Универзитет у Београду
Математички факултет

мастер рад

Теорема Чеботарева о густини и њене примене на аритметику елиптичких кривих

Никола Лелас

ментор
др Горан Ђанковић

Београд, 2015.

Садржај

Предговор **1**

1 Мотивација– Уопштење Дирихлеових L-функција **3**
1.1 Дирихлеова теорема о простим бројевима 3
1.2 Норма идеала 4
1.3 Најједноставније уопштење Дирихлеових L-функција 6

2 Алгебарска бројевна поља **9**
2.1 Комплетирање поља 9
2.1.1 Комплетирање поља рационалних бројева $\mathbb{Q}$ 12
2.2 Дирихлеова теорема о инвертибилним елементима 17
2.3 Модул. Група класа зрака у односу модул 19
2.4 Кондуктори група идеала 25
2.5 Прости бројеви и Галуаова раширења бројевних поља 27
2.5.1 Рамификација простих бројева 28
2.5.2 Група декомпозиције 30
2.5.3 Група инерције 31
2.6 Фробенијусов аутоморфизам и Артиново пресликавање 32
2.6.1 Фробенијусов аутоморфизам 32
2.6.2 Артиново пресликавање 34

3 L-функције **39**
3.1 Уопштене Дирихлеове L-функције. Дедекиндова зета функција 39
3.2 Репрезентације коначне групе 43
3.3 Артинове L-функције 51
3.3.1 Артинова хипотеза (АНС) 57
3.3.2 Доказ Теореме 3.1.1 60

4 Теореме о густини– Дирихлеа и Чеботарева **62**
4.1 Појам Дирихлеове густине. Дирихлеова теорема о густини 62
4.2 Теорема Чеботарева о густини 65

4.3 Примери примена теореме Чеботарева 68
4.3.1 Природна густина и њен однос са Дирихлеовом густином 68
4.3.2 Артиново пресликавање је сурјективно 71
4.3.3 Карактеризација Галуаових раширења бројевних поља помоћу простих идеала који се у њима цепају 73
4.3.4 Лежандров симбол и Дирихлеова густина 78

5 Асимптотски поглед на теорему Чеботарева **80**
5.1 Ефективна верзија теореме Чеботарева о густини 81
5.1.1 Оцена дискриминанте бројевног поља 82
5.1.2 Приказ неколико ефективних верзија теореме Чеботарева о густини 85
5.2 Неколико значајних тврђења општијег карактера уз ефективне верзије теореме Чеботарева 91

6 Елиптичке криве **93**
6.1 Дефиниција елиптичке криве 93
6.1.1 Алгебарска дефиниција елиптичке криве 94
6.1.2 Геометријска дефиниција елиптичке криве 95
6.1.3 Однос геометријске и алгебарске дефиниције 96
6.2 Групни закон на елиптичкој кривој и изогеније 97
6.3 Елиптичке криве над коначним пољима и редукција елиптичке криве . 100

7 Фробенијусова поља елиптичких кривих **103**
7.1 Уводно разматрање 103
7.2 Комбиноване Галуаове репрезентације 105
7.2.1 Репрезентација везана за елиптичку криву $E/\mathbb{Q}$ 105
7.2.2 Репрезентација везана за квадратно имагинарно бројевно поље K 106
7.2.3 Дефиниција комбиноване Галуаове репрезентације 109
7.3 Асимптотска формула за $\Pi_E(K;x)$ 114

Додатак: Хипотеза о корелацији парова (PCC) **125**

Литература **130**

Листа симбола и ознака **132**

Индекс **134**

Предговор

Елиптичке криве представљају један од најзначајних и најизучаванијих објеката, како у теорији бројева, тако и у модерној математици уопште. Циљ овог рада је да се прикаже један приступ изучавању неких значајних (аритметичко-алгебарских) особина које поседују елиптичке криве. Основно средство у таквом изучавању ће бити *Теорема Чеботарева о густини*, односно прецизније, ефективне верзије те теореме. Сама Теорема Чеботарева пружа веома моћан алат који се може користити у многим контекстима: од бројевних поља, преко елиптичких кривих, све до модуларних форми. Наравно, као што то обично бива, моћан алат се не може стећи без одређеног напора и изучавања општије теорије која иза њега лежи. Због тога је у овом раду велики простор посвећен темама како из алгебарске, тако и из аналитичке теорије бројева, који на први поглед можда није јасно да заслужују. Приказана општа (алгебарска и аналитичка) теорија има велики значај и сама по себи, па се може посматрати и независно од већ поменуте сврхе коју има у овом раду. Управо у тој чињеници лежи објашњење неуобичајено великог обима који сам рад има- поред главног циља, што је приказивање Теореме Чеботарева о густини и њене примене на аритметику елиптичких кривих, обрађене су и теме које заузимају значајна места како у алгебарској, тако и у аналитичкој теорији бројева, пружајући још једну значајну димензију поред главног тока излагања.

Рад је конципиран у седам поглавља и један додатак:

- Прво поглавље је уводног карактера и служи пружању мотивације за правац излагања којим ћемо се кретати.

- Друго поглавље је највећим делом посвећено теорији поља класа, као једној од централних тема у алгебарској теорији бројева и оквиру који дефинише Теорему Чеботарева о густини.

- Треће поглавље се бави уопштеним Дирихлеовим и Артиновим L-функцијама које пружају основно средство за доказивање Теореме Чеботарева о густини. Поред тога, један део излагања у овој глави је посвећен репрезентацијама коначних група, што је појам неопходан за дефинисање Артинових L-функција.

- Четврто поглавље се бави доказивањем теорема о густини Дирихлеа и Чеботарева, као и приказом неких примена Теореме Чеботарева.
- Пето поглавље се највећим делом бави приказањем неколико ефективних верзија Теореме Чеботарева, уз различите претпоставке.
- У шестом поглављу дат је кратак приказ основних појмова из теорије елиптичких кривих.
- Седмо поглавље представља кулминацију рада и у њему је детаљно приказан механизам примене Теореме Чеботарева на аритметику елиптичких кривих.
- У додатку је дат кратак приказ Хипотезе о корелацији парова на примеру Риманове зета функције.

За крај овог предговора, желео бих да се захвалим свом ментору, др Горану Ђанковићу, на изузетној помоћи коју ми је пружио током свих фаза израде овог рада, на мотивацији да истажим и додам теме које ми на први поглед нису деловале претерано значајне, на подстицају да одем корак даље тамо где бих стао, као и на целокупном позитивном утицају који је допринео да овај рад достигне свој обим и своју форму.

ГЛАВА 1

Мотивација– Уопштење Дирихлеових L-функција

1.1 Дирихлеова теорема о простим бројевима

Још је Ојлер приметио да сваки аритметички низ који почиње са 1 садржи бесконачно много простих бројева. Пошто није умео да докаже то тврђење оно је остало само као хипотеза. Касније, радећи на закону квадратног реципроцитета, Лежандр је посматрао аритметички низ:

$$a, a+q, a+2q, a+3q, a+4q, \ldots \tag{1.1}$$

при чему су a и q узајамно прости бројеви и дошао до хипотезе да у њему има бесконачно много чланова који су прости бројеви, природно уопштивши Ојлерову претпоставку. На доказ овог тврђења се чекало до Дирихлеа и оно је данас познато као Дирихлеова теорема о простим бројевима.

Теорема 1.1.1 (Дирихлеова о простим бројевима у аритметичкој прогресији). *Нека су a и q узајамно прости природни бројеви. Тада постоји бесконачно много простих бројева p таквих да је $p \equiv a \pmod{q}$.*

Доказ. Комплетан доказ Дирихлеове теореме о простим бројевима у аритметичкој прогресији може се пронаћи у [5]. □

Дирихлеов доказ наведене теореме је својом неелементарношћу дао вишеструке доприносе математици који значајем далеко превазилазе значај саме теореме. Пре свега ту се мисли на Дирихлеове карактере и Дирихлеове L-функције, као и на зачетак потпуно нове теорије– *аналитичке теорије бројева* и њено прво велико достигнуће.

Једна од основних особина простих бројева је да се, иако их има бесконачно много, они проређују у скупу природних бројева. Неформално говорећи, то значи да како посматрани природни број расте, број простих бројева који су мањи од њега расте све спорије. Како Дирихлеова теорема установљава егзистенцију бесконачно много простих бројева у низу (1.1), природно се намеће питање њихове густине у том низу.

Управо је решавање тог питања правац у коме ће ићи даље излагање. При томе, разматраћемо ситуацију уопштену у контексту бројевног поља и простих идеала његовог прстена целих.

1.2 Норма идеала

Наведимо прво неке стандардне ознаке које ћемо користити у тексту:

- $K-$ произвољно бројевно поље
- $\mathscr{O}_K-$ прстен целих бројевног поља K
- $J-$ скуп свих идеала прстена $\mathscr{O}_K$
- M_K- скуп свих ненула простих идеала прстена $\mathscr{O}_K$
- I_K- група свих ненула идеала разломака прстена целих $\mathscr{O}_K$ бројевног поља K. Подсетимо се да је I_K слободна Абелова група чији су генератори прости идеали прстена $\mathscr{O}_K$
- уколико се другачије не нагласи, s је по правилу ознака за комплексну променљиву, уз стандардно, али помало неуобичајено $s = \sigma + it$
- $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}-$ Риманова зета функција
- $\mathbb{F}_q-$ коначно поље са q елемената
- $\mathbb{S}^1-$ јединична кружница у комплексној равни, $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

Познато је да је $\mathscr{O}_K$ Дедекиндов домен, што значи да иако не мора бити прстен са јединственом факторизацијом, на скупу његових идеала она постоји. Прецизније, важи следеће тврђење:

Тврђење 1.2.1. *Нека је R домен целих. Тада је R Дедекиндов домен ако и само ако се сваки идеал прстена R различит од 0 може на јединствен начин представити као производ простих идеала.*

Доказ. За потпуну карактеризацију Дедекиндових домена, што укључује и доказ ове теореме погледати [5]. □

Из претходне теореме је јасно због чега се приликом рада са прстеном целих бројевног поља тежиште интересовања премешта са елемената тог прстена на његове идеале. Од нарочитог интересовања су прости идеали који представљају уопштење простих бројева. Управо због тога се питања о густини простих бројева у неком скупу

природних бројева у контексту прстена целих бројевног поља интерпретирају као испитивање густине скупа простих идеала у неком скупу идеала тог прстена. Иако ово питање можда на први поглед изгледа наивно, оно је веома комплексно; треба дефинисати нумеричку величину која на добар начин квантификује колико „простора"у неком скупу идеала заузимају прости идеали.

