UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET

Nikola Velov

PRINCIPI REFLEKSIJE ZA PIKAROVE GRUPE

master rad

Beograd, 2022.

Mentor:

prof. dr Goran Đanković, vanredni profesor
Univerzitet u Beogradu, Matematički fakultet

Članovi komisije:

prof. dr Aleksandar Lipkovski, redovni profesor
Univerzitet u Beogradu, Matematički fakultet

prof. dr Marko Radovanović, vanredni profesor
Univerzitet u Beogradu, Matematički fakultet

Datum odbrane: ____________________

Mojoj sestri Ivani

Naslov master rada: Principi refleksije za Pikarove grupe

Rezime: U ovom master radu su predstavljene osnove teorije shema, kao i tehnike etalne kohomologije. Prikazane su primene savremene algebarske geometrije u teoriji brojeva, pre svega u kontekstu veza između Pikarove grupe i klasne grupe prstena celih brojevnog polja. Dat je i originalan doprinos dobijanjem novih principa refleksije za raširenja polja funkcija u slučaju Galoaove grupe Q_8.

Ključne reči: algebarska geometrija, teorija shema, etalna kohomologija, Pikarova grupa, principi refleksije

Sadržaj

Glava 1

Uvod

Razvojem teorije shema je postalo moguće dodeliti geometrijsku strukturu proizvoljnom komutativnom prstenu sa jedinicom. Mnoge strukture koje se pojavljuju u teoriji brojeva su upravo ovakvi prstenovi, pa je postalo moguće koristiti ideje već razvijenih geometrijskih teorija, kao što je algebarska topologija, u teoriji brojeva.

U glavi o shemama uvodimo jezik moderne algebarske geometrije, kao i neke osnovne alate za rad sa shemama. Teorija shema je nastala proučavanjem algebarskih varijeteta, ali u svom najopštijem obliku, moguće ju je direktno izučavati bez prethodnog poznavanja klasične algebarske geometrije. Ovaj stav je zastupao i Aleksandar Grotendik, koji je i otkrio teoriju shema, tvrdeći da preterano oslanjanje na teoriju algebarskih varijeteta samo može da oteža usvajanje ovog novog jezika.

Sledeća glava uvodi pojam algebarske fundamentalne grupe i etalne morfizme. U kontekstu ovog master rada, ona se pre svega zasniva na beskonačnoj teoriji Galoa. Ovime se uspostavlja neophodna terminologija za rad sa etalnom kohomologijom.

Tehnička srž ovog rada je o raznim kohomološkim teorijama koje se koriste u modernoj algebarskoj geometriji, sa posebnim akcentom na etalnoj kohomologiji, koju ćemo i koristiti u poslednjoj glavi. Ova glava je jako tehnička i prioritet nam je da u njoj uspostavimo neophodan alat koji ćemo koristiti, iako neki detalji izlaze izvan okvira ovog master rada.

Nakon toga uvodimo Pikarovu grupu i povezujemo je sa klasnom grupom ideala kod prstena celih brojevnog polja. U istoj glavi dajemo i račun za etalnu kohomologiju na krivama, na čemu se zasniva poslednja glava.

Konačno, poslednja glava se tiče principa refleksije i proučava savremene metode povezivanja algebarska teorije brojeva i algebarske geometrije. Suštinsku ideju ovog pristupa su razvili Klis [8] i Cimerman [12].

Nakon prikaza njihovog metoda, dajemo i originalnu novu primenu istog. U pitanju je novi princip refleksije kod polja funkcija za slučaj Galoaovog raširenja kod kojeg je Galoaova grupa izomorfna kvaternionskoj grupi Q_8.

Osim toga, na kraju ove glave navodimo i neke ideje za dalji rad, kao i konkretna pitanja. Autor ovog master rada je dugo razmišljao o njima i ovde je naveden delimičan napredak ka njihovom razrešenju.

Najzad, treba napomenuti da je savremena algebarska geometrija izuzetno tehnički zahtevna oblast i da je jako lako izgubiti se u mnoštvu pojmova, definicija i tvrđenja. Ovo je u skladu sa glavnom idejom njenog začetnika. Naime, Grotendik je poredio rešavanje problema sa potapanjem ostrva u nadolazeće more jednostavnijih dokazanih tvrđenja.

Jedna od ključnih veština koja je neophodna za primene algebarske geometrije je sposobnost da se odredi najkraći put kroz teoriju do rešenja samog problema. U skladu sa ovom filozofijom, nećemo se uvek truditi da sva tvrđenja koja navodimo i dokažemo. Nekada dokaz kompletno izostavljamo, nekad dajemo skicu.

Mnogi od ovih dokaza se mogu naći u zaista obimnoj literaturi o algebarskoj geometriji. Tu su knjige čiji su autori Liu [13], Hartshorn [14], Vakil [15], predavanja o etalnoj kohomologiji koja je pisao Miln [11], kao i onlajn referenca Stacks Project [3]. Pri izboru tema su pomogla i predavanja koja je pripremio Donu Arapura [4]. Naravno, izvorna referenca za teoriju shema je [1], gde je Aleksandar Grotendik prvi put uveo mnoge od ključnih ideja savremene algebarske geometrije. Prevod termina iz algebarske geometrije na srpski jezik je zasnovan na pionirskom magistarskom radu [2], a neophodno tehnično predznanje iz komutativne algebre se može pronaći u [7].

Ovaj master rad ima dva ključna cilja. Prvi cilj je da se da originalni naučni doprinos kroz dobijanje novih principa refleksije i njihovo bolje razumevanje. Drugi, jednako važan cilj, je da se predstave tehnike moderne algebarske geometrije i njene primene u teoriji brojeva.

Za kraj, želeo bih da se zahvalim mom mentoru, profesoru Goranu Đankoviću, koji me je usmerio na konkretan problem gde sam mogao samostalno da isprobam i konkretno vidim kako se koriste mnogobrojne tehnike algebarske geometrije u teoriji brojeva. Uz njegovu pomoć, shvatio sam da je najbolji način da se savladaju zahtevne veštine ove teorije tako što se prvo počne od problema koji se rešava, vraćajući se nazad kroz literaturu i usvajajući usput neophodne tehnike.

Glava 2

Teorija shema

U ovoj glavi uvodimo neophodne pojmove i tvrđenja iz teorije shema. U pitanju je jako tehnička oblast matematike, tako da se nećemo uvek truditi da damo kompletne dokaze za sva tvrđenja, već je cilj da uspostavimo neophodne tehnike koje ćemo koristiti u dobijanju daljih rezultata. Ovaj uvod je adaptiran na osnovu nekoliko knjiga kao što su [13] i [14], kao i na osnovu open source udžbenika [3] i predavanja [4].

Ključna ideja Grotendikove teorije shema je da proizvoljnom komutativnom prstenu sa jedinicom R dodelimo geometrijsku strukturu i na taj način adaptiramo tehnike iz drugih geometrijskih teorija kao što su topologija i diferencijalna geometrija.

Značaj ove teorije se ogleda u tome što svaki prsten poseduje izvesne geometrijske osobine, pa čak i prsten celih brojeva $\mathbb{Z}$. Ovo je otvorilo put ubrzanom razvoju teorije brojeva upotrebom geometrijskih metoda, a kao rezultat je nastala moderna aritmetička geometrija.

2.1 Spektar i topologija Zariskog

Neka je R komutativni prsten sa jedinicom. Skupu svih prostih ideala u prstenu R zadajemo topologiju i od njega dobijamo topološki prostor. Podrazumevamo da ceo prsten nije prost ideal, po konvenciji.

Definicija 2.1.1. Neka je R komutativan prsten sa jedinicom. *Spektar* prstena R, u oznaci $\operatorname{Spec} R$, je skup svih njegovih prostih ideala.

Primer 2.1.2. Ako je k polje, $\operatorname{Spec} k$ se sastoji iz samo jedne tačke, a to je prost ideal (0).

Primetimo da je $\operatorname{Spec}\{0\} = \emptyset$, zato što ceo prsten po konvenciji nije prost ideal. Za ideal I u R definišemo $V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}$. Ako je $f \in R$, definišemo i $D(f) := \operatorname{Spec} R \setminus V(fR)$. Na ovaj način dolazimo do topologije na spektru, što je sadržaj sledećeg tvrđenja.

Teorema 2.1.3. *Na* $\operatorname{Spec} R$ *postoji topologija u kojoj skupovi* $D(f)$ *za* $f \in R$ *čine bazu, a zatvoreni skupovi su oblika* $V(I)$ *za neki ideal* $I \subset R$*. Ova topologija se zove* *topologija Zariskog.*

Ako imamo homomorfizam $h : R \to S$, on indukuje preslikavanje $\operatorname{Spec} S \to \operatorname{Spec} R$ koji je dat sa $\mathfrak{p} \mapsto h^{-1}(\mathfrak{p})$, koje je neprekidno u odnosu na topologiju Zariskog. Skupovi $D(f)$ i $V(I)$ se mogu videti i kao injektivne slike spektara odgovarajućih prstenova, kao u sledećoj lemi:

Lema 2.1.4. *Neka je* $f \in R$ *i neka je* I *ideal u* R*. Ako je* $R[1/f] = R[x]/(xf - 1)$ *lokalizacija od* R *u* f*, tada su (kanonska) preslikavanja* $\operatorname{Spec} R[1/f] \to \operatorname{Spec} R$ *i* $\operatorname{Spec} R/I \to \operatorname{Spec} R$ *injektivna i njihove slike su* $D(f)$ *i* $V(I)$*, redom.*

Vidimo da na ovaj način dobijamo kontravarijantni funktor iz kategorije komutativnih prstenova u kategoriju topoloških prostora. Naime, prstenovi se preslikavaju u njihove spektre, a homomorfizmi među njima postaju neprekidna preslikavanja među spektrima.

Primer 2.1.5. Neka je $R = \mathbb{C}[x]$. Tada se $\operatorname{Spec} \mathbb{C}[x]$ sastoji iz maksimalnih ideala oblika $(x - a)$ za svako $a \in \mathbb{C}$, kao i od tačke (0).

Primer 2.1.6. Neka je $\mathbb{A}^1_{\mathbb{Z}} := \operatorname{Spec} \mathbb{Z}[x]$ i označimo sa $f : \mathbb{A}^1_{\mathbb{Z}} \to \operatorname{Spec} \mathbb{Z}$ neprekidno preslikavanje indukovano kanonskim homomorfizmom $\mathbb{Z} \to \mathbb{Z}[x]$. Tada imamo particiju

$$\mathbb{A}^1_{\mathbb{Z}} = f^{-1}(\{0\}) \cup (\cup_{p \text{ prost}} f^{-1}(p\mathbb{Z})).$$

Neka je S multiplikativni deo $\mathbb{Z} \setminus \{0\}$ od $\mathbb{Z}[x]$. Tada je prost ideal $\mathfrak{p} \in \mathbb{A}^1_{\mathbb{Z}}$ sadržan u $f^{-1}(\{0\})$ ako i samo ako je $\mathfrak{p} \cap \mathbb{Z} = 0$, što je ekvivalentno sa $\mathfrak{p} \cap S = \emptyset$. Kako je lokalizacija $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$, imamo kanonski homeomorfizam između $f^{-1}(\{0\})$ i $\operatorname{Spec} \mathbb{Q}[x] = \mathbb{A}^1_{\mathbb{Q}}$. Ako je p prost broj, tada je $\mathfrak{p} \in f^{-1}(p\mathbb{Z})$ ako i samo ako je $p \in \mathfrak{p}$. Zbog $\mathbb{Z}[x]/(p) = \mathbb{F}_p[x]$ imamo homeomorfizam između $f^{-1}(p\mathbb{Z})$ i $\operatorname{Spec} \mathbb{F}_p[x] = A^1_{\mathbb{F}_p}$.

2.2 Afine sheme

Do pojma afine sheme dolazimo apstrakcijom sledeće situacije: neka je X neki topološki prostor i neka je za proizvoljan otvoren skup $U \subseteq X$ sa $\mathcal{C}(U)$ označen skup svih neprekidnih funkcija $f : U \to \mathbb{R}$. Na ovaj način za svaki otvoren skup dobijamo Abelovu grupu neprekidnih funkcija definisanih na njemu.

Osim toga, ako su U i V otvoreni skupovi takvi da je $V \subseteq U$, tada imamo prirodan homomorfizam $\rho_{UV} : \mathcal{C}(U) \to \mathcal{C}(V)$ koji je dat sa $\rho_{UV}(f) = f|_V$ za $f \in \mathcal{C}(U)$. Uslov neprekidnosti je lokalan, pa ako se U razbije na uniju manjih otvorenih skupova, tada $f \in \mathcal{C}(U)$ zavisi od njenih restrikcija na skupove koji učestvuju u ovom razbijanju.

Ovaj primer možemo da uopštimo uvođenjem pojma *pramena*. Dajemo definiciju za slučaj Abelovih grupa, dok analogne definicije važe za pramenove prstenova, pramenove algebri nad fiksnim prstenom i drugih.

Definicija 2.2.1. Neka je X topološki prostor. *Pretpramen $\mathcal{F}$ (Abelovih grupa) na X se sastoji iz:*

- Abelove grupe $\mathcal{F}(U)$ za svaki otvoren skup $U \subseteq X$,
- homomorfizma grupa $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ za svaki par otvorenih skupova $V \subseteq U$

koji zadovoljavaju sledeće uslove*:*

1. $\mathcal{F}(\emptyset) = 0$;
2. $\rho_{UU} = \mathrm{Id}$;
3. ako imamo otvorene skupove $W \subseteq V \subseteq U$, tada je $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

Često se koristi oznaka $f|_V = \rho_{UV}(f)$. Za element od $\mathcal{F}(U)$ kažemo da je *sekcija* od $\mathcal{F}$ nad U. Pramen je pretpramen koji je određen lokalnim informacijama, u smislu sledeće definicije:

Definicija 2.2.2. Za pretpramen $\mathcal{F}$ kažemo da je *pramen* ako zadovoljava sledeća dva uslova:

- (Jedinstvenost) Neka je U otvoren podskup od X, $f \in \mathcal{F}(U)$, a $\{U_i\}_i$ neko pokrivanje skupa U otvorenim podskupovima U_i. Ako za sve i važi $f|_{U_i} = 0$, tada je $f = 0$.

- (Lepljenje lokalnih sekcija) Zadržavamo oznake iz prethodnog uslova. Neka su $f_i \in \mathcal{F}(U_i)$, $i \in I$, sekcije takve da je $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ za sve indekse $i, j \in I$. Tada postoji sekcija $f \in \mathcal{F}(U)$ takva da je $f|_{U_i} = f_i$.

Primer 2.2.3. Neka je A netrivijalna Abelova grupa i neka je X topološki prostor. Definišimo $\mathcal{A}_X(U) = A$ za otvoren skup U i $\rho_{UV} = \mathrm{Id}_A$ ako su U i V neprazni. Ovo zadaje pretpramen na X. U opštem slučaju, $\mathcal{A}_X$ ne mora biti pramen. Na primer, ako je X disjunktna unija dva neprazna otvorena skupa, tada uslov lepljenja lokalnih sekcija nije zadovoljen.

Primetimo da uslov jedinstvenosti garantuje da je sekcija dobijena lepljenjem jedinstvena. Spektar prstena R je topološki prostor, ali osim toga ima i dodatnu strukturu pramena komutativnih prstenova, koji sledeća teorema preciznije određuje.

Teorema 2.2.4. *Neka je R komutativni prsten. Tada postoji pramen komutativnih prstenova $\mathcal{O}_{\operatorname{Spec} R}$ na $\operatorname{Spec} R$ takav da je*

1. $\mathcal{O}_{\operatorname{Spec} R}(D(f)) \cong R[1/f]$;

2. Dijagram

$$\begin{array}{ccc} \mathcal{O}_{\operatorname{Spec} R}(D(f)) & \xrightarrow{\rho} & \mathcal{O}_{\operatorname{Spec} R}(D(fg)) \\ \cong\downarrow & & \downarrow\cong \\ R[1/f] & \xrightarrow{k} & R[1/fg] \end{array}$$

komutira, gde je sa k označeno kanonsko preslikavanje lokalizacije.

Ovaj pramen je jedinstveno određen gore navedenim svojstvima do na izomorfizam.

Ako je X topološki prostor i $\mathcal{O}_X$ jedan pramen komutativnih prstenova na X, tada se par $(X, \mathcal{O}_X)$ zove *prstenovan prostor*. Na primer, $(\mathbb{R}^n, C^{\infty}_{\mathbb{R}^n})$ je jedan prstenovan prostor. *Afina shema* koja odgovara prstenu R je prstenovan prostor $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$. Oznaka $\operatorname{Spec} R$ se isto koristi i za afinu shemu. Takođe, nekada se koristi oznaka $\Gamma(U, \mathcal{O}_X)$ umesto $\mathcal{O}_X(U)$.

Primetimo i da ako znamo $\operatorname{Spec} R$, da tada možemo dobiti ponovo prsten R kao $\mathcal{O}_{\operatorname{Spec} R}(\operatorname{Spec} R)$. Dajemo nekoliko primera afinih shema.

Primer 2.2.5. Neka je $X = \operatorname{Spec} \mathbb{Z}$. Bazni otvoreni skupovi u X su oblika $D(f)$, gde je f ceo broj koji nije 0. Tada je $\mathcal{O}_X(D(f)) = \mathbb{Z}_f \subseteq \mathbb{Q}$. Racionalan broj a/b sa $(a,b) = 1$ pripada $\mathcal{O}_X(D(f))$ ako i samo ako svaki prost delilac od b deli i f.

Primer 2.2.6. Neka je $X = \operatorname{Spec} \mathbb{Z}[T]$. Neka je p prost broj. Tada je (T,p) maksimalni ideal u $\mathbb{Z}[T]$, pa odgovara zatvorenoj tački. Označimo sa U komplement odgovarajuće zatvorene tačke (to je otvoren skup). Imamo da je $U = D(p) \cup D(T)$, pa je zato $\mathcal{O}_X(U) \subseteq \mathcal{O}_X(D(T)) \cap \mathcal{O}_X(D(p)) = \mathbb{Z}[T, 1/T] \cap \mathbb{Z}[T, 1/p] = \mathbb{Z}[T]$. Odavde je $\mathcal{O}_X(U) = \mathbb{Z}[T] = \mathcal{O}_X(X)$.

