n$ copies of A. Next we have

$$\operatorname{im} d^{2n} = 2A \oplus 0 \oplus 2A \oplus \cdots \oplus 0 \oplus 2A.$$

Thus:

$$H^{2n}(G, A) \ = \ \frac{\ker d^{2n+1}}{\operatorname{im} d^{2n}}$$

$$
\begin{aligned}
&= \frac{A \oplus \mathrm{T}_A(2) \oplus A \oplus \ldots \mathrm{T}_A(2) \oplus A}{2A \oplus 0 \oplus 2A \oplus \cdots \oplus 0 \oplus 2A} \\
&= \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \frac{A}{2A} \oplus \cdots \oplus \frac{A}{2A} \oplus \mathrm{T}_A(2) \\
&= \big(\mathrm{T}_A(2)\big)^n \oplus \big(\frac{A}{2A}\big)^{n+1}.
\end{aligned}
$$

Next, let us calculate $H^{2n-1}(G, A) = \ker d^{2n} / \operatorname{im} d^{2n-1}$. We have

$$\ker d^{2n} = \mathrm{T}_A(2) \oplus B \oplus \cdots \oplus B \oplus \mathrm{T}_A(2),$$

where $B = \{(a, b) \in A \oplus A : \ 2a + 2b = 0\}$. We can interpret this as "given an element $a \in A$, find $b \in A$ such that $a + b \in \mathrm{T}_A(2)$". This logic leads us to the correspondence $\varphi : B \to A \oplus \mathrm{T}_A(2)$ given by $(a, b) \mapsto (a, a + b)$. This is trivially an isomorphism, hence $B \cong A \oplus \mathrm{T}_A(2)$. Next,

$$\operatorname{im} d^{2n-1} = 0 \oplus (-2, 2)A \oplus \cdots \oplus (-2, 2)A \oplus 0,$$

where $(-2, 2)A$ is the submodule of $A \oplus A$ generated by $(-2, 2)$. As $(-2, 2) \in B$, this means $(-2, 2)A \subseteq B$. The image of this submodule under the isomorphism φ is $2A \oplus 0$, hence

$$\frac{B}{(-2, 2)A} \cong \frac{A \oplus \mathrm{T}_A(2)}{2A \oplus 0} \cong \frac{A}{2A} \oplus \mathrm{T}_A(2).$$

Thus, we now calculate

$$
\begin{aligned}
H^{2n-1}(G, A) &= \frac{\ker d^2 n}{\operatorname{im} d^{2n-1}} \\
&= \frac{\mathrm{T}_A(2) \oplus B \oplus \ldots B \oplus \mathrm{T}_A(2)}{0 \oplus (-2, 2)A \oplus \cdots \oplus (-2, 2)A \oplus 0} \\
&= \mathrm{T}_A(2) \oplus \frac{B}{(-2, 2)A} \oplus \ldots \frac{B}{(-2, 2)A} \oplus \mathrm{T}_A(2) \\
&= \mathrm{T}_A(2) \oplus \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \ldots \frac{A}{2A} \oplus \mathrm{T}_A(2) \oplus \mathrm{T}_A(2) \\
&= \big(\mathrm{T}_A(2)\big)^{n+1} \oplus \big(\frac{A}{2A}\big)^{n-1}.
\end{aligned}
$$

Thus, we have calculated the cohomology groups of $G = V$ over a group A with trivial G-action:

$$
H^k(G, A) = \begin{cases}
A & k = 0 \\
\big(\mathrm{T}_A(2)\big)^{n+1} \oplus \big(\frac{A}{2A}\big)^{n-1} & k = 2n - 1, \ n \geq 1 \\
\big(\mathrm{T}_A(2)\big)^{n} \oplus \big(\frac{A}{2A}\big)^{n+1} & k = 2n, \ n \geq 1.
\end{cases}
$$

6.4 Extensions of order 12

Our goal in this section is to use the theory of group extensions to help us classify all groups of order 12. By Sylow theory, every group of order 12 does, in fact, factor as an extension of one of its subgroups by another.

Suppose G is a group of order 12. Let $s_3 = |\mathrm{Syl}_3(G)|$ be the number of Sylow 3-subgroups of G. By the third Sylow theorem, we must have $s_3|4$ and $s_3 \equiv 1 \mod 3$. This means $s_3 = 1$ or $s_3 = 4$. Suppose $s_3 = 4$. Then, this means we have 4 Sylow 3-subgroups in G. As these subgroups are each of order 3, they are generated by any of their non-trivial elements. Hence, the intersection of any two distinct 3-subgroups must be trivial. Counting the number of distinct elements in each subgroup, we have $4 \cdot 2 = 8$ elements of order 3, which along with the neutral element, gives us 9 elements in total. The remaining 3 elements, together with the neutral element, must form the sole Sylow 2-group. Hence, $s_2 = 1$.