Пут ка њеном дефинисању следи идеју која се крије иза појма Дирихлеове L-функције и зато је од значаја дати уопштење тог појма за произвољна бројевна поља. Подсетимо се да је Дирихлеова L-функција придружена Дирихлеовом карактеру χ дата са

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \tag{1.2}$$

одакле се за њено уопштавање јасно намеће потреба претходног уопштења појма Дирихлеовог карактера. Поред ове очигледне, јавља се и друга мање очигледна потреба за дефинисањем још једног појма. Наиме, пошто је, као што смо већ нагласили, фокус интересовања пребачен са елемената прстена целих бројевног поља на његове идеале, потребно је имати сваком од њих придружену вредност која говори нешто о његовој „величини"– његову норму. Управо то је појам који ћемо следећи дефинисати.

Нека је $\mathfrak{a} \neq 0$ произвољан идеал прстена $\mathscr{O}_K$. Приметимо да су $\mathscr{O}_K$ и $\mathfrak{a}$ слободни $\mathbb{Z}$-модули, као и да је $\mathfrak{a}$ коначног индекса у $\mathscr{O}_K$. Према томе, $[\mathscr{O}_K : \mathfrak{a}]$ је коначно, па је следећа дефиниција коректна.

Дефиниција 1.2.1. *Нека је $\mathfrak{a} \neq 0$ идеал прстена целих $\mathscr{O}_K$ бројевног поља K. Његову норму $\mathfrak{N}(\mathfrak{a})$ дефинишемо као $\mathfrak{N}(\mathfrak{a}) = [\mathscr{O}_K : \mathfrak{a}]$. Додатно, норма нула идеала је дата са $\mathfrak{N}(0) = 0$.*

Основна и веома значајна особина норме је њена мултипликативност. Поред те особине од значаја је и карактеризација норме простих идеала дата следећим тврђењем.

Тврђење 1.2.2. *Нека је $\mathfrak{a} \neq 0$ произвољан идеал прстена целих $\mathscr{O}_K$ бројевног поља K степена n над $\mathbb{Q}$. Тада важе следећа тврђења:*

1. *Ако је $\mathfrak{N}(\mathfrak{a})$ прост рационалан број, онда је $\mathfrak{a}$ прост идеал.*

2. *Ако је $\mathfrak{a}$ прост идеал, онда постоји тачно један прост рационалан број p такав да је $\mathfrak{N}(\mathfrak{a}) = p^f$ за неки природан број $f \leq n$.*

Доказ. За доказ мултипликативности норме, доказ ове теореме и друге карактеризације норме погледати [5]. □

1.3 Најједноставније уопштење Дирихлеових L-функција

Следећи задатак коме ћемо се окренути је већ најављено уопштење Дирихлеовог карактера. У својој потпуности тај задатак је прилично дуготрајан и захтеван, па ћемо зато, за почетак, кренути од најједноставнијег случаја.

Подсетимо се да је појам дељивости у скупу идеала произвољног комутативног прстена са јединицом дефинисан аналогно као што се дефинише дељивост целих бројева. Дакле, нека су $\mathfrak{a}$ и $\mathfrak{b}$ два идеала комутативног прстена са јединицом R. Тада кажемо да $\mathfrak{a}$ *дели* $\mathfrak{b}$ и пишемо $\mathfrak{a} \mid \mathfrak{b}$ ако постоји идеал $\mathfrak{c}$ прстена R такав да је $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$. Додатно, да за два идеала $\mathfrak{a}$ и $\mathfrak{b}$ прстена R каже да су узајамно прости ако је $\mathfrak{a}+\mathfrak{b} = R$.

Ако је $\mathfrak{a}$ произвољан идеал прстена целих $\mathscr{O}_K$ бројевног поља K, подгрупу групе I_K генерисану свим простим идеалима који су узајамно прости са $\mathfrak{a}$ ћемо означавати са $J^{\mathfrak{a}}$. Уочимо произвољан карактер χ групе $J^{\mathfrak{a}}$, односно произвољан хомоморфизам

$$\chi : J^{\mathfrak{a}} \to \mathbb{S}^1.$$

Тај карактер можемо проширити до скупа J свих идеала прстена $\mathscr{O}_K$ стављајући $\chi(\mathfrak{b}) = 0$ за све $\mathfrak{b}$ који нису узајамно прости са $\mathfrak{a}$. Оваквим проширивањем добијамо пресликавање $\chi : J \to \mathbb{C}$ које ћемо називати *карактером скупа свих идеала* J.

У случају најједноставнијег бројевног поља, односно поља рационалних бројева $\mathbb{Q}$, имамо да је прстен целих $\mathbb{Z}$ главноидеалски. Због тога имамо да је у овом случају $J = \mathbb{Z}$. Према томе, карактер скупа свих идеала J представља аналоган објекат Дирихлеовом карактеру.
Сваком карактеру χ скупа свих идеала J можемо придружити генераторни Дирихлеов ред који је описан наредном дефиницијом.

Дефиниција 1.3.1. *Нека је K бројевно поље и χ карактер скупа J свих идеала прстена целих $\mathscr{O}_K$ тог поља. L-функција придружена карактеру χ дефинише се као сума Дирихлеовог реда*

$$L(s, \chi) = \sum_{\mathfrak{a} \in J \setminus \{0\}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}.$$

Наредна теорема приказује основна својства L-функције дате претходном дефиницијом. Као малу напомену, приметимо да је карактер χ мултипликативан, па чињеница да $L(s, \chi)$ има Ојлеров производ није нимало изненађујућа.

Тврђење 1.3.1. *L-функција $L(s, \chi)$ придружена карактеру χ скупа J конвергира апсолутно и униформно на домену $\Re(s) \geq 1 + \delta$ за све $\delta > 0$ и при томе се може на том домену написати у облику Ојлеровог производа*

$$L(s, \chi) = \prod_{\mathfrak{p} \in M_K} \frac{1}{1 - \chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}. \tag{1.3}$$

Доказ. Означимо са $E(s)$ десну страну једнакости (1.3). Формално логаритмујући и развијајући у Тејлоров ред добијамо да је

$$\log E(s) = \sum_{\mathfrak{p}\in M_K} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n}{n\mathfrak{N}(\mathfrak{p})^{ns}}$$

Приметимо да за произвољан идеал $\mathfrak{p}$ важи $|\chi(\mathfrak{p})| \leq 1$, као и да важи оцена:

$$|\mathfrak{N}(\mathfrak{p})^s| = |\mathfrak{N}(\mathfrak{p})|^\sigma \geq p^{f(1+\delta)} \geq p^{1+\delta},$$

где је p одређен Теоремом 1.2.2. Користећи основне особине расцепљивања простих идеала, имамо да је $\#\{\mathfrak{p} \mid p\} \leq d = [K : \mathbb{Q}]$, па $\log E(s)$ можемо са горње стране ограничити конвергентним редом који не зависи од промењиве s:

$$\sum_{\mathfrak{p}\in M_K} \sum_{n=1}^{\infty} \frac{d}{np^{n(1+\delta)}} = d \log \zeta(1+\delta)$$

Одатле следи да је функција $\log E(s)$ униформно и апсолутно конвергира на области $\Re(s) \geq 1+\delta$ за све $\delta > 0$, па исто важи и за функцију $E(s) = \prod_{\mathfrak{p}\in M_K} \frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}$.

Да бисмо завршили доказ тврђења потребно је још да покажемо да је $L(s,\chi) = E(s)$. Фиксирајмо природан број N. Тада постоји само коначно много простих идеала $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ таквих да је $\mathfrak{N}(\mathfrak{p}_i) \leq N, 1 \leq i \leq r$. За сваког од њих имамо развој

$$\frac{1}{1-\chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} = 1 + \frac{\chi(\mathfrak{p}_i)}{\mathfrak{N}(\mathfrak{p}_i)^s} + \frac{\chi(\mathfrak{p}_i)^2}{\mathfrak{N}(\mathfrak{p}_i)^{2s}} + \ldots$$

Множењем свих таквих једнакости добијамо

$$\prod_{i=1}^{r} \frac{1}{1-\chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} = \sum_{\nu_1,\ldots,\nu_r=0}^{\infty} \frac{\chi(\mathfrak{p}_1)^{\nu_1}\ldots\chi(\mathfrak{p}_r)^{\nu_r}}{(\mathfrak{N}(\mathfrak{p}_1)^{\nu_1}\ldots\ \mathfrak{N}(\mathfrak{p}_r)^{\nu_r})^s} = {\sum_{\mathfrak{a}\in J\setminus\{0\}}}' \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} \tag{1.4}$$

при чему је $\sum'$ ознака за суму узету по свим идеалима $\mathfrak{a}$ дељивим највише простим идеалима $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Пошто се у тој суми појављују сви чланови за које је $0 < \mathfrak{N}(\mathfrak{a}) \leq N$ можемо такође писати

$$\prod_{i=1}^{r} \frac{1}{1-\chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} = \sum_{0<\mathfrak{N}(\mathfrak{a})\leq N} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} + {\sum_{\mathfrak{N}(\mathfrak{a})>N}}' \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}.$$

Означимо са $J_{N,r}$ скуп свих идеала $\mathfrak{a} \in J$ за које је $\mathfrak{N}(\mathfrak{a}) > N$ и $\mathfrak{p}_i \nmid \mathfrak{a}$ за бар једно $1 \leq i \leq r$. Упоређујући сада једнакост (1.4) са $L(s,\chi)$ добијамо

$$\left| \prod_{i=1}^{r} \frac{1}{1-\chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} - L(s,\chi) \right| \leq \left| \sum_{\mathfrak{a}\in J_{N,r}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} \right| \leq \sum_{\mathfrak{N}(\mathfrak{a})>N} \frac{1}{\mathfrak{N}(\mathfrak{a})^{1+\delta}} \tag{1.5}$$

Приметимо да је сума са десне стране неједнакости (1.5) остатак реда који се може изразити као гранична вредност низа парцијалних сума $(\sum_{0<\mathfrak{N}(\mathfrak{a})\leq N} \frac{1}{\mathfrak{N}(\mathfrak{a})^{1+\delta}})_{N\in\mathbb{N}}$. Тај низ је очигледно монотон, а његова ограниченост следи из

$$\begin{aligned}\sum_{0<\mathfrak{N}(\mathfrak{a})\leq N} \frac{1}{\mathfrak{N}(\mathfrak{a})^{1+\delta}} &\leq {\sum_{\mathfrak{a}\in J\setminus\{0\}}}' \frac{1}{\mathfrak{N}(\mathfrak{a})^{1+\delta}} \\ &= \prod_{i=1}^{r} (1-\mathfrak{N}(\mathfrak{p}_i)^{-(1+\delta)})^{-1}\end{aligned}$$

и оцена

$$\begin{aligned}\log(\prod_{i=1}^{r} (1-\mathfrak{N}(\mathfrak{p}_i)^{-(1+\delta)})^{-1}) &= \sum_{i=1}^{r} \log((1-\mathfrak{N}(\mathfrak{p}_i)^{-(1+\delta)})^{-1}) \\ &= \sum_{i=1}^{r}\sum_{n=1}^{\infty} \frac{1}{n\mathfrak{N}(\mathfrak{p}_i)^{(1+\delta)n}} \\ &\leq \sum_{\mathfrak{p}\in M_K}\sum_{n=1}^{\infty} \frac{1}{n\mathfrak{N}(\mathfrak{p})^{(1+\delta)n}} \\ &\leq \sum_{p=1}^{\infty}\sum_{n=1}^{\infty} d\frac{1}{np^{n(1+\delta)}} \\ &= d\log(\zeta(1+\delta)).\end{aligned}$$

Одатле закључујемо да је десна страна неједнакости (1.5) остатак конвергентног реда, па тежи ка 0 када $N\to\infty$. Приметимо да тада и $r\to\infty$. Због тога, пуштајући $N\to\infty$ у (1.5) добијамо коначно $L(s,\chi)=E(s)$, чиме је доказ завршен.