Kolekcija svih (pret)pramenova na topološkom prostoru X čini kategoriju ($PSh(X)$) $Sh(X)$. *Morfizam pramenova* je $\eta : \mathcal{F} \to \mathcal{G}$ je kolekcija homomorfizama

$$\eta_U : \mathcal{F}(U) \to \mathcal{G}(U)$$

koja se slaže sa restrikcijom, u smislu da sledeći dijagram komutira za sve otvorene $V \subseteq U$:

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r, "\eta_U"] \arrow[d, "\rho"'] & \mathcal{G}(U) \arrow[d, "\rho"] \\ \mathcal{F}(V) \arrow[r, "\eta_V"] & \mathcal{G}(V) \end{tikzcd}$$

Za morfizam η kažemo da je *izomorfizam* ako je svako η_U izomorfizam.

Neka su $(X, \mathcal{O}_X)$ i $(Y, \mathcal{O}_Y)$ prstenovani prostori. *Izomorfizam prstenovanih prostora* se sastoji iz homeomorfizma $f : X \to Y$ i kolekcije izomorfizama $\eta_U : \mathcal{O}_Y(U) \cong \mathcal{O}_X(f^{-1}U)$ koji su kompatibilni sa restrikcijom.

2.3 Sheme

Kao što se glatke mnogostrukosti dobijaju lepljenjem skupova koji su difeomorfni otvorenim skupovima u Euklidskom prostoru, tako se i sheme dobijaju lepljenjem afinih shema. Naime, shema je prstenovan prostor koji je lokalno afina shema.

Definicija 2.3.1. *Shema* je prstenovan prostor $(X, \mathcal{O}_X)$ takav da postoji otvoreno pokrivanje $\{U_i\}_{i\in I}$ za koje je $(U_i, \mathcal{O}_{X|U_i}) \cong (\operatorname{Spec} R_i, \mathcal{O}_{\operatorname{Spec} R_i})$ za sve $i \in I$, gde se restrikcija pramena definiše pomoću $\mathcal{O}_{X|U_i}(V) = \mathcal{O}_X(V)$ za $V \subseteq U_i$. Skupovi U_i čine *afino otvoreno pokrivanje.*

Nove sheme se mogu dobiti od starih *lepljenjem*. Neka su X_1 i X_2 sheme. Otvoreni skupovi $U_1 \subseteq X_1$ i $U_2 \subseteq X_2$ su takvi da je $\phi : (U_1, \mathcal{O}_{X_1|U_1}) \to (U_2, \mathcal{O}_{X_2|U_2})$ izomorfizam prstenovanih prostora. Tada možemo da dobijemo novu shemu X tako što *zalepimo* X_1 i X_2 po U_1 i U_2 pomoću ϕ. Topološki prostor X se dobija kao količnički prostor disjunktne unije $X_1 \cup X_2$ po relaciji ekvivalencije $x_1 \sim \phi(x_1)$ za svako $x_1 \in U_1$.

Tako dobijamo preslikavanja $i_1 : X_1 \to X$ i $i_2 : X_2 \to X$, pri čemu je skup $V \subseteq X$ otvoren ako i samo ako je $i_1^{-1}(V)$ otvoren u X_1 i $i_2^{-1}(V)$ otvoren u X_2. Tada je strukturalni pramen $\mathcal{O}_X$ definisan ovako: za $V \subseteq X$ je

$$\mathcal{O}_X(V) = \left\{ (f_1, f_2) \,|\, f_1 \in \mathcal{O}_{X_1}(i_1^{-1}(V)) \text{ i } f_2 \in \mathcal{O}_{X_2}(i_2^{-1}(V)) \text{ i } \phi(f_1|_{i_1^{-1}(V) \cap U_1}) = f_2|_{i_2^{-1}(V) \cap U_2} \right\}.$$

Jedan primer sheme koja nije afina shema je dobro poznata projektivna prava.

Primer 2.3.2. (Projektivna prava) Neka je k polje. Neka je $X_1 = \operatorname{Spec}(k[x])$ i $X_2 = \operatorname{Spec}(k[y])$. Neka je $0 \in X_1$ tačka koja odgovara maksimalnom idealu $(x) \subset k[x]$, a ∞ tačka koja odgovara maksimalnom idealu $(y) \subset k[y]$. Uvedimo $U_1 = X_1 \setminus \{0\} = D(x) = \operatorname{Spec} k[x, 1/x]$ i $U_2 = X_2 \setminus \{\infty\} = D(y) = \operatorname{Spec} k[y, 1/y]$. Neka je $\phi : U_1 \to U_2$ izomorfizam dobijen od izomorfizma k-algebri $k[y, 1/y] \to k[x, 1/x]$ koji slika y u $1/x$. Lepljenjem shema X_1 i X_2 pomoću ϕ dobijamo shemu $\mathbb{P}^1_k$. Možemo smatrati da su $X_1, X_2 \subset \mathbb{P}^1_k$ otvorene podsheme.

Primetimo i da je $\mathcal{O}(\mathbb{P}^1_k) = k$, zbog toga što su jedini polinomi $g(x)$ po x takvi da je i $g(1/y)$ polinom po y upravo konstantni polinomi. Osim toga, $\mathbb{P}^1_k$ nije afina shema, zato što ima beskonačno elemenata. Primetimo i da postoji afini otvoren skup $U \subset \mathbb{P}^1_k$ koji sadrži i 0 i ∞. Naime, neka je $U = \mathbb{P}^1_k \setminus \{1\}$, gde je 1 tačka u X_1 koja odgovara maksimalnom idealu $(x-1)$ i tačka u X_2 koja odgovara maksimalnom idealu $(y-1)$. Vidimo da je tada $s = 1/(x-1) = 1/(y-1) \in \mathcal{O}_U(U)$. Može se pokazati da je $\mathcal{O}_U(U)$ jednako prstenu polinoma $k[s]$ i da je odgovarajući morfizam $U \to \operatorname{Spec}(k[s])$ izomorfizam shema.

2.4 Lokalizacija i sheme

Zanima nas kada se neko svojstvo $\mathcal{P}$ komutativnog prstena (na primer svojstvo da je integralni domen) prenosi na sheme. Cilj nam je da shema X ima svojstvo $\mathcal{P}$ ako ima afino otvoreno pokrivanje spektrima prstenova koji zadovoljavaju to svojstvo. Međutim, treba da obezbedimo da ovo ne zavisi od izbora pokrivanja, kao i da kada se vratimo sa afine sheme na odgovarajući prsten dobijamo početnu definiciju.

Podsetimo se pojma *lokalizacije* iz komutativne algebre. Neka je R komutativni prsten. Za podskup $S \subset R$ kažemo da je *multiplikativan* ako je $1 \in S$ i S je zatvoren za množenje. Tada se lokalizacija $S^{-1}R = R[S^{-1}]$ dobija formalnim dodavanjem inverza elemenata iz S. Na primer, za $f \in R$ je skup $S = \{f^n \mid n \in \mathbb{N}_0\}$ multiplikativan, pa ima smisla posmatrati lokalizaciju $S^{-1}R = R[1/f]$. Lokalizacija nam omogućava da odredimo kada se svojstvo prenosi sa prstena na shemu.

Definicija 2.4.1. Za svojstvo $\mathcal{P}$ kažemo da je *lokalno* ako poseduje sledeće osobine:

1. Svojstvo $\mathcal{P}$ je zadovoljeno za $S^{-1}R$ kada god je zadovoljeno za R.

2. Ako postoje elementi $f_1, ..., f_n$ takvi da je $(f_1, f_2, ..., f_n)$ trivijalan ideal i svojstvo $\mathcal{P}$ važi za sve $R[1/f_i]$, tada svojstvo $\mathcal{P}$ važi i za R.

Sada možemo karakterisati svojstva koja se prenose sa prstenova na sheme.

Princip: Svojstvo $\mathcal{P}$ komutativnih prstenova se prenosi na sheme ako je lokalno.

Treba nam metod da jednostavnije proverimo da li je neko svojstvo lokalno. Neka je dat prost ideal $\mathfrak{p} \subset R$. Tada je njegov komplement $S = R \setminus \mathfrak{p}$ multiplikativan skup, pa je lokalizacija $R_\mathfrak{p} = S^{-1}R$ dobro definisana. Ovaj prsten ima jedinstveni maksimalan ideal $\mathfrak{p}R_\mathfrak{p}$, pa je u pitanju lokalni prsten. Vidimo da je svojstvo $\mathcal{P}$ lokalno kada: R zadovoljava $\mathcal{P}$ ako i samo ako svi $R_\mathfrak{p}$ zadovoljavaju $\mathcal{P}$.

Prsten je *redukovan* ako nema nilpotentnih elemenata. Redukovanost prstena je primer lokalnog svojstva. Naime, iz komutativne algebre je poznato da prsten R nema nilpotentnih elemenata ako i samo ako $A_\mathfrak{p}$ nema nilpotentnih elemenata za svaki prost ideal $\mathfrak{p} \subset A$.

Lokalizacija u prostom idealu $\mathfrak{p}$ ima interpretaciju i u kontekstu teorije pramenova. Trebaće nam prvo sledeća opšta definicija u kontekstu proizvoljnog pramena na topološkom prostoru:

Definicija 2.4.2. Neka je $\mathcal{F}$ pramen na X i neka je $x \in X$. *Sloj od* $\mathcal{F}$ *u* x je direktan limes

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U)$$

po svim otvorenim okolinama U od x. Ako je $\mathcal{F}$ pramen prstenova, tada je i $\mathcal{F}_x$ prsten. Za sekciju $f \in \mathcal{F}(U)$ i $x \in U$ sliku od f u $\mathcal{F}_x$ označavamo sa f_x i zovemo je *klica od* f *u* x.

Vidimo da je preslikavanje $\mathcal{F}(U) \to \mathcal{F}_x$ koje je dato sa $f \mapsto f_x$ homomorfizam. Sloj $\mathcal{F}_x$ nam daje lokalno ponašanje pramena u blizini x.

Primer 2.4.3. Neka je $X = \mathbb{R}^n$ sa Euklidskom topologijom. Posmatrajmo pretpramen $\mathcal{C}^\infty$ (glatkih) funkcija na X, u oznaci $\mathcal{C}^\infty_{\mathbb{R}^n}$. Tada je $\mathcal{C}^\infty_{\mathbb{R}^n}(U)$ skup svih glatkih funkcija $f : U \to \mathbb{R}$. Jednostavno se proverava da je ovo zapravo pramen $\mathbb{R}$-vektorskih prostora. Neka je dalje $x \in X = \mathbb{R}^n$ tačka. Element sloja $\mathcal{C}^\infty_{\mathbb{R}^n,x}$ je dat glatkom funkcijom čiji domen sadrži x i svake dve takve funkcije f i g određuju istu klicu ako se poklapaju na nekoj okolini od x.

Kada je X shema, tada tačka x ima okolinu koja je izomorfna spektru nekog prstena R. Ovde možemo tačku x da posmatramo kao prost ideal. Skupovi oblika $D(f)$ takvi da $f \notin x$ formiraju kofinalan sistem kao otvorene okoline, pa dobijamo isti direktan limes, odnosno

Teorema 2.4.4. Sloj $\mathcal{O}_{X,x}$ je izomorfan sa $\varinjlim R[1/f]$, koji je izomorfan sa lokalizacijom R_x.

2.5 Morfizmi

Ako imamo neprekidno preslikavanje $f : X \to Y$ i pramen $\mathcal{F}$ na X, *direktna slika* $f_*\mathcal{F}$ je pramen na Y koji je definisan sa $f_*\mathcal{F}(U) = \mathcal{F}(f^{-1}U)$. Sada možemo da definišemo morfizme.

Definicija 2.5.1. *Morfizam shema* $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ se sastoji iz:

1. neprekidnog preslikavanja $f : X \to Y$,
2. morfizma pramenova $f^\# : \mathcal{O}_Y \to \mathcal{O}_X$ takvog da je za sve $x \in X$ indukovani homomorfizam $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,f(x)}$ lokalni, u smislu da je inverzna slika od $m_{f(x)}$ upravo m_x.

Da bismo bolje razumeli ovu definiciju, posmatrajmo situaciju gde imamo homomorfizam prstenova $h : R \to S$. Tada ovaj homomorfizam indukuje neprekidno preslikavanje $f : \operatorname{Spec} S \to \operatorname{Spec} R$ dato sa $f(\mathfrak{p}) = h^{-1}(\mathfrak{p})$. Imamo preslikavanje pramenova $f^\# : \mathcal{O}_{\operatorname{Spec} R} \to \mathcal{O}_{\operatorname{Spec} S}$ koje je na baznim otvorenim skupovima određeno sa

$$\begin{array}{ccc} \mathcal{O}(D(r)) & \longrightarrow & \mathcal{O}(f^{-1}D(r)) \\ {\scriptstyle\cong}\downarrow & & \downarrow{\scriptstyle\cong} \\ R[1/r] & \longrightarrow & S[1/h(r)] \end{array}$$

pri čemu je donje preslikavanje dato sa $x/r^n \mapsto f(x)/h(r)^n$. Nije teško videti da je preslikavanje $R_{h^{-1}(\mathfrak{p})} \to S_{\mathfrak{p}}$ lokalno. Obrnuto, svaki morfizam shema $\operatorname{Spec} S \to \operatorname{Spec} R$ dolazi od homomorfizma $R \to S$ datog sa $\mathcal{O}(\operatorname{Spec} R) \to \mathcal{O}(\operatorname{Spec} S)$.

Opišimo sada morfizam među shemama X i Y u opštem slučaju. Pretpostavimo da imamo neprekidno preslikavanje $f : X \to Y$, afino otvoreno pokrivanje $U_i = \operatorname{Spec} R_i$ od Y, afino otvoreno pokrivanje $\operatorname{Spec} S_{ij}$ od svakog $f^{-1}U_i$ i homomorfizme $h_{ij} : R_i \to S_{ij}$ koji zadovoljavaju odgovarajuće uslove kompatibilnosti. Tada se svojstvo $\mathcal{P}$ homomorfizama prstenova $h : R \to S$ prenosi na homomorfizme shema ako se $\mathcal{P}$ može karakterisati preko lokalnih homomorfizama $R_{h^{-1}(\mathfrak{p})} \to S_{\mathfrak{p}}$.

Uvedimo ovde još jedan ključan pojam iz teorije shema. U pitanju je vrsta proizvoda shema.

Definicija 2.5.2. Neka su $f : X \to S$ i $g : Y \to S$ morfizmi shema. Njihov *proizvod fibri* je shema $X \times_S Y$ zajedno sa morfizmima projekcije $p : X \times_S Y \to X$ i $q : X \times_S Y \to Y$ koji čine sledeći komutativni dijagram

$$\begin{array}{ccc} X \times_S Y & \xrightarrow{q} & Y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & S \end{array}$$

koji poseduje univerzalno svojstvo u odnosu na sve dijagrame ovog tipa.

Za afine sheme se proizvod fibri svodi na spektar tenzorskog proizvoda odgovarajućih prstenova. Ilustrujmo to na sledećem primeru:

$$\operatorname{Spec} \mathbb{Z}[x_1, ..., x_n]/(f_1, ..., f_N) \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Z}/p\mathbb{Z} = \operatorname{Spec}(\mathbb{Z}[x_1, ..., x_n]/(f_1, ..., f_N) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z})$$

$$= \operatorname{Spec} \mathbb{Z}/p\mathbb{Z}[x_1, ..., x_n]/(f_1, ..., f_N).$$

U prethodnom primeru se proizvod fibri zapravo svodi na redukciju po modulu p.

Glava 3

Algebarska fundamentalna grupa

Algebarska fundamentalna grupa, poznata i kao *etalna* fundamentalna grupa predstavlja analog fundamentalne grupe topološkog prostora u teoriji shema. Ona se može izraziti kao Galoaova grupa raširenja polja. Mi ćemo ovde predstaviti ključne rezultate u vezi sa algebarskom fundamentalnom grupom, a glavna referenca nam je [11]. Detaljniji prikaz rezultata koje navodimo se može naći u [9]. Uvodni deo o beskonačnoj teoriji Galoa je klasičan i može se naći u bilo kojem naprednijem kursu o Galoaovoj teoriji.

3.1 Beskonačna teorija Galoa

U algebarskoj teoriji brojeva se najčešće susrećemo sa konačnim Galoaovim raširenjima. Konačne grupe su topološke grupe sa diskretnom topologijom, tako da u ovom slučaju njihove topološke osobine ne dolaze do izražaja. Kada radimo sa poljima funkcija, neophodno je razumeti strukturu Galoaove grupe beskonačnog raširenja polja.

Pretpostavimo da imamo niz grupa $\{G_n\}_{n\geq 0}$ i homomorfizme $f_n : G_n \to G_{n-1}$ među njima za $n \geq 1$:

$$... \to G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0.$$

Tada možemo da definišemo njihov *inverzni limes* kao grupu

$$\varprojlim_n G_n = \left\{ (g_n) \in \prod G_n \mid f_n(g_n) = g_{n-1} \right\}.$$

Za grupu kažemo da je *profinitna* ako je jednaka inverznom limesu konačnih grupa (sa podrazumevanom diskretnom topologijom). Najpoznatiji primer profinitne grupe je aditivna grupa p-adičkih brojeva.

Primer 3.1.1. Neka je p fiksan prost broj. Imamo niz grupa $G_n = \mathbb{Z}/p^n\mathbb{Z}$ sa prirodno definisanim homomorfizmima među njima. *Aditivna grupa p-adičkih brojeva* je profinitna grupa koja se dobija kao inverzni limes

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Ako svakoj konačnoj grupi dodelimo diskretnu topologiju, tada je profinitna grupa dobijena kao njihov inverzni limes topološka grupa. Naime, uzimanje inverznog limesa u kategoriji topoloških grupa je isto kao da uzimamo inverzni limes u kategoriji grupa i kategoriji topoloških prostora odvojeno.

Trebaće nam topološki pojam *totalne nepovezanosti* kako bismo karakterisali profinitne grupe. Naime, kažemo da je topološki prostor totalno nepovezan ako ima bazu koja se sastoji od skupova koji su i otvoreni i zatvoreni.

Teorema 3.1.2. Topološka grupa je profinitna ako i samo ako je kompaktna Hausdorfova i totalno nepovezana.

Kod beskonačnih Galoaovih grupa imamo situaciju da ne mora svaka podgrupa od $\mathrm{Gal}(L/K)$ da odgovara međuraširenju od L/K. Zbog toga uvodimo topologiju na $\mathrm{Gal}(L/K)$ koja prepoznaje takve podgrupe.

