SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Helena Schill

PROŠIRENJA GRUPA

Diplomski rad

Voditelj rada:
Izv. prof. dr. Ozren Perše

Zagreb, rujan,2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Sadržaj **iii**

Uvod **1**

1 Grupe, prsteni, moduli **2**

2 Semidirektan produkt **9**

3 Generalne ekstenzije i kohomologija **16**

Bibliografija **31**

Uvod

Algebra je grana matematike koju koriste svi matematičari, bez obzira koje im je područje istraživanja, od analize, kombinatorike, geometrije, logike itd. Svi se slažu da je znanje iz linearne algebre, grupa i komutativnih prstenova nužno. U svom najopćenitijem obliku, algebra je proučavanje matematičkih simbola i pravila kojima vršimo operacije s tim simbolima. Korijeni algebre sežu do antičkih Babilonaca a njome su se bavili i Grci, Egipćani, Kinezi te Perzijanci. Međutim, algebra se kao grana matematike pojavljuje krajem 16. stoljeća u Europi radovima Francoisa Viètea. Prva proučavanja grupa javljaju se u radovima Lagrangea u kasnom 18. stoljeću, međutim početkom teorije grupa smatraju se radovi Cauchya i Galoisa 1846. godine. U periodu od 1870. do 1900. uvelike se razvila teorija grupa zbog Sylowljevih teorema, Hölderove klasifikacije grupa te početaka Frobeniusove teorije simbola. Teorija grupa se nastavila produbljivati i proširivati sa pojmovima algebarskih grupa i ekstenzija grupa što je i tema ovog rada. Opišimo ukratko sadržaj ovog rada.
U prvom poglavlju navodimo osnovne definicije koje se koriste u radu kao što su grupa, podgrupa, homomorfizam grupa, normalna podgrupa, kvocijentna grupa, direktan produkt, prsten, komutativni prsten, grupni prsten. Navodimo i sva tri Sylowljeva teorema.
Drugo poglavlje se bavi semidirektnim produktom. U njemu uvodimo pojam proširenja grupe kao kratkog egzaktnog niza i funkcije podizanja kao i samog semidirektnog produkta kao srednje grupe u razvojenoj ekstenziji.
U trećem poglavlju dolazimo do najbitnih rezultata rada. Ono se bavi generalnim ekstenzijama i kohomologijom. Proučavamo kako za dane dvije grupe Q i K naći sva proširenja G od K po Q. Za to će nam biti potrebna funkcija kociklus koju definiramo pomoću podizanja definiranog u prethodnom poglavlju. Isto tako definiramo i funkciju korub te drugu grupu kohomologije. Glavni rezultat je Schreierov teorem koji riješava problem proširenja koristeći kocikluse. Drugi bitan rezultat ovog rada je Schur-Zassenhausova lema.

Poglavlje 1

Grupe, prsteni, moduli

Grupa je kao algebarska struktura jedan od osnovnih pojmova u matematici. Definicija grupe je:

Definicija 1.1. *Neprazan skup $G = (G, \cdot)$ gdje je $\cdot : G \times G \to G$ binarna operacija, zove se grupa ako vrijede sljedeća svojstva (aksiomi grupe):*

1. *asocijativnost* $(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad \forall x, y, z \in G$
2. *neutralni element* $(\exists e \in G) : e \cdot x = x \cdot e = x \quad \forall x \in G$
3. *inverzni element* $(\forall x \in G)(\exists x^{-1} \in G) : x \cdot x^{-}1 = x^{-1} \cdot x = e.$

Element e ili e_G nazivamo neutralni element grupe (neutral grupe), a inverzni element za zadani $x \in G$ je element $x^{-1} \in G$ koji zadovoljava treće svojstvo.

Lema 1.2. *Neka je G grupa, tada vrijedi:*

1. *Ako je $x \cdot a = x \cdot b$ ili $a \cdot x = b \cdot x$, tada je $a = b$.*
2. *Neutralni element $e \in G$ je jedinstven.*
3. *Svaki $x \in G$ ima jedinstveni inverz, postoji samo jedan element $x^{-1} \in G$ takav da je $e = x \cdot x^{-1} = x^{-1} \cdot x$.*
4. $(x^{-1})^{-1} = x \qquad \forall x \in G.$

Komutativna grupa G je ona za koju vrijedi (uz osnovna tri svojstva iz definicije) i svojstvo: $x \cdot y = y \cdot x \qquad \forall x, y \in G$.
Komutativna grupa se još naziva i **Abelova**, a grupa koja nije komutativna se naziva nekomutativna ili ne-Abelova. **Grupoid** je skup G na kojemu je definirana operacija $\cdot : G \times G \to G$ (za bilo koje $x, y \in G$ je i $x \cdot y \in G$). **Poulugrupa** je grupoid za kojeg vrijedi i asocijativnost. Polugrupa koja ima jedistven neutralni element se zove **monoid**.

Definicija 1.3. ***Kompleks*** *je proizvoljan podskup $A \subseteq G$, G grupa.*

Produkt kompleksa $A, B \subseteq G$ definiramo kao:

$$AB := \{ab \mid a \in A \quad \& \quad b \in B\}.$$

Podgrupa od G je kompleks $H \subseteq G$ za koji vrijede uvjeti:

1. $(\forall x, y \in H) : \qquad x \cdot y \in H$
2. $(\forall x \in H) : \qquad x^{-1} \in H$

H je podgrupa od G označavamo sa $H \leq G$.

Propozicija 1.4. *Kompleks H je podgrupa grupe G ako vrijedi uvjet:*
$(\forall x, y \in H) \qquad xy^{-1} \in H.$

Prethodna propozicija se naziva i kriterij podgrupe. Kriterij po kojem razlučujemo konačne i beskonačne grupe je red kojeg definiramo na sljedeći način:

Definicija 1.5. ***Red grupe*** *G u oznaci $|G|$ je kardinalni broj skupa G.*

Grupa je konačna ako je $|G| < \infty$ a inače je beskonačna. Sada ćemo definirati preslikavanja među grupama, tj. na koji način se povezuju grupe kao objekti.

Definicija 1.6. *Neka su H, G grupe. Preslikavanje $f : G \to H$ je* ***homomorfizam grupa*** *ako vrijedi*

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G.$$

Skup svih homomorfizama iz G u H označavamo sa $Hom(G, H)$. Monomorfizam je homomorfizam f koji je i injekcija. Epimorfizam je homomorfizam f koji je i surjekcija. Izomorfizam je homomorfizam f koji je bijektivan, tj. i epimorfizam i monomorfizam.
Grupe su izomorfne ako postoji izomorfizam među njima. Neka su G i H dvije izomorfne grupe, to označavamo sa $G \cong H$. Tako se definira relacija $\cong$, relacija "izomorfizam grupa".

Propozicija 1.7. *Izomorfizam grupa je relacija ekvivalencije.*

Endomorfizam f je kada imamo jednakost $G = H$, odnosno homomorfizam $f : G \to G$. Skup svih endomorfizama od G je $EndG$. Automorfizam je bijektivni endomorfizam, a skup svih automorfizama od G je $AutG$.
Jezgra homomorfizma $f : G \to H$ je $Kerf := \{x \in G \mid f(x) = e_H\}$. A slika $Imf := \{f(x) \mid x \in G\}$.

Lema 1.8. *Za homomorfizme grupa $f : G \to H$ i $g : H \to K$ je i njihova kompozicija $g \circ f : G \to K$ homomorfizam grupa. Ako su f i g oba izomorfizmi(ili epimorfizmi, monomorfizmi) onda je i njihova kompozicija izomorfizam(epimorfizam, monomorfizam).*

Za elemente $x, y \in G$ za koje postoji $a \in G$ takav da je $y = axa^{-1}$, kažemo da su **G-konjugirani ili konjugirani u grupi** G.

Lema 1.9. *Neka je G grupa i $\{H_i \mid i \in I\}$ neke njene podgrupe. Tada je podgrupa od G i njihov presjek $\bigcap_{i \in I} H_i$.*

Definicija 1.10. *Neka je S proizvoljan podskup grupe G, definiramo:*

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

S se zove skup generatora, podgrupa iz definicije se naziva grupa generirana sa S. Ako postoji konačan podskup $S = \{x_1, ..., x_n\}$ takav da je $G = \langle S \rangle$, G je konačnogenerirana grupa i $G = \langle x_1, ..., x_n \rangle$. Ako se G može generirati jednim elementom ($\exists g \in G$ takav da je $G = \langle g \rangle$) ona je **cikličk**a, a g se naziva generatorom cikličke grupa G.
Definirajmo relaciju ekvivalencije $\sim$ na $G \times G$ gdje je G neka grupa i $H \leq G$ sa

$$x, y \in G \qquad x \sim y \quad \Leftrightarrow \quad xH = yH \quad \Leftrightarrow \quad y^{-1}x \in H$$

$$(\Leftrightarrow \quad Hx = Hy \Leftrightarrow \quad x^{-1}y \in H).$$

Grupa G je disjunktna unija svih svojih klasa ekvivalencije u odnosu na relaciju $\sim$.

Definicija 1.11. *Sa xH (odnosno Hx) označavamo klase na koje dijeli grupu G relacija ekvivalencije $\sim$ i zovemo ih lijeve(odnosno desne) klase od G po $\sim$. Skup svih klasa $G/\sim$ označavamo G/H (odnosno $H\backslash G$).*

Indeks od G po H se definira kao $|G/H|$ za $|G/H| < \infty$ i označavamo ga s $[G : H]$.

Teorem 1.12. *(Lagrange) Neka je G konačna grupa i H neka njena podgrupa. Red grupe G djeljiv je redom podgrupe H. Preciznije, vrijedi $|G| = |H|[G : H]$.*

Normalna podgrupa grupe G je podgrupa N za koju vrijedi $Nc = cN$ za svaki $c \in G$. Ako danu jednakost pomnožimo zdesna sa c^{-1} dobijemo $N = cNc^{-1}$ što nas vodi do sljedeće definicije.