When $s_p = 1$, it means we have a single Sylow p-group, which implies that that subgroup is normal. Our group G is therefore guaranteed to have a normal subgroup of order 3 or 4. Let us call it A, noting that it must be abelian. Suppose A is of order 3. In G there is at least one 2-subgroup, i.e. subgroup of order 4. As none of its elements can be of order 3, this means it is disjoint with the normal abelian subgroup A. Hence, G is in fact equivalent to the extension of A by this subgroup. Conversely, if A is of order 4, then G is equivalent to the extension of A by a Sylow 3-group. To keep consistent with our notation thus far, let us rename G to E, and name G the subgroup by which we are extending A.

We have therefore come to the conclusion that every group of order 12 can be represented by the group extension

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

where A is a group of order 3 or 4, and G is a group of order $12/|A|$. As there exists only one group of order 3, $\mathbb{Z}_3 \cong C_3^T$, and two groups of order 4, namely $\mathbb{Z}_4 \cong C_4^T$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$, we cover all cases in the following four examples.

Example 13 *Extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_4$.*

$$0 \longrightarrow \mathbb{Z}_3 \xrightarrow{\iota} E \xrightarrow{\pi} C_4^T \longrightarrow 0.$$

The action is determined by a mapping $C_4^T \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$, so as T must map to an element of order dividing 2, we have either $T \cdot a = a$ or $T \cdot a = -a$.

Let $T \cdot a = a$. Now,

$$\mathbb{Z}_3^{\mathbb{Z}_4} = \mathbb{Z}_3$$

and

$$N\mathbb{Z}_3 = (1 + T + T^2 + T^3)\mathbb{Z}_3 = (1 + 1 + 1 + 1)\mathbb{Z}_3 = 4\mathbb{Z}_3 = \mathbb{Z}_3,$$

thus

$$H^2(\mathbb{Z}_4, \mathbb{Z}_3) = \frac{\mathbb{Z}_3^{\mathbb{Z}_4}}{N\mathbb{Z}_3} = \frac{\mathbb{Z}_3}{\mathbb{Z}_3} \cong 0.$$

The extension is $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$, by Lemma 27.

Let $T \cdot a = -a$. Now, the only fixed element is 0.

$$\mathbb{Z}_3^{\mathbb{Z}_4} = 0$$

and

$$N\mathbb{Z}_3 = (1 + T + T^2 + T^3)\mathbb{Z}_3 = (1 - 1 + 1 - 1)\mathbb{Z}_4 = \{0\},$$

thus

$$H^2(\mathbb{Z}_4, \mathbb{Z}_3) = \frac{\mathbb{Z}_3^{\mathbb{Z}_4}}{N\mathbb{Z}_3} = \frac{\{0\}}{\{0\}} \cong 0.$$

The factor system corresponds to the trivial cohomology class, and the composition law becomes

$$(a, T^k)(b, T^l) = (a + T^k \cdot b, T^{k+l}) = (a + (-1)^k b, T^{k+l}).$$

This group is isomorphic to the dicyclic group

$$\mathrm{Dic}_3 = \langle x, y \mid x^6 = y^4 = 1,\ y^2 = x^3,\ yxy^{-1} = x^{-1} \rangle$$

where $x = (1, T^2)$ and $y = (0, T)$. Indeed, $y^2 = x^3 = (0, T^2) = (0, T^2)$, and as $(0, T^2)(0, T^2) = (0, 1)$, it means $x^6 = y^4 = 1$. Finally,

$$yxy^{-1} = (0, T)(1, T^2)(0, T)^{-1} = (0 - 1, T^3)(0, T^3) = (-1, T^2) = x^{-1}.$$

Example 14 *Extensions of* $\mathbb{Z}_3$ *by* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let us replace $\mathbb{Z}_2 \times \mathbb{Z}_2$ with the isomorphic group $V = \{1, R, S, RS\}$,, the Klein 4-group generated by T and S, as in Example 11. We consider the extension

$$0 \longrightarrow \mathbb{Z}_3 \xrightarrow{\iota} E \xrightarrow{\pi} V \longrightarrow 0.$$

The group action is determined by the homomorphism $\varphi : V \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$. The non-trivial automorphism here is multiplication by -1 (or 2, equivalently), which has order 2. Both the generators T and S, are of order 2, so they can both act either as multiplication by 1 or -1, independently of each other. This means we have the following four cases:

1. $T \mapsto 1$, $S \mapsto 1$;
2. $T \mapsto 1$, $S \mapsto -1$;

3. $T \mapsto -1$, $S \mapsto 1$;

4. $T \mapsto -1$, $S \mapsto -1$.