Lema 3.1.3. Neka je L/K Galoaovo raširenje sa Galoaovom grupom $G = \mathrm{Gal}(L/K)$. Ako je F/K normalno međuraširenje od L/K, tada je $H = \mathrm{Gal}(L/F)$ normalna podgrupa od G sa fiksnim poljem F, pri čemu imamo tačan niz

$$1 \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \to 1,$$

gde je prvo preslikavanje inkluzija, a drugo preslikavanje je indukovano restrikcijom i važi

$$G/H \cong \mathrm{Gal}(F/K).$$

Međutim, u slučaju beskonačnih Galoaovih raširenja, normalna podgrupa H od $\mathrm{Gal}(L/K)$ sa fiksnim poljem F *ne mora* da bude jednaka $\mathrm{Gal}(L/F)$, već može biti i njena prava podgrupa. Na primer, ovo je slučaj kod svih osim prebrojivo mnogo podgrupa H indeksa 2 od $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Zbog toga se uvodi posebna topologija na Galoaovoj grupi.

Definicija 3.1.4. Neka je L/K Galoaovo raširenje sa Galoaovom grupom $G = \mathrm{Gal}(L/K)$. *Krulova topologija* na G je topologija čiji su bazni otvoreni skupovi svi koseti podgrupa $H_F = \mathrm{Gal}(L/F)$, gde F prolazi kroz sva konačna normalna raširenja od K u L.

Topološka grupa koja se dobija tako što se Krulova topologija dodeli grupi $\mathrm{Gal}(L/K)$ je profinitna grupa. Navodimo teoremu koja nam daje način da Galoaovu grupu predstavimo kao inverzni limes.

Teorema 3.1.5. Neka je L/K Galoaovo raširenje. U Krulovoj topologiji, preslikavanja restrikcije indukuju prirodni izomorfizam topoloških grupa

$$\phi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(F/K),$$

gde F prolazi kroz sva konačna Galoaova raširenja od K u L. Specijalno, $\mathrm{Gal}(L/K)$ je profinitna grupa čije su normalne podgrupe oblika $\mathrm{Gal}(L/F)$ za neko konačno Galoaovo raširenje F/K.

Kao i u slučaju konačne teorije Galoa, imamo teoremu o Galoaovoj korespondenciji. Ovde dolazi do izražaja topologija, zato što su podgrupe koje odgovaraju međuraširenjima upravo one koje su zatvorene.

Teorema 3.1.6. (Galoaova korespondencija) Postoji bijektivna korespondencija između zatvorenih podgrupa od $\mathrm{Gal}(L/K)$ i međuraširenja polja: $H \subseteq \mathrm{Gal}(L/K)$ odgovara raširenju $L^H = \{f \in L \mid \forall h \in H,\ hf = f\}$. Galoaova raširenja odgovaraju zatvorenim normalnim podgrupama.

3.2 Etalni morfizmi shema

Ovaj odeljak se oslanja na tehnike komutativne algebre, pre svega na osobine *ravnih morfizama*. Podsetimo se da je homomorfizam prstenova $A \to B$ *ravan* ako je funktor $M \mapsto B \otimes_A M$ iz A-module u B-module tačan. Možemo da kažemo i da je B *ravna* A-algebra. Ako imamo morfizam shema $\varphi : Y \to X$, cilj nam je da definišemo kada je on ravan.

Definicija 3.2.1. Neka su X i Y sheme. Morfizam $\varphi : Y \to X$ shema je *ravan* ako su lokalni homomorfizmi $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ ravni za sve $y \in Y$.

Da bismo proverili da je homomorfizam prstenova $f : A \to B$ ravan, dovoljno je za svaki maksimalan ideal $\mathfrak{m}$ u B proveriti da je lokalni homomorfizam $A_{f^{-1}(\mathfrak{m})} \to B_{\mathfrak{m}}$ ravan. U slučaju Dedekindovih domena je homomorfizam ravan ako i samo ako je injektivan.

Na osnovu prethodnog, da bismo proverili da li je morfizam shema ravan, dovoljno je da to proverimo za zatvorene tačke $y \in Y$. Ako je Z zatvorena podshema od X, inkluzija $Z \hookrightarrow X$ je ravna ako i samo ako je Z istovremeno i otvorena u X.

Sledeći pojam se pojavljuje i u kontekstu algebarkse teorije brojeva, a definicija koju dajemo ovde se poklapa sa onom iz algebarske teorije brojeva gde posmatramo prstenove sa diskretnom valuacijom.

Definicija 3.2.2. Lokalni homomorfizam $f : A \to B$ lokalnih prstenova je *nerazgranat* ako je $B/f(\mathfrak{m}_A)B$ konačno separabilno raširenje od $A/\mathfrak{m}_A$.

Ekvivalentno, f je nerazgranat ako je $f(\mathfrak{m}_A)B = \mathfrak{m}_B$ i polje $B/\mathfrak{m}_B$ je konačno i separabilno raširenje od $A/\mathfrak{m}_A$. Ovu definiciju možemo da prenesemo i na sheme, a ispunjenost uslova iz definicije je dovoljno proveriti za zatvorene tačke $y \in Y$.

Primer 3.2.3. Neka je L/K konačno raširenje polja. Tada je $\operatorname{Spec} L \to \operatorname{Spec} K$ nerazgranat ako i samo ako je raširenje L/K separabilno.

Primer 3.2.4. Neka je L/K raširenje brojevnih polja i neka su $\mathcal{O}_L$ i $\mathcal{O}_K$ njihovi odgovarajući prstenovi celih. Tada je $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ ravan i za svaki prosti ideal $\mathfrak{q}$ od $\mathcal{O}_L$, postavljanjem $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, raširenje $k(\mathfrak{q})$ od $k(\mathfrak{p})$ je separabilno. Morfizam $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ je nerazgranat u prostom idealu $\mathfrak{q}$ od $\mathcal{O}_L$ ako i samo ako je $\mathfrak{q}(\mathcal{O}_L)\mathfrak{q}$ generisan sa $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Vidimo da se ovde definicija svodi na poznatu definiciju nerazgranatosti iz teorije brojeva.

Definicija 3.2.5. Za morfizam shema $\varphi : Y \to X$ kažemo da je *etalni morfizam* ako je ravan i nerazgranat.

Ako imamo homomorfizam prstenova $f : A \to B$, on je etalni morfizam ako je odgovarajući morfizam $\operatorname{Spec} B \to \operatorname{Spec} A$ etalni morfizam. Ovakve homomorfizme prstenova možemo karakterisati i jezikom komutativne algebre pomoću sledeće teoreme:

Teorema 3.2.6. Homomorfizam prstenova $f : A \to B$ je etalni morfizam ako važi:

- B je konačno generisana A-algebra;

- B je ravna A-algebra;
- za sve maksimalne ideale $\mathfrak{n}$ u B, $B_{\mathfrak{n}}/f(\mathfrak{p})B_{\mathfrak{n}}$ je konačno separabilno raširenje polja $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, gde je $\mathfrak{p} = f^{-1}(\mathfrak{n})$.

Primetimo da je etalni morfizam u nekom smislu lokalni izomorfizam. U diferencijalnoj geometriji inkluzija prave zatvorene podmnogostrukosti u povezanu mnogostrukost nije lokalni izomorfizam. Slična je situacija i ovde: neka je $X = \operatorname{Spec} A$, gde je A integralni domen. Ako uzmemo bilo koji pravi ideal $\mathfrak{a} \subset A$, preslikavanje $Z \hookrightarrow X$ koje odgovara homomorfizmu $A \to A/\mathfrak{a}$ je nerazgranato, ali nije ravno, pa nije etalni morfizam.

Primer 3.2.7. Neka je k polje, $P(T) \in k[T]$ moničan polinom i $X = \operatorname{Spec} k[T]/(P)$. Tada tačka $x \in X$ odgovara nerastavljivom faktoru $Q(T)$ od $P(T)$. Kanonski izomorfizam $X \to \operatorname{Spec} k$ je etalni u x ako i samo ako je $Q(T)$ separabilan polinom i ako je $Q(T)$ faktor od $P(T)$ višestrukosti jedan.

3.3 Definicija i osobine algebarske fundamentalne grupe

Pre nego što definišemo algebarsku fundamentalnu grupu, podsetimo se prvo pojma fundamentalne grupe u algebarskoj topologiji. Neka je X povezan topološki prostor. Fundamentalna grupa $\pi_1(X)$ je grupa homotopskih klasa ekvivalencije zatvorenih puteva u X sa datom baznom tačkom.

Ova definicija nam nije praktična, pa dajemo karakterizaciju koja nam je od veće koristi u cilju definisanja algebarske fundamentalne grupe. Podsetimo se da je natkrivanje $\pi : Y \to X$ lokalno homeomorfizam. *Univerzalno natkrivanje* $\pi : \tilde{X} \to X$ je natkrivanje takvo da je $\tilde{X}$ povezan i prosto povezan, odnosno $\pi_1(\tilde{X}) = \{1\}$. Tada se $\pi_1(X)$ može identifikovati sa grupom homeomorfizama $\tilde{X} \to \tilde{X}$ koji komutiraju sa π. Glavni nedostatak definicije fundamentalne grupe na koju smo navikli u algebarskoj topologiji je u ovom kontekstu to što univerzalno natkrivanje nema značenje u algebarskoj geometriji.

Sledeća teorema nam sugeriše kako možemo da prevaziđemo ovaj problem. Za preslikavanje $f : X \to Y$ kažemo da je *„konačno na jedan”* ako je za sve $y \in Y$ skup $f^{-1}(\{y\})$ konačan.

Teorema 3.3.1. (Rimanova teorema o egzistenciji) Svaki etalni morfizam $Y \to X$ je „konačno na jedan" natkrivanje od X sa standardnom topologijom. Obrnuto, svako „konačno na jedan" natkrivanje se dobija na ovaj način od jedinstvenog etalnog pokrivanja.

Ideja je da dobijemo neki vid fundamentalne grupe od kolekcije etalnih pokrivanja. Zbog jednostavnosti pretpostavljamo da je X *normalna shema*. Podsetimo se da je prsten R *normalan* ako su svi njegovi lokalni prstenovi normalni domeni, a da je domen *normalan domen* ako je integralno zatvoren u svojem polju razlomaka. Kada kažemo da je shema X normalna, to znači da je za sve $x \in X$ lokalni prsten $\mathcal{O}_{X,x}$ normalni domen. Ova pretpostavka praktično znači da je X ireducibilan topološki prostor koji je pokriven spektrima normalnih prstenova.

Neka je sad X normalna shema. Tada je $X = \cup_{i \in I} \operatorname{Spec} R_i$, gde je polje razlomaka $\operatorname{Frac}(R_i)$ nezavisno od i. Zbog toga postoji polje $K(X)$ takvo da je za sve $i \in I$ $\operatorname{Frac}(R_i) = K(X)$ i ovo polje se zove *polje razlomaka* od X.

Neka je sada L konačno raširenje polja $K(X)$. Neka je $\tilde{R}_i$ integralno zatvorenje od R_i u L. Ako zalepimo spektre $\operatorname{Spec} \tilde{R}_i$ dobijamo novu normalnu shemu $X_L \to X$ sa poljem funkcija L. Sada možemo definisati algebarsku fundamentalnu grupu.

Definicija 3.3.2. *Maksimalno nerazgranato raširenje* se definiše kao

$$K(X)_{unr} = \bigcup \{L \supset K(X) \mid X_L \to X \text{ je etalno}\}.$$

Kada radimo sa normalnim shemama, algebarska fundamentalna grupa je zapravo Galoaova grupa raširenja polja. Naime, maksimalno nerazgranato raširenje je Galoaovo raširenje polja funkcija $K(X)$.

Definicija 3.3.3. *Algebarska fundamentalna grupa* je Galoaova grupa

$$\pi_1^{et}(X) = \operatorname{Gal}(K(X)_{unr}/K(X)).$$

Za računanje algebarske fundamentalne grupe je korisna i sledeća teorema koju je dokazao Grotendik, a koja povezuje algebarsku fundamentalnu grupu sa topološkom fundamentalnom grupom.

Teorema 3.3.4. (Grotendik) Neka je X shema konačnog tipa nad $\mathbb{C}$. Tada je $\pi_1^{et}(X)$ profinitno kompletiranje fundamentalne grupe $\pi_1(X)$.

Sledeći primeri pokazuju kako se algebarska fundamentalna grupa računa u primerima iz teorije brojeva.

Primer 3.3.5. Neka je $X = \operatorname{Spec}\mathbb{Z}$. Tada je $K(X) = \mathbb{Q}$. Kako je X normalna shema, konačne etalne sheme nad X su oblika $\operatorname{Spec}\mathcal{O}_K$ za neko brojevno polje K, zbog toga što je $\mathcal{O}_K$ normalizacija od $\mathbb{Z}$ u brojevnom polju K. Neka je sad stepen raširenja $n = r_1 + 2r_2$ gde je r_1 broj realnih a r_2 broj kompleksnih utapanja od K i neka je Δ_K diskriminanta od K. Iz granice Minkovskog, svaka klasa u klasnoj grupi $\mathrm{Cl}(K)$ ima integralni ideal sa normom koja je odozgo ograničena sa

$$M_K = \sqrt{|\Delta|_K}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

Međutim, po definiciji integralni ideal u $\mathcal{O}_K$ ima normu barem 1, pa je $1 \leq M_K$ i zato je

$$\sqrt{|\Delta|_K} \geq \left(\frac{\pi}{4}\right)^{r_2}\cdot\frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n/2}\cdot\frac{n^n}{n!}.$$

Zato ako K ima stepen $n > 1$, tada je $|\Delta_K| > 1$, pa postoji prost broj p koji deli Δ_K. To znači da je $\operatorname{Spec}\mathcal{O}_K \to \operatorname{Spec}\mathbb{Z}$ negde razgranato, osim kada je $K = \mathbb{Q}$, pa je zbog toga $\pi_1^{et}(\operatorname{Spec}\mathbb{Z}) = 1$.

Primer 3.3.6. Neka je $X = \operatorname{Spec}\mathbb{Z}[1/n]$. Kao i ranije, konačne etalne sheme nad X su oblika $\operatorname{Spec}\mathcal{O}_K[1/n]$, gde je $\mathcal{O}_K$ nerazgranat iznad $\operatorname{Spec}\mathbb{Z}$ dalje od prostih koji dele n (kažemo nerazgranat dalje od n). Zbog toga je $\pi_1^{et}(\operatorname{Spec}\mathbb{Z}[1/n]) \cong \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})$, gde je $\mathbb{Q}^{(n)}$ maksimalno raširenje od $\mathbb{Q}$ nerazgranato dalje od n.

Primer 3.3.7. Neka je $X = \operatorname{Spec} k$, gde je k neko polje. Tada je $K(X)_{unr} = k^{sep}$ separabilno zatvorenje od k. Zato je u ovom slučaju $\pi_1^{et}(X) = \mathrm{Gal}(k^{sep}/k)$ apsolutna Galoaova grupa od k.

3.4 Prva etalna kohomologija

Motivacija nam ponovo dolazi iz algebarske topologije. Teorema Hurevica nam govori da je Abelizacija fundamentalne grupe $\pi_1(X)/[\pi_1(X), \pi_1(X)]$ izomorfna prvoj homologiji $H_1(X, \mathbb{Z})$. Zajedno sa teoremom o univerzalnim koeficijentima dobijamo prvu kohomologiju sa koeficijentima u Abelovoj grupi A:

$$H^1(X, A) \cong \mathrm{Hom}(H_1(X, \mathbb{Z}), A) \cong \mathrm{Hom}(\pi_1(X), A).$$

Ovo motiviše sledeću definiciju

Definicija 3.4.1. Neka je A konačna Abelova grupa. *Prva etalna kohomologija* je

$$H^1(X_{et}, A) = \mathrm{Hom}(\pi_1^{et}(X), A).$$

Ako je X definisano nad $\mathbb{C}$, ova definicija se poklapa sa standardnom kohomologijom. Ako je X definisana nad poljem k koje nije algebarski zatvoreno, čije separabilno zatvorenje je k^{sep}, tada niz raširenja $k \subset k^{sep} \subset K(X)_{unr}$ daje tačan niz kao u lemi 3.1.3.

$$1 \to \mathrm{Gal}(K(X)_{unr}/k^{sep}) \to \pi_1^{et}(X) \xrightarrow{p} \mathrm{Gal}(k) \to 1,$$

gde je $\mathrm{Gal}(k)$ apsolutna Galoaova grupa.

Grupa levo u tačnom nizu se može identifikovati sa algebarskom fundamentalnom grupom odgovarajuće sheme $\bar{X} = X \times_{\mathrm{Spec}\, k} k^{sep}$ nad k^{sep}. Ako izaberemo neprekidnu sekciju za p, dobijamo dejstvo $\mathrm{Gal}(k)$ na $\pi_1^{et}(\bar{X})$, što nam daje dobro definisano dejstvo na $H^1(X_{et}, A)$. Na ovaj način dobijamo strukturu Galoaovog modula.

Glava 4

Etalna kohomologija

Aleksandar Grotendik i Majkl Artin su razvili *etalnu kohomologiju* u ranim šezdesetim godinama prošlog veka, sa ciljem razvijanja kohomološke teorije svojstvene shemama. Možda i najpoznatija primena etalne kohomologije je u dokazu Vejlovih hipoteza.

Jedno od ključnih Grotendikovih zapažanja je da se generalizacijom definicije topološkog prostora dobijaju razni korisni primeri, kao što je *etalna topologija*. Etalna „topologija" na X je ona za koju su „otvoreni skupovi" etalni morfizmi $U \to X$.

U ovoj glavi je predstavljen najznačajniji tehnički aparat koji se koristi u ovom master radu. Cilj nam je da u ovoj glavi uvedemo osnove kohomologije koje ćemo primenjivati u preostalom delu rada, te je zato ova glava najobimnija.

Pratimo izlaganje u [11], [6] i [4].