Definicija 1.13. *Podgrupa $N \leq G$ grupe G je **normalna podgrupa** ako vrijedi*

$$xNx^{-1} = N \qquad \text{za svaki } x \in G.$$

Činjenicu da je N normalna podgrupa od G zapisujemo kao $N \lhd G$.

Objasnimo pojam **kvocijentne grupe**. Neka je sa G/N označen skup svih N-klasa u G (N normalna podgrupa grupe G). Uvedimo binarnu operaciju:

$$(aN)(bN) = abN, \qquad aN, bN \in G/N \quad \text{tj. } a, b \in G$$

gdje abN ne ovisi o a, b kao predstavnicima dvije N-klase (jer je N normalna podgrupa). Skup N-klasa G/N uz prethodno definiranu binarnu operaciju postaje grupa. U toj grupi neutralni element je $N = eN$, a inverzni element za neki aN je $a^{-1}N$. Grupa G/H je kvocijentna grupa grupe G po N. Preslikavanje

$$\pi = \pi_N : G \to G/N \qquad x \longmapsto xN$$

je epimorfizam grupa a jezgra mu je N i π se zove **kanonski epimorfizam** (kanonska surjekcija).

Propozicija 1.14. *Neka su N_i normalne podgrupe od G $\forall\, i \in I$,tj. $N_i \lhd G$ $\forall i \in I$. Tada je normalna podgrupa od G i presjek svih takvih podgrupa, tj.*

$$\bigcap_I N_i \qquad \textit{je normalna podgrupa.}$$

Definicija 1.15. ***Centar grupe*** *G označen sa $Z(G)$ je*

$$Z(G) = \{z \in G \ : \ zg = gz \text{ za sve } g \in G\}$$

, tj. $Z(G)$ se sastoji od svih elemenata koju komutiraju sa svime iz G.

Lako je pokazati da je $Z(G)$ podgrupa od G, također to je i normalna podgrupa jer ako je $z \in Z(G)$ i $g \in G$, tada vrijedi $gzg^{-1} = zgg^{-1} = z \in Z(G)$. Grupa je Abelova ako i samo ako je $Z(G) = G$.

Propozicija 1.16. *Za bilo koju grupu G, ako je $H \lhd G$, tada je $Z(H) \lhd G$.*

Definicija 1.17. ***Normalizator*** *grupe H u grupi G je podgrupa $N_G(H) = \{a \in G \ : \ aHa^{-1} = H\}$.*

Ako je H podgrupa konačne grupe G, tada je broj konjugiranih elementa od H u G, $[G \ : \ N_G(H)]$. Očito je $H \lhd N_G(H)$ pa je definirana i kvocijentna grupa $N_G(H)/H$.

Definicija 1.18. *Neka je G grupa i neka su $x, y \in G$ njeni proizvoljni elementi. Njihov* ***komutator*** *je*

$$[x, y] = xyx^{-1}y^{-1} \ \in G.$$

Komutatorska podgrupa *grupe G je podgrupa generirana svim komutatorima elemenata grupe G*

$$C(G) := \langle [x, y] \mid x, y \in G \rangle.$$

Propozicija 1.19. *Neka je G grupa i $C(G)$ njena komutatorska podgrupa, tada je $C(G) \lhd G$ i kvocijentna grupa $G/C(G)$ je komutativna. Ako je $N \lhd G$ takva da je kvocijentna podgrupa G/N komutativna, onda N sadrži $C(G)$.*

Za svaku podgrupu H od G, možemo definirati $C(H)$ kao podgrupu generiranu sa $\langle [h,k] \mid h,k \in H \rangle$ što je skup svih komutatora elemenata iz H.
Definirajmo $C^k(G)$, $k \in \mathbb{N}$:

$$C^1(G) = C(G) \qquad C^k(G) = C(C^{k-1}(G)) \quad k \geq 2.$$

Rješiva grupa G je ona za koju postoji prirodan broj n takav da je $C^n(G) = \{e\}$. Iz ovoga slijedi da je svaka Abelova grupa rješiva ($C^1(G) = C(G) = \{e\}$).
Prosta grupa G je ona grupa koja nema netrivijalne normalne podgrupe, tj. jedine njene normalne podgrupe su $\{e\}$ i G.

Teorem 1.20. *Rješiva grupa G je prosta ako i samo ako je ciklička i njen red $|G|$ je prost broj.*

Napomena 1.21. *Neutralni element u grupi odsada označavamo sa* 1*, odnosno* 0 *umjesto sa e.*

Definicija 1.22. *Neka su H i K grupe. Njihov **direktan produkt**, u oznaci $H \times K$ je skup svih uređenih parova (h,k) gdje je $h \in H$, $k \in K$ zajedno sa operacijom*

$$(h,k)(h',k') = (hh',kk').$$

Lako se vidi da je direktan produkt $H \times K$ grupa (neutralni element je $(1,1)$ a inverz za (h,k) je (h^{-1},k^{-1})).

Propozicija 1.23. *Ako je G grupa koja sadrži normalne podgrupe H i K takve da vrijedi $H \cap K = \{1\}$ i $HK = G$, tada je $G \cong H \times K$.*

Za grupu u kojoj je red svakog elementa oblika p^r, $r \geq 1$ gdje je p fiksiran prost broj; kažemo da je p-grupa. Ako je G grupa i H podgrupa od G koja je p-grupa, kažemo da je H p-podgrupa od G.

Definicija 1.24. *Neka je p prost broj. **Sylowljeva p-podgrupa** konačne grupe G je maksimalna p-podgrupa P.*

Teorem 1.25. *(Prvi Sylowljev teorem) Neka je G konačna grupa reda $p_1^{e_1}, p_2^{e_2}, ..., p_t^{e_t}$ i neka je P Sylowljeva p-podgrupa od G za neki prost $p = p_j$.*

1. *Svaka Sylowljeva p-podgrupa je konjugirana s P.*

2. *Ako postoji r_j Sylowljevih p_j-podgrupa, tada je r_j dijelitelj od $|G|/p_j^{e_j}$ i $r_j \equiv 1$ mod p_j.*

Teorem 1.26. *(Drugi Sylowljev teorem) Ako je G je konačna grupa reda $p^e m$, gdje je p prost i $p \nmid m$, tada je svaka Sylowljeva p-podgrupa P od G reda p^e.*

Teorem 1.27. *(Treći Sylowljev teorem) Ako je G konačna grupa reda $p^e m$, gdje je p prost broj i $p \nmid m$, tada G ima podgrupu reda p^e.*

Propozicija 1.28. *(Frattinijev argument) Neka je K normalna podgrupa konačne grupe G. Ako je P Sylowljeva p-podgrupa od K za neki prost broj p, tada vrijedi*

$$G = KN_G(P),$$

gdje je $KN_G(P) = \{ab : a \in K \, i \, b \in N_G(P)\}$.

Definicija 1.29. ***Prsten*** *R je aditivna Abelova grupa zajedno sa operacijom množenja $R \times R \to R$, $(a, b) \mapsto ab$, za koju vrijedi za sve $a, b, c \in R$:*

1. *a(bc)=(ab)c*
2. *a(b+c)=ab+ac i (b+c)a=ba+ca*
3. *postoji $1 \in R$ takav da za svaki $a \in R$ vrijedi $1a = a = a1$.*

Prsten *R* je **komutativan** ako vrijedi

$$x \cdot y = y \cdot x, \text{ za sve } x, y \in R.$$

Definicija 1.30. *Neka su k komutativni prsten i G grupa, tada definiramo* ***grupni prsten*** *kao skup kG koji sadrži sve formalne izraze oblika $\sum_{g \in G} a_g g$ gdje su $a_g \in k$ za sve $g \in G$ i skoro svi $a_g = 0$, odnosno, ima konačno mnogo a_g različitih od 0. Operacije zbrajanja i množenja su definirane na slijedeći način:*

$$\Big(\sum_{g \in G} a_g g\Big) + \Big(\sum_{g \in G} b_g g\Big) = \sum_{g \in G} (a_g + b_g) g$$

$$\Big(\sum_{g \in G} a_g g\Big)\Big(\sum_{h \in G} b_h h\Big) = \sum_{z \in G} \Big(\sum_{gh = z} a_g b_h\Big) z$$

gdje su $a_g, b_g \, i \, b_h \in K$ te $g, h \in G$.

Grupni prsten *kG* je komutativan ako i samo ako je grupa *G* Abelova.

Definicija 1.31. *Neka je R prsten.* ***Lijevi R-modul*** *je aditivna Abelova grupa M zajedno s množenjem skalarom $R \times M \to M$, $(r, m) \mapsto rm$, takva da za sve m, m' i sve r,r',1 $\in R$ vrijedi*

1. *r(m+m')=rm+rm'*
2. *(r+r')m=rm+r'm*
3. *(rr')m=r(r'm)*
4. *1m=m.*

Poglavlje 2

Semidirektan produkt

Jedan od osnovnih problema u teoriji grupa su njena proširenja. Grupa G koja ima normalnu podgrupu K se može "faktorizirati" u K i G/K. Proučavanja ekstenzija grupa uključuje pitanje za suprotan slučaj: koliko informacija o grupi G se može "izvući" iz normalne podgrupe K i kvocijenta $Q = G/K$. Npr, znamo da je $|G| = |K||Q|$ ako su K i Q konačne.

Definicija 2.1. ***Egzaktni niz grupa*** *je niz oblika*

$$... \to G_{n+1} \xrightarrow{d_{n+1}} G_n \xrightarrow{d_n} G_{n-1} \to ...$$

pri čemu su G_i grupe, d_i homomorfizmi grupa, te vrijedi

$$Imd_{i+1} = Kerd_i \qquad za\ sve\ i.$$

Definicija 2.2. *Ako su K i Q grupe, tada je* ***proširenje*** *od K po Q kratki egzaktni niz:*

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1.$$

Notacije su K i Q da nas asociraju na jezgru i kvocijent.
Postoji i alternativna upotreba izraza proširenja koja naziva tzv. srednju grupu G (a ne kratki egzaktni niz) proširenjem (ekstenzijom) ako ona sadrži normalnu podgrupu K_1 takvu da je $K_1 \cong K$ i $G/K_1 \cong Q$. Pojam proširenja (ekstenzije) ćemo koristiti u oba smisla.