□

Посматрајући сличност L-функција придружених карактеру χ скупа J са Дирихлеовим L-функцијама природно се намеће питање њиховог аналитичког проширења и успостављања одговарајућих функционалних једначина. Приметимо да је у случају („обичних") Дирихлеових L-функција за такав подухват веома значајна особина периодичности коју поседују Дирихлеови карактери. Због тога се намеће потреба да видимо како се периодичност може изразити у контексту произвољног бројевног поља (који нас занима) и да ли уопштење Дирихлеовог карактера које смо дали у овом одељку поседује ту особину. За такве потребе биће неопходно додатно обогатити (алгебарски) простор којим се крећемо. Управо тој теми посвећене су наредне странице.

ГЛАВА 2

Алгебарска бројевна поља

2.1 Комплетирање поља

Посматрајмо иницијално ситуацију у најопштијем контексту, одакле ћемо после донети специфичне закључке од интереса за бројевна поља. Нека је F произвољно поље. Циљ је да за њега дефинишемо поступак аналоган поступку којим се од поља $\mathbb{Q}$ добија поље $\mathbb{R}$, односно да га комплетирамо. Да би се уопште размишљало о комплетности поља, потребно је на њему имати дефинисану конвергенцију. На пољу F она ће бити индукована валуацијом и наредне дефиниције посвећене су управо њеном дефинисању.

Дефиниција 2.1.1. *Нека је F произвољно поље. Пресликавање $|\cdot| : F \to \mathbb{R}$ назива се* ***валуацијом*** *на F ако има следеће особине:*

1. $|x| \geq 0$ *за све* $x \in F$ *и* $|x| = 0$ *ако и само ако је* $x = 0$.
2. $|x||y| = |xy|$ *за све* $x, y \in F$.
3. *За све* $x, y \in F$ *важи неједнакост троугла*

$$|x + y| \leq |x| + |y|. \tag{2.1}$$

Валуацију називамо тривијалном ако је $|x| = 1$ за све $x \neq 0$. Она није од претераног интереса и надаље ћемо за све валуације са којима будемо радили сматрати да су нетривијалне.

Дефиниција 2.1.2. *Валуација $|\cdot|$ на F се назива* ***неархимедовом*** *ако важи $|x+y| \leq \max\{|x|, |y|\}$ за све $x, y \in F$. У супротном, валуација се назива* ***архимедовом****.*

За две валуације $|\cdot|$ и $|\cdot|'$ кажемо да су еквивалентне ако за све $x \in F$ важи: $|x| < 1$ ако и само ако је $|x|' < 1$. Овако дефинисана релација на скупу свих валуација је релација еквиваленције, чије су класе од великог значаја и описане су наредном дефиницијом.

Дефиниција 2.1.3. *Класе еквиваленције релације еквивалентности дефинисане на скупу свих валуација називају се* ***простим бројевима*** *у пољу F. Ако је прост број поља F класа еквиваленције архимедове валуације он се назива* ***бесконачним****, док се класе еквиваленција неархимедових валуација називају* ***коначним*** *простим бројевима у F.*

Помоћу валуације се може дефинисати конвергенција на пољу F на потпуно аналоган начин на који се дефинише конвергенција индукована нормом на нормираном векторском простору. Имајући то у виду наредне две дефиниције су потпуно природне и нимало неочекиване.

Дефиниција 2.1.4. *Нека је F произвољно поље са валуацијом $|\cdot|$. Низ $\{a_n\}$ елемената тог поља конвергира ка елементу $a \in F$ ако је испуњено*

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Дефиниција 2.1.5. *Низ $\{a_n\}$ елемената поља F назива се Кошијевим низом ако је испуњено да за свако $\varepsilon > 0$ постоји природан број N такав да за свако $m, n > N$ важи*

$$|a_m - a_n| < \varepsilon.$$

Као и у случају нормираних векторских простора, произвољан Кошијев низ не мора бити конвергентан. За поље са валуацијом $|\cdot|$ у коме сваки Кошијев низ конвергира каже се да је *комплетно* у односу на ту валуацију. Поља комплетна у односу на архимедову валуацију могу се релативно једноставно одредити у потпуности и описана су следећом фундаменталном теоремом Островског.

Теорема 2.1.1 (Островски). *Нека је F поље комплетно у односу на архимедову валуацију $|\cdot|$. Тада је F изоморфно или пољу реалних бројева $\mathbb{R}$ или пољу комплексних бројева $\mathbb{C}$ са уобичајеним валуацијама.*

Напомена. *Уобичајена валуација на $\mathbb{R}$ је одређена са*

$$|x| = \begin{cases} x, & \text{ако је } x \geq 0 \\ -x, & \text{ако је } x < 0. \end{cases}$$

док је уобичајена валуација на $\mathbb{C}$ одређена са

$$|s| = \sqrt{\sigma^2 + t^2}.$$

Доказ. Погледати [8]. □

Посматрајући произвољно поље F (које није комплетно у односу на валуацију $|\cdot|$) намеће се питање његовог комплетирања, односно проналажења раширења F_0 тог поља на коме је дефинисано проширење валуације $|\cdot|$ и које је комплетно у односу на ту валуацију. Поступак конструкције поља F_0 је аналоган комплетирању нормираног векторског простора (или комплетирању поља $\mathbb{Q}$ до поља $\mathbb{R}$) и описан је следећом теоремом.

Теорема 2.1.2. *Нека је F поље са валуацијом $|\cdot|$. Означимо са F_0 раширење поља F које је једнако прстену свих Кошијевих низова елемената поља F посеченим максималним идеалом свих Кошијевих низова који теже ка нули. Тада је F_0 комплетно у односу на валуацију $|\cdot|_0$ дату са*

$$|[x_n]|_0 = \lim_{n\to\infty} |x_n|$$

која представља проширење валуације $|\cdot|$. Другим речима, F_0 је комплетирање поља F.

Доказ. Комплетан поступак комплетирања поља F може се пронаћи у [8]. □

Када је показана егзистенција комплетирања поља, битно је испитати и њену јединственост, односно испитати однос комплетирања истог поља добијених на различите начине. Наредно тврђење је посвећена управо томе и говори да је комплетирање поља приказано у Теореми 2.1.2 суштински јединствено.

Тврђење 2.1.1. *Комплетирање F_0 поља F дефинисано Теоремом 2.1.2 је јединствено до на изоморфизам који чува валуацију на пољу F.*

Доказ. Погледати [8]. □

Нека су $|\cdot|$ и $|\cdot|'$ две еквивалентне валуације над пољем F. Из дефиниција релације еквивалентности валуација и Кошијевог низа непосредно следи да су скупови Кошијевих низова у односу на њих једнаки. Означимо са F_0 и F_0' комплетирања поља F у односу на одговарајуће валуације. Имајући у виду Теорему 2.1.2 и Тврђење 2.1.1 важи да су поља F_0 и F_0' изоморфна. Зато је коректно дефинисан појам комплетирања поља у његовом простом броју дат следећом дефиницијом.

Дефиниција 2.1.6. *Нека је F произвољно поље и $\mathfrak{p}$ неки прост број у њему. Комплетирање поља F у $\mathfrak{p}$ дефинише се као комплетирање поља F у односу на било коју валуацију из $\mathfrak{p}$ и означава се са $F_\mathfrak{p}$.*

2.1.1 Комплетирање поља рационалних бројева $\mathbb{Q}$

Илуструјмо теорију приказану у овом одељку на примеру најједноставнијег бројевног поља– поља рационалних бројева $\mathbb{Q}$. Такав скроман одабир бројевног поља надоместићемо амбициозним циљем намењеним за њега, који ће се огледати у приказивању свих могућих комплетирања поља $\mathbb{Q}$. Наравно, да би се уопште могло започети икакво размишљање о комплетирању поља потребно је прво имати познату валуацију у односу на коју се оно може извршити. Према томе, први задатак на путу одређивања свих комплетирања поља $\mathbb{Q}$ биће одређивање свих нееквивалентних валуација на том пољу.

Описивање свих валуација на пољу $\mathbb{Q}$ започињемо описом једне једноставне и добро познате валуације на том пољу. Посматрајмо стандардну апсолутну вредност $|\cdot|$ на $\mathbb{Q}$ одређену са

$$|x| = \begin{cases} x, & \text{ако је } x \geq 0 \\ -x, & \text{ако је } x < 0, \end{cases}$$

дефинисану за сваки рационалан број x. Веома лако се показује да претходно дефинисана стандардна апсолутна вредност на пољу рационалних бројева има следеће особине:

1. $|x| \geq 0$ за све $x \in \mathbb{Q}$ и $|x| = 0$ ако и само ако је $x = 0$.
2. $|x||y| = |xy|$ за све $x, y \in \mathbb{Q}$.
3. $|x + y| \leq |x| + |y|$ за све $x, y \in \mathbb{Q}$.

Одатле, одмах по дефиницији закључујемо да $|\cdot|$ представља једну валуацију на $\mathbb{Q}$. Надаље ћемо је називати *валуацијом у бесконачности* на пољу $\mathbb{Q}$ и означавати са $|\cdot|_\infty$. Имајући у виду да неједнакост

$$|x + y|_\infty \leq \max\{|x|_\infty, |y|_\infty\}$$

не важи за све рационалне бројеве x, y, приметимо на овом месту још да $|\cdot|_\infty$ можемо окарактерисати као *архимедову* валуацију поља $\mathbb{Q}$.

Наставак описа свих валуација на пољу рационалних бројева настављамо у правцу веома интересантном са становишта аритметике. Уочимо произвољан рационалан прост број p. Тада се сваки цео број $n \in \mathbb{Z} \setminus \{0\}$ може на јединствен начин записати у облику

$$n = p^v n' \tag{2.2}$$

за неке $v \in \mathbb{N} \cup \{0\}$ и $n' \in \mathbb{Z}$ такве да $p \nmid n'$. Из записа (2.2) закључујемо да је број v одређен само са p и n, па има смисла дефинисати пресликавање v_p са $v_p(n) = v$.

Пресликавање v_p се може са скупа $\mathbb{Z}\setminus\{0\}$ проширити до пресликавања V_p дефинисаног на скупу $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, стављајући

$$V_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b), \tag{2.3}$$

за произвољан $\frac{a}{b} \in \mathbb{Q}^*$. Основне особине тог пресликавања описане су наредним тврђењем.