4.1 Grotendikove topologije

Da bismo definisali pramen $\mathcal{F}$, ne treba nam kompletna topologija, već samo pojam otvorenog pokrivanja. Aksiome koje su nam neophodne da bismo mogli da definišemo pramen su istaknute u sledećoj definiciji

Definicija 4.1.1. Neka je $\mathcal{C}$ kategorija. *Grotendikova topologija T na $\mathcal{C}$* se sastoji od kolekcija istaknutih preslikavanja $\{U_i \to U\}_{i\in I}$, koja se zovu *pokrivanja od U*, za svako U iz $\mathcal{C}$ tako da su zadovoljene sledeće aksiome:

1. Ako su $U_i \to U$ i $U_j \to U$ pokrivanja, tada je $U_i \times_U U_j \to U$ isto pokrivanje.
2. Ako su $\{U_i \to U\}_{i\in I}$ i $\{U_{ij} \to U_i\}_{j\in J}$ pokrivanja od U i U_i, redom, tada je $\{U_{ij} \to U\}_{(i,j)\in I\times J}$ pokrivanje od U.

3. Skup koji se sastoji od identičkog preslikavanja $\{U \to U\}$ je pokrivanje.

Ako imamo Grotendikovu topologiju T na kategoriji $\mathcal{C}$ kao u definiciji iznad, tada se par $(\mathcal{C}, T)$ zove *mesto.*

Primer 4.1.2. Neka je X topološki prostor. Skup svih otvorenih skupova u X u oznaci $Op(X)$ je jedna kategorija, gde $U \to V$ znači $U \subseteq V$. Pokrivanje $\{U_i \to U\}$ je pokrivanje u klasičnom smislu.

Primer 4.1.3. Neka je X shema i neka je $Et(X)$ kategorija čiji su objekti etalni morfizmi $U \to X$, a morfizmi komutativni trouglovi

$$\begin{tikzcd} U \arrow[r] \arrow[dr] & V \arrow[d] \\ & X \end{tikzcd}$$

Kažemo da je $\{\pi_i : U_i \to U\}$ pokrivanje ako je $\bigcup \pi_i(U_i) = U$. Kategorija $Et(X)$ sa ovom Grotendikovom topologijom se zove *etalno mesto* od X u oznaci X_{et}.

Za shemu X kažemo da je *lokalno Neterina* ako svako $x \in X$ ima afinu otvorenu okolinu $\mathrm{Spec}(R) = U \subset X$ takvu da je prsten R Neterin. Shema X je *Neterina* ako je lokalno Neterina i kvazikompaktna (svako otvoreno pokrivanje ima konačno potpokrivanje).

Primer 4.1.4. Neka je X Neterina shema. Neka je $Flat(X)$ kategorija koja kao objekte ima ravne morfizme $U \to X$ uz sledeći uslov konačnosti: inverzna slika afinog otvorenog skupa u X je pokrivena sa konačno mnogo afinih otvorenih skupova u U. Morfizmi su komutativni trouglovi kao u prethodnom primeru. Kažemo da je $\{\pi_i : U_i \to U\}$ pokrivanje ako slike pokrivaju U. Kategoriju $Flat(X)$ sa ovom Grotendikovom topologijom nazivamo *ravnim mestom od X,* u oznaci X_{flat}.

Neka je $(\mathcal{C}, T)$ mesto. Cilj nam je da uopštimo definiciju pramena na Grotendikove topologije. Pramen grupa, prstenova ili algebri je kontravarijantni funktor $\mathcal{F}$ iz $\mathcal{C}$ u kategoriju grupa, prstenova odnosno algebri. Ako imamo neko pokrivanje $\{U_i \to U\}$, definišemo skup *zakrpljivih sekcija* kao

$$\tilde{H}^0(\{U_i \to U\}, \mathcal{F}) = \Big\{(f_i) \in \prod \mathcal{F}(U_i) \mid \operatorname{Im} f_i = \operatorname{Im} f_j \text{ u } \mathcal{F}(U_i \times_U U_j)\Big\}.$$

Imamo kanonsko preslikavanje

$$\mathcal{F}(U) \to \tilde{H}^0(\{U_i \to U\}, \mathcal{F})$$

koje svako $f \in \mathcal{F}(U)$ šalje u kolekciju njegovih slika u $\mathcal{F}(U_i)$. U opštem smislu, kažemo da je $\mathcal{F}$ pramen ako je za svako pokrivanje $\{U_i \to U\}$ zadovoljeno

$$\mathcal{F}(U) \cong \tilde{H}^0(\{U_i \to U\}, \mathcal{F}).$$

Primetimo da se ovo poklapa sa klasičnom definicijom kada radimo u $Op(X)$. Sledeće tvrđenje nam daje kriterijum za proveru da li je nešto pramen kod ravnog mesta i etalnog mesta.

Teorema 4.1.5. Pretpramen $\mathcal{F}$ na X_{et}, odnosno X_{flat}, je pramen ako i samo ako:

- $\mathcal{F}$ je pramen u odnosu na topologiju Zariskog na X,
- Za svako pokrivanje $U' \to U$ afinih shema u X_{et}, odnosno X_{flat} je

$$\mathcal{F}(U) \cong \tilde{H}^0(\{U' \to U\}, \mathcal{F}).$$

Zanimljivo je uporediti ove topologije u slučaju polja. Neka je $X = \operatorname{Spec} k$, gde je k neko polje. Topologija Zariskog na X je trivijalna, ali je etalna topologija na X dosta bogatija. Naime, elementi od X_{et} su oblika $\operatorname{Spec} \prod L_i$, gde su L_i separabilna raširenja. Neka je $K = k^{sep}$ i $G = \operatorname{Gal}(K/k)$. Tada ovo može da se zapiše kao $\operatorname{Spec} \prod K^{G_i}$ za neke otvorene $G_i \subset G$. Podsetimo se da je G-modul Abelova grupa M sa diskretnom topologijom na koju G ima neprekidno dejstvo. Poslednji uslov je ekvivalentan tome da svaki element od M ima konačnu orbitu. Za dato M možemo da definišemo

$$\mathcal{F}_M(\operatorname{Spec} \prod K^{G_i}) = \bigoplus M^{G_i}.$$

Teorema 4.1.6. Sa $\mathcal{F}_M$ je zadat pramen na X_{et}. Korespondencija $M \to \mathcal{F}_M$ daje ekvivalenciju između kategorija G-modula i pramenova Abelovih grupa.

Primer 4.1.7. Neka je X normalna shema i neka je M jedan $\pi_1^{et}(X)$-modul. Ako je $U \to X$ etalna i povezana, tada $\pi_1^{et}(U)$ ima dejstvo na M preko homeomorfizma $\pi_1^{et}(U) \to \pi_1^{et}(X)$. Tada

$$\mathcal{F}_M(U) = M^{\pi_1^{et}(U)}$$

određuje jedan pramen na X_{et}. Pramenovi koji nastaju na ovaj način se zovu *lokalno konstantni.* Pramen $\mathcal{F}_M$ je lokalno konstantan ako je dejstvo $\pi_1^{et}(X)$ trivijalno.

4.2 Primeri pramenova u etalnim mestima

Neka je $A \to B$ homomorfizam prstenova koji odgovara surjektivnom etalnom morfizmu $V \to U$ afinih shema. U ovom odeljku radimo sa *verno ravnim* homomorfizmima prstenova (nije neophodno da budu nerazgranati). Podsetimo se prvo ove definicije iz komutativne algebre.

Definicija 4.2.1. Homomorfizam prstenova $A \to B$ je *verno ravan* ako zadovoljava jedan od sledećih ekvivalentnih uslova:

- Ako je A-modul M nenula, tada je $B \otimes_A M$ nenula.
- Ako niz A-modula $M' \to M \to M''$ nije tačan, tada nije tačan ni niz
$$B \otimes_A M' \to B \otimes_A M \to B \otimes_A M''.$$
- Preslikavanje $\operatorname{Spec} B \to \operatorname{Spec} A$ je surjektivno.

Sledeće tvrđenje iz komutativne algebre često koristimo u konstrukciji primera pramenova.

Teorema 4.2.2. Za svaki verno ravni homomorfizam $A \to B$ je sledeći niz tačan:

$$0 \longrightarrow A \longrightarrow B \xrightarrow{h} B \otimes_A B,$$

gde je $h(b) = 1 \otimes b - b \otimes 1$.

Dokaz. 1° Tvrđenje je tačno ako $f : A \to B$ dozvoljava sekciju, odnosno ako postoji homomorfizam $s : B \to A$ takav da je $s \circ f = \mathrm{id}$. Da bismo videli ovo, neka je $k : B \otimes_A B \to B$ dato sa $k(b \otimes b') = b \cdot f(s(b'))$. Tada je

$$k(1 \otimes b - b \otimes 1) = f(s(b)) - b.$$

Dakle, ako je $1 \otimes b - b \otimes 1 = 0$, tada je $b = f(s(b)) \in f(A)$.

2° Ako je tvrđenje tačno za $a' \mapsto a' \otimes 1 : A' \to A' \otimes_A B$, gde je $A \to A'$ verno ravni homomorfizam, tada je tačno i za $A \to B$. Zaista, niz za $A' \to A' \otimes B$ se dobija od niza za $A \to B$ tenzorovanjem sa A'.

3° Homomorfizam $b \mapsto b \otimes 1 : B \to B \otimes_A B$ ima sekciju, naime preslikavanje $b \otimes b' \mapsto bb'$.

Po pretpostavci je $A \to B$ verno ravan, pa je dokaz posledica ova tri dokazana koraka.

□

Za bilo koje $U \to X$ koje je etalno, definišemo $\mathcal{O}_{X_{et}}(U) = \Gamma(U, \mathcal{O}_U)$. Njegova restrikcija na U_{zar} je pramen za svako U koje je etalno nad X. Pomoću prethodnog tvrđenja vidimo da je u pitanju i pramen na X_{et}.

Fiksna X-shema Z daje kontravarijantan funktor

$$\mathcal{F} : Et(X) \to \mathbf{Set}, \quad \mathcal{F}(U) = \mathrm{Hom}_X(U, Z).$$

Ovako dobijamo jedan pramen skupova. Lako se vidi da $\mathcal{F}$ zadovoljava uslov za pramen u odnosu na otvorena Zariski pokrivanja. U pitanju je pramen i u odnosu na etalno mesto. Ako je Z afina shema definisana prstenom C, dovoljno je dokazati da je sledeći niz tačan:

$$\mathrm{Hom}_{A-\mathrm{alg}}(C, A) \to \mathrm{Hom}_{A-\mathrm{alg}}(C, B) \to \mathrm{Hom}_{A-\mathrm{alg}}(C, B \otimes_A B),$$

što sledi direktno iz teoreme 4.2.2. Ovo važi i kada Z nije afina. Specijalno, ako Z ima strukturu grupe, tada je $\mathcal{F}_Z$ pramen grupa.

Primer 4.2.3. Neka je μ_n shema definisana jednačinom $T^n - 1 = 0$. Tada je $\mu_n(U)$ grupa n-tih korena iz 1 u $\Gamma(U, \mathcal{O}_U)$.

Primer 4.2.4. Neka je $\mathbb{G}_a$ afina prava posmatrana kao grupa u odnosu na sabiranje. Tada je $\mathbb{G}_a(U) = \Gamma(U, \mathcal{O}_U)$ posmatrano kao Abelova grupa.

Primer 4.2.5. Neka je $\mathbb{G}_m = \mathrm{Spec}\,\mathbb{Z}[x, x^{-1}]$ multiplikativna grupna shema i neka je $Y = \mathbb{G}_m \times X$. Tada je $Y(U) = \Gamma(U, \mathcal{O}_U)^\times$. Obično ovo označavamo samo sa $\mathbb{G}_m$.

4.3 Tačni nizovi i Kumerov niz

Neka je $(\mathcal{C}, T)$ mesto i neka je $PSh(\mathcal{C})$ kategorija predsnopova Abelovih grupa u odnosu na $\mathcal{C}$. U ovoj kategoriji su objekti kontravarijantni funktori iz $\mathcal{C}$ u kategoriju Abelovih grupa, a morfizmi su prirodne transformacije, odnosno kolekcije homomorfizama $\eta_U : \mathcal{F}(U) \to \mathcal{G}(U)$ takvi da je

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\eta_U} & \mathcal{G}(U) \\ \downarrow & & \downarrow \\ \mathcal{F}(V) & \xrightarrow{\eta_V} & \mathcal{G}(V) \end{array}$$

dijagram koji komutira. Kategorija $PSh(\mathcal{C})$ je zapravo Abelova kategorija, pa u njoj postoji pojam tačnosti. Naime, niz pretpramenova

$$... \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to ...$$

je tačan ako je niz

$$... \to \mathcal{F}(U) \to \mathcal{G}(U) \to \mathcal{H}(U) \to ...$$

za svako $U \in \mathcal{C}$.

Alternativno, možemo da definišemo jezgro i sliku dodeljenu morfizmu η sa

$$\mathrm{pker}(\eta)(U) = \ker(\eta_U), \quad \mathrm{pim}(\eta)(U) = \mathrm{im}(\eta_U).$$

Tada se uslov tačnosti svodi na to da se $\mathrm{pim}(\eta)$ svakog morfizma u nizu poklapa sa $\mathrm{pker}(\eta)$ sledećeg morfizma.

Kategorija $Sh(\mathcal{C})$ ima za objekte pramenove Abelovih grupa, dok su morfizmi definisani kao iznad. Ova kategorija je isto tako Abelova kategorija, ali se definicija tačnosti razlikuje u odnosu na kategoriju $PSh(\mathcal{C})$. Koren problema je u tome što ako je $\eta : \mathcal{F} \to \mathcal{G}$ morfizam pramenova, tada $\mathrm{pim}(\eta)$ ne mora da bude pramen. Rešenje je da se pim zameni sa

$$\mathrm{im}(\eta)(U) = \left\{ f \in \mathcal{F}(U) \mid \text{postoji pokrivanje } \{U_i\} \text{ takvo da je } f|_{U_i} \in \mathrm{im}(\eta_{U_i}) \right\}.$$

Tada se tačnost svodi na uslov $\ker = \mathrm{im}$.

Ako radimo sa topološkim prostorom X, tada je niz pramenova

$$... \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to ...$$

tačan ako i samo ako je za svako $x \in X$ niz slojeva u x tačan u uobičajenom smislu:

$$... \to \mathcal{F}_x \to \mathcal{G}_x \to \mathcal{H}_x \to ...$$

U opštem slučaju nemamo analog za ovo, ali imamo kod etalnog mesta.

Neka je X shema. *Geometrijska tačka* se sastoji iz tačke $x \in X$ i izbora separabilnog zatvorenja $k(x)^{sep}$ polja ostataka $\mathcal{O}_x/\mathfrak{m}_x$. Ekvivalentno, geometrijska tačka je morfizam $\overline{x} : \operatorname{Spec} k(x)^{sep} \to X$. *Etalna okolina* geometrijske tačke je komutativan dijagram

$$\begin{tikzcd} \overline{x} \arrow[r] \arrow[dr] & U \arrow[d, "\pi"] \\ & X \end{tikzcd}$$

gde je π etalni morfizam.

Ako je $\mathcal{F}$ pramen na X_{et}, definišemo *sloj u* $\overline{x}$ sa

$$\mathcal{F}_{\overline{x}} = \varinjlim \mathcal{F}(U),$$

gde U prolazi kroz sve etalne okoline. Navodimo sledeći ključni rezultat:

Teorema 4.3.1. Niz pramenova na X_{et}

$$... \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to ...$$

je tačan ako i samo ako je niz

$$... \to \mathcal{F}_{\overline{x}} \to \mathcal{G}_{\overline{x}} \to \mathcal{H}_{\overline{x}} \to ...$$

tačan za sve geometrijske tačke $\overline{x}$

Sloj $\mathcal{O}_{X,\overline{x}}$ se zove *stroga Henselizacija* lokalnog prstena $\mathcal{O}_{X,x}$. Nju je moguće opisati pomoću sledeće teoreme

Teorema 4.3.2. Stroga Henselizacija R^{sh} lokalnog prstena R sa poljem ostataka k je lokalni prsten sa poljem ostataka k^{sep}. Štaviše, R^{sh} zadovoljava Henselovu lemu: za dati $f(x) \in R^{sh}[x]$ sa prostim korenom $\overline{r} \in k^{sep}$, postoji koren $r \in R^{sh}$ koji se slika u $\overline{r}$.

Pomoću ove teoreme dolazimo do izuzetno značajnog tačnog niza, poznatog kao *Kumerov niz.*

Teorema 4.3.3. Neka je X shema takva da n ne deli karakteristiku nijednog polja ostataka. Tada je Kumerov niz

$$1 \to \mu_n \to \mathbb{G}_m \overset{f \mapsto f^n}{\to} \mathbb{G}_m \to 1$$

tačan na X_{et}.

Dokaz. Treba proveriti tačnost na slojevima. Ako je $R = \mathcal{O}^{sh}_{X,x}$, tada je dovoljno proveriti da je

$$1 \to \mu_n(R) \to R^* \xrightarrow{n} R^* \to 1$$

tačan niz. Jedini netrivijalan deo je surjektivnost poslednjeg preslikavanja. Ako je $r \in R^*$, tada polinom $f(x) = x^n - r$ ima prosti koren u separabilno zatvorenom polju k^{sep}. Zbog Henselove leme, on se podiže do korena u R, pa je preslikavanje zaista surjektivno.

□

4.4 Kohomologija pramenova

Ako imamo mesto $(\mathcal{C}, T)$, videli smo da je jezgro kod pretpramena jedan pramen. Zbog toga je

Lema 4.4.1. Neka je dato mesto $(\mathcal{C}, T)$, kratak tačan niz pramenova

$$0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$$

i objekat $X \in \mathcal{C}$. Tada postoji tačan niz

$$0 \to \mathcal{F}_1(X) \to \mathcal{F}_2(X) \to \mathcal{F}_3(X).$$

U opštem slučaju preslikavanje iznad ne mora da bude surjektivno, kao što vidimo u sledećem primeru:

Primer 4.4.2. Posmatrajmo Kumerov niz sa $R = \mathbb{Q}$ i $n = 2$

$$1 \to \{\pm 1\} \to \mathbb{Q}^* \xrightarrow{x \mapsto x^2} \mathbb{Q}^*.$$

Vidimo da poslednje preslikavanje ne mora da bude surjektivno.

Ovaj problem se može prevazići. Naime, neka je F funktor iz jedne Abelove kategorije u drugu koji je aditivan. Pretpostavimo i da F slika kratke tačne nizove

$$0 \to A \to B \to C \to 0$$

u tačne nizove

$$0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C).$$

Potrebne su nam neke dodatne tehničke pretpostavke koje izlaze izvan okvira ovog rada, ali koje su zadovoljene kod objekata sa kojima radimo. Ključni rezultat koji ćemo koristiti je sledeća teorema.