Primjer 2.3. *Direktan produkt $K \times Q$ je proširenje od K po Q ali također i proširenje od Q po K.*

Očito je da za bilo koji uređeni par grupa postoji proširenje jedne po drugoj (tj. njihov direktni produkt) ali to nije jedino moguće proširenje. Problem proširenja je klasifikacija svih mogućih ekstenzija za zadani par grupa K i Q.

Definicija 2.4. ***Transverzala*** *podgrupe K grupe G je podskup T od G koji sadrži od točno jedan element iz svake klase Kt od K.*

Definicija 2.5. *Ako je egzaktni niz* $1 \to K \to G \xrightarrow{p} Q \to 1$ *proširenje, tada je* ***podizanje*** *funkcija* $\ell : Q \to G$ *(ne nužno homomorfizam) takva da je* $p\ell = 1_Q$.

Za danu transverzalu, možemo konstruirati podizanje. Za svaki $x \in Q$, iz surjektivnosti od p slijedi $\ell(x) \in G$ i $p\ell(x) = x$, te funkcija $x \mapsto \ell(x)$ je podizanje. S druge strane, za dano podizanje, tvrdimo da je $Im(\ell)$ tranverzala od K. Ako je Kg klasa, tada $p(g) \in Q$ i označimo $p(g) = x$. Slijedi $p(g\ell(x)^{-1}) = 1$ te $a = g\ell(x)^{-1} \in K$ i $Kg = K\ell(x)$. Dakle svaka klasa ima predstavnika u $\ell(Q)$. Konačno, moramo pokazati da $\ell(Q)$ ne sadrži dva elementa iz iste klase. Ako je $K\ell(x) = K\ell(y)$, tada postoji $a \in K$ takav da $a\ell(x) = \ell(y)$. Primjenimo p na ovaj izraz; kako je $p(a) = 1$, imamo $x = y$ pa i $\ell(x) = \ell(y)$.

Definicija 2.6. *Prisjetimo se da je automorfizam grupe K izomorfizam* $K \to K$. *Grupa automorfizama, Aut(K) je grupa svih automorfizama od K sa kompozicijom kao operacijom.*

Proširenja su definirana za proizvoljne grupe K, ali ćemo smanjiti naša promatranja za poseban slučaj kada je K Abelova. Ako je G ekstenzija od K po Q, bilo bi zbunjujuće zapisivati G multiplikativno a njenu podgrupu K aditivno. Koristimo sljedeću notaciju: iako G ne mora biti Abelova, koristimo aditivnu notaciju za operacije u G.

Propozicija 2.7. *Neka je*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

ekstenzija Abelove grupe K po grupi Q i neka je $\ell : Q \to G$ *podizanje.*

1. *Za svaki* $x \in Q$, *konjugacija* $\theta_x : K \to K$ *definirana sa*

$$\theta_x : a \mapsto \ell(x) + a - \ell(x)$$

   ne ovisi o izboru podizanja $\ell(x)$ *od x. (pretpostavili smo da je i inkluzija, to nam dopušta da pišemo a umjesto i(a)).*

2. *Funkcija* $\theta : Q \to Aut(K)$ *definirana sa* $x \mapsto \theta_x$ *je homomorfizam.*

Dokaz. 1. Pokažimo kako je θ_x neovisna o izboru podizanja $\ell(x)$ od x. Pretpostavimo da je $\ell'(x) \in G$ i $p\ell'(x) = x$. Postoji $b \in K$ takav da je $\ell'(x) = \ell(x) + b$ (jer je $-\ell(x) + \ell'(x) \in Ker(p) = Im(i) = K$).

Slijedi

$$\begin{aligned}&\ell'(x) + a - \ell'(x)\\ &= \ell(x) + b + a - b - \ell(x)\\ &= \ell(x) + a - \ell(x)\end{aligned}$$

jer je K Abelova.

2. Vrijedi $\theta_x(a) \in K$ zbog $K \lhd G$ tako da svaki $\theta_x : K \to K$, isto tako θ_x je automorfizam od K jer su konjugacije automorfizmi.
Ostaje pokazati da je $\theta : Q \to Aut(K)$ homomorfizam. Ako su $x, y \in Q$ i $a \in K$ tada

$$\begin{aligned}\theta_x(\theta_y(a)) &= \theta_x(\ell(y) + a - \ell(y))\\ &= \ell(x) + \ell(y) + a - \ell(y) - \ell(x)\end{aligned}$$

dok je

$$\theta_{xy}(a) = \ell(xy) + a - \ell(xy).$$

Ali $\ell(x) + \ell(y)$ i $\ell(xy)$ su oboje podizanja od xy tako da jednakost $\theta_x\theta_y = \theta_{xy}$ slijedi iz dijela 1.

□

Propozicija 2.8. *Neka su K i Q grupe i K Abelova. Tada homomorfizam $\theta : Q \to Aut(K)$ daje K strukturu lijevog $\mathbb{Z}Q$-modula pri čemu je množenje skalarom definirano sa*

$$xa = \theta_x(a)$$

za sve $a \in K$ i $x \in Q$. Obrnuto, ako je K lijevi $\mathbb{Z}Q -$ modul, tada $x \mapsto \theta_x$ definira homomorfizam $\theta : Q \to Aut(K)$, gdje je $\theta_x : a \mapsto xa$.

Dokaz. Definirajmo množenje skalarom. Svaki $u \in \mathbb{Z}Q$ je jedinstvenog oblika $u = \sum_{x\in Q} m_x x$ gdje je $m_x \in \mathbb{Z}$ i skoro svi $m_x = 0$; definirajmo

$$\Big(\sum_x m_x x\Big)a = \sum_x m_x\theta_x(a) = \sum_x m_x(xa).$$

Provjerimo aksiome modula. Kako je θ homomorfizam, $\theta(1) = 1_K$, pa i $1a = \theta_1(a)$ za sve $a \in K$. Kako $\theta_x \in Aut(K)$ implicira $x(a + b) = xa + xb$ iz čega slijedi da vrijedi $u(a + b) = ua + ub$ za sve $u \in \mathbb{Z}Q$. Slično, $(u + v)a = ua + va$ za $u, v \in \mathbb{Z}Q$. Konačno, $(uv)a = u(va)$ slijedi iz $(xy)a = x(ya)$ za sve $x, y \in Q$, ali

$$(xy)a = \theta_{xy}(a) = \theta_x(\theta_y(a)) = \theta_x(ya).$$

Obrat slično. □

Korolar 2.9. *Ako je* $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *ekstenzija Abelove grupe K po grupi Q, tada je K lijevi* $\mathbb{Z}Q$*-modul ako definiramo*

$$xa = \ell(x) + a - \ell(x)$$

gdje je $\ell : Q \to G$ *podizanje,* $x \in Q$ *i* $a \in K$*, štoviše, skalarni multiplikator je neovisan o izboru podizanja* ℓ*.*

Dokaz Korolara 2.9. direktno slijedi iz dokaza Propozicija 2.7. i 2.8.
Odsada, izraz "lijevi $\mathbb{Z}Q$-modul" ćemo skratiti u "Q-modul".

Definicija 2.10. *Ekstenzija grupe*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

je razdvojena ako postoji homomorfizam $j : Q \to G$ *takav da je* $pj = 1_Q$*. Srednja grupa G u razdvojenoj ekstenziji se naziva* ***semidirektan produkt*** *od K po Q.*

Slijedi da je proširenje razdvojeno ako i samo ako postoji podizanje, nazovimo ga j koje je ujedno i homomorfizam. Koristimo sljedeću notaciju: elementi od K će biti označeni sa $a, b, c, ...$ a elementi od Q će biti označeni sa $x, y, z, ...$

Propozicija 2.11. *Neka je G aditivna grupa čija je normalna podgrupa K.*

1. *Ako je* $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *razdvojena ekstenzija, gdje* $j : Q \to G$ *zadovoljava* $pj = 1_Q$*, tada* $i(K) \cap j(Q) = \{0\}$ *i* $i(K) + j(Q) = G$*.*

2. *U ovom slučaju, svaki* $g \in G$ *ima jedinstven izraz* $g = i(a) + j(x)$ *gdje su* $a \in K$ *i* $x \in Q$*.*

3. *Neka su K i Q podgrupe grupe G i* $K \lhd G$*. Tada je G semidirektan produkt od K po Q ako i samo ako* $K \cap Q = \{0\}$*,* $K + Q = G$ *i svaki* $g \in G$ *ima jedinstven izraz* $g = a + x$ *gdje su* $a \in K$*,* $x \in Q$*.*

Dokaz. 1. Ako je $g \in i(K) \cap j(Q)$, tada $g = i(a) = j(x)$ za $a \in K$ i $x \in Q$. Sada $g = j(x)$ implicira $p(g) = pj(x) = x$, te $g = i(a)$ implicira $p(g) = pi(a) = 0$. Iz toga slijedi $x = 0$ i $g = j(x) = 0$. Ako je $g \in G$, tada $p(g) = pjp(g)$ (jer vrijedi $pj = 1_Q$), pa je $g - (jp(g)) \in Ker(p) = Im(i)$; stoga postoji $a \in K$ takav da je $g - (jp(g)) = i(a)$ i $g = i(a) + j(pg) \in i(K) + j(Q)$.

2. Svaki element $g \in G$ se može faktorizirati kao $g = i(a) + j(pg)$ jer je $G = i(K) + j(Q)$. Da bi dokazali jedinstvenost pretpostavimo da je $i(a) + j(x) = i(b) + j(y)$, gdje su $b \in K$ i $y \in Q$. Tada vrijedi $-i(b) + i(a) = j(y) - j(x) \in i(K) \cap j(Q) = \{0\}$, pa je $i(a) = i(b)$ i $j(x) = j(y)$.

3. Nužnost je specijalan slučaj dijela 2.) gdje su oboje i i j inkluzije. Obratno, svaki $g \in G$ ima jedinstvenu faktorizaciju $g = ax$ za $a \in K$ i $x \in Q$. Definirajnmo $p : G \to Q$ sa $p(ax) = x$. Lako se provjeri da je p surjektivni homomorfizam sa $Kerp = K$.