By symmetry, the third case is equivalent the second simply by swapping the generators. Less obviously, the fourth case is also equivalent to the previous two, since $TS \mapsto (-1)(-1) = 1$, i.e. TS acts trivially. So, by simply considering TS and S to be two generators of V, this case is also equivalent to the second one. Therefore, we have two distinct cases: when V acts trivially on $\mathbb{Z}_3$, and when one non-trivial element acts trivially while the other two act as multiplication by -1.

Case 1: V acts trivially on $\mathbb{Z}_3$, i.e. $T \cdot a = S \cdot a = a$, for all $a \in \mathbb{Z}_3$. The extensions are determined by $H^2(V, \mathbb{Z}_3)$, which we calculated in Example 12:

$$H^2(V, \mathbb{Z}_3) = \mathrm{T}_{\mathbb{Z}_3}(2) \oplus \left(\frac{\mathbb{Z}_3}{2\mathbb{Z}_3}\right)^2 \cong 0 \oplus 0^2 \cong 0.$$

Thus, there is only one extension, $E = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$.

Case 2: $T \cdot a = a$ and $S \cdot a = -a$, for all $a \in \mathbb{Z}_3$. In Example 12 we portrayed the resolution and boundary maps d^* for the general case. Let us substitute T and S into d^2 and d^3 as is needed for this example:

$$d^2 = \begin{pmatrix} S+1 & 0 \\ T-1 & -S+1 \\ 0 & T+1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -2 \\ 0 & 2 \end{pmatrix},$$

$$d^2 = \begin{pmatrix} S-1 & 0 & 0 \\ T-1 & -S-1 & 0 \\ 0 & T+1 & S-1 \\ 0 & 0 & T-1 \end{pmatrix} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now, we can easily calculate

$$\begin{aligned} \ker d^3 &= \{(x, y, z) \in \mathbb{Z}_3^3 \mid -2x = 0,\ 2y - 2z = 0\} \\ &= \{(x, y, z) \in \mathbb{Z}_3^3 \mid 2x = 0,\ y = z\} \\ &= \mathrm{T}_{\mathbb{Z}_3}(2) \oplus (1, 1)\mathbb{Z}_3, \end{aligned}$$

$$\begin{aligned} \operatorname{im} d^2 &= \{d^2(a, b) \mid a, b \in \mathbb{Z}_3\} \\ &= \{(0, 2b, 2b) \mid b \in \mathbb{Z}_3\} \\ &= 0 \oplus (1, 1)\mathbb{Z}_3. \end{aligned}$$

Hence, we get

$$H^2(\mathbb{Z}_3, V) = \frac{\ker d^3}{\operatorname{im} d^2} \cong \frac{0 \oplus (1, 1)\mathbb{Z}_3}{0 \oplus (1, 1)\mathbb{Z}_3} \cong 0,$$

and so, once again, there is only one possible extension, which corresponds to the trivial cohomology class.

The composition law for the trivial factor system is given for all $a, b \in \mathbb{Z}_3$ and $g, h \in V$ by

$$(a, g)(b, h) = (a + g \cdot b, gh).$$

We see that the element $(1, S)$ is of order 6, hence it generates a subgroup of order 6. The element $(0, T)$ is of order 2, and acts on $(1, S)$ by conjugation as

$$(0, T)(1, S)(0, T) = (0, T)(1, TS) = (2, S) = (1, S)^{-1}.$$

This means that the elements $(1, S)$ and $(0, T)$ form the generators for the dihedral group with 12 elements. Therefore, $E \cong \mathbb{D}_6$.

Example 15 *Extensions of* $\mathbb{Z}_4$ *by* $\mathbb{Z}_3$.

$$0 \longrightarrow \mathbb{Z}_4 \xrightarrow{\iota} E \xrightarrow{\pi} C_3^T \longrightarrow 0.$$

The action is determined by a mapping $C_3^T \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, so as T must map to an element of order dividing 3, the action must be trivial. Now, $\mathbb{Z}_4^{\mathbb{Z}_3} = \mathbb{Z}_4$, and

$$N\mathbb{Z}_4 = (1 + T + T^2)\mathbb{Z}_4 = (1 + 1 + 1)\mathbb{Z}_4 = 3\mathbb{Z}_4 = \mathbb{Z}_4,$$

thus

$$H^2(\mathbb{Z}_3, \mathbb{Z}_4) = \frac{\mathbb{Z}_4^{\mathbb{Z}_3}}{N\mathbb{Z}_4} = \frac{\mathbb{Z}_4}{\mathbb{Z}_4} \cong 0.$$

Our extension is then $\mathbb{Z}_4 \times \mathbb{Z}_3$.