Teorema 4.4.3. Postoji niz aditivnih funktora $H^i(X,-)$, $i=0,1,2,...$ iz $Sh(\mathcal{C})$ u Abelove grupe takav da je $H^0(X,\mathcal{F})=\mathcal{F}(X)$ i kratak tačan niz pramenova

$$0\to\mathcal{F}_1\to\mathcal{F}_2\to\mathcal{F}_3\to 0$$

generiše dugi tačni niz

$$0\to H^0(X,\mathcal{F}_1)\to H^0(X,\mathcal{F}_2)\to H^0(X,\mathcal{F}_3)\to H^1(X,\mathcal{F}_1)\to H^1(X,\mathcal{F}_2)\to ...$$

4.5 Kohomologija Čeha

Neka je X topološki prostor i neka je $\mathcal{F}$ jedan pretpramen na njemu. Neka je $\mathcal{U}=\{U_i\}$ otvoreno pokrivanje od X indeksirano linearno uređenim skupom I. Pretpostavljamo da je I konačan. Ako je $\mathcal{F}$ pramen, to praktično znači da je on pretpramen takav da je niz

$$0\to\mathcal{F}(X)\to\prod_i\mathcal{F}(U_i)\to\prod_{i,j}\mathcal{F}(U_i\cap U_j)$$

tačan niz. Nastavljanjem ovog niza dolazimo do kompleksa. Naime, to je kompleks koji se dobija dodavanjem $\mathcal{F}(U_{i_1}\cap U_{i_2}\cap...\cap U_{i_r})$ po svim presecima $U_{i_1}\cap...\cap U_{i_r}$, gde su indeksi strogo rastući nizovi $i_0<...<i_p$ elemenata iz I.

Definicija 4.5.1. Za pretpramen $\mathcal{F}$ na X definišemo *kompleks Čeha $C^\bullet(\mathcal{U},\mathcal{F})$ od $\mathcal{F}$ u odnosu na pokrivanje $\mathcal{U}$* kao

$$C^0(\mathcal{U},\mathcal{F})\xrightarrow{d^0}C^1(\mathcal{U},\mathcal{F})\xrightarrow{d^1}C^2(\mathcal{U},\mathcal{F})\xrightarrow{d^2}...$$

gde je

$$C^p(\mathcal{U},\mathcal{F})=\prod_{i_0<i_1<...<i_p}\mathcal{F}(U_{i_0}\cap...\cap U_{i_p}),$$

a preslikavanja kogranica $d^p:C^p(\mathcal{U},\mathcal{F})\to C^{p+1}(\mathcal{U},\mathcal{F})$ su data sa

$$(d^p\sigma)_{i_0,...,i_{p+1}}=\sum_{j=1}^{p+1}(-1)^j\sigma_{i_0,...,\hat{i}_j,...,i_{p+1}}\big|_{U_{i_0}\cap...\cap U_{i_p}}$$

gde $i_0,...,\hat{i}_j,...,i_{p+1}$ znači $i_0,...,i_{p+1}$ sa izostavljenim indeksom i_j.

Za malo p je

$$C^0(\mathcal{U},\mathcal{F}) = \prod_{i_0} \mathcal{F}(U_{i_0}) \quad \text{i} \quad C^1(\mathcal{U},\mathcal{F}) = \prod_{i_0<i_1} \mathcal{F}(U_{i_0} \cap U_{i_1}).$$

Primetimo i da je pokrivanje konačno po pretpostavci, pa ako ima r elemenata, tada je $C^p(\mathcal{U},\mathcal{F}) = 0$ ako je $p \geq r$, zbog toga što su prazni proizvodi nula. Zato je kompleks Čeha konačan kompleks.

Primer 4.5.2. Preslikavanje kogranice stepena nula $d^0 : C^0(\mathcal{U},\mathcal{F}) \to C^1(\mathcal{U},\mathcal{F})$ je dato na sledeći način: ako je $\sigma = (\sigma_i)$, tada je

$$(d^0\sigma)_{ij} = \sigma_j - \sigma_i$$

gde je $i < j$.

Primer 4.5.3. Preslikavanje kogranice stepena jedan $d^1 : C^1(\mathcal{U},\mathcal{F}) \to C^2(\mathcal{U},\mathcal{F})$ zadovoljava: ako je $\sigma = (\sigma_{ij})$, tada je

$$(d^1\sigma)_{ijk} = \sigma_{jk} - \sigma_{ik} + \sigma_{ij}$$

gde je $i < j < k$.

Direktnom proverom vidimo da je $d^1 \circ d^0 = 0$, zato što se svi σ_{ij} skrate. Računom se može pokazati da ovo važi i za više stepene, pa imamo sledeće tvrđenje:

Lema 4.5.4. Za $p \geq 0$ je zadovoljeno $d^{p+1} \circ d^p = 0$.

Specijalno, $C^\bullet(\mathcal{U},\mathcal{F})$ formira kompleks Abelovih grupa. Kažemo da je element $\sigma \in C^p(\mathcal{U},\mathcal{F})$ *kocikl* ako je $d^p\sigma = 0$, dok za element σ kažemo da je *kogranica* ako je $\sigma = d^{p-1}\tau$ i ove skupove označavamo sa $Z^p(\mathcal{U},\mathcal{F})$ i $B^p(\mathcal{U},\mathcal{F})$, redom.

Definicija 4.5.5. Definišemo *p-tu kohomologiju Čeha od $\mathcal{F}$ u odnosu na $\mathcal{U}$* kao

$$H^p(\mathcal{U},\mathcal{F}) = Z^p(\mathcal{U},\mathcal{F})/B^p(\mathcal{U},\mathcal{F}) = (\ker d^p)/(\operatorname{im} d^{p-1}).$$

Nije teško videti da morfizam pramenova $\mathcal{F} \to \mathcal{G}$ indukuje preslikavanje Čehovih kohomoloških grupa, pa dobijamo funktore $\mathcal{F} \to H^p(\mathcal{U},\mathcal{F})$.

Primer 4.5.6. Posmatrajmo projektivnu pravu $\mathbb{P}^1_k$ nad poljem k. Ona je pokrivena sa dve afine sheme $U_0 = \operatorname{Spec} k[x]$ i $U_1 = \operatorname{Spec} k[x^{-1}]$ sa presekom $U_0 \cap U_1 = \operatorname{Spec} k[x, x^{-1}]$. Za strukturni pramen $\mathcal{O}_{\mathbb{P}^1_k}$ kompleks Čeha ima oblik

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_{\mathbb{P}^1_k}(U_0) \times \mathcal{O}_{\mathbb{P}^1_k}(U_1) \arrow[r, "d^0"] & \mathcal{O}_{\mathbb{P}^1_k}(U_0 \cap U_1) \arrow[r] & 0 \\ & k[x] \times k[x^{-1}] \arrow[u, "\cong"'] \arrow[r, "d"'] & k[x, x^{-1}], \arrow[u, "\cong"] & \end{tikzcd}$$

gde d preslikava par $(p(x), q(x^{-1}))$ u $q(x^{-1}) - p(x)$. Odatle vidimo da je $\ker d = k$, a sa druge strane, jasno je da svaki element iz $k[x, x^{-1}]$ može da se zapiše kao suma polinoma po x i polinoma po x^{-1}. Zato je d surjektivno, pa imamo

$$H^1(\mathcal{U}, \mathcal{O}_{\mathbb{P}^1}) = \operatorname{coker} d = 0.$$

4.6 Galoaova kohomologija

Neka je $X = \operatorname{Spec} k$, gde je k polje, $K = k^{sep}$ i $G = \operatorname{Gal}(K/k)$. Znamo da je tada kategorija pramenova na X_{et} ekvivalentna kategoriji G-modula. Pri ovoj korespondenciji je

$$\mathcal{F}(X) = M^G$$

Zbog ovoga je logično očekivati da se i viša kohomologija može opisati na sličan način. Ako je M dato, jedan *Galoaov n-kocikl* je neprekidno preslikavanje $f : G^n \to M$ takvo da je

$$\delta(f)(g_1, ..., g_{n+1}) =$$
$$g_1 f(g_2, ..., g_{n+1}) + \sum_i (-1)^i f(g_1, ..., g_i g_{i+1}, ..., g_n) + (-1)^{n+1} f(g_1, ..., g_n) = 0.$$

Nekada je korisno dodati uslov normalizacije da je f nula kada je neko $g_i = 1$. Neka je $Z^n(G, M)$ grupa normalizovanih kociklova. Direktno se proverava da je $\delta^2 = 0$, pa su elementi u slici od δ, koji se zovu *kogranice*, specijalno i kociklovi. Neka je $B^n(G, M)$ grupa normalizovanih n-kogranica. Definišemo *n-tu Galoaovu kohomologiju* kao

$$H^n(G, M) = Z^n(G, M)/B^n(G, M).$$

Navodimo sledeću teoremu koja povezuje Galoaovu kohomologiju sa etalnom kohomologijom:

Teorema 4.6.1. Neka M odgovara pramenu $\mathcal{F} \in X_{et}$, tada je

$$H^i(X_{et}, \mathcal{F}) \cong H^i(G, M).$$

Imamo i sledeću posledicu ove teoreme:

Posledica 4.6.2. Ako je $\mathcal{F}$ konstantan pramen koji odgovara modulu M, tada je

$$H^1(X_{et}, \mathcal{F}) \cong \mathrm{Hom}_{cont}(G, M).$$

Nekada je korisno predstaviti Galoaovu kohomologiju kao limes.

Lema 4.6.3. Kohomologija $H^i(G, M)$ se može predstaviti kao

$$H^i(G, M) = \varinjlim H^i(\mathrm{Gal}(L/k), M^{\mathrm{Gal}(K/L)}),$$

gde L/k prolazi kroz sva konačna Galoaova raširenja.

Primetimo i da nam Hilbertova teorema 90, poznata iz teorije Galoa, zapravo određuje prvu Galoaovu kohomologiju.

Teorema 4.6.4. (Hilbertova teorema 90) Neka je k polje i neka je $K = k^{sep}$. Neka je $G = \mathrm{Gal}(K/k)$. Tada je

$$H^1(G, K^*) = 0.$$

Glava 5

Pikarova grupa i kohomologija krivih

U ovoj glavi uvodimo pojam Pikarove grupe i povezujemo je sa klasnom grupom brojevnog polja. Potom povezujemo Pikarovu grupu sa kohomologijom i prikazujemo kohomološki račun na krivama. Glavne reference za ovu glavu su [14], [11], [10], kao i [3].

5.1 Divizori

U ovom odeljku uvodimo divizore, linearnu ekvivalenciju i grupu klasa divizora. Fokusiramo se na Vejlove divizore koje je jednostavnije geometrijski motivisati i koji su često dovoljni za naše potrebe.

Definicija 5.1.1. Kažemo da je shema X *regularna u kodimenziji* 1 ako je svaki lokalni prsten dimenzije jedan $\mathcal{O}_x$ u X regularan.

Kada radimo sa Vejlovim divizorima, pretpostavljamo da je X Neterina integralna rastavljena shema koja je regularna u kodimenziji 1. Rastavljenost sheme je tehnički uslov na koji nećemo obraćati previše pažnje. Naime, ako je $f : X \to Y$ morfizam shema, uvodimo dijagonalni morfizam $\Delta : X \to X \times_Y X$. Morfizam f je *rastavljen* ako je $\Delta(X)$ zatvorena podshema od $X \times_Y X$, dok je shema X *rastavljena* ako je rastavljen morfizam $X \to \operatorname{Spec} \mathbb{Z}$.

Definicija 5.1.2. Neka je X Neterina integralna rastavljena shema regularna u kodimenziji 1. *Prosti divizor* na X je zatvorena integralna podshema Y kodimenzije jedan. *Vejlov divizor* je element slobodne Abelove grupe $\operatorname{Div} X$ generisane prostim divizorima. Drugim rečima, Vejlov divizor se može zapisati kao $D = \sum_i n_i Y_i$, gde su Y_i prosti divizori, n_i su celi brojevi i samo konačno mnogo n_i su različiti od nule.

Ako je $D = \sum_i n_i Y_i$, pri čemu su svi $n_i \geq 0$, tada je divizor D *efektivan*. Podsetimo se da je *generička tačka* topološkog prostora svaka tačka čije je zatvorenje ceo taj prostor. Ako je Y prost divizor na X, neka je $\eta \in Y$ njegova generička tačka. Tada je lokalni prsten $\mathcal{O}_{\eta,X}$ prsten sa diskretnom valuacijom čije je količničko polje K polje funkcija od X. Neka je v_Y odgovarajuća diskretna valuacija, koja se zove *valuacija od* Y.

Može se pokazati da je Y određeno ovom valuacijom. Ako je $f \in K^*$ neka nenula racionalna funkcija na X, tada je $v_Y(f)$ ceo broj. Ako je ovaj broj pozitivan, kažemo da f ima *nulu duž* Y *reda* $v_Y(f)$, a ako je negativan kažemo da f *ima pol duž* Y *reda* $-v_Y(f)$.

Lema 5.1.3. Neka je X Neterina integralna rastavljena shema regularna u kodimenziji 1. Neka je $f \in K^*$ nenula funkcija na X. Tada je $v_Y(f) = 0$ za sve osim za konačno mnogo prostih divizora Y.

Dokaz. Neka je $U = \operatorname{Spec} A$ otvoreni afini podskup od X gde je f regularna. Tada je $Z = X \setminus U$ pravi zatvoreni podskup od X. Kako je X Neterina shema, Z ima najviše konačno mnogo prostih divizora od X. Zbog toga je dovoljno dokazati da postoji samo konačno mnogo prostih divizora Y od U za koje je $v_Y(f) \neq 0$. Regularna funkcija f na U svakako zadovoljava $v_Y(f) \geq 0$. Zapravo, važi $v_Y(f) > 0$ ako i samo ako je Y sadržano u zatvorenom podskupu od U definisanim idealom Af u A. Kako $f \neq 0$, ovo je pravi zatvoreni podskup, pa postoji samo konačno mnogo zatvorenih nerastavljivih podskupova kodimenzije jedan od U.

$\square$

Postoji posebna klasa divizora koja je generisana funkcijama. Naime, ne može se svaki divizor dobiti od neke funkcije, pa posebno izdvajamo one koji su u korespondenciji sa funkcijama. Idalje koristimo iste pretpostavke za shemu X.

Definicija 5.1.4. Neka je X shema (uz navedene pretpostavke) i neka je $f \in K^*$. Definišemo *divizor funkcije* f u oznaci (f) pomoću

$$(f) = \sum v_Y(f) \cdot Y$$

gde se suma uzima po svim prostim divizorima od X. Po lemi, ovo je konačna suma, pa je u pitanju dobro definisan divizor. Divizor dobijen na ovaj način se zove *glavni divizor*.

Primetimo da ako su $f, g \in K^*$, da je zbog osobina valuacije tada $(f/g) = (f) - (g)$. Zbog toga $f \mapsto (f)$ zadaje homomorfizam iz multiplikativne grupe K^* u aditivnu grupu $\operatorname{Div} X$. Slika ovog homomorfizma je *grupa glavnih divizora* i ona je podgrupa od $\operatorname{Div} X$.

Definicija 5.1.5. Neka je X Neterina integralna rastavljena shema regularna u kodimenziji 1. Dva divizora D i D' su *linearno ekvivalentna,* u oznaci $D \sim D'$, ako je $D - D'$ glavni divizor. Količnik grupe svih divizora $\operatorname{Div} X$ sa grupom glavnih divizora se zove *grupa klasa divizora od* X i označava se sa $\operatorname{Cl} X$.

Grupa klasa divizora sheme je veoma značajna invarijanta, ali je u opštem slučaju teško da se ona izračuna. Grupa klasa divizora sheme je uopštenje klasne grupe brojevnog polja. Navodimo prvo jedan rezultat iz komutativne algebre.

Teorema 5.1.6. Neka je A integralno zatvoren Neterin domen. Tada je

$$A = \bigcap_{\operatorname{ht} \mathfrak{p}=1} A_{\mathfrak{p}},$$

gde se presek uzima po svim prostim idealima visine 1.

Sledeće tvrđenje uopštava činjenicu da je klasna grupa kod domena sa jednoznačnom faktorizacijom trivijalna.

Teorema 5.1.7. Neka je A Neterin domen. Tada je A domen sa jednoznačnom faktorizacijom ako i samo ako je $X = \operatorname{Spec} A$ normalna i $\operatorname{Cl} X = 0$.

Dokaz. Svaki domen sa jednoznačnom faktorizacijom je integralno zatvoren, pa je shema X normalna. Sa druge strane, A ima jednoznačnu faktorizaciju ako i samo ako je svaki prost ideal visine 1 glavni. Dakle, treba dokazati da ako je A integralno zatvoren domen, da je tada svaki prost ideal visine 1 glavni ako i samo ako je $\operatorname{Cl}(\operatorname{Spec} A) = 0$.

Pretpostavimo prvo da je svaki prost ideal visine 1 glavni. Posmatrajmo prost divizor $Y \subseteq X = \operatorname{Spec} A$. Tada Y odgovara prostom idealu $\mathfrak{p}$ visine 1. Ako je $\mathfrak{p}$ generisan elementom $f \in A$, tada je divizor koji odgovara f upravo $1 \cdot Y$. Dakle, svaki prost divizor je glavni, pa je $\operatorname{Cl} X = 0$.

Obrnuto, neka je $\operatorname{Cl} X = 0$. Neka je $\mathfrak{p}$ prost ideal visine 1 i neka je Y odgovarajući prost divizor. Tada postoji $f \in K$ (gde je K količničko polje od A) sa $(f) = Y$. Dokazaćemo da je $f \in A$ i da f generiše $\mathfrak{p}$. Kako je $v_Y(f) = 1$, imamo da je

$f \in A_{\mathfrak{p}}$ i da f generiše $\mathfrak{p}A_{\mathfrak{p}}$. Ako je $\mathfrak{p}' \subseteq A$ neki drugi prost ideal visine 1, tada $\mathfrak{p}'$ odgovara prostom divizoru Y' od X i $v_{Y'}(f) = 0$, pa je $f \in A_{\mathfrak{p}'}$. Prethodna teorema iz komutativne algebre nam sada daje $f \in A$. Zapravo, važi $f \in A \cap \mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}$. Dokažimo još da f generiše $\mathfrak{p}$. Uzmimo bilo koji drugi element $g \in \mathfrak{p}$. Tada je $v_Y(g) \geq 1$ i $v_{Y'}(g) \geq 0$ za sve $Y' \neq Y$. Zato je $v_{Y'}(g/f) \geq 0$ za *sve* proste divizore Y' (pa i za Y). Zato je $g/f \in A_{\mathfrak{p}'}$ za sve $\mathfrak{p}'$ visine 1, pa je opet na osnovu teoreme iznad $g/f \in A$. Drugim rečima, $g \in Af$, pa je ideal $\mathfrak{p}$ glavni i generisan sa f.