Тврђење 2.1.2. *Нека је p рационалан прост број и V_p пресликавање дефинисано на $\mathbb{Q}^*$ формулом (2.3). Тада важи:*

1. *Пресликавање V_p је коректно дефинисано, односно не зависи од избора записа произвољног броја $x \in \mathbb{Q}^*$ у облику разломка.*
2. *$V_p(xy) = V_p(x) + V_p(y)$ за све $x, y \in \mathbb{Q}^*$.*
3. *$V_p(x + y) \geq \min(V_p(x), V_p(y))$ за све $x, y \in \mathbb{Q}^*$.*

Доказ. Пре доказа самих ставки из исказа тврђења покажимо једно значајно помоћно тврђење везано за пресликавање v_p дефинисано на $\mathbb{Z}\setminus\{0\}$. Уочимо произвољне $m, n \in \mathbb{Z}\setminus\{0\}$. По дефиницији пресликавања v_p важи

$$m = p^{v_p(m)}m'$$

и

$$n = p^{v_p(n)}n',$$

при чему $p \nmid m', n'$. Одатле добијамо

$$mn = p^{v_p(m)}m'p^{v_p(n)}n' = p^{v_p(m)+v_p(n)}m'n', \tag{2.4}$$

као и $p \nmid m'n'$ због тога што је број p прост. Из (2.4) онда, имајући у виду дефиницију пресликавања v_p, следи

$$v_p(mn) = v_p(m) + v_p(n). \tag{2.5}$$

Помоћно тврђење добијено у (2.5) биће кључно у наставку доказа тврђења, што ће одмах постати јасно из доказа њене прве ставке на који прелазимо.
1. Из дефиниције пресликавања V_p следи да је довољно показати да за све $a, b, c, d \in \mathbb{Z}\setminus\{0\}$ такве да је

$$\frac{a}{b} = \frac{c}{d}$$

важи

$$v_p(a) - v_p(b) = v_p(c) - v_p(d).$$

Због тога, посматрајмо произвољне $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ такве да је

$$\frac{a}{b} = \frac{c}{d}$$

и приметимо да је тада $ad = bc$. Одатле на основу формуле (2.5) добијамо $v_p(a) + v_p(d) = v_p(b) + v_p(c)$, што је еквивалентно са траженим

$$v_p(a) - v_p(b) = v_p(c) - v_p(d).$$

2. Уочимо произвољне $x, y \in \mathbb{Q}^*$. Из доказаног дела *1.* следи да је довољно показати да важи

$$V_p\left(\frac{a}{b} \cdot \frac{c}{d}\right) = V_p\left(\frac{a}{b}\right) + V_p\left(\frac{c}{d}\right)$$

за произвољне $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ такве да је $x = \frac{a}{b}$ и $y = \frac{c}{d}$.
Рачунамо

$$\begin{aligned} V_p\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= V_p\left(\frac{ac}{bd}\right) \\ &= v_p(ac) - v_p(bd) \quad (\text{ из дефиниције } V_p) \\ &= v_p(a) + v_p(c) - v_p(b) - v_p(d) \quad (\text{ из } (2.5)) \\ &= v_p(a) - v_p(b) + v_p(c) - v_p(d) \\ &= V_p\left(\frac{a}{b}\right) + V_p\left(\frac{c}{d}\right) \quad (\text{ из дефиниције } V_p), \end{aligned}$$

одакле добијамо тражено тврђење.
3. Уочимо произвољан $x \in \mathbb{Q}^*$ и напишимо га у облику разломка $x = \frac{m}{n}$ за неке $a, b \in \mathbb{Z} \setminus \{0\}$. Тада по дефиницији пресликавања v_p важи

$$m = p^{v_p(m)} m', \ \ p \nmid m'$$

и

$$n = p^{v_p(n)} n', \ \ p \nmid n'.$$

Одатле следи

$$x = \frac{m}{n} = p^{v_p(m) - v_p(n)} \frac{m'}{n'},$$

при чему $p \nmid m'n'$. Користећи дефиницију (2.3) пресликавања V_p добијамо коначно да се произвољан $x = \frac{m}{n}$ може записати у облику

$$x = p^{V_p(x)} \frac{a}{b} \tag{2.6}$$

за неке $a, b \in \mathbb{Z} \setminus \{0\}$ такве да је $p \nmid ab$.

Помоћу својства (2.6) релативно брзо доказујемо *3.* Уочимо произвољне $x, y \in \mathbb{Q}^*$ и у складу са (2.6) запишимо их у облику

$$x = p^{V_p(x)} \frac{a}{b}, \ \ p \nmid ab$$

односно

$$y = p^{V_p(y)} \frac{c}{d}, \ \ p \nmid cd.$$

Тада је

$$\begin{aligned} V_p(x+y) &= V_p\left(p^{V_p(x)} \frac{a}{b} + p^{V_p(y)} \frac{c}{d}\right) \\ &= V_p\left(p^{\min(V_p(x),V_p(y))}\left(p^{V_p(x)-\min\left(V_p(x),V_p(y)\right)} \cdot \frac{a}{b} + p^{V_p(y)-\min\left(V_p(x),V_p(y)\right)} \cdot \frac{c}{d}\right)\right) \\ &\geq \min(V_p(x), V_p(y)) \end{aligned}$$

чиме је доказано *3.* □

Упоређујући особине пресликавања V_p установљене Тврђењем 2.1.2 са особинама која неко пресликавање треба да има да би било валуација на $\mathbb{Q}$ долазимо до интересантне сличности. Наиме, особине пресликавања V_p су на неки начин инверзне особинама валуација:

- Важи $V_p(xy) = V_p(x) + V_p(y)$ уместо $V_p(xy) = V_p(x)V_p(y)$
- Важи $V_p(x+y) \geq \min(V_p(x), V_p(y))$ уместо $V_p(x+y) \leq \max(V_p(x), V_p(y))$.

Због тога следи да пресликавање V_p можемо „поправити" до валуације поља $\mathbb{Q}$ композицијом са пресликавањем $x \to -x$ и експоненцијалним пресликавањем. Наравно, на овај начин добијамо валуацију која је дефинисана на $\mathbb{Q}^*$, па је морамо још проширити до $\mathbb{Q}$ на једини могући начин– нулом. Формалније говорећи имамо следећу дефиницију.

Дефиниција 2.1.7. *Нека је $p \in \mathbb{Z}$ прост број и V_p пресликавање дефинисано на $\mathbb{Q}^*$ формулом (2.3) . Пресликавање $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ дефинисано са*

$$|x|_p = \begin{cases} p^{-V_p(x)}, & \text{ако је } x \neq 0 \\ 0, & \text{ако је } x = 0. \end{cases}$$

се назива ***p-адична валуација*** *на $\mathbb{Q}$.*

Из Тврђења 2.1.2 одмах следи наредна теорема.

Теорема 2.1.3. *За сваки прост број $p \in \mathbb{Z}$ p-адична валуација $|\cdot|_p$ представља једну* ***неархимедову*** *валуацију поља $\mathbb{Q}$.*

Нека је $|\cdot|_p$ произвољна p-адична валуација на $\mathbb{Q}$ и x произвољан рационалан број. Тада интуитивну представу о смислу $|\cdot|_p$ можемо добити из саме дефиниције тог пресликавања: на неки начин (који је можда на први поглед необичан)$|x|_p$ мери „колико је број x дељив простим бројем p".

Формални значај пресликавању $|\cdot|_p$ пружа Теорема 2.1.3, која га препознаје као неархимедову валуацију поља $\mathbb{Q}$. При томе су очигледно за два различита проста броја p и q одговарајућа p-адична и q-адична валуација нееквивалентне. Због тога, имајући у виду и архимедову валуацију $|\cdot|_\infty$ коју смо дефинисали на почетку овог пододељка можемо уочити да имамо већ приличан број међусобно неекивалентних валуација дефинисаних на $\mathbb{Q}$. Таквим посматрањем природно долазимо до питања да ли смо наведеним примерима исцрпели све могућности за дефинисање валуација на $\mathbb{Q}$, односно да ли је могуће на пољу рационалних бројева дефинисати још неку валуацију која није еквивалентна ниједној од валуација на $\mathbb{Q}$ које смо до сада видели. Одговор на то питање даје наредна изузетно позната теорема Островског.

Теорема 2.1.4 (Островски). *Произвољна нетривијална валуација $|\cdot|$ на пољу рационалних бројева $\mathbb{Q}$ еквивалентна је*

- *p-адичној валуацији за неки прост број $p \in \mathbb{Z}$ ако је $|\cdot|$ неархимедова.*
- *валуацији у бесконачности $|\cdot|_\infty$ ако је $|\cdot|$ архимедова.*

Доказ. Доказ теореме може се пронаћи у [8]. □

Теорема 2.1.4 показује да на пољу $\mathbb{Q}$ осим p-адичних и валуације у бесконачности *не постоји* других валуација. Одатле добијамо и решење задатка којим смо започели овај пододељак, а то је одређивање свих комплетирања поља рационалних бројева. Решење тог задатка ћемо приказати раздвојено у два карактеристична случаја- неархимедовом и неархимедовом.

- Нека је $|\cdot|_p$ p-адична валуација на $\mathbb{Q}$ за неки прост број $p \in \mathbb{Z}$. Комплетирање поља $\mathbb{Q}$ у односу на ту неархимедову валуацију називамо *пољем p-адичних бројева* и обележавамо са $\mathbb{Q}_p$.
- Комплетирање поља $\mathbb{Q}$ у односу на архимедову валуацију $|\cdot|_\infty$ изоморфно је пољу реалних бројева $\mathbb{R}$.

Дакле, добијамо да се поред уобичајеног комплетирања $\mathbb{R}$ поља рационалних бројева, оно може комплетирати још до поља p-адичних бројева $\mathbb{Q}_p$ за сваки прост број

$p \in \mathbb{Z}$. Поља p-адичних бројева имају веома интересантна својства (аритметичка, геометријска, тополошка), која су помало необична и неочекивана посматрана са уобичајеног становишта поља реалних или комплексних бројева. Велики део тих својстава потиче од ултраметричке неједнакости

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

која важи за све x и y у произвољном пољу p-адичних бројева $\mathbb{Q}_p$. Ипак, њихово приказивање није циљ нашег излагања и њиме се нећемо бавити. За крај овог пододељка приказаћемо само дефиницију p-адичних целих бројева који ће бити од великог значаја касније, при дефинисању Галуаових репрезентација. Више о p-адичним бројевима може се пронаћи у [6].