□

Definicija 2.12. *Ako $K \leq G$ i $C \leq G$ zadovoljavaju $C \cap K = \{1\}$ i $KC = G$, tada C nazivamo **komplement** od K.*

U semidirektnom produktu G, podgrupa K je normalna; s druge strane, slika $j(Q)$, za koju Propozicija 2.11. pokazuje da je komplement od K koji ne mora biti normalan. Definicija semidirektnog produkta dopušta da jezgra od K ne mora biti Abelova i takve grupe prirodno proizlaze. Ipak, pretpostavljamo da je K Abelova iako ta pretpostavka nije uvijek nužna.

Primjer 2.13. *1. Direktan produkt $K \times Q$ je semidirektan produkt od K po Q (ali također i od Q po K).*

2. Abelova grupa G je semidirektan produkt ako i samo ako je direktan produkt (obično se naziva direktnom sumom), budući da je svaka podgrupa Abelove grupe normalna.

Definicija 2.14. *Neka je K Q-modul. Proširenje G od K po Q **realizira operatore** ako za sve $x \in Q$ i $a \in K$, imamo*

$$xa = \ell(x) + a - \ell(x)$$

tj. dano množenje skalarom od $\mathbb{Z}Q$ na K poklapa se sa množenjem skalarom iz Korolara 2.9. koje proizlazi iz konjugacije.

Slijedi konstrukcija semidirektnog produkta.

Definicija 2.15. *Neka je Q grupa i K Q-modul. Definirajmo*

$$G = K \rtimes Q$$

kao skup svih uređenih parova $(a, x) \in K \times Q$ sa operacijom

$$(a, x) + (b, y) = (a + xb, xy).$$

Primjetimo da $(a, 1) + (0, x) = (a, x)$ u $K \rtimes Q$.

Propozicija 2.16. *Za danu grupu Q i Q-modul K, $G = K \rtimes Q$ je semidirektan produkt od K po Q koji realizira operatore.*

Dokaz. Počnimo s dokazom da je G grupa. Za asocijativnost,

$$\begin{aligned}&[(a,x)+(b,y)]+(c,z)\\&=(a+xb,xy)+(c,z)\\&=(a+xb+(xy)c,(xy)z).\end{aligned}$$

S druge strane,

$$\begin{aligned}&(a,x)+[(b,y)+(c,z)]\\&=(a,x)+(b+yc,yz)\\&=(a+x(b+yc),x(yz)).\end{aligned}$$

Naravno, $(xy)z = x(yz)$ zbog asocijativnosti u Q. Prve koordinate su također jednake: kako je K Q-modul, imamo

$$x(b+yc) = xb + x(yc) = xb + (xy)c.$$

Stoga, operacija je asocijativna. Neutralni element od G je $(0,1)$ jer vrijedi $(0,1)+(a,x) = (0+1a,1x) = (a,x)$, a inverz od (a,x) je $(-x^{-1}a, x^{-1})$ zbog

$$(-x^{-1}a, x^{-1}) + (a,x) = (-x^{-1}a + x^{-1}a, x^{-1}x) = (0,1).$$

Slijedi da je G grupa.
Definirajmo funkciju $p : G \to Q$ sa $p : (a,x) \mapsto x$. Kako se jedina "deformacija" javlja u prvoj koordinati, p je surjektivni homomorfizam sa $Ker(p) = \{(a,1) \ : \ a \in K\}$. Ako definiramo $i : K \to G$ sa $i : a \mapsto (a,1)$, tada je

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

ekstenzija. Definirajmo $j : Q \to G$ sa $j : x \mapsto (0,x)$. Vrijedi da je j homomorfizam, jer je $(0,x)+(0,y) = (0,xy)$. Sada je $pjx = p(0,x) = x$ pa je $pj = 1_Q$ i proširenje je razdvojeno pa slijedi da je G semidirektan produkt od K po Q. Konačno, G realizira operatore: ako je $x \in Q$, tada svako podizanje od x ima oblik $\ell(x) = (b,x)$ za neki $b \in K$ i

$$\begin{aligned}(b,x)+(a,1)-(b,x) &= (b+xa,x)+(-x^{-1}b,x^{-1})\\&=(b+xa+x(-x^{-1}b),xx^{-1})\\&=(b+xa-b,1)=(xa,1).\end{aligned}$$

□

Vratimo se na trenutak na multiplikativnu notaciju. U sljedećem dokazu ćemo vidjeti da operacija u $K \rtimes Q$ proizlazi iz jednakosti

$$(ax)(by) = a(xbx^{-1})xy.$$

Teorem 2.17. *Neka je K Abelova grupa. Ako je grupa G semidirektan produkt od K po grupi Q, tada postoji struktura Q-modula na K takva da je* $G \cong K \rtimes Q$.

Dokaz. Možemo pretpostaviti da je G grupa sa normalnom podgrupom K, te da joj je Q komplement. Nastavljamo pisati G aditivno (iako ne mora biti Abelova), pa ćemo zapisati i njenu podgrupu Q također aditivno. Ako su $a \in K$ i $x \in Q$, definirajmo $xa = x+a-x$, tj. xa je konjugat od a po x. Po Propoziciji 2.9., svaki $g \in G$ ima jedinstven zapis kao $g = a + x$, gdje su $a \in K$ i $x \in Q$. Slijedi da je $\varphi : G \to K \rtimes Q$ definirano sa $\varphi : a + x \mapsto (a, x)$ bijekcija. Pokažimo da je φ izomorfizam. Vrijedi

$$\begin{aligned}\varphi((a + x) + (b + y)) &= \varphi(a + x + b + (-x + x) + y)\\ &= \varphi(a + (x + b - x) + x + y) = (a + xb, x + y).\end{aligned}$$

Definicija zbrajanja u $K \rtimes Q$ nam daje

$$(a + xb, x + y) = (a, x) + (b, y) = \varphi(a + x) + \varphi(b + y).$$

□

Poglavlje 3

Generalne ekstenzije i kohomologija

Kao što je već rečeno, jedan od glavnih problema u teoriji grupa je problem proširenja, tj. za danu grupu Q i Abelovu grupu K treba pronaći sva (ne nužno razdvojena) proširenja G od K po Q. Po prijašnjim razmatranjima u poglavlju o semidirektnom produktu, razumno je "pročistiti" problem tako da pretpostavimo da je K Q-modul i tada tražiti sva proširenja koja realiziraju operatore.
Jedan način opisa grupe G je tablica množenja za nju, tj. zapis svih njenih elemenata $a_1, a_2, ...$ i svih njihovih produkata $a_i \cdot a_j$. Tako zapravo i tvorimo semidirektan produkt; svi elementi su u uređenim parovima (a, x) tako da je $a \in K$ i $x \in Q$ i množenje je

$$(a, x) + (b, y) = (a + xb, xy).$$

Otto Schreier je riješio problem proširenja grupa na način koji ćemo prikazati u nastavku. Međutim, Schreierovo rješenje nam ne dopušta da odredimo broj ne-izomorfnih srednjih grupa G. Odgovor na taj problem nije lako naći. Ako je grupa G reda n, tada postoji $n!$ različitih lista njenih elemenata pa i najviše $(n!)^n$ različitih tablica množenja za G (postoji $n!$ mogućnosti za svaki od n redova).
Pretpostavimo da imamo H, neku drugu grupu reda n. Problem određivanja izomorfnosti među G i H je zapravo problem uspoređivanja familije njihovih tablica množenja gdje se vidi da li ima jedna za G i jedna za H koje se podudaraju. Strategija je izvući dovoljno svojstava iz dane ekstenzije G koja će biti dovoljna za rekonstrukciju same grupe G.
Možemo pretpostaviti da je K Q-modul, G proširenje od K po Q koje realizira operatore i da je odabrano podizanje $\ell : Q \to G$. Tada vidimo da svaki $g \in G$ ima jedinstveni zapis oblika

$$g = a + \ell(x) \qquad a \in K \quad \text{i} \quad x \in Q;$$

što slijedi iz toga što je G disjunktna unija klasa $K + \ell(x)$. Nadalje, ako su $x, y \in Q$, tada su $\ell(x) + \ell(y)$ i $\ell(xy)$ oboje predstavnici iste klase pa tako postoji element $f(x, y) \in K$ takav da je $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$.

Definicija 3.1. *Za dano podizanje $\ell : Q \to G$, $\ell(1) = 0$ proširenja G od K po Q,* ***kociklus*** *je funkcija $f : Q \times Q \to K$ takva da je*

$$\ell(x) + \ell(y) = f(x, y) + \ell(xy) \qquad \forall x, y \in Q.$$

Prirodno je izabrati podizanje takvo da je $\ell(1) = 0$ pa je to uključeno u definiciju kociklusa koji se često nazivaju i normalizirani kociklusi. Kociklus ovisi o izboru podizanja ℓ. Kada je G razdvojena ekstenzija, tada postoji podizanje koje je homomorfizam, a odgovarajući kociklus je identički 0. Prema tome, možemo smatrati kociklus kao zapreku homomorfizma za podizanja, odnosno kociklusi opisuju kako se proširenje razlikuje od razdvojenog proširenja.