□

Moguće je dokazati još opštije tvrđenje, da je grupa klasa divizora zapravo klasna grupa brojevnog polja. Ovo zapravo važi za bilo koji Dedekindov domen, a klasičan rezultat algebarske teorije brojeva je da je prsten celih brojevnog polja Dedekindov domen.

Teorema 5.1.8. Neka je A jedan Dedekindov domen. Tada je $\mathrm{Cl}(\operatorname{Spec} A)$ klasna grupa ideala od A.

5.2 Pikarova grupa

U ovom odeljku dajemo opštu definiciju Pikarove grupe i povezujemo je sa grupom klasa divizora. Videćemo da Pikarova grupa ima i kohomološku interpretaciju.

Definicija 5.2.1. Neka je X lokalno prstenovan prostor. *Invertibilan $\mathcal{O}_X$-modul na X* je pramen $\mathcal{O}_X$-modula $\mathcal{L}$ takav da svaka tačka ima otvorenu okolinu $U \subset X$ tako da je $\mathcal{L}_U$ izomorfno sa $\mathcal{O}_U$ kao $\mathcal{O}_U$-modul. Kažemo da je $\mathcal{L}$ *trivijalan* ako je izomorfan sa $\mathcal{O}_X$ kao $\mathcal{O}_X$-modul.

Ako je $f : X \to Y$ morfizam lokalno prstenovanih prostora i $\mathcal{L}$ invertibilan $\mathcal{O}_Y$-modul, nije teško videti da je $f^*\mathcal{L}$ invertibilan $\mathcal{O}_X$-modul. Za R-modul M kažemo da je *invertibilan* ako je ravan, sa konačnom prezentacijom, projektivan i lokalno slobodan ranga 1.

Lema 5.2.2. Neka su $\mathcal{L}$ i $\mathcal{M}$ invertibilni pramenovi na prstenovanom prostoru $(X, \mathcal{O}_X)$. Tada je i pramen $\mathcal{L} \otimes \mathcal{M}$ invertibilan. Za svaki invertibilan pramen $\mathcal{L}$ na X postoji invertibilan pramen $\mathcal{L}^{-1}$ na X takav da je $\mathcal{L} \otimes \mathcal{L}^{-1} \cong \mathcal{O}_X$.

Dokaz. Prvo tvrđenje je jasno, zato što su $\mathcal{L}$ i $\mathcal{M}$ lokalno slobodni ranga 1 i važi $\mathcal{O}_X \otimes \mathcal{O}_X \cong \mathcal{O}_X$. Što se tiče drugog tvrđenja, neka je $\mathcal{L}$ bilo koji invertibilni pramen i uzmimo za $\mathcal{L}^{-1}$ dualni pramen $\mathrm{Hom}(\mathcal{L}, \mathcal{O}_X)$. Tada je

$$\mathcal{L}^{-1} \otimes \mathcal{L} \cong \mathrm{Hom}(\mathcal{L}, \mathcal{L}) = \mathcal{O}_X,$$

što je i trebalo dokazati. $\square$

Sada možemo da damo opštu definiciju Pikarove grupe, koja se zasniva na prethodnoj lemi.

Definicija 5.2.3. Neka je $(X, \mathcal{O}_X)$ prstenovan prostor. *Pikarova grupa od X,* u oznaci $\mathrm{Pic}\, X$, je grupa klasa izomorfizama invertibilnih pramenova na X u odnosu na operaciju $\otimes$.

U ovom radu se bavimo shemama koje poseduju dodatne osobine zbog kojih se Pikarova grupa zapravo svodi na grupu klasa divizora. Dokaz sledeće teoreme se može naći u [14]:

Teorema 5.2.4. Neka je X Neterina, integralna, rastavljena shema takva da je za svako $x \in X$ prsten $\mathcal{O}_{X,x}$ domen sa jednoznačnom faktorizacijom. Tada postoji prirodni izomorfizam $\mathrm{Cl}\, X \cong \mathrm{Pic}\, X$.

Sledeći cilj nam je da povežemo Pikarovu grupu sa kohomologijom. Za ovo će nam biti potrebni takozvani torzori.

Definicija 5.2.5. Neka je X topološki prostor. Neka je $\mathcal{G}$ pramen grupa (ne obavezno Abelovih) na X. *$\mathcal{G}$-Torzor na X* je pramen skupova $\mathcal{F}$ zajedno sa dejstvom $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ takav da:

- kada god je $\mathcal{F}(U)$ neprazan, dejstvo $\mathcal{G}(U) \times \mathcal{F}(U) \to \mathcal{F}(U)$ je prosto tranzitivno,
- za svako $x \in X$ je sloj $\mathcal{F}_x$ neprazan.

Morfizam $\mathcal{G}$-torzora $\mathcal{F} \to \mathcal{F}'$ je morfizam pramenova skupova koji je kompatibilan sa $\mathcal{G}$-dejstvom. *Trivijalan $\mathcal{G}$-torzor* je pramen $\mathcal{G}$ zajedno sa očiglednim levim $\mathcal{G}$-dejstvom.

Navodimo sledeća dva tvrđenja o torzorima. Drugo tvrđenje povezuje torzore i prvu kohomološku grupu.

Lema 5.2.6. Neka je X topološki prostor. Neka je $\mathcal{G}$ pramen grupa na X. Tada je $\mathcal{G}$-torzor $\mathcal{F}$ trivijalan ako i samo ako $\mathcal{F}(X) \neq \emptyset$.

Teorema 5.2.7. Neka je X topološki prostor i neka je $\mathcal{H}$ Abelov pramen na X. Tada postoji kanonska bijekcija između skupa klasa izomorfizma $\mathcal{H}$-torzora i $H^1(X, \mathcal{H})$.

Sada smo u poziciji da povežemo Pikarovu grupu sa prvom kohomološkom grupom. Skiciraćemo dokaz ove teoreme, ali izostavljamo neke tehničke delove.

Teorema 5.2.8. Neka je $(X, \mathcal{O}_X)$ lokalno prstenovan prostor. Tada postoji kanonski izomorfizam Abelovih grupa

$$H^1(X, \mathcal{O}_X^*) = \operatorname{Pic} X.$$

Skica dokaza. Neka je $\mathcal{L}$ invertibilni $\mathcal{O}_X$-modul. Posmatrajmo pretpramen $\mathcal{L}^*$ definisan sa

$$U \longmapsto \Big\{ s \in \mathcal{L}(U) \text{ tako da je } \ \mathcal{O}_U \stackrel{s\cdot-}{\to} \mathcal{L}_{\mathcal{U}} \ \text{ izomorfizam} \Big\}$$

Ovaj pretpramen zadovoljava uslov za pramen. Štaviše, ako je $f \in \mathcal{O}_X^*(U)$ i $s \in \mathcal{L}^*(U)$, tada je jasno da je $fs \in \mathcal{L}^*(U)$. Dalje, ako su $s, s' \in \mathcal{L}^*(U)$, tada postoji jedinstven $f \in \mathcal{O}_X^*(U)$ takav da je $fs = s'$. Pramen $\mathcal{L}^*$ ima sekcije lokalno, pa će zapravo biti $\mathcal{O}_X^*$-torzor.

Na ovaj način dobijamo preslikavanje iz invertibilnih pramenova na $(X, \mathcal{O}_X)$ do na izomorfizam u $\mathcal{O}_X^*$-torzore do na izomorfizam. Izostavljamo proveru da je ovo homomorfizam Abelovih grupa. Iz prethodne teoreme su torzori u kanonskoj bijekciji sa $H^1(X, \mathcal{O}_X^*)$. Dakle, treba pokazati surjektivnost i injektivnost ove korespondencije.

Što se tiče injektivnosti, torzor $\mathcal{L}^*$ je trivijalan, pa zbog leme o trivijalnim torzorima znamo da $\mathcal{L}^*$ ima globalnu sekciju. To znači da je baš $\mathcal{L} \cong \mathcal{O}_X$ neutralni element u $\operatorname{Pic} X$.

Preostaje da se dokaže surjektivnost. Neka je $\mathcal{F}$ jedan $\mathcal{O}_X^*$-torzor. Posmatrajmo pretpramen skupova

$$\mathcal{L}_1 : U \longmapsto (\mathcal{F}(U) \times \mathcal{O}_X(U))/\mathcal{O}_X^*(U),$$

gde je dejstvo od $f \in \mathcal{O}_X^*(U)$ na (s, g) dato sa $(fs, f^{-1}g)$. Tada $\mathcal{L}_1$ postaje pretpramen $\mathcal{O}_X$-modula ako zadamo $(s, g) + (s', g') = (s, g + (s'/s)g')$, gde je s'/s lokalna sekcija od f u $\mathcal{O}_X^*$ takva da je $fs = s'$ i $h(s, g) = (s, hg)$ za lokalnu sekciju h od $\mathcal{O}_X$. Izostavljamo proveru da se od ovog pretpramena dobija pramen $\mathcal{L}$ koji je invertibilan $\mathcal{O}_X$-modul čiji pridruženi $\mathcal{O}_X^*$-torzor $\mathcal{L}^*$ je izomorfan sa $\mathcal{F}$.

□

5.3 Etalna kohomologija za krive

Akcenat u ovom delu je da uspostavimo račun kohomologije za povezane nesingularne krive nad algebarski zatvorenim poljem k, gde je n prirodan broj uzajamno prost sa karakteristikom polja k. Pratimo izlaganje u [11].

Podsetimo se da je nad $\mathbb{Z}$ pramen μ_n predstavljen sa $\mathbb{Z}[x]/(x^n - 1)$. Nad opštom shemom X pramen μ_n preslikava etalni otvoren skup U od X u n-te korene iz jedinice u $\mathcal{O}_U(U)$.

U ovom izlaganju navodimo i koristimo bez dokaza tvrđenja iz teorije Jakobijevih varijeteta i kvazi-algebarski zatvorenih polja. Takođe, neki od dokaza koriste spektralne nizove, pa njih izostavljamo. Osim toga, navodimo i sledeću karakterizaciju Pikarove grupe, koja se nekada zove Hilbertova teorema 90:

Teorema 5.3.1. Za shemu X postoji kanonska identifikacija

$$H^1(X_{et}, \mathbb{G}_m) \cong H^1(X_{zar}, \mathcal{O}_X^*) \cong \operatorname{Pic} X.$$

Cilj nam je da dobijemo kompletnu kohomologiju za $\mathbb{G}_m$ za povezane nesingularne krive nad k. Počinjemo od sledećeg tačnog niza:

Teorema 5.3.2. Neka je X povezan nesingularni varijetet sa generičkom tačkom $g : \eta \to X$. Tada je niz etalnih pramenova Abelovih grupa

$$0 \longrightarrow \mathbb{G}_m \longrightarrow g_*\mathbb{G}_{m,\eta} \longrightarrow \operatorname{Div} X \longrightarrow 0$$

tačan niz.

Za polje k kažemo da je *kvazi-algebarski zatvoreno* ako svaki nekonstantan homogen polinom f po d promenljivih sa $\deg(f) < d$ ima nulu. Jednostavan primer kvazi-algebarski zatvorenog polja je bilo koje konačno polje. Pre nego što nastavimo dalje, navodimo teoremu koja nam je ključan izvor primera ovakvih polja.

Teorema 5.3.3. (Cenova teorema) Neka je k algebarski zatvoreno polje i neka je K konačno generisano raširenje stepena transcendentnosti 1. Tada je polje K kvazi-algebarski zatvoreno.

Kvazi-algebarski zatvorena polja su nam bitna pre svega u kontekstu narednog tvrđenja. Modul M je diskretni G-modul ako je dejstvo G neprekidno kada se M posmatra sa diskretnom topologijom.

Teorema 5.3.4. Neka je k kvazi-algebarski zatvoreno polje i neka je $G = \mathrm{Gal}(k^{sep}/k)$. Tada je

1. $H^2(G, (k^{sep})^*) = 0$,
2. za svako $r > 1$ je $H^r(G, M) = 0$ ako je M torzioni diskretni G-modul,
3. za svako $r > 2$ je $H^r(G, M) = 0$ ako je M diskretan G-modul.

Pomoću prethodne teoreme i spektralnih nizova je moguće izračunati $H^r(X_{et}, \mathbb{G}_m)$.

Teorema 5.3.5. Neka je X povezana nesingularna kriva nad algebarski zatvorenim poljem k. Tada imamo sledeću formulu:

$$H^r(X_{et}, \mathbb{G}_m) = \begin{cases} \Gamma(X, \mathcal{O}_X^*) & r = 0 \\ \mathrm{Pic}\, X & r = 1 \\ 0 & r > 1 \end{cases}$$

Možemo da dobijemo i $H^r(X_{et}, \mu_n)$ pomoću Kumerovog niza

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0.$$

Da bismo izračunali kohomologiju za μ_n, razdvajamo slučajeve kada je X kompletna i kada nije.

Teorema 5.3.6. Neka je X kompletna povezana nesingularna kriva roda g nad algebarski zatvorenim poljem k. Za svaki prirodan broj n koji je uzajamno prost sa karakteristikom od k imamo formulu

$$H^r(X_{et}, \mu_n) = \begin{cases} \mu_n(k) & r = 0 \\ (\mathbb{Z}/n\mathbb{Z})^{2g} & r = 1 \\ \mathbb{Z}/n\mathbb{Z} & r = 2 \\ 0 & r > 2 \end{cases}$$

Dokaz. Dugi tačan niz pridružen Kumerovom nizu je

$$\cdots \longrightarrow H^{r-1}(X_{et}, \mathbb{G}_m) \longrightarrow H^r(X_{et}, \mu_n) \longrightarrow H^r(X_{et}, \mathbb{G}_m) \longrightarrow H^r(X_{et}, \mathbb{G}_m) \longrightarrow \cdots$$

Odavde odmah dobijamo rezultat za $r > 2$. Ako je $r = 1$, primetimo da je preslikavanje $H^0(X, \mathbb{G}_m) \to H^0(X, \mathbb{G}_m)$ dato množenjem sa n na k^*. Kako je k

algebarski zatvoreno, ovo preslikavanje je surjektivno i dobijamo sledeći dugi tačan niz:

$$0 \longrightarrow H^1(X_{et}, \mu_n) \longrightarrow \operatorname{Pic} X \xrightarrow{n} \operatorname{Pic} X \longrightarrow H^2(X_{et}, \mu_n) \longrightarrow 0.$$

Sada koristimo sledeći rezultat iz teorije Jakobijevih varijeteta: preslikavanje $n : \operatorname{Pic} X \to \operatorname{Pic} X$ ima jezgro izomorfno sa $(\mathbb{Z}/n\mathbb{Z})^{2g}$ i kojezgro izomorfno sa $\mathbb{Z}/n\mathbb{Z}$ gde je n uzajamno prost sa karakteristikom, što završava dokaz.

□

Kada X nije kompletna, dovoljno je posmatrati kohomologiju krive u odnosu na zatvorenu tačku. Tada možemo da dobijemo kohomologiju krive koja nije kompletna preko dugog tačnog niza para prostora.

Teorema 5.3.7. Neka je X povezana nesingularan kriva nad algebarski zatvorenim poljem k i neka je $x \in X$ zatvorena tačka. Ako je n uzajamno prost sa karakteristikom od k, tada je

$$H^r_x(X_{et}, \mu_n) = \begin{cases} \mathbb{Z}/n\mathbb{Z} & r = 2 \\ 0 & \text{inače} \end{cases}$$

Skica dokaza. Neka je R strogo lokalni prsten od x. Tada je moguće iskoristiti isecanje da zamenimo X sa $\operatorname{Spec} R = V$. Prvo računamo relativnu kohomologiju od $\mathbb{G}_m$, pa potom relativnu kohomologiju od μ_n.

Iz kohomologije za $\mathbb{G}_m$ znamo da je $H^r(V_{et}, \mathbb{G}_m) = 0$ za $r > 1$. Štaviše, imamo $H^1(V_{et}, \mathbb{G}_m) = 0$ zbog toga što je R prsten sa diskretnom valuacijom. Dugi tačan niz para $(V, V \setminus x)$ je dat sa

$$\cdots \longrightarrow H^{r-1}(\operatorname{Spec} K, \mathbb{G}_m) \longrightarrow H^r_x(V_{et}, \mathbb{G}_m) \longrightarrow H^r(\operatorname{Spec} K, \mathbb{G}_m) \longrightarrow \cdots$$

gde je K polje razlomaka od V. (Primetimo da je $\operatorname{Spec} K = V \setminus x$.) Zato za $r > 1$ imamo izomorfizam $H^{r-1}(\operatorname{Spec} K, \mathbb{G}_m) \cong H^r_x(V_{et}, \mathbb{G}_m)$. Sada koristeći rezultate o kvazi-algebarski zatvorenim poljima i Hilbertovu teoremu 90 za kohomologiju dobijamo da je $H^r(\operatorname{Spec} K, \mathbb{G}_m)$ nula za $r > 0$, pa je i $H^r_x(V_{et}, \mathbb{G}_m)$ nula za $r > 1$. Takođe, očigledno važi $H^0_x(V_{et}, \mathbb{G}_m) = 0$.

Konačno, imamo i $H^1(V_{et}, \mathbb{G}_m) \cong H^0(\operatorname{Spec} K, \mathbb{G}_m)/H^0(V, \mathbb{G}_m) \cong \mathbb{Z}$. Zaključak sada sledi iz Kumerovog niza.

□

Glava 6

Principi refleksije

Ova glava predstavlja ključni deo ovog rada. Naime, u njoj primenjujemo tehnike koje smo razvili u prethodnim glavama i dobijamo konkretne primene savremene algebarske geometrije u teoriji brojeva.

Tvrđenja koja upoređuju p-rang klasnih grupa različitih brojevnih polja se zovi *principi refleksije*. Mnogi od ovih rezultata su prvenstveno bili bazirani na vezama između Kumerove teorije i teorije polja klasa. Detaljnije o istoriji principa refleksije se može pročitati u radu [5].