Дефиниција 2.1.8. *За произвољан прост број $p \in \mathbb{Z}$ дефинишемо прстен p-адичних целих бројева као прстен валуације*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Напомена. *Дефиниција прстена p-адичних целих бројева је само одраз општије конструкције везане за бројевна поља. Нека је K произвољно бројевно поље са неархимедовом валуацијом $|\cdot|$. Дефинишимо*

$$R = \{x \in K \mid |x| \leq 1\}$$

и

$$\mathfrak{p} = \{x \in K \mid |x| < 1\}.$$

*Може се показати да је R локални прстен чији је максимални идеал $\mathfrak{p}$ и поље разломака K. Називамо га **прстеном валуације** бројевног поља K у односу на неархимедову валуацију $|\cdot|$. Дакле, као што и дефиниција 2.1.8 сугерише, $\mathbb{Z}_p$ је прстен валуације поља $\mathbb{Q}_p$. Из кратког приказа опште теорије датог у овој напомени одмах добијамо и једну особину прстена p-адичних целих бројева- $\mathbb{Z}_p$ је локални прстен чији се максимални идеал може изразити као*

$$\mathfrak{p} = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}.$$

2.2 Дирихлеова теорема о инвертибилним елементима

Пре преласка на примену опште теорије приказане у претходном одељку на нама интересантан контекст бројевних поља, прикажимо једну теорему алгебарске теорије бројева, познату као *Дирихлеова теорема о инвертибилним елементима.* Значај наведене теореме се огледа у томе што она пружа увид у структуру групе инвертибилних елемената неког бројевног поља.

Посматрајмо произвољно бројевно поље F, чији је прстен целих $\mathscr{O}_F$. Јасно је да скуп $\mathscr{O}_F^*$ свих инвертибилних елемената прстена $\mathscr{O}_F$ представља једну групу у односу на операцију множења, коју називамо *групом инвертибилних елемената* бројевног поља F. Оно што није очигледно је каква је структура те групе. Посматрајући прстене целих неких једноставних бројевних поља, попут прстена $\mathbb{Z}$ целих бројева или прстена $\mathbb{Z}[i]$ Гаусових целих, могао би се стећи утисак да је група инвертибилних елемената бројевног поља прилично једноставне структуре. Наиме, у првом случају имамо $\mathbb{Z}^* = \{1, -1\}$, а у другом $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$. Ипак, овакви примери не гарантују једноставност групе инвертибилних елемената произвољног бројевног поља. Штавише, испоставља се да би такав закључак донесен на основу наведених примера био погрешан– постоје бројевна поља чије су групе инвертибилних елемената великог ранга. Због тога се поставља питање има ли икакве правилности везане за ранг групе инвертибилних елемената и, у случају позитивног одговора, да ли се та правилност може изразити у терминима који зависе искључиво од одговарајућег бројевног поља. Потребне одговоре пружа наредна класична *Дирихлеова теорема о инвертибилним елементима.*

Теорема 2.2.1 (Дирихлеова теорема о инвертибилним елементима)**.** *Нека је F бројевно поље за кога постоји r различитих утапања у поље реалних бројева $\mathbb{R}$ и s међусобно конјугованих парова утапања у поље комплексних бројева $\mathbb{C}$. Тада је група инвертибилних елемената $\mathscr{O}_F^*$ бројевног поља F изоморфна директном производу коначне цикличне групе и слободне Абелове групе ранга $r + s - 1$.*

Напомена. *Означимо са μ_F групу корена из јединице који се налазе у пољу F. Другим речима,*

$$\mu_F = \{\xi \in F \mid \xi^m = 1, \text{ за неко } m \in \mathbb{N}\}.$$

Може се показати да је торзиони део групе инвертибилних елемената бројевног поља F једнак групи μ_F. Одатле добијамо

$$\mathscr{O}_F^* \cong \mu_F \times \mathbb{Z}^{r+s-1},$$

што је стандардни исказ Дирихлеове теореме о инвертибилним елементима.

Доказ. За доказ теореме и више детаља о реченом у напомени, погледати [5]. □

У наредном примеру, применом Дирихлеове теореме о инвертибилним елементима добијамо једну особину квадратних имагинарних бројевних поља која ће бити од значаја у нашем каснијем излагању.

Пример 2.1. Нека је K произвољно квадратно имагинарно бројевно поље. Тада постоји бесквадратан цео број $D > 0$ такав да је $K = \mathbb{Q}(i\sqrt{D})$. Одатле следи да не постоји ниједно утапање бројевног поља K у поље реалних бројева $\mathbb{R}$. Додатно,

постоје само два, међусобно конјугована утапања поља K у поље комплексних бројева $\mathbb{C}$ која су одређена пресликавањима

$$i\sqrt{D} \to i\sqrt{D} \quad \text{и} \quad i\sqrt{D} \to -i\sqrt{D}.$$

Према томе, на основу Дирихлеове теореме о инвертибилним елементима, закључујемо да је ранг слободног дела групе инвертибилних елемената $\mathscr{O}_K^*$ бројевног поља K једнак $0+1-1=0$. Другим речима, група инвертибилних елемената бројевног поља K састоји се само од торзионог дела, што значи да је та група коначна.
□

2.3 Модул. Група класа зрака у односу модул

Погледајмо сада како се општа теорија дефинисана у одељку 2.1 рефлектује на нама интересантна бројевна поља. Нека је K бројевно поље. Подсетимо се да је прост број $\mathfrak{p}$ у K бесконачан ако садржи архимедову валуацију, па је на основу Теореме 2.1.1 Островског комплетирање $K_\mathfrak{p}$ у односу на такав прост број изоморфно са $\mathbb{R}$ или $\mathbb{C}$. Ова особина даје једноставан начин за поделу бесконачних простих бројева у K на *реалне*, за које је $K_\mathfrak{p} = \mathbb{R}$ и *комплексне*, за које је $K_\mathfrak{p} = \mathbb{C}$. Приметимо још да реалним простим бројевима бројевног поља K одговарају различита утапања поља K у $\mathbb{R}$, док комплексним одговарају два међусобно конјугована утапања поља K у $\mathbb{C}$. Правећи аналогију са основном теоремом аритметике, на бројевном пољу K дефинишемо модул који ће бити кључан објекат приликом дефиниције уопштеног Дирихлеовог карактера и описан је наредном дефиницијом.

Дефиниција 2.3.1. *Модул бројевног поља K је формални производ*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

узет по свим коначним и бесконачним простим бројевима у K, при чему је $n(\mathfrak{p})$ ненегативан цео број и $n(\mathfrak{p}) > 0$ за само коначно много простих бројева $\mathfrak{p}$. Додатно, ако је $\mathfrak{p}$ реалан бесконачан прост број онда је $n(\mathfrak{p}) = 0$ или $n(\mathfrak{p}) = 1$, као и $n(\mathfrak{p}) = 0$ за комплексан бесконачан број $\mathfrak{p}$.

Напомена. *Разлог због кога приликом дефиниције модула не узимамо у обзир комплексне бесконачне просте бројеве лежи умногоме у рамификацији простих бројева. Због тога у вези бољег разумевања ове дефиниције, као и интуиције која се иза ње крије, погледати напомену на крају пододелька 2.5.1.*

Произвољан модул $\mathfrak{m}$ можемо изразити као производ $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, где је

$$\mathfrak{m}_0 = \prod_{\mathfrak{p} \text{ коначан}} \mathfrak{p}^{n(\mathfrak{p})}, \quad \mathfrak{m}_\infty = \prod_{\mathfrak{p} \text{ реалан}} \mathfrak{p}^{n(\mathfrak{p})}.$$

Приметимо да је $\mathfrak{m}_0$ идеал прстена целих $\mathscr{O}_K$, који се често назива коначним делом од $\mathfrak{m}$. Са друге стране, $\mathfrak{m}_\infty$ је производ елемената неког подскупа реалних бесконачних простих бројева у K и назива се често бесконачним делом од $\mathfrak{m}$.

Пример 2.2. Посматрајмо поље рационалних бројева $\mathbb{Q}$. У теореми Островског 2.1.4 видели смо да је произвољна валуација $|\cdot|$ на $\mathbb{Q}$ еквивалентна

- p-адичној валуацији $|\cdot|_p$ за неки прост број p ако је $|\cdot|$ неархимедова.
- валуацији у бесконачности $|\cdot|_\infty$ ако је $|\cdot|$ архимедова.

Због тога, коначне просте бројеве, односно класе еквиваленције неархимедових валуација на $\mathbb{Q}$, можемо идентификацијом $|\cdot|_p \to p$ видети као (уобичајене) рационалне просте бројеве. Такође, у $\mathbb{Q}$ постоји само један бесконачан прост број, пошто је свака архимедова валуација еквивалентна са $|\cdot|_\infty$. Тај прост број ћемо означавати скраћено са ∞. На тај начин добијамо да је произвољан модул $\mathfrak{m}$ поља $\mathbb{Q}$ облика

$$\mathfrak{m} = \prod_{p \text{ прост}} p^{n(p)} \cdot \infty^{\epsilon},$$

где су $n(p)$ ненегативни цели бројеви и $n(p) > 0$ за само коначно много простих бројева p, а $\epsilon \in \{0, 1\}$. Тако, на пример, имамо да је

$$\mathfrak{m} = 2^3 \cdot 17^2 \cdot 19 \cdot \infty$$

модул у $\mathbb{Q}$. За његов коначан и бесконачан део, $\mathfrak{m}_0$ и $\mathfrak{m}_\infty$, важи

$$\mathfrak{m}_0 = 2^3 \cdot 17^2 \cdot 19$$

и

$$\mathfrak{m}_\infty = \infty.$$

□

Релација дељивости између два модула бројевног поља K дефинише се на очекивани начин и описана је наредном дефиницијом.

Дефиниција 2.3.2. *Нека су* $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ *и* $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ *два модула у бројевном пољу* K*. Кажемо да модул* $\mathfrak{m}$ *дели модул* $\mathfrak{n}$ *и пишемо*

$$\mathfrak{m} \mid \mathfrak{n}$$

ако је испуњено

$$m(\mathfrak{p}) \leq n(\mathfrak{p})$$

за све просте бројеве $\mathfrak{p}$ *у* K*.*

Означимо са K^* мултипликативну групу бројевног поља K и са $\mathfrak{m}$ модул у том пољу. Проширујући појам релације конгруенције у односу на идеале прстена целих $\mathscr{O}_K$, дефинисаћемо конгруенцију елемената K^* по у односу на модул $\mathfrak{m}$. Такву конгруенцију ћемо називати мултипликативном. У сам поступак њеног дефинисања ћемо ићи постепено, дефинишући прво конгруенцију у односу на (степен) простих бројева у K.

Нека је $\mathfrak{p}$ реалан прост број у K и нека је $x \to x_\mathfrak{p}$ ознака за утапање $x \in K$ у комплетирање $K_\mathfrak{p} = \mathbb{R}$. За произвољне $a, b \in K^*$ кажемо да су конгруентни у односу на $\mathfrak{p}$ и пишемо

$$a \equiv^* b \pmod{\mathfrak{p}}$$

ако су $a_\mathfrak{p}$ и $b_\mathfrak{p}$ истог знака у $\mathbb{R}$, тј. ако је $\frac{a_\mathfrak{p}}{b_\mathfrak{p}} > 0$.