Example 16 *Extensions of* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *by* $\mathbb{Z}_3$.

$$0 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} C_3^T \longrightarrow 0.$$

Denote $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$ where $V = \{1, R, S, RS\}$ is, again, the Klein 4-group generated by T and S. The action is determined by a mapping $C_3^T \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$, so as T must map to an element of order dividing 3, the action must be trivial or a 3-cycle.

Let the action be trivial. Here, $A^{\mathbb{Z}_3} = A$, and

$$NA = (1 + T + T^2)A = (1 + 1 + 1)A = 3A = A,$$

thus

$$H^2(\mathbb{Z}_3, A) = \frac{A^{\mathbb{Z}_3}}{NA} = \frac{A}{A} \cong 0.$$

Our extension is then $A \times \mathbb{Z}_3$.

Now, let us consider the non-trivial action of C_3^T on $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Let us label the elements of A; $e = (0,0)$, $a = (0,1)$, $b = (1,0)$ and $c = (1,1)$, and use multiplicative notation for the group operation of A. T acts on A as a 3-cycle, so without loss of generality, let us assume that T corresponds to the 3-cycle $(a\ b\ c)$, i.e. $T \cdot a = b$, $T \cdot b = c$, and $T \cdot c = a$. Now, we can calculate $A^G = \{e\}$, and

$$NA = (1 + T + T^2)A = \{eee,\ abc\} = \{e\}.$$

Thus,

$$H^2(A, G) = \frac{A^G}{NA} = \frac{0}{0} \cong 0,$$

which means we only have one extension. The composition law on this extension E is thus defined as

$$(x, g)(y, h) = (x(g \cdot h), gh),$$

for all $x, y \in A$ and $g, h \in G$. Let us note that

$$(e, g)(x, 1)(e, g)^{-1} = (e, g)(x, g^2) = (g \cdot x, 1),$$

for all $x \in A$ and $g \in G$. Hence, (e, T) and $(a, 1)$ generate all of E.

The group A can act on itself by multiplication. This gives us the embedding $A \hookrightarrow \mathrm{Sym}(A)$ given by $a \mapsto \sigma_a = (e\ a)(b\ c)$, $b \mapsto \sigma_b = (e\ b)(a\ c)$ and $c \mapsto \sigma_c = (e\ c)(a\ b)$. Similarly, the action of G on A can be interpreted as the embedding $G \hookrightarrow \mathrm{Sym}(A)$ given by $T \mapsto \tau = (a\ b\ c)$. This means we can embed E by treating the element (x, g) as the composition of x and g. Indeed, as $(e, T)(a, 1)(e, T)^{-1}$ maps to

$$\tau(e\ a)(b\ c)\tau^{-1} = (e\ \tau(a))(\tau(b)\ \tau(c)) = \sigma_{\tau(a)} = \sigma_{T \cdot a} = \sigma_b,$$

we have that $(e, T)(a, 1)(e, T)^{-1} = (b, 1)$. Thus, the embedding is well defined. The image of the embedding is generated by the double transposition σ_a and the 3-cycle τ, hence it is isomorphic to the alternating group $\mathbb{A}_4$.

Therefore, we have shown that the extension in this case corresponds to the alternating group $\mathbb{A}_4$.

We have now found all the groups of order 12, up to isomorphism of course. They are:

$$\mathbb{Z}_{12},\ \mathbb{Z}_2 \otimes \mathbb{Z}_6,\ \mathbb{D}_6,\ \mathbb{A}_4,\ \mathrm{Dic}_3.$$

However, groups of order 12 can be viewed as group extensions in other ways, not just as the extension of $\mathbb{Z}_3$ by a group of order 4 and vice versa. For completion's sake, let us cover the remaining such examples. A group of order 12 can have subgroups of order 2, 3, 4, and 6. Thus, a group of order 12 can be portrayed as the extension of an abelian group A by a group G in the following ways:

- $\mathbb{Z}_2$ by $\mathbb{Z}_6$ or $\mathbb{D}_3$;
- $\mathbb{Z}_3$ by $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_3$;
- $\mathbb{Z}_6$ by $\mathbb{Z}_2$.

We will cover the remaining cases in the examples that follow.

Example 17 *Extensions of* $\mathbb{Z}_6$ *by* $\mathbb{Z}_2$.

$$0 \longrightarrow \mathbb{Z}_6 \xrightarrow{\iota} E \xrightarrow{\pi} C_2^T \longrightarrow 0.$$

The action is determined by a mapping $C_2^T \to \mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$, so as T must map to an element of order dividing 2, we have either $T \cdot a = a$ or $T \cdot a = -a$.