Videli smo u prethodnoj glavi da se Pikarova grupa kod prstena celih brojevnog polja svodi na klasnu grupu ideala. Ovo nam omogućava da dobijamo različite principe refleksije koristeći kohomološku definiciju Pikarove grupe. Ovaj metod je pre svega razvijen u [8].

Mi ćemo se ovde pozvati na tvrđenja iz [8] koja čine okosnicu ovog metoda i prikazati kako se u navedenom radu on koristi u slučaju Galoaove grupe S_3.

Potom dajemo originalnu novu primenu ovog metoda za slučaj polja funkcija kada je Galoaova grupa raširenja kvaternionska grupa Q_8. Ovaj rezultat do sada nije bio poznat i predstavlja naučni doprinos autora ovog master rada.

Na kraju navodimo neke ideje za dalji rad, kao i neka pitanja do kojih je autor došao kroz proučavanje ovog problema. Osim toga, navodimo i parcijalan napredak ka odgovoru na njih.

6.1 Preliminarni rezultati

Metod koji koristimo se potpuno bazira na osnovnim tehnikama iz [8] i u ovom delu iznosimo sve neophodne preliminarne rezultate i notaciju, kompletno preuzete odatle. Pod H^i nadalje uvek podrazumevamo etalnu kohomologiju.

Sheme i Pikarove grupe. Neka je l prost broj i neka je S shema koja je jednaka ili $\operatorname{Spec}\mathbb{Z}[1/l]$ ili $\mathbb{P}^1_{\mathbb{F}_p}$, gde je p prost broj različit od l. Označimo sa $\eta = \operatorname{Spec} F$ generičku tačku od S i neka je $g : \eta \to S$ inkluzija. Neka je shema $\pi : X \to s$ pokrivanje od S konačnog stepena n. Ako je $S = \mathbb{P}^1_{\mathbb{F}_p}$, tada uzimamo za X kompletnu povezanu glatku krivu, dok kod $S = \operatorname{Spec}\mathbb{Z}[1/l]$ za X uzimamo $\operatorname{Spec}\mathcal{O}_K[1/l]$, gde je K neko brojevno polje. Uvodimo još i $Z \subset S$ kao konačan skup tačaka iznad kojih je π razgranata. Neka je $\operatorname{Spec} K$ generička tačka od X, tako da je $[K : F] = n$.

Posmatrajmo Kumerov niz etalnih pramenova na X

$$1 \longrightarrow \mu_l \longrightarrow \mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 1.$$

Pretpostavljamo da X ima ostatak karakteristike uzajamno proste sa l u svakoj tački, tako da je Kumerov niz tačan. Ako uzmemo kohomologiju ovog niza i iskoristimo da je $H^1(X, \mathbb{G}_m) = \operatorname{Pic} X$ dobijamo

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}_X(X)^*[l] \arrow[r] & \mathcal{O}_X(X)^* \arrow[r] & \mathcal{O}_X(X)^* \arrow[dll] \\ & H^1(X,\mu_l) \arrow[r] & \operatorname{Pic} X \arrow[r] & \operatorname{Pic} X \end{tikzcd}$$

Neka je $\mathcal{L} = \pi_*\mu_l$. Ovo je konačan lokalno konstantan pramen na $S \setminus Z$, pri čemu je $H^1(X, \mu_l) = H^1(S, \mathcal{L})$. Ovo se može kompaktno zapisati preko sledeće leme:

Lema 6.1.1. Neka je $\pi : X \to S$ konačno pokrivanje i neka je $\mathcal{L} = \pi_*\mu_l$. Tada je

$$\operatorname{Pic}(X)[l] \cong H^1(S, \mathcal{L})/(\mathcal{O}_X(X)^*/l\mathcal{O}_X(X)^*).$$

Pramenovi i Galoaovi moduli. Dalje navodimo neke osobine konačnih lokalno konstantnih pramenova, koristeći istu notaciju kao iznad. Neka je $U = S \setminus Z$. Primetimo da je Z zatvoren, pa je U otvoren i neka je $j : U \to S$ otvorena imerzija. Fiksirajmo geometrijsku tačku $\overline{\eta} = \operatorname{Spec}\overline{F}$ iznad generičke tačke $\eta = \operatorname{Spec} F$ od S. Kao iznad, neka je $\mathcal{L} = \pi_*\mu_l$.

Postoji kategorijska ekvivalencija između konačnih $\pi_1(U, \overline{\eta})$-modula, konačnih etalnih shema nad U i konačnih lokalno konstantnih pramenova Abelovih grupa na U. Ona kaže da je konačan lokalno konstantan pramen $\mathcal{F}$ na U predstavljen nekom shemom Y konačno etalnom nad U čije geometrijske tačke iznad $\overline{\eta}$ su $\pi_1(U, \overline{\eta})$-modul.

Dokazi sledeće dve leme se mogu naći u [10].

Lema 6.1.2. Neka je M jedan G_F-modul koji predstavlja pramen $\mathcal{F}$ na η. Pretpostavimo da se dejstvo od G_F faktoriše kroz $\mathrm{Gal}(L/F)$ za neko konačno raširenje L. Neka je $V \subset S$ skup tačaka koje su nerazgranate u L. Tada se $\mathcal{F}$ proširuje do lokalno konstantnog pramena na V kojeg predstavlja M sa dejstvom od $\pi_1(V, \overline{\eta})$.

Lema 6.1.3. Neka je $\mathcal{F}$ lokalno konstantan pramen na U predstavljen $\pi_1(U, \overline{\eta})$-modulom M. Tada za bilo koju tačku $z \in S \setminus U$ imamo da je $(j_*\mathcal{F})_{\overline{z}} \cong M^{I_z}$ kao D_z/I_z-modul, gde je I_z grupa inercije u z.

Budući da je $\mathcal{L}\big|_U$ konačan lokalno konstantan pramen, on će na osnovu prethodnih lema biti predstavljen na U svojim slojem $\mathcal{L}_{\overline{\eta}}$. Može se pokazati i da je $j_*(\mathcal{L}\big|_U) = \mathcal{L}$. Dakle, da bismo opisali sloj $\mathcal{L}_{\overline{z}}$ za bilo koje $z \in Z$ uzimamo u I_z invarijante od $\mathcal{L}_{\overline{\eta}}$.

Podsetimo se da je $[K : F] = n$. Sledeća lema daje eksplicitni opis za M koristeći definiciju za $\mathcal{L}$. Lema i njen dokaz se mogu naći u [8].

Lema 6.1.4. Neka je M jedan G_F-modul koji predstavlja sloj $\mathcal{L}_{\overline{\eta}}$. Neka su $\sigma_1, ..., \sigma_n$ utapanja od K u $\overline{F}$. Neka je L konačno raširenje od F koje sadrži normalno zatvorenje od K u $\overline{F}$, kao i $\mu_l(\overline{F})$. Tada je $M \cong \mathbb{Z}/l\mathbb{Z}\langle \sigma_1, ..., \sigma_n \rangle$ i dejstvo od G_F se faktoriše kroz $\mathrm{Gal}(L/F)$.

Opis metoda. Prethodna lema je ključna za ovaj metod. Posmatrajmo dve sheme $\pi_i : X_i \to S$ za $i = 1, 2$ koje su u obliku koji je opisan na početku ovog odeljka, sa generičkim tačkama $\mathrm{Spec}\, K_i$. Neka je $\mathcal{L}_i = (\pi_i)_*\mu_l$. Cilj nam je da nađemo vezu između $\mathrm{rk}_l \mathrm{Pic}\, X_1$ i $\mathrm{rk}_l \mathrm{Pic}\, X_2$, što radimo tako što povežemo $\mathrm{rk}_l H^1(S, \mathcal{L}_1)$ i $\mathrm{rk}_l H^1(S, \mathcal{L}_2)$, pa iskoristimo lemu 6.1.1.

Ova dva l-ranga povezujemo tako što konstruišemo familiju tačnih nizova pramenova na S koja sadrži oba $\mathcal{L}_i$, kao i neke međupramenove. Potom uzimamo kohomologiju ovih nizova što nas dovodi do zaključka. Međupramenovi zavise od konkretnog primera.

Problem se zapravo svodi na rad sa Galoaovim modulima. Strategija je prvo da se pronađe kolekcija tačnih nizova $G(L/F)$-modula koja sadrži $\mathcal{L}_i$ - svaki od ovih nizova odgovara tačnom nizu pramenova u generičkoj tački. Potom fiksiramo podgrupu $I \subset G(L/F)$ koja je grupa inercije nekog razgranatog prostog i uzimamo I-invarijante modula. Zahtevamo da ovo čuva tačnost, što odgovara tačnosti pramenova u toj razgranatoj tački.

Kohomološki račun za polja funkcija. Koristićemo oznaku $h^i(X, \mathcal{F}) = \log_l |H^i(X, \mathcal{F})|$. Kada kohomološka grupa ima eksponent l ovo je upravo l-rang.

Prvo ćemo navesti račun za polja funkcija. Neka je $S = \mathbb{P}^1_{\mathbb{F}_p}$ i $F = \mathbb{F}_p(T)$. Konačna raširenja od $\mathbb{F}_p(T)$ odgovaraju krivama koje su konačna pokrivanja od $\mathbb{P}^1(\mathbb{F}_p)$. Svaka takva kriva C odgovara polju funkcija $\mathbb{F}_p(C)$.

Dokazi sledećih računskih lema se mogu naći u [8].

Lema 6.1.5. Za proizvoljnu krivu C konačnu nad S imamo

$$\mathcal{O}_C(C)^*/(\mathcal{O}_C(C)^*)^l = \begin{cases} \mathbb{Z}/l\mathbb{Z} & \text{ako je } \mu_l \in \mathbb{F}_p \\ 1 & \text{ako je } \mu_l \notin \mathbb{F}_p. \end{cases}$$

Lema 6.1.6. Za pramen μ_l na S imamo

$$H^0(\mu_l), H^1(\mu_l), H^2(\mu_l) = \begin{cases} \mathbb{Z}/l\mathbb{Z}, \mathbb{Z}/l\mathbb{Z}, \mathbb{Z}/l\mathbb{Z} & \text{ako je } \mu_l \in \mathbb{F}_p \\ 0, 0, \mathbb{Z}/l\mathbb{Z} & \text{ako je } \mu_l \notin \mathbb{F}_p. \end{cases}$$

Lema 6.1.7. Neka je $\mathcal{F}$ konstruktibilan pramen na $\mathbb{P}^1$ sa $l\mathcal{F} = 0$. Pretpostavimo da je $\mathcal{F} = g_*\mathcal{F}_0$ za neki pramen $\mathcal{F}_0$ na $\eta = \operatorname{Spec} F$, gde je $g : \eta \to S$. Tada je

$$h^2(\mathcal{F}) \leq h^1(\mathcal{F}) - h^0(\mathcal{F}) + \operatorname{rk}_l \mathcal{F}_{\overline{\eta}}.$$

Kohomološki račun za brojevna polja. Neka je sada $S = \operatorname{Spec} \mathbb{Z}[1/l]$ i $F = \mathbb{Q}$. Navodimo sledeće leme analogne slučaju polja funkcija, čiji se dokazi opet mogu naći u [8].

Lema 6.1.8. Neka je K brojevno polje i neka je $s = r_1 + r_2 - 1$, gde su r_1 i r_2 brojevi realnih i kompleksnih utapanja. Neka je u broj prostih u K iznad l. Postavljamo $t = 1$ ako l deli red od μ_K, a u suptrotnom je $t = 0$. Tada je

$$\mathcal{O}_K^*[1/l]/(\mathcal{O}_K^*[1/l])^l = (\mathbb{Z}/l\mathbb{Z})^{s+u+t}.$$

Lema 6.1.9. Za pramen μ_l na S imamo

$$H^0(\mu_l), H^1(\mu_l), H^2(\mu_l) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/2\mathbb{Z} & \text{ako je } l = 2 \\ 0, \mathbb{Z}/l\mathbb{Z}, 0 & \text{ako } l \neq 2. \end{cases}$$

Lema 6.1.10. Neka je $\mathcal{F}$ konstruktibilan pramen na $S = \operatorname{Spec} \mathbb{Z}[1/l]$ sa $l\mathcal{F} = 0$. Pretpostavimo da je $\mathcal{F} = g_*\mathcal{F}_0$ za neki pramen $\mathcal{F}_0$ na $\eta = \operatorname{Spec} F$, gde je $g : \eta \to S$. Nadalje pretpostavljamo da je $\mathcal{F}(\mathbb{R}) = 0$ ako $l \neq 2$ i da se $\mathcal{F}$ trivijalizuje na $\mathbb{R}$ ako je $l = 2$. Tada je

$$h^2(\mathcal{F}) \leq h^1(\mathcal{F}) - h^0(\mathcal{F}).$$

Navedene oznake i leme nam omogućavaju da u sledeća tri odeljka pokažemo direktnu primenu ovog metoda za dobijanje principa refleksije.

Odeljak za Galoaovu grupu S_3 je baziran na radu [8], dok je odeljak za Galoaovu grupu Q_8 originalan i sadrži novi rezultat dobijen adaptacijom ovog metoda.

6.2 Galoaova grupa S_3

Uvodni komentari. Prva primena kohomologije za dobijanje principa refleksije koju navodimo je za slučaj Galoaovih raširenja sa Galoaovom grupom S_3. Ovaj primer je preuzet iz rada [8], ali navodimo ga ovde kao model na osnovu kojeg dobijamo slične rezultate za sledeća dva primera.

U ovom i u sledeća dva primera imamo dve sheme $\pi_i : X_i \to S$ za $i = 1, 2$, kao i u prethodnim odeljcima, sa generičkim tačkama $\operatorname{Spec} K_i$.

Neka je L/F Galoaovo raširenje koje sadrži K_i i neka je $G = \operatorname{Gal}(L/F)$. Uvodimo $L' = L(\mu_l)$ i pretpostavljamo da je K_2 disjunktno sa $F(\mu_l)$. Neka je $B = \operatorname{Gal}(F(\mu_l)/F)$. Tada je ili $B = (\mathbb{Z}/l\mathbb{Z})^*$ ili $B = 1$. Neka je $G' = \operatorname{Gal}(L'/F) = G \times B$. Primetimo da je $(|B|, l) = 1$.

Neka je $\mathcal{L}_i = (\pi_i)_*\mu_l$. Neka je $M = \mathcal{L}_{1,\overline{\eta}}$ i $N = \mathcal{L}_{2,\overline{\eta}}$. Ovo su G_F-moduli gde se sabiranje faktoriše kroz $G \times B$ i B dejstvuje množenjem. Koristimo lemu 6.1.4 da bismo opisali M i N i potom računamo tačne nizove koji ih povezuju.

Napomena. Kako su svi moduli zapravo G-moduli, iz leme 6.1.2 oni predstavljaju pramenove na U, što je skup tačaka gde se nijedan od π_1 i π_2 ne granaju. Potom primenjujemo funktor j_* da dobijemo pramenove na S (ovo vraća pramenove $\mathcal{L}_i$). Proveravanje tačnosti niza pramenova je ekvivalentno proveravanju tačnosti niza slojeva u svakoj geometrijskoj tački. Zato, na osnovu leme 6.1.3 treba proveriti da početni niz modula ostaje tačan nakon uzimanja I_z-invarijanti u odnosu na grupu inercije I_z svake razgranate tačke z.

Tačan niz. Neka je $l = 3$. Neka je L/F Galoaovo raširenje sa $\operatorname{Gal}(L/F) = S_3$ i neka je K_1 kubno potpolje koje nije Galoaovo. Neka je K_2 jedinstveno kvadratno potpolje.

Imamo prezentaciju $S_3 = \langle \sigma, \tau \mid \sigma^2 = \tau^3 = 1, \sigma\tau\sigma = \tau^{-1} \rangle$. Tada imamo S_3-module

$$M = \mathbb{Z}/3\mathbb{Z}\langle 1, \tau, \tau^2 \rangle$$

gde τ^i predstavlja koset po modulu podgrupe $\langle\sigma\rangle \subset S_3$ i slično

$$N = \mathbb{Z}/3\mathbb{Z}\langle 1, \sigma\rangle$$

gde σ^i predstavlja koset po modulu podgrupe $\langle\tau\rangle \subset S_3$.

Sada dajemo tačne nizove koji povezuju ove module. Neka je $N' = \mathbb{Z}/3\mathbb{Z}\langle 1-\sigma\rangle$ i neka je T modul koji predstavlja pramen μ_3. To je jednodimenzionalni modul sa trivijalnim G dejstvom. Označimo sa M' količnik M sa podmodulom $\langle 1+\tau+\tau^2\rangle$. Tada je

$$\begin{gathered} 0 \longrightarrow \langle 1+\tau+\tau^2\rangle \longrightarrow M \longrightarrow M' \longrightarrow 0 \\ 0 \longrightarrow N' \longrightarrow M' \longrightarrow T \longrightarrow 0. \end{gathered} \tag{6.1}$$

Preslikavanje $N' \to M'$ je dato sa $1-\sigma \longmapsto 1-\tau$. Osim toga, važi

$$N = N' \oplus \langle 1+\sigma\rangle. \tag{6.2}$$

Primetimo da T odgovara pramenu μ_3.

Ovako dobijamo niz pramenova u generičkoj tački. Sada primenimo napomenu iz uvodnih komentara. Pretpostavka da je L/K_2 nerazgranato povlači da je grupa inercije u svakoj tački reda 2. Koristimo činjenicu da je $H^1(G, M) = 0$ kada je red grupe G uzajamno prost sa redom od M. Svi moduli iznad imaju za red stepen broja 3, pa dobijamo tačne nizove pramenova na S. Primetimo i da se T proširuje do μ_3 na S.

Kohomologija u polju funkcija. Neka je $G = S_3$. U zavisnosti od toga da li je $\mu_3 \in \mathbb{F}_p$ imamo dva slučaja.