Нека сада $\mathfrak{p}$ означава коначан прост број. Због његове коначности, простом броју $\mathfrak{p}$ одговара прост идеал у прстену целих $\mathscr{O}_K$, кога ћемо, једноставности ради, такође означавати са $\mathfrak{p}$. Уочимо произвољан $c \in K^*$ и означимо са $\langle c \rangle$ главни идеал разломака у $\mathscr{O}_K$ генерисан са c. Подсетимо се да је $\mathscr{O}_K$ Дедекиндов домен, као прстен целих бројевног поља K. Због тога се идеал разломака $\langle c \rangle$ може на јединствен начин факторисати на производ простих идеала у $\mathscr{O}_K$. Означимо са $v(c)$ степен простог идеала $\mathfrak{p}$ у таквој факторизацији за $\langle c \rangle$. Показује се да је на овај начин, уз обавезно стављање $v(0) = 0$, дефинисана једна валуација на K. Њу називамо *нормализована валуација у* $\mathfrak{p}$ и најчешће је означавамо са $\mathrm{ord}_\mathfrak{p}$.

Користећи појам нормализоване валуације у коначном простом броју $\mathfrak{p}$ дефинишемо конгруенцију у односу на $\mathfrak{p}^n$ за цео број $n > 0$. За произвољне $a, b \in K^*$ кажемо да су конгруентни у односу на $\mathfrak{p}^n$ и пишемо

$$a \equiv^* b \pmod{\mathfrak{p}^n}$$

ако је

$$\mathrm{ord}_\mathfrak{p}\left(\frac{a}{b} - 1\right) \geq n.$$

Имајући у виду његову дефиницију, користећи претходно коначно можемо дефинисати конгруенцију у односу на модул на следећи начин.

Дефиниција 2.3.3. *За произвољне $a, b \in K^*$ кажемо да су конгруентни у односу на модул $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ и пишемо*

$$a \equiv^* b \pmod{\mathfrak{m}}$$

ако важи

$$a \equiv^* b \pmod{\mathfrak{p}^{n(\mathfrak{p})}}$$

за све просте бројеве $\mathfrak{p}$ у K за које је $n(\mathfrak{p}) > 0$.

Из претходне дефиниције лако следи да за произвољне $a, b, a_1, b_1 \in K^*$, ако је

$$a \equiv^* b \pmod{\mathfrak{m}} \text{ и } a_1 \equiv^* b_1 \pmod{\mathfrak{m}}$$

онда важи

$$aa_1 \equiv^* bb_1 \pmod{\mathfrak{m}}.$$

Отуда постаје јасан и раније поменути назив *мултипликативна конгруенција*. Са друге стране, релација конгруенције у односу на модул се не чува сабирањем, као што показује наредни пример.

Пример 2.3. Нека је $\mathfrak{m} = \infty$ модул једнак једином бесконачном простом броју у пољу $\mathbb{Q}$. Тада су по дефиницији $a, b \in \mathbb{Q}^*$ конгруентни у односу на $\mathfrak{m}$ ако и само ако су истог знака. Тако, на пример, важи

$$5 \equiv^* 3 \pmod{\mathfrak{m}}$$

и

$$-4 \equiv^* -11 \pmod{\mathfrak{m}}.$$

Међутим, приметимо да је

$$1 \not\equiv^* -8 \pmod{\mathfrak{m}},$$

што показује да се релација конгруенције у односу на модул у општем случају не чува сабирањем.
□

У вези са произвољним модулом $\mathfrak{m}$ дефинишемо две значајне подгрупе од K^* описане следећом дефиницијом.

Дефиниција 2.3.4. *Нека је $\mathfrak{m}$ модул у бројевном пољу K са коначним делом $\mathfrak{m}_0$ и бесконачним делом $\mathfrak{m}_\infty$. Дефинишемо подгрупе $K_\mathfrak{m}$ и $K_{\mathfrak{m},1}$ мултипликативне групе K^* као*

$$K_\mathfrak{m} = \{a/b \mid a, b \in \mathscr{O}_K \text{ и } a\mathscr{O}_K, b\mathscr{O}_K \text{ узајамно прости са } \mathfrak{m}_0\} \subseteq K^*$$

$$K_{\mathfrak{m},1} = \{\alpha \in K_\mathfrak{m} \mid \alpha \equiv^* 1 \pmod{\mathfrak{m}}\} \subseteq K_\mathfrak{m}$$

Приметимо да $K_\mathfrak{m}$ зависи само од коначних простих бројева који деле $\mathfrak{m}$, а не и њихових експонената. Група $K_{\mathfrak{m},1}$ зависи и од коначних и бесконачних простих бројева који деле $\mathfrak{m}$, као и од експонената коначних простих бројева и називамо је *зрак* по модулу $\mathfrak{m}$.

Означимо са $J^\mathfrak{m}$ подгрупу групе I_K свих ненула идеала разломака прстена целих $\mathscr{O}_K$ бројевног поља K, генерисану свим простим идеалима који не деле коначни део $\mathfrak{m}_0$ модула $\mathfrak{m}$. Она зависи од коначних простих бројева који деле $\mathfrak{m}$, али не и од њихових експонената. Нека је ς пресликавање које елемент $\alpha \in K^*$ слика у главни идеал разломака $\varsigma(\alpha) = \alpha\mathscr{O}_K$. Тада ς слика $K_\mathfrak{m}$ и $K_{\mathfrak{m},1}$ у $J^\mathfrak{m}$.

Дефиниција 2.3.5. *Количничка група*

$$J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$$

назива се ***група класа зрака по модулу*** $\mathfrak{m}$*, а косети од* $\varsigma(K_{\mathfrak{m},1})$ *у тој групи се називају* ***класе зрака*** *по модулу* $\mathfrak{m}$*.*

Пример 2.4. Претпоставимо да је $K = \mathbb{Q}$. Нека је $m \geq 2$ фиксирани цео број и $\mathfrak{m}$ модул у $\mathbb{Q}$ који је једнак главном идеалу $\langle m \rangle$ у $\mathbb{Z} = \mathscr{O}_K$. Одредимо групу класа зрака по модулу $\mathfrak{m}$. Како је $\mathbb{Z}$ главноидеалски, група $J^{\mathfrak{m}}$ је генерисана главним идеалима $\langle a \rangle$, при чему је a произвољан цео број који је узајамно прост са m. Посматрајмо хомоморфизам

$$\Phi : J^{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^*$$

дефинисан са

$$\Phi(\langle a \rangle) = r,$$

где је r остатак броја a при дељењу са m. Пресликавање Φ је очигледно епиморфизам, а његово језгро чине сви идеали $\langle a \rangle$, такви да је $a \equiv 1 \pmod{m}$. Са друге стране, из $\mathfrak{m} = \langle m \rangle$ следи да се мултипликативна конгруенција у односу на модул $\mathfrak{m}$ поклапа са конгруенцијом по модулу m у прстену $\mathbb{Z}$. По дефиницији подгрупе $K_{\mathfrak{m},1}$ и утапања ς онда имамо

$$\varsigma(K_{\mathfrak{m},1}) = \{\langle a \rangle \mid a \equiv 1 \pmod{m}\}.$$

Закључујемо да је језгро хомоморфизма Φ једнако $\varsigma(K_{\mathfrak{m},1})$. Одатле из прве теореме о изоморфизму група следи

$$J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1}) \cong (\mathbb{Z}/m\mathbb{Z})^*.$$

Дакле, добили смо да је група класа зрака по модулу $\langle m \rangle$ у $\mathbb{Q}$ изоморфна групи $(\mathbb{Z}/m\mathbb{Z})^*$. Приметимо да тим изоморфизмом добијамо потпуно увид у структуру групе класа зрака по модулу $\langle m \rangle$: она се састоји од тачно $|(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$ различитих класа по зраку $\langle m \rangle$ и свака од њих је облика $a + m\mathbb{Z}$, где је a узајамно прост са m. □

Група класа зрака по модулу биће централна у даљем разматрању. Прецизније, посматраћемо карактере дефинисане на тој групи. Због тога ће од великог значаја бити следећа фундаментална теорема о коначности групе класа зрака.

Теорема 2.3.1. *Нека је* $\mathfrak{m}$ *произвољан модул бројевног поља* K*. Онда је група класа зрака* $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$ *коначна.*

Доказ. Приказаћемо кратку скицу доказа.

Први корак је да се докаже слабија верзија теореме по којој је група $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ коначна. Та слабија верзија суштински почива на следећем тврђењу:

- Нека су $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_\mathfrak{r}$ узајмно прости модули у паровима и

$$\mathfrak{m} = \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdot \cdots \cdot \mathfrak{m}_r$$

  њихов производ. Тада је

$$\frac{K_\mathfrak{m}}{K_{\mathfrak{m},1}} \cong \frac{K_{\mathfrak{m}_1}}{K_{\mathfrak{m}_1,1}} \times \frac{K_{\mathfrak{m}_2}}{K_{\mathfrak{m}_2,1}} \times \cdots \times \frac{K_{\mathfrak{m}_r}}{K_{\mathfrak{m}_r,1}}.$$

Затим посматрамо произвољан коначан скуп S простих бројева у K. Означимо са I_K групу свих ненула идеала разломака прстена целих $\mathscr{O}_K$ бројевног поља K и са I^S подгрупу те групе генерисану свим простим идеалима прстена $\mathscr{O}_K$ који не припадају скупу S. Показује се да важи

$$I_K/\varsigma(K^*) \cong I^S/I^S \cap \varsigma(K^*).$$

Из дефиниције пресликавања ς добијамо да је

$$I_K/\varsigma(K^*) = \mathrm{Cl}(K),$$

где је $\mathrm{Cl}(K)$ група класа идеала бројевног поља K. Због тога имамо и изоморфизам

$$\mathrm{Cl}(K) \cong I^S/I^S \cap \varsigma(K^*). \tag{2.7}$$

Посматрајмо сада групу класа зрака $J^\mathfrak{m}/\varsigma(K_{\mathfrak{m},1})$. Свакако важи

$$[J^\mathfrak{m} : \varsigma(K_{\mathfrak{m},1})] = [J^\mathfrak{m} : \varsigma(K_\mathfrak{m})][\varsigma(K_\mathfrak{m}) : \varsigma(K_{\mathfrak{m},1})]. \tag{2.8}$$

Из дефиниције групе $J^\mathfrak{m}$ и пресликавања ς следи да је $J^\mathfrak{m} \cap \varsigma(K^*)$ скуп свих главних идеала прстена $\mathscr{O}_K$ који су узајамно прости са коначним делом $\mathfrak{m}_0$ модула $\mathfrak{m}$, па имамо

$$J^\mathfrak{m} \cap \varsigma(K^*) = \varsigma(K_\mathfrak{m}).$$

Због тога, коришћењем изоморфизма утврђеног у (2.7) за $S = \mathfrak{m}$ добијамо да је

$$[J^\mathfrak{m} : \varsigma(K_\mathfrak{m})] = [J^\mathfrak{m} : J^\mathfrak{m} \cap \varsigma(K^*)] = |\mathrm{Cl}(K)|.$$

Како је група класа идеала коначна, број $|\mathrm{Cl}(K)|$, па самим тим и $[J^\mathfrak{m} : \varsigma(K_\mathfrak{m})]$ је коначан.