Propozicija 3.2. *Neka je Q grupa, K Q-modul i $0 \to K \to G \to Q \to 1$ proširenje koje realizira operatore. Ako je $\ell : Q \to G$ podizanje definirano sa $\ell(1) = 0$ i $f : Q \times Q \to K$ odgovarajući kociklus, tada*

1. $\forall x, y \in Q \qquad f(1, y) = 0 = f(x, 1)$
2. *Vrijedi kocikličkí identitet:*
   $\forall x, y, z \in Q \qquad f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$

Dokaz. Uzmimo da je $x = 1$ u izrazu koji definira $f(x, y)$,

$$\ell(x) + \ell(y) = f(x, y) + \ell(xy)$$

iz čega je vidljivo da je $\ell(y) = f(1, y) + \ell(y)$ (budući da je $\ell(1) = 0$ po pretpostavci) pa slijedi $f(1, y) = 0$. Isto tako, postavljajući $y = 1$ daje drugi dio tvrdnje 1.).
Kocikličkí identitet slijedi iz asocijativnosti od G. Za svaki $x, y, z \in Q$ imamo

$$[\ell(x) + \ell(y)] + \ell(z) = f(x, y) + \ell(xy) + \ell(z) = f(x, y) + f(xy, z) + \ell(xyz).$$

Sa druge strane,

$$\begin{aligned} \ell(x) + [\ell(y) + \ell(z)] &= \ell(x) + f(y, z) + \ell(yz) \\ &= xf(y, z) + \ell(x) + \ell(yz) = xf(y, z) + f(x, yz) + \ell(xyz). \end{aligned}$$

□

Zanimljivo je da je i obrnuta tvrdnja istinita. Sljedeći rezultat generalizira konstrukciju $K \rtimes Q$ u Propoziciji 2.16.

Teorem 3.3. *Za danu grupu Q i Q-modul K, funkcija $f : Q \times Q \to K$ je kociklus ako i samo ako zadovoljava kociklički identitet*

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$$

i

$$f(1,y) = 0 = f(x,1) \qquad \forall x,y,z \in Q.$$

Preciznije, postoji proširenje G od K po Q koje realizira operatore, te postoji podizanje $\ell : Q \to G$ čiji je odgovorajući kociklus f.

Dokaz. Nužnost je Propozicija 2.16. Za dovoljnost, definira se G kao skup svih uređenih parova (a,x) u $K \times Q$ zajedno sa operacijom

$$(a,x) + (b,y) = (a + xb + f(x,y), xy).$$

(ako je f identički 0, tada je $G = K \rtimes Q$). Dokaz da je G grupa sličan je dokazu Propozicije 2.16. Kociklički identitet se koristi u dokazu asocijativnosti:

$$\begin{aligned}((a,x) + (b,y)) + (c,z) &= (a + xb + f(x,y), xy) + (c,z)\\ &= (a + xb + f(x,y) + xyc + f(xy,z), xyz)\end{aligned}$$

i

$$\begin{aligned}(a,x) + ((b,y) + (c,z)) &= (a,x) + (b + yc + f(y,z), yz)\\ &= (a + xb + xyc + xf(y,z) + f(x,yz), xyz).\end{aligned}$$

Kociklički identitet pokazuje nam da su ti elementi ekvivalentni. Neutralni element je $(0,1)$ a inverz od (a,x) je

$$-(a,x) = (-x^{-1}a - x^{-1}f(x,x^{-1}), x^{-1}).$$

Definirajmo $p : G \to Q$ sa $p : (a,x) \mapsto x$. Zato jer se jedina "deformacija" pojavljuje u prvoj koordinati, lako je vidjeti da je p surjektivni homomorfizam sa $Kerp = \{(a,1) : a \in K\}$. Ako definiramo $i : K \to G$ sa $i : a \mapsto (a,1)$, tada imamo proširenje $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$. Kako bi pokazali da ovo proširenje realizira operatore moramo pokazati da za svako podizanje ℓ vrijedi $xa = \ell(x) + a - \ell(x)$ za svaki $a \in K$ i $x \in Q$. Sada je $\ell(x) = (b,x)$ za neke $b \in K$ i

$$\begin{aligned}\ell(x) + (a,1) - \ell(x) &= (b,x) + (a,1) - (b,x)\\ &= (b + xa, x) + (-x^{-1}b - x^{-1}f(x,x^{-1}), x^{-1})\\ &= (b + xa + x[-x^{-1}b - x^{-1}f(x,x^{-1})] + f(x,x^{-1}), 1) = (xa,1).\end{aligned}$$

Na kraju, trebamo pokazati da je f kociklus određen sa ℓ. Izaberimo podizanje takvo da je $\ell(x) = (0, x)$ za svaki $x \in Q$. Kociklus F određen sa ℓ je definiran sa

$$\begin{aligned} F(x,y) &= \ell(x) + \ell(y) - \ell(xy) \\ &= (0,x) + (0,y) - (0,xy) \\ &= (f(x,y), xy) + (-(xy)^{-1} f(xy,(xy)^{-1}), (xy)^{-1}) \\ &= (f(x,y) + xy[-(xy)^{-1} f(xy,(xy)^{-1})] + f(xy(xy)^{-1}), xy(xy)^{-1}) = (f(x,y), 1). \end{aligned}$$

□

Sljedeći rezultat pokazuje da smo našli sva proširenja od Q-modula K po grupi Q.

Definicija 3.4. *Za danu grupu Q, Q-modul K i kociklus f, neka $G(K, Q, f)$ označava* ***srednju grupu proširenja*** *od K po Q konstruirano u Teoremu 3.3.*

Teorem 3.5. *Neka je Q grupa, K Q-modul i G proširenje od K po Q koje realizira operatore. Tada postoji kociklus $f : Q \times Q \to K$ takav da*

$$G \cong G(K, Q, f).$$

Dokaz. Neka je $\ell : Q \to G$ podizanje i neka je $f : Q \times Q \to K$ odgovarajući kociklus što znači da za sve $x, y \in Q$ imamo

$$\ell(x) + \ell(y) = f(x,y) + \ell(x,y).$$

Kako je G disjunktna unija klasa, $G = \bigcup_{x \in Q} K + \ell(x)$, svaki $g \in G$ ima jedinstven zapis $g = a + \ell(x)$ za $a \in K$ i $x \in Q$. Jedinstvenost implicira da je funkcija $\varphi : G \to G(K, Q, f)$ dana sa

$$\varphi : g = a + \ell(x) \mapsto (a, x),$$

dobro definirana bijekcija. Sada pokazujemo da je φ izomorfizam.

$$\begin{aligned} \varphi(a + \ell(x) + b + \ell(y)) &= \varphi(a + \ell(x) + b - \ell(x) + \ell(x) + \ell(y)) \\ &= \varphi(a + xb + \ell(x) + \ell(y)) = \varphi(a + xb + f(x,y) + \ell(xy)) \\ &= (a + xb + f(x,y), xy) = (a,x) + (b,y) = \varphi(a + \ell(x)) + \varphi(b + \ell(y)). \end{aligned}$$

□

Napomena 3.6. *Za kasniju upotrebu, primjetimo ako je $a \in K$, tada $\varphi(a) = \varphi(a + \ell(1)) = (a, 1)$ i ako je $x \in Q$, tada $\varphi(\ell(x)) = (0, x)$. To ne bi bilo tako da smo odabrali podizanje za koje je $\ell(1) \neq 0$.*

Sada smo opisali sva proširenja u terminima kociklusa ali oni su određeni podizanjima. Svako proširenje ima puno različitih podizanja pa tako i naš opis koji ovisi o izboru podizanja mora imati ponavljanja.

Lema 3.7. *Za danu grupu Q i Q-modul K, neka je G proširenje od K po Q koje realizira operatore. Neka su ℓ i ℓ' podizanja koja daju kocikluse f odnosno f'. Tada postoji funkcija $h : Q \to K$ za koju je $h(1) = 0$ i za sve $x, y \in Q$ vrijedi*

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Dokaz. Za svaki $x \in Q$, oboje $\ell(x)$ i $\ell'(x)$ leže u istoj klasi od K u G pa tako postoji i element $h(x) \in K$ definiran sa

$$\ell'(x) = h(x) + \ell(x).$$

Kako je $\ell(1) = 0 = \ell'(x)$, imamo $h(1) = 0$. Glavna formula se izvede ovako:

$$\begin{aligned} \ell'(x) + \ell'(y) &= [h(x) + \ell(x)] + [h(y) + \ell(y)] \\ &= h(x) + xh(y) + \ell(x) + \ell(y) \end{aligned}$$

jer G realizira operatore. Jednakost se nastavlja

$$\begin{aligned} \ell'(x) + \ell'(y) &= h(x) + xh(y) + f(x, y) + \ell(xy) \\ &= h(x) + xh(y) + f(x, y) - h(xy) + \ell'(xy). \end{aligned}$$

Po definiciji, f' zadovoljava $\ell'(x) + \ell'(y) = f'(x, y) + \ell'(xy)$ pa zbog toga vrijedi

$$f'(x, y) = h(x) + xh(y) + f(x, y) - h(xy)$$

i na kraju

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

□

Definicija 3.8. *Za danu grupu Q i Q-modul K, funkcija $g : Q \times Q \to K$ se zove* ***korub*** *ako postoji funkcija $h : Q \to K$ i $h(1) = 0$ takva da za sve $x, y \in Q$,*

$$g(x, y) = xh(y) - h(xy) + h(x).$$

Pokazali smo da ako su f i f' kociklusi proširenja G koja se dobivaju iz različitih podizanja, tada je $f' - f$ korub.

Definicija 3.9. *Za danu grupu Q i Q-modul K, definiramo*

$$Z^2(Q, K) = \{\textit{svi kociklusi } f : Q \times Q \to K\},$$

$$B^2(Q, K) = \{\textit{svi korubovi } g : Q \times Q \to K\}.$$

Propozicija 3.10. *Za danu grupu Q i Q-modul K, $Z^2(Q,K)$ je Abelova grupa sa zbrajanjem definiranim po točkama*

$$f + f' : (x,y) \mapsto f(x,y) + f'(x,y),$$

i $B^2(Q,K)$ je podgrupa od $Z^2(Q,K)$.

Dokaz. Da bi vidjeli da je Z^2 grupa, dovoljno je dokazati da $f - f'$ zadovoljava dva identiteta iz Propozicije 3.2. To je očito, samo se oduzmu izrazi za f i f'.
Dokaz da je B^2 podgrupa od Z^2 počinje tako da se prvo direktno pokaže da je svaki korub g kociklus, tj. da g zadovoljava dva identiteta iz Propozicije 3.2. Zatim treba pokazati da je B^2 neprazan podskup a to slijedi iz toga da je nul-funkcija, $g(x,y) = 0$ za sve $x, y \in Q$ očito korub. Na kraju, pokazujemo da je B^2 zatvorena na oduzimanje. Ako $h, h' : Q \to K$ pokazuju da su g i g' korubovi, tj. $g(x,y) = xh(y) - h(xy) + h(x)$ i $g'(x,y) = xh'(y) - h'(xy) + h'(x)$, tada vrijedi

$$(g - g')(x,y) = x(h - h')(y) - (h - h')(xy) + (h - h')(x).$$

□

Dano proširenje ima puno podizanja pa stoga i kociklusa, ali razlika bilo koja dva od tih kociklusa je korub pa se sljedeća kvocijentna grupa sama nameće.