Lema 6.2.1. Ako je $\mu_3 \in \mathbb{F}_p$, tada je

$$\mathrm{rk}_3 \operatorname{Pic} C_2 - 2 \leq \mathrm{rk}_3 \operatorname{Pic} C_1 \leq \mathrm{rk}_3 \operatorname{Pic} C_2.$$

Dokaz. Već smo izračunali da je $H^i(\mu_3) = \mathbb{Z}/3\mathbb{Z}$ za $i = 0, 1, 2$. Dalje, imamo da je $H^0(M) = H^0(N) = \mathbb{Z}/3\mathbb{Z}$ i $H^0(M') = H^0(N') = 0$. Sada ako uzmemo kohomologiju nizova (6.1) i iskoristimo istu oznaku za pramenove proširene na $\mathbb{P}^1$, iz prvog niza dobijamo

$$
\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/3\mathbb{Z} \arrow[r] & \mathbb{Z}/3\mathbb{Z} \arrow[r] & 0 \arrow[dll] \\
 & \mathbb{Z}/3\mathbb{Z} \arrow[r] & H^1(M) \arrow[r] & H^1(M') \arrow[dll] \\
 & \mathbb{Z}/3\mathbb{Z} \arrow[r] & H^2(M) \arrow[r] & H^2(M')
\end{tikzcd}
$$

dok nam drugi niz daje

$$
\begin{tikzcd}
0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}/3\mathbb{Z} \arrow[dll] \\
 & H^1(N') \arrow[r] & H^1(M') \arrow[r] & \mathbb{Z}/3\mathbb{Z} \arrow[dll] \\
 & H^2(N') \arrow[r] & H^2(M') \arrow[r] & \mathbb{Z}/3\mathbb{Z}
\end{tikzcd}
$$

Odatle dobijamo jednakosti

$$
\begin{aligned}
1 + h^1(M') &= s + h^1(M), \\
1 + h^1(M') &= t + h^1(N')
\end{aligned}
$$

gde su $s \leq 1$ i $t \leq 1$. Iz (6.2) dobijamo i

$$
1 + h^1(N') = h^1(N).
$$

Ove jednakosti nam zajedno daju

$$
h^1(N) - 2 \leq h^1(M) \leq h^1(N).
$$

Sada nam lema 6.1.1 daje $\mathrm{rk}_3 \operatorname{Pic} C_1 = h^1(M) - 1$ i slično za C_2.

□

Pretpostavimo sada da $\mu_3 \notin \mathbb{F}_p$. Tada je $H^i(\mu_3) = 0$ za $i = 0, 1$ i $H^2(\mu_3) = \mathbb{Z}/3\mathbb{Z}$. Dalje je $H^0(M) = H^0(N) = H^0(M') = H^0(N') = 0$ zato što su ovo G-invarijante sloja i u ovom slučaju G ima element koji dejstvuje kao množenje sa 2, što ne fiksira nijedan element nijednog od slojeva. Sličan račun kao iznad daje

Lema 6.2.2. Ako je $G = S_3$ i $\mu_3 \notin \mathbb{F}_p$ tada je

$$\mathrm{rk}_3 \operatorname{Pic} C_2 - 1 \leq \mathrm{rk}_3 \operatorname{Pic} C_1 \leq \mathrm{rk}_3 \operatorname{Pic} C_2.$$

Kohomologija u brojevnom polju. Sličan metod radi i u slučaju brojevnih polja, gde krive zamenimo sa $\operatorname{Spec} \mathcal{O}_K[1/l]$, gde je $\mathcal{O}_K$ prsten celih brojevnog polja K. Pridružujemo element $1/l$ kako bismo osigurali da je Kumerov niz za prost broj l tačan.

Neka je S konačan skup prostih u K i neka je $\mathrm{Cl}_S(K)$ klasna grupa od K dalje od prostih iz S. Veza sa uobičajenom klasnom grupom je sledeća: postoji surjektivni morfizam

$$\phi : \mathrm{Cl}(K) \to \mathrm{Cl}_S(K)$$

koji preslikava proste iz S u trivijalnu klasu. Zato je $\mathrm{rk}_l \mathrm{Cl}_S(K) + \mathrm{rk}_l \ker \phi = \mathrm{rk}_l \mathrm{Cl}(K)$. Element iz $\mathrm{Cl}\, K$ je u jezgru ako ima predstavnika sa nosačem isključivo sadržanom u prostima iz S. Zato je $\mathrm{rk}_l \ker \phi \leq l^{|S|-1}$, gde -1 u eksponentu dolazi iz činjenice da uvek postoji barem jedna relacija između punog skupa prostih u K što leže iznad bilo kojeg prostog.

Do kraja ovog odeljka pretpostavljamo da se S sastoji iz skupa prostih iznad l. Zbog diskusije iznad je zato $\operatorname{Pic}(\operatorname{Spec} \mathcal{O}_K[1/l]) = \mathrm{Cl}_S(K)$. Neka je $s_i = r_1(K_i) + r_2(K_i) - 1$ i neka u_i označava broj prostih iz K_i iznad l. Konačno, neka je $t_i = s_i + u_i$.

Račun je vrlo sličaj slučaju polja funkcija, tako da neke detalje izostavljamo.

Lema 6.2.3. Ako je $G = S_3$ i $K_2 \neq \mathbb{Q}(\zeta_3)$, tada je

$$\mathrm{rk}_3 \mathrm{Cl}_S(K_2) - 1 + (t_2 - t_1) \leq \mathrm{rk}_3 \mathrm{Cl}_S(K_1)$$

kao i

$$\mathrm{rk}_3 \mathrm{Cl}_S(K_1) \leq \mathrm{rk}_3 \mathrm{Cl}_S(K_2) + (t_2 - t_1).$$

Dokaz. Već smo izračunali da je $H^1(\mu_3) = \mathbb{Z}/3\mathbb{Z}$ i da je $H^i(\mu_3) = 0$ za $i = 0, 2$. Nadalje, imamo da je $H^0(M) = H^0(N) = 0$, kao i $H^0(M') = H^0(N')$.

Ako posmatramo (6.1) i uzmemo kohomologiju ovih nizova dobijamo iz prvog od njih:

$$
\begin{tikzcd}
0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & H^0(M') \arrow[dll] \\
 & \mathbb{Z}/3\mathbb{Z} \arrow[r] & H^1(M) \arrow[r] & H^1(M') \arrow[dll] \\
 & 0 \arrow[r] & H^2(M) \arrow[r] & H^2(M').
\end{tikzcd}
$$

Primenom kohomologije na drugi od ovih nizova dobijamo:

$$
\begin{tikzcd}
0 \arrow[r] & H^0(N') \arrow[r] & H^0(M') \arrow[r] & 0 \arrow[dll] \\
 & H^1(N') \arrow[r] & H^1(M') \arrow[r] & \mathbb{Z}/3\mathbb{Z} \arrow[dll] \\
 & H^2(N') \arrow[r] & H^2(M') \arrow[r] & 0.
\end{tikzcd}
$$

Iz ova dva niza sledi zaključak. □

6.3 Principi refleksije za polja funkcija u slučaju Galoaove grupe Q_8

Koristeći iste ključne ideje kao [8], dolazimo do novih principa refleksija, ovog puta za raširenja kod kojih je Galoaova grupa kvaternionska grupa Q_8. Ovaj odeljak je najznačajniji originalni doprinos ovog master rada.

Tačan niz. Uzmimo $l = 2$, tada je svakako μ_2 sadržan u svim navedenim poljima. Neka je L/F Galoaovo raširenje i neka je $\mathrm{Gal}(L/F) = Q_8$, gde je Q_8 kvaternionska grupa, gde koristimo standardne oznake za njene elemente. Imamo prezentaciju $Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\rangle$. Sve podgrupe kvaternionske grupe su normalne podgrupe. To znači da je za svaku podgrupu H od $\mathrm{Gal}(L/F)$ fiksno polje L^H jedno Galoaovo raširenje od F.

Posmatrajmo dve podgrupe $H_1 = \{1, -1\}$ i $H_2 = \{1, i, -1, -i\}$ od Q_8. Neka je $K_1 = L^{H_1}$ i $K_2 = L^{H_2}$. Iz teoreme o Galoaovoj korespondenciji je K_1 raširenje od F stepena $[K_1 : F] = [L : F]/[L : K_1] = 8/|H_1| = 4$ i $[K_2 : F] = [L : F]/[L : K_2] = 8/|H_2| = 2$.

Osim toga, imamo da je $\mathrm{Gal}(K_1/F) \cong Q_8/H_1$, čiji koseti se mogu označiti sa 1, i, j i k. Ovde 1 i -1, i i $-i$, j i $-j$, kao i k i $-k$ pripadaju istom kosetu.

Slično $\mathrm{Gal}(K_2/F) \cong Q_8/H_2$, gde su koseti H_2 i kH_2, koje zbog jednostavnosti redom označavamo opet sa 1 i k. Primetimo da su $1, i, -1, -i$ u kosetu H_2, dok su $k, j, -k, -j$ u kosetu kH_2.

Koristeći lemu 6.1.4 dobijamo Q_8-module M i N:

$$M = \mathbb{Z}/2\mathbb{Z}\langle 1, i, j, k\rangle,$$

$$N = \mathbb{Z}/2\mathbb{Z}\langle 1, k\rangle.$$

Neka je T jednodimenzionalni modul sa trivijalnim dejstvom. Uvedimo i $M_1 = \langle 1+i, 1+j, 1+k\rangle$. Tada imamo tačne nizove Galoaovih modula:

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow T \longrightarrow 0, \tag{6.3}$$

$$0 \longrightarrow N \longrightarrow M_1 \longrightarrow T \longrightarrow 0. \tag{6.4}$$

Preslikavanja u ovim tačnim nizovima možemo eksplicitno opisati. U prvom nizu je M_1 podmodul od M, pa je prvo preslikavanje samo inkluzija, dok je T izomorfno sa količnikom modula M sa podmodulom M_1. Ovo je očigledno tačan niz Galoaovih modula.

Posmatrajmo sada drugi tačan niz. Preslikavanje $N \longrightarrow M_1$ je određeno sa $1 \mapsto 1+i$ i $k \mapsto k+j$ (gde zloupotrebljavamo oznake, koristeći oznaku k za kosete različitih podgrupa). Nije teško videti da je ovo injektivni homomorfizam Galoaovih modula.

Slika ovog preslikavanja se sastoji iz 0, $1+i$, $k+j$, $1+i+j+k$. Ako uzmemo količnik M_1 sa ovom slikom, dobijamo modul izomorfan sa T, pa preslikavanje $M_1 \longrightarrow T$ odgovara projekciji. Odatle odmah vidimo da je i drugi niz tačan.

Sada ćemo, slično kao u slučaju Galoaove grupe S_3, pretpostaviti da grupa inercije u svakoj tački ima red 2. Jedina podgrupa reda dva od Q_8 je $\{1, -1\}$. Ako je I grupa inercije u nekoj tački reda dva, vidimo da uzimanjem I-invarijanti zapravo dobijamo iste tačne nizove pramenova.

Kohomološki račun. Već smo izračunali da je $H^i(\mu_2) = \mathbb{Z}/2\mathbb{Z}$ za $i = 0, 1, 2$. Dalje je $H^0(M) = H^0(N) = \mathbb{Z}/2\mathbb{Z}$ (svakako $\mathbb{F}_p$ sadrži kvadratne korene iz 1). Uzimajući kohomologiju niza (6.3), dobijamo:

$$
\begin{tikzcd}
0 \arrow[r] & H^0(M_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[dll] \\
& H^1(M_1) \arrow[r] & H^1(M) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[dll] \\
& H^2(M_1) \arrow[r] & H^2(M) \arrow[r] & \mathbb{Z}/2\mathbb{Z}.
\end{tikzcd}
$$

Slično, uzimamo kohomologiju niza (6.4) i dobijamo

$$
\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & H^0(M_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[dll] \\
& H^1(N) \arrow[r] & H^1(M_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[dll] \\
& H^2(N) \arrow[r] & H^2(M_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}
$$

Iz ova dva duga tačna niza dobijamo da postoje $r, s, t \leq 1$ takvi da je

$$h^1(M_1) + s = h^1(M) + 1$$

$$t = h^1(M_1) - h^1(N) + r.$$

Odavde je

$$h^1(N) + t - r + s - 1 = h^1(M),$$

pa odatle dobijamo

$$h^1(N) - 2 \leq h^1(M) \leq h^1(N) + 1.$$

Odavde dobijamo sledeću teoremu:

Teorema 6.3.1. Ako je $G = Q_8$, tada važe nejednakosti

$$\operatorname{rk}_2 \operatorname{Pic} C_2 - 2 \leq \operatorname{rk}_2 \operatorname{Pic} C_1 \leq \operatorname{rk}_2 \operatorname{Pic} C_2 + 1.$$

6.4 Ideje za dalji rad

Koliko je autoru ovog master rada poznato, trenutno ne postoji neki opšti metod za dobijanje ovih i sličnih principa refleksije. Kao što se vidi u ovom radu, najčešće se dobijaju tako što se radi sa malim grupama i direktno se konstruišu odgovarajući Galoaovi moduli, dok se neophodne osobine proveravaju neposrednim računom.

Čini se da se situacija dodatno komplikuje kada se radi sa cikličnim Galoaovim grupama. Autor je neuspešno pokušao da izvede sličnu proceduru za Galoaovu grupu C_6 kao u slučaju grupe S_3 (obe imaju isti broj elemenata), međutim, izuzetno je komplikovano konstruisati odgovarajuće module, pre svega zbog toga što tada G ima netrivijalno dejstvo na sve kosete, pa je glavni problem to što homomorfizmi potencijalnih modula u tačnim nizovima ne poštuju dejstvo grupe G.

Sličan problem se javlja čak i kada se posmatra grupa C_{l-1}, gde je $l = 6k + 1$ prost broj (kojih ima beskonačno mnogo na osnovu Dirihleove teoreme o prostim brojevima).

Pitanje. Neka je $l = 6k + 1$ prost broj. Da li postoje analogni principi refleksije u slučaju raširenja sa Galoaovom grupom C_{l-1}?

Koren ovog pitanja potiče iz problema izučavanja klasnih grupa kod ciklotomičnih raširenja, što je bila i ključna motivacija autora za njegovo razmatranje.

Drugi smer za potencijalni dalji rad je da se proveri da li postoje slični principi refleksije za druge nekomutativne grupe malog reda. Autor ovog rada se pre svega bavio grupom $SL(2, 3)$, zbog njene relativno jednostavne prezentacije i činjenice da je poznato da se ona realizuje kao Galoaova grupa polinoma

$$x^8 - 3x^7 - 8x^6 + 24x^5 + 9x^4 - 34x^3 - 4x^2 + 11x - 1.$$

Međutim, što je grupa veća, to su provere da su konstruisani nizovi Galoaovih modula zaista tačni su sve zahtevniji računski, pa je neophodna i pomoć računara kako bi se obavile sve potrebne provere.

Osim toga, da bi dobijeni principi refleksije imali primene i u algebarskoj teoriji brojeva, važno je pitanje da li se data grupa može realizovati kao Galoaova grupa nekog konačnog raširenja od $\mathbb{Q}$. Za kraj, postavljamo sledeći problem, čije rešavanje verovatno zahteva i pomoć nekog matematičkog softvera:

Problem. Otkriti principe refleksije za Galoaova raširenja čija Galoaova grupa je Q_{16}, Q_{20} ili $SL(2, 3)$.

Bibliografija

[1] A. Grothendieck, J. A. Dieudonné, *Éléments de géométrie algébrique I.,* (English) [B] Die Grundlehren der mathematischen Wissenschaften. 166. Berlin-Heidelberg-New York: SpringerVerlag. IX, 466 p. (1971).

[2] A. Lipkovski, *Algebarski koherentni pramenovi: magistarska teza*, Beograd: Univerzitet u Beogradu, Matematički fakultet, 1978.

[3] Autori stranice Stacks Project, *Stacks Project*, URL: http://stacks.math.columbia.edu.

[4] D. Arapura, *An Introduction to Etale Cohomology*, 2012., URL: https://www.math.purdue.edu/ arapura/

[5] F. Lemmermeyer, *Class groups of dihedral extensions*, Math. Nachr., 278(6):679–691, 2005.

[6] G. Ellingsrud, J. C. Ottem, *Introduction to Schemes (v2.2)*, University of Oslo, 2022.

[7] H. Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[8] J. Klys, *Reflection principles for class groups*, Journal of Number Theory, 177. 10.1016/j.jnt.2017.01.008, 2016.

[9] J. P. Murre, *Lectures on An Introduction to Grothendieck's Theory of the Fundamental Group*, Tata Institute of Fundamental Research, 1967.

[10] J. S. Milne, *Étale Cohomology*, (PMS-33). Princeton University Press, **4** 1980.

[11] J. S. Milne, *Lectures on Étale Cohomology (v2.21)*, 2013., URL: https://www.jmilne.org/

[12] J. Tsimerman, *Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points*, J. Amer. Math. Soc., 25(4):1091–1117, 2012.

[13] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, R. Erné trans., Oxford Grad. Texts in Math. **6**, Oxford U.P., Oxford, 2002.

[14] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. **52**, Springer-Verlag, New York-Heidelberg, 1977.

[15] R. Vakil, *The Rising Sea: Foundations of Algebraic Geometry*, 2017., URL: http://math.stanford.edu/ vakil/216blog/

Biografija autora

Nikola Velov (*18. april 1998.*) je diplomirao teorijsku matematiku i primene na Matematičkom fakultetu 2021. godine sa prosečnom ocenom 10.00. Kao srednjoškolac je osvojio bronzanu medalju na Međunarodnoj matematičkoj olimpijadi (IMO 2017) i srebrnu medalju na Balkanskoj matematičkoj olimpijadi 2017.

Na osnovnim studijama je učestvovao na mnogim međunarodnim takmičenjima i osvojio tri zlatne i jednu srebrnu medalju na međunarodnom takmičenju IMC (International Mathematics Competition for University Students). U momentu pisanja ovog rada je student Matematičkog fakulteta sa najviše osvojenih zlatnih medalja na ovom takmičenju.

Aktivno učestvuje u matematičkim seminarima, radionicama, letnjim školama i konferencijama. Bio je jedan od predavača na konferenciji Macedonian Workshop on Graph Theory and Applictions 2021. Radio je i praksu na MISANU tokom leta 2021. godine.

Učestvuje u radu Saveza matematičara Makedonije (SMM) od 2019. godine, gde je član komisije za matematičke olimpijade osnovaca i srednjoškolaca. Vodio je makedonsku reprezentaciju na Balkansku matematičku olimpijadu 2020, 2021. i 2022. godine.

Autor je preko 30 zadataka koji su bili izabrani na raznim matematičkim takmičenjima. Jedan je od autora knjige „25 godina Juniorska makedonska matematička olimpijada 1997-2021".