Са друге стране, $[\varsigma(K_\mathfrak{m}) : \varsigma(K_{\mathfrak{m},1})]$ дели ред $[K_\mathfrak{m} : K_{\mathfrak{m},1}]$ групе $K_\mathfrak{m}/K_{\mathfrak{m},1}$ за коју је у слабијој верзији теореме утврђено да је коначна. Због тога је и $[\varsigma(K_\mathfrak{m}) : \varsigma(K_{\mathfrak{m},1})]$ коначан број.

Дакле, оба броја фактора са десне стране једнакости (2.8) су коначни, па закључујемо да је и $[J^\mathfrak{m} : \varsigma(K_{\mathfrak{m},1})]$ коначан број. Другим речима, закључујемо да је група класа зрака $J^\mathfrak{m}/\varsigma(K_{\mathfrak{m},1})$ коначна. □

Напомена. *Приметимо да је за доказ коначности групе класа зрака у односу на произвољни модул кључна коначност групе класе идеала бројевног поља. Та веза између групе класа зрака и групе класа идеала, установљена скицом доказа Теореме 2.3.1, додатно је објашњена наредним примером.*

Пример 2.5. Подсетимо се да је модул бројевног поља K по дефиницији формални производ

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

узет по свим коначним и бесконачним простим бројевима у K, при чему је $n(\mathfrak{p})$ ненегативан цео број и $n(\mathfrak{p}) > 0$ за само коначно много простих бројева $\mathfrak{p}$. Посматрајмо модул $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ за кога је $n(\mathfrak{p}) = 0$ за сваки прост број $\mathfrak{p}$ у K. Њега називамо *тривијални модул* у K и обележавамо $\mathfrak{m} = 1$. Приметимо да је у овом случају група $J^{\mathfrak{m}}$ једнака целој групи I_K свих ненула идеала разломака у K, због тога што ниједан прост идеал не дели коначни део од $\mathfrak{m}$. Слично, због тривијалности модула $\mathfrak{m}$, свако $\alpha \in K^*$ се налази у $K_{\mathfrak{m},1}$. Како по дефиницији пресликавање ς слика елемент α из K^* у главни идеал разломака $\alpha\mathscr{O}_K$, добијамо да је групу $\varsigma(K_{\mathfrak{m},1})$ чине сви главни идеали разломака у $\mathscr{O}_K$. Према томе, по дефиницији имамо да је група класа зрака

$$J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$$

у односу на тривијални модул $\mathfrak{m} = 1$ ништа друго до група класа идеала бројевног поља K. Према томе, групу класа зрака по неком модулу можемо видети и као уопштење групе класа идеала.
□

2.4 Кондуктори група идеала

У дефиницији 2.3.4 видели смо како се помоћу модула $\mathfrak{m}$ индукују две значајне подгрупе мултипликативне групе K^* бројевног поља K које смо обележили са $K_{\mathfrak{m}}$ и $K_{\mathfrak{m},1}$. Имајући у виду његову дефиницију, лако је наслутити да поред ове везе, модул има тесну везу и са идеалима бројевног поља $\mathscr{O}_K$. Окренимо се раду на, до сада пропуштеном, детаљнијем испитивању те везе.

Као и до сада, за произвољан модул $\mathfrak{m}$ у K са $J^{\mathfrak{m}}$ ћемо означавати подгрупу групе I_K генерисану свим простим идеалима у $\mathscr{O}_K$ који не деле коначни део $\mathfrak{m}_0$ од $\mathfrak{m}$. Следећи сличну идеју као у дефиницији 2.3.4, дефинишемо значајне погрупе те групе на следећи начин.

Дефиниција 2.4.1. *Подгрупа $H^{\mathfrak{m}}$ групе I_K се назива* ***конгруентна подгрупа*** *ако постоји модул $\mathfrak{m}$ у K такав да је*

$$\varsigma(K_{\mathfrak{m},1}) \subseteq H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}} \subseteq I_K.$$

Тада кажемо да је $H^{\mathfrak{m}}$ дефинисана по модулу $\mathfrak{m}$.

У претходној дефиницији смо конгруентну подгрупу дефинисану по модулу $\mathfrak{m}$ означавали са $H^{\mathfrak{m}}$, са циљем да нагласимо модул по коме је та погрупа дефинисана. Међутим, сама дефиниција не гарантује да је модул $\mathfrak{m}$ по коме је дефинисана $H^{\mathfrak{m}}$ јединствен. Такво питање јединствености је веома значајно и управо ћемо се његовим испитивањем бавити у овом одељку.

Нека је $\mathfrak{m}$ модул у K и $H^{\mathfrak{m}}$ одговарајућа конгруентна подгрупа. Уочимо произвољан модул $\mathfrak{n}$ такав да $\mathfrak{n} \mid \mathfrak{m}$. Оно што нас интересује је да нађемо начин да испитамо да ли су конгруентне подгрупе у односу на $\mathfrak{n}$ у вези са конгруентним подгрупом $H^{\mathfrak{m}}$. Пре свега, приметимо да из $\mathfrak{n} \mid \mathfrak{m}$ следи $J^{\mathfrak{m}} \subseteq J^{\mathfrak{n}}$. Због тога, имајући у виду дефиницију 2.4.1, добијамо барем интуитивно схватање да за конгруентне подгрупе у односу на $\mathfrak{n}$ има више „простора". Таквим размишљањем долазимо до питања да ли постоји конгруентна подгрупа $G^{\mathfrak{n}}$ дефинисана по модулу $\mathfrak{n}$ таква да је $H^{\mathfrak{m}} = J^{\mathfrak{m}} \cap G^{\mathfrak{n}}$. У случају позитивног одговора на то питање кажемо да је $H^{\mathfrak{m}}$ *рестрикција* $G^{\mathfrak{n}}$ на $J^{\mathfrak{m}}$. Приметимо да овако дефинисан појам рестрикције конгруентних подгрупа има исти смисао као уобичајени појам рестрикције (пресликавања): $H^{\mathfrak{m}}$ можемо видети као „прилагођавање" конгруентне подгрупе $G^{\mathfrak{n}}$ модулу $\mathfrak{m}$.

Нарочито значајан случај када две различите конгруентне подгупе имају исту рестрикцију описан је наредном дефиницијом.

Дефиниција 2.4.2. *За две конгруентне подгрупе $H_1^{\mathfrak{m}_1} \subseteq J^{\mathfrak{m}_1}$ и $H_2^{\mathfrak{m}_2} \subseteq J^{\mathfrak{m}_2}$ дефинисане редом у односу на модуле $\mathfrak{m}_1$ и $\mathfrak{m}_2$ кажемо да имају* ***заједничку рестрикцију*** *и пишемо $H_1^{\mathfrak{m}_1} \sim H_2^{\mathfrak{m}_2}$ ако постоји модул $\mathfrak{m}$ у K такав да важи*

$$H_1^{\mathfrak{m}_1} \cap J^{\mathfrak{m}} = H_2^{\mathfrak{m}_2} \cap J^{\mathfrak{m}}. \tag{2.9}$$

Наредно тврђење показује да је релација заједничке рестрикције описана претходном дефиницијом коректно дефинисана.

Тврђење 2.4.1. *Нека су $\mathfrak{m}$ и $\mathfrak{n}$ модули такви да $\mathfrak{n} \mid \mathfrak{m}$. Претпоставимо да постоје конгруентне подгрупе $H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$ и $G^{\mathfrak{n}} \subseteq J^{\mathfrak{n}}$ дефинисане по одговарајућим модулима такве да је $H^{\mathfrak{m}}$ рестрикција $G^{\mathfrak{n}}$ на $J^{\mathfrak{m}}$, односно такве да је $H^{\mathfrak{m}} = J^{\mathfrak{m}} \cap G^{\mathfrak{n}}$. Тада важи*

1. $J^{\mathfrak{m}}/H^{\mathfrak{m}} \cong J^{\mathfrak{n}}/G^{\mathfrak{n}}$
2. $G^{\mathfrak{n}} = H^{\mathfrak{m}}\varsigma(K_{\mathfrak{n},1})$.

Доказ. Погледати [8]. □

Приметимо да ако (2.9) важи за модул $\mathfrak{m}$, та релација онда важи и за сваки модул $\mathfrak{m}'$ кога $\mathfrak{m}$ дели, јер је тада $J^{\mathfrak{m}'} \subseteq J^{\mathfrak{m}}$. Имајући ту особину у виду, веома лако се показује наредно тврђење.

Тврђење 2.4.2. *Релација $\sim$ је релација еквиваленције на скупу свих конгруентних подгрупа од I_K.*

Релација $\sim$ има и нешто суптилнију особину, која ће се значајно одразити на њене класе еквиваленције и дата је следећим тврђењем.

Тврђење 2.4.3. *Нека су $H_1^{\mathfrak{m}_1} \subseteq J^{\mathfrak{m}_1}$ и $H_2^{\mathfrak{m}_2} \subseteq J^{\mathfrak{m}_2}$ две конгруентне подгрупе које су дефинисане редом по модулу $\mathfrak{m}_1$, односно $\mathfrak{m}_2$ и имају заједничку рестрикцију $H_3^{\mathfrak{m}_3} = H_i^{\mathfrak{m}_i} \cap J^{\mathfrak{m}_3}$, $i = 1, 2$ дефинисану по модулу $\mathfrak{m}_3$. Означимо са $\mathfrak{m}$ највећи заједнички делилац за $\mathfrak{m}_1$ и $\mathfrak{m}_2$. Тада постоји конгруентна подгрупа $H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$ дефинисана по модулу $\mathfrak{m}$ таква да је $H^{\mathfrak{m}} \cap J^{\mathfrak{m}_i} = H_i$, $i = 1, 2$.*

Доказ. Погледати [8]. □

Класа еквиваленције релације $\sim$ се назива *група идеала*. Уочимо групу идеала, односно једну класу еквиваленције $\mathbb{H}$ релације $\sim$ и произвољан модул $\mathfrak{m}$. Ако постоји конгруентна подгрупа дефинисана по модулу $\mathfrak{m}$ која припада класи $\mathbb{H}$, она је јединствена и означаваћемо је са $\mathbb{H}^{\mathfrak{m}}$. Дакле, $\mathbb{H}^{\mathfrak{m}}$ није ништа друго до јединствени представник класе еквиваленције $\mathbb{H}$ који је дефинисан по модулу $\mathfrak{m}$ (под условом да такав представник постоји).