Definicija 3.11. ***Druga grupa kohomologije*** *je definirana sa*

$$H^2(Q,K) = Z^2(Q,K)/B^2(Q,K).$$

Definicija 3.12. *Za danu grupu Q i Q-modul K, dva proširenja G i G' od K po Q koja realiziraju operatore su* ***ekvivalentna*** *ako postoje kociklus f od G i kociklus f' od G', takvi da je $f' - f$ korub.*

Propozicija 3.13. *Za danu grupu Q i Q-modul K, dva proširenja G i G' od K po Q koja realiziraju operatore su ekvivalentna ako i samo ako postoji izomorfizam $\gamma : G \to G'$ takav da slijedeći dijagram komutira:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1 \end{array}$$

Napomena 3.14. *Dijagram pokazuje da bilo koji homomorfizam γ za koji dijagram komutira je nužno izomorfizam.*

Dokaz. Pretpostavimo da su dva proširenja ekvivalentna. Počinjemo prvo sa notacijom. Neka su $\ell : Q \to G$ i $\ell' : Q \to G'$ podizanja, te f, f' odgovarajući kociklusi, te za sve $x, y \in Q$ vrijedi $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$, sa sličnim izrazom za f' i ℓ'. Ekvivalencija znači da postoji funkcija $h : Q \to K$, $h(1) = 0$ i

$$f(x, y) - f'(x, y) = xh(y) - h(xy) + h(x) \qquad \text{za sve } x, y \in Q.$$

Kako je $G = \bigcup_{x \in Q} K + \ell(x)$ disjunktna unija, svaki $g \in G$ ima jedinstveni zapis $g = a + \ell(x)$ za $a \in K$ i $x \in Q$. Slično, svaki $g' \in G'$ ima jedinstveni zapis $g' = a + \ell'(x)$. Ovaj dio dokaza generalizira Teorem 3.5.
Definirajmo $\gamma : G \to G'$ sa

$$\gamma(a + \ell(x)) = a + h(x) + \ell'(x).$$

Ovom funkcijom dijagram komutira. Ako je $a \in K$, tada vrijedi

$$\begin{aligned} \gamma(a) &= \gamma(a + \ell(1)) \\ &= a + h(1) + \ell'(1) = a, \end{aligned}$$

nadalje

$$\begin{aligned} p'\gamma(a + \ell(x)) &= p'(a + h(x) + \ell'(x)) \\ &= x = p(a + \ell(x)). \end{aligned}$$

Na kraju, γ je homomorfizam:

$$\begin{aligned} \gamma([a + \ell(x)] + [b + \ell(y)]) &= \gamma(a + xb + f(x, y) + \ell(xy)) \\ &= a + xb + f(x, y) + h(xy) + \ell'(xy,) \end{aligned}$$

dok je

$$\begin{aligned} \gamma(a + \ell(x)) + \gamma(b + \ell(y)) &= (a + h(x) + \ell'(x)) + (b + h(y) + \ell'(y)) \\ &= a + xb + h(x) + xh(y) + f'(x, y) + \ell'(xy) \\ &= a + xb + f(x, y) + h(xy) + \ell'(xy). \end{aligned}$$

Iskoristili smo dani izraz za $f - f'$ (svi pribrojnici osim $\ell'(xy)$ se nalaze u Abelovoj grupi K pa se mogu premještati po volji).
Obrnuto, pretpostavimo da postoji izomorfizam γ kojim dijagram komutira, tj.
$\gamma(a) = a \quad \forall a \in K$ i

$$x = p(\ell(x)) = p'\gamma(\ell(x)) \qquad \forall x \in Q.$$

Slijedi da je $\gamma\ell : Q \to G'$ podizanje. Primjenivši γ na izraz $\ell(x)+\ell(y) = f(x,y)+\ell(xy)$ koji definira kociklus f, vidimo da je γf kociklus određen sa podizanjem $\gamma\ell$. Ali $\gamma f(x,y) = f(x,y)$ za sve $x, y \in Q$ zbog $f(x,y) \in K$. Prema tome, f je kociklus druge ekstenzije. S druge strane, ako je f' bilo koji drugi kociklus druge ekstenzije, tada Lema 3.7. pokazuje da je $f - f' \in B^2$, tj. ekstenzije su ekvivalentne. □

Kažemo da izomorfizam γ u Propoziciji 3.13. implementira ekvivalenciju. Napomena nakon Teorema 3.5. pokazuje da izomorfizam $\gamma : G \to G(K,Q,f)$ implementira ekvivalenciju proširenja.

Primjer 3.15. *Ako su dva proširenja od K po Q koja realiziraju operatore ekvivalentna, tada su njihove srednje grupe izomorfne. Međutim, obrat ne vrijedi: dajemo primjer dva ne-ekvivalentna proširenja sa izomorfnim srednjim grupama. Neka je p neparan prost broj, te je dan sljedeći dijagram:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{\pi} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{\pi'} & Q & \longrightarrow & 1 \end{array}$$

Definirajmo $K = \langle a\rangle$, cikličku grupu reda p, $G = \langle g\rangle = G'$ cikličke grupe reda p^2 i $Q = \langle x\rangle$ gdje je $x = g + K$. U prvom redu, definirajmo $i(a) = pg$ i π prirodno preslikavanje, a u donjem redu definirajmo $i'(a) = 2pg$ i π' prirodno preslikavanje. Primjetimo da je i' injekcija jer je p neparan. Pretpostavimo da postoji izomorfizam $\gamma : G \to G'$ kojim dijagram komutira. Komutativnost prvog kvadrata implicira $\gamma(pa) = 2pa$ a to povlači $\gamma(g) = 2g$; zbog toga što je p neparan prost broj i $G = \langle g\rangle = G'$ ciklička grupa reda p^2, pa se može pokazati da je $\gamma : G \to G$, $\gamma : a \mapsto 2a$ jedinstveni automorfizam za koji vrijedi $\gamma(pg) = 2pg$. Komutativnost drugog kvadrata daje $g + K = 2g + K$ za $g \in K$. Zaključujemo da te dvije ekstenzije nisu ekvivalentne.

Sljedeći teorem predstavlja glavni rezultat ovog rada.

Teorem 3.16. *(Schreier) Neka je Q grupa, K Q-modul i $e(Q,K)$ označava familiju svih ekvivalentnih klasa proširenja od K po Q koja realiziraju operatore. Postoji bijekcija*

$$\varphi : H^2(Q,K) \to e(Q,K)$$

koja preslikava 0 u klasu razdvojenog proširenja.

Dokaz. Označimo klasu ekvivalencije proširenja $0 \to K \to G \to Q \to 1$ sa $[G]$. Definirajmo $\varphi : f + B^2 \to [G(K,Q,f)]$ gdje je f kociklus proširenja, a $G(K,Q,f)$ konstruirano u

Teoremu 3.3.
Prvo, φ je dobro definirana injekcija: f i g su kociklusi takvi da $f + B^2 = g + B^2$ ako i samo ako $[G(K, Q, f)] = [G(K, Q, g)]$ po Propoziciji 3.13. Da bi vidjeli da je γ surjekcija, neka je $[G] \in e(Q, K)$. Po Teoremu 3.5. i Napomeni iza njega, $[G] = [G(K, Q, f)]$ za neki kociklus f pa je $[G] = \varphi(f + B^2)$. Konačno, kociklus 0 odgovara semidirektnom produktu. □

Ako je H grupa i postoji bijekcija $\varphi : H \to X$, gdje je X skup, tada postoji jedinstvena operacija definirana na X koja čini X grupom i φ izomorfizmom.
Za dani $x, y \in X$, postoje $g, h \in H$ takvi da $x = \varphi(g)$ i $y = \varphi(h)$ pa definiramo $xy = \varphi(gh)$.

Korolar 3.17. *Ako je Q grupa, K Q-modul i $H^2(Q, K) = \{0\}$, tada je svako proširenje od K po Q koje realizira operatore semidirektan produkt.*

Dokaz. Po teoremu, $e(Q, K)$ ima samo jedan element, a kako razdvojene ekstenzije uvijek postoje, taj jedan element mora biti klasa ekvivalencije razdvojene ekstenzije. Iz toga slijedi, svaka ekstenzija od K po Q koje realizira operatore je razdvojena, pa je i njena srednja grupa semidirektan produkt. □

Sada primjenimo Schreierov teorem.

Teorem 3.18. *Neka je G konačna grupa reda mn gdje je $(m, n) = 1$. Ako je K Abelova normalna podgrupa reda m, tada K ima komplement i G je semidirektan produkt.*

Dokaz. Definirajmo $Q = G/K$. Po Korolaru 3.17. dovoljno je pokazati da je svaki kociklus $f : Q \times Q \to K$ korub. Definirajmo $\sigma : Q \to K$ sa

$$\sigma(x) = \sum_{y \in Q} f(x, y);$$

σ je dobro definirana jer je Q konačna i K Abelova. Sada sumirajmo kociklički identitet

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

za sve $z \in Q$, i dobijemo:

$$x\sigma(y) - \sigma(xy) + \sigma(x) = nf(x, y)$$

(kako z varira po cijelom Q, pa tako i yz). Kako je $(m, n) = 1$, postoje cijeli brojevi s i t takvi da je $sm + tn = 1$. Definirajmo $h : Q \to K$ sa $h(x) = t\sigma(x)$.
Primjetimo da je $h(1) = 0$ i

$$xh(y) - h(xy) + h(x) = f(x, y) - msf(x, y).$$

Ali $sf(x, y) \in K$ pa je $msf(x, y) = 0$. Prema tome, f je korub. □

Napomena 3.19. *P.Hall je dokazao da ako je G konačna rješiva grupa reda mn, gdje je* $(m, n) = 1$*, tada G ima podgrupu reda m i svake dvije takve podgrupe su konjugirane. Zbog ovog teorema, (ne nužno normalna) podgrupa H konačne grupe G se zove Hallova podgrupa ako je* $(|H|, [G : H]) = 1$*. Po ovome, Teorem 3.18. se često iskazuje kao svaka normalna Hallova podgrupa proizvoljne konačne grupe ima komplement.*

Sada ćemo pokušati izostaviti hipotezu da je K Abelova.
Prije iskaza Teorema navodimo Lemu čiji je dokaz jednostavan pa ga izostavljamo.