Let $T \cdot a = a$. Now,

$$\mathbb{Z}_6^{\mathbb{Z}_2} = \mathbb{Z}_6$$

and

$$N\mathbb{Z}_6 = (1+T)\mathbb{Z}_6 = (1+1)\mathbb{Z}_6 = 2\mathbb{Z}_6$$

thus

$$H^2(\mathbb{Z}_2, \mathbb{Z}_6) = \frac{\mathbb{Z}_6^{\mathbb{Z}_2}}{N\mathbb{Z}_6} = \frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \cong \mathbb{Z}_2.$$

The extensions are $\mathbb{Z}_6 \times \mathbb{Z}_2$ and $\mathbb{Z}_{12}$, analogously to Example 7.

Let $T \cdot a = -a$. Now, the only fixed elements are 0 and 3.

$$\mathbb{Z}_6^{\mathbb{Z}_2} = \{0, 3\}$$

and

$$N\mathbb{Z}_3 = (1-T)\mathbb{Z}_6 = (1-1)\mathbb{Z}_6 = \{0\}$$

thus

$$H^2(\mathbb{Z}_2, \mathbb{Z}_6) = \frac{\mathbb{Z}_6^{\mathbb{Z}_2}}{N\mathbb{Z}_6} = \frac{\{0, 3\}}{\{0\}} \cong \mathbb{Z}_2.$$

As we calculated in Examples 7 and 8, the factor system is 0 everywhere except at $f(T, T)$, where we have $2f(T, T) = 0$, so $f(T, T) = 0$, which corresponds to the extension $\mathbb{D}_6$, or $f(T, T) = 3$. Here, we have the composition law determined by the following equations:

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

$$(a,T)(b,T) \;=\; (a-b+3,1).$$

The elements of the form $(a,1)$ generate the normal subgroup isomorphic to $\mathbb{Z}_6$. The elements of the form (a,T) are of order 4, as $(a,T)(a,T)=(3,1)$. We show that this group is isomorphic to the dicyclic group

$$\mathrm{Dic}_3 = \langle a,b \mid a^6=b^4=1,\ b^2=a^3,\ bab^{-1}=a^{-1}\rangle.$$

By setting $a=(1,1)$ and $b=(0,T)$ we see that indeed $a^6=b^4=(0,1)$ and $b^2=a^3=(3,1)$. All that's left is to show the final condition:

$$bab^{-1}=(0,T)(1,1)(0,T)^{-1}=(-1,T)(3,T)=(-1-3+3,1)=(5,1)=a^{-1}.$$

Therefore, all the possible extensions are $\mathbb{Z}_6\times\mathbb{Z}_2$, $\mathbb{Z}_{12}$, $\mathbb{D}_6$ and Dic_3.

Example 18 *Extensions of* $\mathbb{Z}_2$ *by* $\mathbb{Z}_6$.

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } C_6^T \longrightarrow 0.$$

The action is determined by a mapping $C_6^T \to \mathrm{Aut}(\mathbb{Z}_2)\cong 0$, so the G-action is trivial i.e. $T\cdot a=a$. Thus, $\mathbb{Z}_2^{\mathbb{Z}_6}=\mathbb{Z}_2$, and

$$N\mathbb{Z}_2=(1+T+T^2+T^3+T^4+T^5)\mathbb{Z}_2=6\mathbb{Z}_2=0,$$

hence

$$H^2(\mathbb{Z}_6,\mathbb{Z}_2)=\frac{\mathbb{Z}_2^{\mathbb{Z}_6}}{N\mathbb{Z}_2}=\frac{\mathbb{Z}_2}{0}\cong\mathbb{Z}_2.$$

The two extensions are $\mathbb{Z}_2\times\mathbb{Z}_6$ and $\mathbb{Z}_{12}$.

Example 19 *Extensions of* $\mathbb{Z}_2$ *by* $\mathbb{D}_3$.

Let $\mathbb{D}_3=\langle T,S \mid T^3=S^2=1,\ STS=T^{-1}\rangle$.

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } \mathbb{D}_3 \longrightarrow 0.$$

The action is determined by a mapping $\mathbb{D}_3 \to \mathrm{Aut}(\mathbb{Z}_2)\cong 0$, so the G-action is trivial i.e. $T\cdot a=S\cdot a=a$.

By Example 10, we can compute the second cohomology group:

$$H^2(\mathbb{Z}_2,\mathbb{D}_3)=\frac{\mathbb{Z}_2}{2\mathbb{Z}_2}=\frac{\mathbb{Z}_2}{0}\cong\mathbb{Z}_2.$$

Thus, we have two cases. By Lemma 27, the extension corresponding to the trivial cohomology class is $\mathbb{Z}_2 \times \mathbb{D}_3 \cong \mathbb{D}_6$. Let us consider the non-trivial case. Here, the formula for the factor system is

$$f(h,k) + f(gh,k) + f(g,hk) + f(g,h) = 0. \tag{7}$$

Let us define a non-trivial factor system the following way: $f(s^i r^a, s^j r^b) = ij$, for all $s^i r^a, s^j r^b \in \mathbb{D}_3$. Indeed, (7) becomes $jk + (i+j)k + i(j+k) + ij = 0$, which is true for all $i, j, k \in \mathbb{Z}_2$.