Lema 3.20. *Neka je G grupa reda mn, gdje je (m,n)=1. Normalna podgrupa K reda m ima komplement u G ako i samo ako postoji podgrupa* $C \leq G$ *reda n.*

Teorem 3.21. *(Schur-Zassenhausova Lema) Neka je G konačna grupa reda mn, gdje je* $(m, n) = 1$*. Ako je K normalna podgrupa reda m, tada K ima komplement i G je semidirektan produkt.*

Dokaz. Po Lemi 3.20. dovoljno je pokazati da G sadrži podgrupu reda n, dokaz provodimo indukcijom po $m \geq 1$. Očito je baza $m = 1$ istinita.
Pretpostavimo da postoji prava podgrupa T od K takva da je $\{1\} < T \lhd G$. Tada je $K/T \lhd G/T$ i $(G/T)/(K/T) \cong G/K$ je reda n. Kako je $T < K$, vrijedi $|K/T| < |K| = m$ pa induktivna pretpostavka daje podgrupu $N/T \leq G/T$ i $|N/T| = n$. Sada $|N| = n|T|$, gdje je $(|T|, n) = 1$ (jer je $|T|$ djelitelj $|K| = m$) pa je T normalna podgrupa od N čiji su red i indeks relativno prosti. Kako je $|T| < |K| = m$, induktivna pretpostavka daje podgrupu C od N (koja je očito podgrupa od G) reda n.
Sada možemo pretpostaviti da je K minimalna normalna podgrupa od G; tj. da ne postoji normalna podgrupa T od G takva da je $\{1\} < T < K$. Neka je p prost djelitelj od $|K|$ i P Sylowljeva p-podgrupa od K. Po Frattinijevom argumentu 1.28 slijedi $G = KN_G P$. Vrijedi

$$G/K = KN_G(P)/K \cong N_G(P)/(K \cap N_G(P)) = N_G(P)/N_K(P).$$

Slijedi, $|N_K(P)|n = |N_K(P)||G/K| = |N_G(P)|$. Ako je $N_G(P)$ prava podgrupa od G, tada $|N_K(P)| < m$ a indukcija daje podgrupu od $N_G(P) \leq G$ reda n. Stoga, možemo pretpostaviti da $N_G(P) = G$, tj. $P \lhd G$.
Kako je $\{1\} < P \leq K$ i P je normalna u G, mora vrijediti $P = K$, jer je K minimalna normalna podgrupa. Ali P je p-grupa, pa je i njen centar, $Z(P)$ netrivijalan. Po Propoziciji 1.16., slijedi $Z(P) \lhd G$ pa je $Z(P) = P$ opet zbog $P = K$ je minimalna normalna podgrupa od G. Iz toga slijedi da je P Abelova pa smo reducirali problem na Teorem 3.18. □

Korolar 3.22. *Ako konačna grupa G ima normalnu Sylowljevu p-podgrupu P, za neke proste djelitelje p od* $|G|$*, tada je G semidirektan produkt. Preciznije, P ima komplement.*

Dokaz. Red i indeks Sylowljeve podgrupe su relativno prosti. □

Postoji drugi dio Schur-Zassenhausove leme koji nismo izrekli:
Ako je K normalna podgrupa od G čiji su red i indeks relativno prosti, tada su svaka dva komplementa od K konjugirane podgrupe. Sada ćemo vidjeti da postoji analogon od $H^2(K, Q)$ čije nestajanje implicira konjugaciju komplementa kada je K Abelova. Ta grupa $H^1(K, Q)$ javlja se kao i $H^2(K, Q)$ iz serije elementarnih razmatranja.
Neka je Q grupa, K Q-modul i $0 \to K \to G \to Q \to 1$ razdvojena ekstenzija. Izaberimo podizanje $\ell : Q \to G$ tako da svaki element $g \in G$ ima jedinstven izraz oblika $g = a + \ell(x)$ gdje su $a \in K$ i $x \in Q$.

Definicija 3.23. *Automorfizam φ grupe G* ***stabilizira*** *proširenje $0 \to K \to G \to Q \to 1$ ako sljedeći dijagram komutira:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \end{array}$$

Skup svih stabilizcijskih automorfizama proširenja K po Q, gdje je K Q-modul čini grupu obilježenu sa $Stab(Q, K)$.
Primjetimo da je stabilizacijski automorfizam izomorfizam koji implementira ekvivalenciju proširenja sa samim sobom.

Propozicija 3.24. *Neka je Q grupa, K Q-modul i*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

razdvojena ekstenzija. Ako je $\ell : Q \to G$ podizanje, tada je svaki stabilizacijski automorfizam $\varphi : G \to G$ oblika

$$\varphi(a + \ell(x)) = a + d(x) + \ell(x),$$

gdje je $d(x) \in K$ nezavisan o odabiru podizanja ℓ. Štoviše, ova formula definira stabilizacijski automorfizam ako i samo ako, za sve $x, y \in Q$ funkcija $d : Q \to K$ zadovoljava

$$d(xy) = d(x) + xd(y).$$

Dokaz. Ako je φ stabilizacijski, tada je $\varphi i = i$ gdje je $i : K \to G$ i $p\varphi = p$. Kako pretpostavljamo da je i funkcija inkluzije (što je samo pogodnost koja nam omogućuje da pišemo a umjesto $i(a)$), imamo $\varphi(a) = a$ za sve $a \in K$. Da bi iskoristili drugo ograničenje na φ, pretpostavimo da je $\varphi(\ell(x)) = d(x) + \ell(y)$ za neki $d(x) \in K$ i $y \in Q$.

Tada vrijedi

$$\begin{aligned} x &= p(\ell(x)) \\ &= p\varphi(\ell(x)) \\ &= p(d(x) + \ell(y)) = y; \end{aligned}$$

tj. $x = y$. Iz toga slijedi $\varphi(a + \ell(x)) = \varphi(a) + \varphi(\ell(x)) = a + d(x) + \ell(x)$.
Da bi vidjeli da je tvrdnja za d istinita, prvo pokazujemo da je d nezavisna o izboru podizanja. Neka je $\ell' : Q \to G$ neko drugo podizanje, takvo da je $\varphi(\ell'(x)) = d'(x) + \ell'(x)$ za neki $d'(x) \in K$. Sada gledamo $k(x) \in K$ za koji je $\ell'(x) = k(x) + \ell(x)$ za $p\ell'(x) = x = p\ell(x)$. Iz toga slijedi

$$\begin{aligned} d'(x) &= \varphi(\ell'(x)) - \ell'(x) \\ &= \varphi(k(x) + \ell(x)) - \ell'(x) \\ &= k(x) + d(x) + \ell(x) - \ell'(x) = d(x), \end{aligned}$$

jer je $k(x) + \ell(x) - \ell'(x) = 0$.
Kako je $d(x)$ neovisan o izboru podizanja ℓ, i kako je proširenje razdvojeno, možemo pretpostaviti da je ℓ homomorfizam: $\ell(x) + \ell(y) = \ell(xy)$. Računamo $\varphi(\ell(x) + \ell(y))$ na dva načina. S jedne strane

$$\begin{aligned} \varphi(\ell(x) + \ell(y)) &= \varphi(\ell(xy)) \\ &= d(xy) + \ell(xy), \end{aligned}$$

dok je s druge strane

$$\begin{aligned} \varphi(\ell(x) + \ell(y)) &= \varphi(\ell(x)) + \varphi(\ell(y)) \\ &= d(x) + \ell(x) + d(y) + \ell(y) \\ &= d(x) + xd(y) + \ell(xy). \end{aligned}$$

Dokaz obrata, ako je $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$ gdje d zadovoljava danu jednakost, tada je φ stabilizirajući izomorfizam što se rutinski provjeri. □

Imenujmo sada funkcije koje su poput d.

Definicija 3.25. *Neka je Q grupa i K Q-modul. **Derivacija** je funkcija $d : Q \to K$ takva da je*

$$d(xy) = xd(y) + d(x).$$

Skup svih derivacija, $Der(Q, K)$ je Abelova grupa uz zbrajanje definirano po točkama (ako je K trivijalan Q-modul, tada je $Der(Q, K) = Hom(Q, K)$).
Ako je d derivacija, tada je $d(11) = 1d(1) + d(1) \in K$ pa je $d(1) = 0$.

Primjer 3.26. *1. Ako je Q grupa i K Q-modul, tada je funkcija $u : Q \to K$ oblika $u(x) = xa_0 - a_0$, gdje je $a_0 \in K$ derivacija:*

$$u(x) + xu(y) = xa_0 - a_0 + x(ya_0 - a_0) = xa_0 - a_0 + xya_0 - xa_0 = xya_0 - a_0 = u(xy).$$

*Derivacija u zadana sa $u(x) = xa_0 - a_0$ se zove **glavna derivacija**. Ako označimo s $xa = x + a - x$ djelovanje od Q na K konjugacijom, tada je $xa_0 - a_0 = x + a_0 - x - a_0$, iz čega slijedi da je $xa_0 - a_0$ komutator od x i a_0.*

2. Lagano se provjeri da je skup PDer(Q,K) svih glavnih derivacija podgrupa od Der(Q,K).

Prisjetimo se da $Stab(Q, K)$ označava grupu svih stabilizirajućih automorfizama proširenja od K po Q.

Propozicija 3.27. *Ako je Q grupa, K Q-modul i $0 \to K \to G \to Q \to 1$ je razdvojeno proširenje, tada postoji izomorfizam $Stab(Q, K) \to Der(Q, K)$.*

Dokaz. Neka je φ stabilizirajući automorfizam. Ako je $\ell : Q \to G$ funkcija podizanja, tada Propozicija 3.24. kaže da je $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$ gdje je d derivacija. Kako ta propozicija nadalje tvrdi da je d nezavisna o izboru podizanja, $\varphi \mapsto d$ je dobro definirana funkcija $Stab(Q, K) \to Der(Q, K)$ i lagano se vidi da je homomorfizam.
Da bi vidjeli da je ovo preslikavanje izomorfizam, konstruirajmo njen inverz. Ako je $d \in Der(Q, K)$, definirajmo $\varphi : G \to G$ sa $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$. Sada je φ stabilizirajući po Propoziciji 3.24. i $d \mapsto \varphi$ je željeni inverz. □

Nije očigledno iz definicije da je $Stab(Q, K)$ Abelova, jer su njene binarne operacije kompozicije. Ipak, $Stab(Q, K)$ je Abelova, jer je $Der(Q, K)$ Abelova.
Prisjetimo se da se automorfizam φ grupe G naziva unutarnji automorfizam ako je konjugacija, tj. ako postoji $c \in G$ takav da je $\varphi(g) = c + g - c$ za sve $g \in G$ (ako je G aditivna).

Lema 3.28. *Neka je $0 \to K \to G \to Q \to 1$ razdvojena ekstenzija i $\ell : Q \to G$ podizanje. Tada je funkcija $\varphi : G \to G$ unuturanji stabilizirajući automorfizam po nekom $a_0 \in K$ ako i samo ako*

$$\varphi(a + \ell(x)) = a + xa_0 - a_0 + \ell(x).$$

Dokaz. Ako zapišemo $d(x) = xa_0 - a_0$, tada $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$. Ali d je (glavna) derivacija, pa je φ stabilizirajući automorfizam po Propoziciji 3.24. Konačno, φ je konjugacija po $-a_0$, jer je

$$\begin{aligned} &- a_0 + (a + \ell(x)) + a_0 \\ &= -a_0 + a + xa_0 + \ell(x) \\ &= \varphi(a + \ell(x)). \end{aligned}$$

Obrnuto, pretpostavimo da je φ stabilizirajuća konjugacija. Da je φ stabilizirajuća daje $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$; a da je konjugacija daje $\varphi(a + \ell(x)) = b + a + \ell(x) - b$ gdje je $b \in K$. Ali $b + a + \ell(x) - b = b + a - xb + \ell(x)$ pa je $d(x) = b - xb$, što smo i htjeli dokazati. □

Definicija 3.29. *Ako je Q grupa i K Q-modul, definirajmo*

$$H^1(Q, K) = Der(Q, K)/PDer(Q, K),$$

gdje je PDer(Q,K) podgrupa od Der(Q,K) sastavljena od svih glavnih derivacija.

Propozicija 3.30. *Neka je* $0 \to K \to G \to Q \to 1$ *razdvojena ekstenzija i neka su C i C′ komplementi od K u G. Ako je* $H^1(Q, K) = 0$*, tada su C i C′ konjugirani.*

Dokaz. Kako je G semidirektan produkt, postoje podizanja $\ell : Q \to G$ sa slikom C i $\ell' : Q \to G$ sa slikom C' koja su homomorfizmi. Stoga, kociklusi f i f' određeni sa ovim podizanjima su identički nula, a tako i $f' - f = 0$. Ali Lema 3.7. kaže da postoji $h : Q \to K$, $h(x) = \ell'(x) - \ell(x)$ gdje vrijedi

$$0 = f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x)$$

pa prema tome h je derivacija. Kako je $H^1(Q, K) = 0$, h je glavna derivacija; postoji $a_0 \in K$ takav da

$$\ell'(x) - \ell(x) = h(x) = xa_0 - a_0$$

za sve $x \in Q$. Kako vrijedi $\ell'(x) - a_0 = -xa_0 + \ell'(x)$, imamo $\ell(x) = a_0 - xa_0 + \ell'(x) = a_0 + \ell'(x) - a_0$.
Ali $Im\ell = C$ i $Im\ell' = C'$, pa su C i C' konjugirani po a_0. □

Sada možemo nadopuniti Schur-Zassenhausenov teorem.

Teorem 3.31. *Neka je G konačna grupa reda mn, gdje je* $(m, n) = 1$*. Ako je K Abelova normalna podgrupa reda m, tada je G semidirektan produkt od K po G/K i bilo koja dva komplementa od K su konjugirana.*

Dokaz. Po Propoziciji 3.30. dovoljno je pokazati da je $H^1(Q, K) = 0$, gdje je $Q = G/K$. Primjetimo prvo da je $|Q| = |G|/|K| = mn/m = n$.
Neka je $d : Q \to K$ derivacija; za sve $x, y \in Q$, vrijedi

$$d(xy) = xd(y) + d(x).$$

Sumirajmo ovaj izraz po svim $y \in Q$ da bi dobili

$$\triangle = x \triangle + nd(x),$$

gdje je $\triangle = \sum_{y \in Q} d(y)$ (kako y varira po Q, tako i xy). Kako je $(m, n) = 1$, postoje cijeli brojevi s i t takvi da je $sn + tm = 1$. Iz toga $d(x) = snd(x) + tmd(x) = snd(x)$ zbog $d(x) \in K$ pa je $md(x) = 0$. Iz toga slijedi

$$d(x) = s \triangle - xs \triangle .$$

Postavljajući $a_0 = -s\triangle$ vidimo da je d glavna derivacija. □

Micanje pretpostavke u Teoremu 3.31. da je K Abelova je puno teže nego micanje te pretpostavke u Teoremu 3.18. Prvo dokazujemo da komplementi konjugiraju ako su ili K ili Q rješive grupe. Kako su $|Q|$ i $|K|$ relativno prosti, barem jedna od K i Q je neparnog reda. Feit-Thompsonov teorem, koji kaže da je svaka grupa neparnog reda rješiva sada dovršava dokaz.

Postoje druge primjene homologije u teoriji grupa osim Schur-Zassenhausove leme. Na primjer, ako je G grupa, $a \in G$, i $\gamma_a : g \mapsto aga^{-1}$ je konjugacija po a, tada vrijedi $\gamma_a^n : g \mapsto a^n g a^{-n}$ za sve n. Stoga, ako je a prostog reda p i $a \notin Z(G)$, tada je γ_a automorfizam reda p. Teorem W.Gaschutza koristi kohomologiju da bi dokazali da svaka konačna ne-Abelova p-grupa ima automorfizam reda p koji nije konjugacija po elementu od G.

Razmislimo o formulama koje su se pojavile:
kociklus: $0 = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y)$
korub: $f(x, y) = xh(y) - h(xy) + h(x)$
derivacija: $0 = xd(y) - d(xy) + d(x)$
glavna derivacija: $d(x) = xa_0 - a_0$
Sve ove formule uključuju alternirajuće sume, čini se da su kociklus i derivacije u jezgri, a korub i glavne derivacije u slici. To motivira slijedeću definiciju:

Definicija 3.32. *Ako je Q grupa i K Q-modul, tada je* ***podmodul fiksnih točaka*** *definiran sa*

$$H^0(Q, K) = \{a \in K : \quad xa = a \text{ za sve } x \in Q\}.$$

Bibliografija

[1] *Topological groups*, http://www.cs.duke.edu/courses/fall06/cps296.1/Lectures/sec-IV-4.pdf, 2008, [Online; accessed 20-May-2013].

[2] Milan Z. Grulović, *Osnove teorije grupa*, Feljton, 1997.

[3] Boris Širola, *Algebarske strukture*, http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf, 2010, [Online; accessed 10-May-2015].

[4] Hrvoje Kraljević, *Algebra*, http://web.math.pmf.unizg.hr/~hrk/nastava/2007-08/algebra_Osijek_2007_8.pdf, 2007, [Online; accessed 10-May-2015].

[5] Joseph.J Rotman, *Advanced modern algebra*, Prentice Hall, 2002.

Sažetak

U ovom radu proučavamo pojam proširenja grupe. Dokazujemo važan rezultat o bijekciji između proširenja i grupe kohomologije.
U prvom poglavlju ponavljamo osnovne definicije i rezultate iz algebarskih struktura.
U drugom poglavlju uvodimo pojam semidirektog produkta i njegova svojstva.
Treće poglavlje se bavi generalnim proširenjima i kohomologijom. Uvodimo pojmove kociklusa koristeći pojam podizanja. U ovom poglavlju dolazimo do najbitnijih rezultata rada, Schreireovog teorema koji koristi kocikluse u riješavanju problema proširenja te kao njegovu posljedicu, Schur-Zassenhausovu lemu.

Summary

In this diploma thesis we study group extensions. We prove important result about bijection between exstensions and group cohomology.
In first chapter we recall basic definitions and results from algebraic structures.
In second chapter we introduce the idea of semidirect product and its properties.
The third chapter is about general extensions and cohomology. We introduce the concept of cocycle using the definition of lifting. In this chapter we prove the most important results of the thesis, Schreir's theorem which uses cocycle to solve the extension problem and Schur-Zassenhaus lemma which is it's consequence.

Životopis

Rođena sam 22.9.1989. godine u Osijeku. Sa svojih 6 godina selim se sa roditeljima u Varaždin gdje 1997.godine upisujem Prvu osnovnu školu. 2004. godine upisujem Prvu gimnaziju Varaždin, prirodoslovno-matematički smjer. Tijekom osnovnoškolskog i srednješkolskog obrazovanja redovito sudjelujem na matematičkim natjecanjima. Učim i strane jezike, engleski i njemački u Školi stranih jezika Kezele u Varaždinu od 2002. do 2008. godine. Upisujem Matematički odsjek Prirodoslovno-matematičkog fakulteta gdje završavam preddiplomski studij 2012. godine i upisujem diplomski smjer Financijske i poslovne matematike koji završavam 2015. godine.