This group is isomorphic to the dicyclic group

$$\mathrm{Dic}_3 = \langle x, y \mid x^6 = y^4 = 1,\ y^2 = x^3,\ yxy^{-1} = x^{-1} \rangle$$

where $x = (1, r)$ and $y = (0, s)$. Indeed, $y^2 = x^3 = (1,1)$, and as $(1,1)(1,1) = (0,1)$, it means $x^6 = y^4 = 1$. Finally,

$$yxy^{-1} = (0,s)(1,r)(0,s)^{-1} = (1,sr)(1,s) = (1,srs) = (1,r^{-1}) = x^{-1}.$$

Hence, the extensions in this example are $\mathbb{D}_6$ and Dic_3.

6.5 Application to p-groups with a Cyclic Subgroup of Index p

The aim of this section is to utilise the application of group cohomology to group extensions to give a classification of p-groups which contain a cyclic subgroup of index p, where p is a prime. Of course, it is a classic result that such a subgroup is normal. We will be splitting our attention to the cases where $p > 2$ and when $p = 2$.

Theorem 31 *Let p be a prime number greater than 2. All finite p-groups with a cyclic subgroup of index p fall into one of the following categories:*

(A) $\mathbb{Z}_q$, *where* $q = p^n$ *and* $n \geq 1$,

(B) $\mathbb{Z}_q \times \mathbb{Z}_p$, *where* $q = p^n$ *and* $n \geq 1$,

(C) $\mathbb{Z}_q \rtimes \mathbb{Z}_p$, *where* $q = p^n$ *and* $n \geq 2$, *where the generator of* $\mathbb{Z}_p$ *acts on* $\mathbb{Z}_q$ *as multiplication by* $1 + p^{n-1}$.

Note that the third category makes sense as $(1 + p^{n-1})^p \equiv 1 \mod p^n$ by the binomial theorem. Let us first prove a lemma that will help us in the proof.

Lemma 32 *Let p be a prime number and a be an integer such that $a^p \equiv 1 \mod p^n$ for some $n \geq 2$. If $p \geq 3$ then $a \equiv 1 \mod p^{n-1}$. If $p = 2$ then $a \equiv \pm 1 \mod 2^{n-1}$.*

Proof: Supposing $a \neq 1$, let us denote by $d(a)$ the largest integer such that $a^p \equiv 1 \mod p^{d(a)}$. By Fermat's little theorem, $a \equiv a^p \equiv 1 \mod p$, so $d(a) \geq 1$. We can write $a = 1 + bp^{d(a)}$. Now, let us apply the binomial expansion to a^p:

$$\begin{aligned} a^p &= (1 + bp^{d(a)})^p \\ &= \sum_{k=0}^{p} \binom{p}{k} b^k p^{d(a)k} \\ &\equiv 1 \mod p^{d(a)+1}, \end{aligned}$$

as $p|\binom{p}{k}$ for $k \geq 1$. Thus, $d(a^p) = d(a) + 1$, However, we assumed that $a^p \equiv 1 \mod p^n$, so $d(a^p) \geq n$. Hence, $d(a) \geq n - 1$, i.e. $a \equiv 1 \mod p^{n-1}$.

Proof of Theorem 31:

Suppose the cyclic subgroup of G is of order $q = p^n$. Thus, G is an extension of $\mathbb{Z}_q$ by $H = C_p^T$:

$$0 \longrightarrow \mathbb{Z}_q \longrightarrow G \longrightarrow H \longrightarrow 1.$$

Suppose H acts trivially on $\mathbb{Z}_q$. Then, for the factor system f, we have

$$f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0.$$

Substituting $g_1 = g_2 = g_3 = g$ we get $f(g, g^2) = f(g^2, g)$. Thus, by induction (substitute $g_1 = g_3 = g$ and $g_2 = g^{k-1}$) we get that $f(g, g^k) = f(g^k, g)$. For arbitrary $g = T^a$ and $h = T^b$ in H, let $k = a^{-1}b$, where a^{-1} is the multiplicative inverse of a in the field of p elements. Now, $h = g^k$, and thus $f(g, h) = f(h, g)$, which we can use in the composition law:

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

Thus, G is an abelian group. This such can only be either $\mathbb{Z}_{p^{n+1}}$ or $\mathbb{Z}_q \times \mathbb{Z}_p$, so G is of type (A) or (B).

Now, let us consider when the action of H on $\mathbb{Z}_q$ is nontrivial, and use Example 5 to calculate $H^2(H, \mathbb{Z}_q)$. The action of an element $h \in H$ is determined by how it acts on the generator $1 \in \mathbb{Z}_q$, acting as multiplication by the result of this action, i.e. $h \cdot a = (h \cdot 1)a$ for all $a \in \mathbb{Z}_q$. As a generator must be sent to another generator, this means the action of H on $\mathbb{Z}_q$ is given by an embedding $\varphi : H \hookrightarrow \mathbb{Z}_q^*$, where $\mathbb{Z}_q^*$ is the group of units of the ring $\mathbb{Z}_q = \mathbb{Z}/p^n\mathbb{Z}$. As each non-trivial element of H is of order p, the image of the embedding must be the subset of elements of the form

$$\operatorname{im} \varphi = \{1 + kp^{n-1} : \ 1 \leq k \leq p - 1\} = \{1 + b : \ b \in p^{n-1}\mathbb{Z}_q\} \subseteq \mathbb{Z}_q.$$

Thus, one of the elements of H, say h, acts as $1+p^{n-1}$, as in (C). As every element of H is a generator of H, this means $\mathbb{Z}_q^H = \mathbb{Z}_q^h$, so, an element x is fixed if $h \cdot x = x$, i.e. $(1+p^{n-1})h \cdot x = x$, i.e.

$$\mathbb{Z}_q^H = \{x \in \mathbb{Z}_q : \ p^{n-1} \cdot x = 0\} = p\mathbb{Z}_q.$$

On the other hand, the norm operator acts as multiplication by

$$N = \sum_{i \in \operatorname{im} \varphi} i = \sum_{k=0}^{p-1} (1 + kp^{n-1}) = p + p^{n-1} \sum_{k=0}^{p-1} k = p + p^{n-1} \frac{p(p-1)}{2} = p + \frac{p-1}{2} p^n.$$

However, $\sum_{k=0}^{p-1} 1 = p$, and

$$\sum_{k=0}^{p-1} kp^{n-1} = p^{n-1} \sum_{k=0}^{p-1} k = p^{n-1} \frac{p(p-1)}{2} = \frac{p-1}{2} p^n,$$

which is congruent to 0 as p is odd, so $p | \frac{p(p-1)}{2}$. Thus, the norm operator acts as multiplication by $N = p$, and so $N\mathbb{Z}_q = p\mathbb{Z}_q$. Therefore,

$$H^2(H, \mathbb{Z}_q) = \frac{\mathbb{Z}_q^H}{N\mathbb{Z}_q} = \frac{p\mathbb{Z}_q}{p\mathbb{Z}_q} = 0.$$

By Lemma 28, we have that the extension is isomorphic to $\mathbb{Z}_q \rtimes_\varphi H$, with composition determined by the action of the generator on H, which we established acts by multiplication by $1 + p^{n-1}$. This is category (C). □

When it comes to the case for $p = 2$, we have a few more categories of possible 2-groups with cyclic subgroup of index 2, alongside the categories (A), (B), and (C) already listed. They are as follows:

(D) Dihedral 2-groups: $D_{2m} = \mathbb{Z}_m \rtimes \mathbb{Z}_2$, where the generator of $\mathbb{Z}_2$ acts on $\mathbb{Z}_m$ as multiplication by -1. We are considering the case when $m = q = 2^n$ for some $n \geq 2$.

(E) Generalized quaternions 2-groups: Q_{4m} is defined to be the multiplicative subgroup of the quaternion algebra $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ generated by $x = e^{\pi i/m}$ and $y = j$. We see that x is of order $2m$ and $yxy^{-1} = x^{-1}$, hence the cyclic subgroup generated by x is normal and of index 2. This means Q_{4m} is of order $4m$, so we take m to be a power of 2 so that Q_{4m} is indeed a 2-group with cyclic subgroup of index 2.

(F) $\mathbb{Z}_q \rtimes \mathbb{Z}_2$, where $q = 2^n$ and $n \geq 2$, where the generator of $\mathbb{Z}_2$ acts on $\mathbb{Z}_q$ as multiplication by $-1 + p^{n-1}$.

We show that this list is complete.

Theorem 33 *If G is a 2-group with a cyclic subgroup of index 2, then G is isomorphic to one of the groups of the above categories (A)-(F).*

Proof: Our proof starts the same as in the proof of Theorem 31. We consider the extension

$$0 \longrightarrow \mathbb{Z}_q \longrightarrow G \longrightarrow H \longrightarrow 1.$$

where $q = 2^n$ for some n and $H = C_2^T$. If H acts trivially on $\mathbb{Z}_q$, then G is of type (A) or (B). If H acts non-trivially, then we calculate $H^2(H, \mathbb{Z}_q)$. The action of H on $\mathbb{Z}_q$ is given by an embedding $\varphi : H \hookrightarrow \mathbb{Z}_q^*$, from H to the group of units of $\mathbb{Z}_q$. Now, like in the previous theorem, we will use Lemma 32, however the result is different for $p = 2$ compared to odd p. Here we have that the image of the embedding is $\{\pm 1 + b : \ b \in 2^{n-1}\mathbb{Z}_q\} = \{1, 1 + 2^{n-1}, -1, -1 + 2^{n-1}\}$. Thus, we have three non-trivial possibilities for the image $a \in \mathbb{Z}_q^*$ of the generator of H:

Case 1: $a = 1 + 2^{n-1}$. Similarly to the last proof, $\mathbb{Z}_q^H = 2\mathbb{Z}_q$ and the norm operator is multiplication by $N = 1 + a = 2 + 2^{n-1} = 2(1 + 2^{n-2})$. If $n = 2$, then $q = 4$ and $a = 1 + 2 = 3 \equiv -1$, which is equivalent to the next case we will cover. Assume $n \geq 3$, Now, $1 + 2^{n-2} \in \mathbb{Z}_q^*$, and so $N\mathbb{Z}_q = 2\mathbb{Z}_q$. Therefore, we have

$$H^2(H, \mathbb{Z}_q) = \frac{2\mathbb{Z}_q}{2\mathbb{Z}_q} \cong 0,$$

hence, by Lemma 28, the extension splits and is of type (C).

Case 2: $a = -1$. In this case $\mathbb{Z}_q^H = 2^{n-1}\mathbb{Z}_q$ and the norm operator is $N = 1 + a = 1 - 1 = 0$, so

$$H^2(H, \mathbb{Z}_q) = \frac{\mathbb{Z}_q^H}{N\mathbb{Z}_q} = \frac{2^{n-1}\mathbb{Z}_{2^n}}{0} \cong \mathbb{Z}_2.$$

Thus, there are exactly two inequivalent extensions corresponding to this action of H on $\mathbb{Z}_q$, so they must be of types (D), corresponding to the trivial cohomology class, and (E) for the non-trivial class (note y indeed acts on x as -1).

Case 3: $a = -1 + 2^{n-1}$. We consider $n \geq 3$, as for $n = 2$ we have $a = -1 + 2 = 1$. Here we have $\mathbb{Z}_q^H = 2^{n-1}\mathbb{Z}_q$ and the norm operator is multiplication by $N = 1 + a = 2^{n-1}$. Thus,

$$H^2(H, \mathbb{Z}_q) = \frac{2^{n-1}\mathbb{Z}_q}{2^{n-1}\mathbb{Z}_q} \cong 0,$$

hence by Lemma 28, the extension splits and is of type (F). $\square$

Biography

Alexander Sean Collins was born in Dublin, Ireland, on the 25th of January, 1999. When he was two years old, his family moved to Brisbane, Australia, where he grew up. In 2012, right after he finished primary school, they moved again to Belgrade, Serbia, where he attended the Mathematical Grammar School. After finishing high school, he went to the University of Cambridge to study Mathematics, where he was awarded his Bachelor's degree. He went to Corpus Christi College, where his director of studies was Dr Christopher Brookes. During the Covid-19 era, he moved back to Belgrade to continue his Master's level studies. He also worked here as a teaching assistant. During his last year at Cambridge, and furthermore during his Master's programme in Belgrade, under the supervision of Dr Zoran Petrović, he developed an interest in subjects such as algebraic topology, differential geometry, homological algebra, and other similar, pure mathematical topics. He wishes to continue working in these areas.

7 Bibliography

1. K. S. Brown *Cohomology of Groups* - Springer-Verlag 1982;

2. Henri Cartan and Samuel Eilenberg *Homological Algebra* - Princeton University Press, 1956;

3. George E. Cooke and Ross L. Finney *Homology of Cell Complexes* - Princeton University Press, 1967;

4. Samuel Eilenberg and Saunders Maclane *Eilenberg-Mac Lane: Collected Works* - Academic Press Inc, 1986;

5. Serge Lang *Algebra* - Springer-Verlag 2002;

6. Saunders Maclane *Homology* - Springer-Verlag 1963;

7. C. B. Thomas *Characteristic Classes and the Cohomology of Finite Groups* - Cambridge University Press 1986;

8. Charles A. Weibel, *An Introduction to Homological Algebra* - Cambridge University Press 1994;

9. Charles A. Weibel, *History of Topology* - Cambridge University Press 1999.