Претпоставимо да су $\mathfrak{m}$ и $\mathfrak{n}$ два модула такви да постоје одговарајуће конгруентне подгрупе $\mathbb{H}^{\mathfrak{m}}$ и $\mathbb{H}^{\mathfrak{n}}$ у групи идеала $\mathbb{H}$. Означимо са $\mathfrak{m}'$ највећи заједнички делилац за $\mathfrak{m}$ и $\mathfrak{n}$. Из Тврђења 2.4.3 онда следи да у групи идеала $\mathbb{H}$ постоји јединствена конгруентна подгрупа $\mathbb{H}^{\mathfrak{m}'}$ које је дефинисана у односу на $\mathfrak{m}'$. Одатле закључујемо да за групу идеала $\mathbb{H}$ постоји јединствени модул $\mathfrak{f}$ за кога је испуњено

- Постоји јединствена конгруентна подгрупа $\mathbb{H}^{\mathfrak{f}} \subseteq J^{\mathfrak{f}}$ која је дефинисана у односу на $\mathfrak{f}$ и припада групи идеала односно класи еквиваленције $\mathbb{H}$ релације $\sim$.
- Ако за произвољни модул $\mathfrak{m}$ постоји конгруентна подгрупа $\mathbb{H}^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}$ дефинисана у односу на $\mathfrak{m}$ која припада $\mathbb{H}$, онда $\mathfrak{f} \mid \mathfrak{m}$.

(Јасно је да се $\mathfrak{f}$ може изразити као највећи заједнички делилац свих модула $\mathfrak{m}$ за које $\mathbb{H}$ садржи конгруентну подгрупу $\mathbb{H}^{\mathfrak{m}}$ дефинисану у односу на $\mathfrak{m}$). Модул $\mathfrak{f}$ се назива **кондуктор** за $\mathbb{H}$.

2.5 Прости бројеви и Галуаова раширења бројевних поља

До сада је целокупно разматрање било у оквиру једног фиксираног бројевног поља, односно коначног раширења поља $\mathbb{Q}$. Међутим, различите потребе рада често намећу потребу за изласком из таквог (релативно скромног) оквира и богаћењем видика у смеру Галуаових раширења бројевних поља[1]. Управо то је тема којој је посвећен наставак нашег излагања. Укратко говорећи, идеја је да погледамо како се до сада

[1]једно сведочанство ове тврдње биће приказано у Глави 3. За потребе доказа фундаменталне Теореме 3.1.1 мораћемо да пређемо из контекста посматрања само једног бројевног поља на контекст разматрања Галуаових раширења бројевних поља

дефинисани појмови рефлектују на Галуаова раширења бројевних поља, откривајући тако неке фундаменталне конструкције алгебарске теорије бројева, попут *Артиновог пресликавања*. Означимо стандардно као и до сада са K произвољно бројевно поље, док ће L представљати стандрардну ознаку за његово Галуаово раширење. Од интереса ће нам бити *Абелова раширења*, односно она раширења за које је Галуаова група $G = G(L/K)$ комутативна. Нагласимо да ће нека тврђења и дефиниције које будемо формулисали важити и у случају неабелових раширења, па чак и за раширења која нису Галуаова. Разлог у ограничавању на Абелова раширења лежи у томе што су она довољна за формулисање Артиновог пресликавања, а рад са њима је доста лакши од рада са произвољним Галуаовим раширењима.

Приметимо да су ресурси за наш подухват којима за сада располажемо прилично скромни: једино што можемо поуздано сматрати познатим од раширења L/K је одговарајућа Галуаова група G. Са друге стране, уочимо колико је појам простог броја у бројевном пољу био централан у досадашњој причи– прости бројеви генеришу модуле у односу на које смо дефинисали све најважније појмове попут уопштеног Дирихлеовог карактера или групе идеала. Наравно, као бројевна поља, K и L имају одговарајуће просте бројеве[2]. Због тога се довођење у везу простих бројева у K и L природно истиче као значајан задатак. На трагу његовог решавања ће се наставити наше излагање.

2.5.1 Рамификација простих бројева

Нека је $\mathfrak{p}$ произвољан прост број у K. Ако је $\mathfrak{p}$ коначан, онда га можемо видети као идеал прстена целих $\mathscr{O}_K$ бројевног поља K. Користећи ово запажање, задатак кога смо се прихватили можемо преформулисати у задатак довођења у везу идеала прстена целих $\mathscr{O}_K$ и $\mathscr{O}_L$ бројевних поља K и L. Овакво разматрање је згодно, јер преформулисани задатак решава добро позната теорија рамификације идеала у расхирењима прстена целих. Из њене целокупности ћемо истаћи само једну значајну последицу по којој за сваки сваки идеал $\mathfrak{p}$ прстена $\mathscr{O}_K$ постоји коначно много простих идеала $\mathfrak{P}_i$ који сви леже изнад $\mathfrak{p}$ и за које важи

$$\mathfrak{p}\mathscr{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}, \tag{2.10}$$

где су $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ одговарајући индекси рамификације, за $1 \leq i \leq r$. Додатно, пошто је раширење L/K које посматрамо Галуаово, важи да су сви индекси рамификације $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ једнаки. Другим речима, важи

$$\mathfrak{p}\mathscr{O}_L = (\mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_r)^e,$$

где је e индекс рамикације сваког од идеала $\mathfrak{P}_i$ изнад идеала $\mathfrak{p}$. Још једном користећи идентификацију коначних простих бројева у бројевном пољу са идеалима његовог прстена целих, претходно тврђење записујемо у облику следеће теореме.

[2]подсећања ради, под простим бројем у бројевном пољу подразумевамо класу еквиваленције валуација дефинисаних на том пољу

Теорема 2.5.1. *Нека је* $\mathfrak{p}$ *коначан прост број у бројевном пољу* K *и* L/K *комутативно Галуаово раширење. Тада постоји коначно много коначних простих бројева* $\mathfrak{P}_i$ *у* L *за које важи*

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_r)^e,$$

где је e *одговарајући индекс рамификације (потекао од идентификације* $\mathfrak{p}$ *са идеалом прстена целих* $\mathscr{O}_K$ *и идентификације* $\mathfrak{P}_i$ *са идеалом прстена целих* $\mathscr{O}_L$ *, за* $1 \leq i \leq r$*). За просте бројеве* $\mathfrak{P}_i$ *кажемо да су раширења простог броја* $\mathfrak{p}$*.*

Преостало је још да се позабавимо бесконачним простим бројевима. Размотримо прво случај када је $\mathfrak{p}$ комплексан прост број у K. Нека је $\tau : K \to \mathbb{C}$ утапање поља K у $\mathbb{C}$ такво да је валуација $x \to |\tau(x)|$ у $\mathfrak{p}$. Поље $\mathbb{C}$ је алгебарски затворено, па користећи теорију Галуа можемо закључити да постоји тачно $r = [L : K]$ различитих утапања $\tau_i : L \to \mathbb{C}$ таквих да је $\tau_i(x) = \tau(x)$ за све $x \in K$. Из чињенице да имају исту рестрикцију на K, два различита пресликавања τ_i и τ_j не могу бити међусобно конјугована, одакле закључујемо да су $\tau_1, \tau_2 \dots \tau_r$ представници r различитих простих бројева $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r$ у L. По узору на Теорему 2.5.1 писаћемо

$$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_r$$

да нагласимо да су прости бројеви $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r$ у L раширења простог броја $\mathfrak{p}$ у K. Такође, формално дефинишемо да су индекси рамификације $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ сви једнаки 1. Зато важи и да се комплексан прост број $\mathfrak{p}$ не рамификује у L.

Коначно, претпоставимо да је $\mathfrak{p}$ реалан прост број у K и означимо са τ њему одговарајуће утапање поља K у $\mathbb{R}$. Посматрајмо τ као пресликавање поља K у $\mathbb{C}$ да на основу Галуаове теорије донесемо закључак да постоји $r = [L : K]$ проширивања тог пресликавања на домен L. Нека од тих пресликавања могу имати слику садржану у $\mathbb{R}$, па ћемо их зато обележити са

$$\tau_1, \dots, \tau_a, \tau_{a+1}, \dots, \tau_{a+b}, \bar{\tau}_{a+1}, \dots, \bar{\tau}_{a+b},$$

при чему је $\tau_i(L) \subset \mathbb{R}$ за $1 \leq i \leq a$, а преосталих b парова $\tau_{a+j}, \bar{\tau}_{a+j}, 1 \leq j \leq b$ представљају међусобно конјугована утапања L у $\mathbb{C}$ (уз овакву нотацију је, наравно, $a + 2b = r$). Тада сваком од $\tau_i, 1 \leq i \leq a$ одговара различит реалан прост број $\mathfrak{P}_i$ у L, док сваком од b парова $\tau_{a+j}, \bar{\tau}_{a+j}, 1 \leq j \leq b$ одговара различит комплексан прост број $\mathfrak{P}_{a+j}$ у L. Прости бројеви $\tau_i, 1 \leq i \leq a + b$ у пољу L представљају раширење реалног простог броја $\mathfrak{p}$ у пољу K. Формално дефинишући њихове индексе рамификације са

$$e(\mathfrak{P}_i \mid \mathfrak{p}) = \begin{cases} 1, & \text{ако је } \mathfrak{P}_i \text{ реалан} \\ 2, & \text{ако је } \mathfrak{P}_i \text{ комплексан} \end{cases}$$

по узору на Теорему 2.5.1 то можемо записати и као

$$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_a\mathfrak{P}_{a+1}^2\mathfrak{P}_{a+2}^2 \dots \mathfrak{P}_{a+b}^2.$$

Напомена. *Појам рамификације простих бројева се значајно осликава на дефиницију модула и саму интуицију која се иза ње крије. Приметимо да смо у овом пододељку установили да се комплексни прости бројеви никада не могу рамификовати (у проширењу L/K). Са друге стране, идеја за дефинисањем појма модула је историјски потекла од потребе да се дефинише објекат који „мери рамификацију". Због тога се у дефиницији модула занемарују сви бесконачни комплексни бројеви– они никада „не доприносе рамификацији".*

2.5.2 Група декомпозиције

Сада почињемо обимније експлоатисање чињенице да је раширење L/K Галуаово. Прво што ћемо урадити је проналажење веза између претходно показане рамификације простих бројева и подгрупа одговарајуће Галуаове групе $G = G(L/K)$. Нека је $\mathfrak{p}$ прост број у K и нека су $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r$ прости бројеви у L који га проширују. Дефинишимо дејство произвољног аутоморфизма $\sigma \in G$ на прост број $\mathfrak{P}_i$, које означавамо са $\sigma(\mathfrak{P}_i)$ на следећи начин:

- У случају да је $\mathfrak{p}$ коначан прост број, $\mathfrak{P}_i$ можемо идентификовати са идеалом прстена целих $\mathscr{O}_L$, па је $\sigma(\mathfrak{P}_i)$ идеал добијен дејством σ на сваки елемент од $\mathfrak{P}_i$.

- Бесконачном простом броју $\mathfrak{P}_i$ у L одговара утапање τ_i поља L у $\mathbb{R}$ или $\mathbb{C}$, па $\sigma(\mathfrak{P}_i)$ представља прост број у L коме одговара утапање $\tau_i\sigma^{-1}$.

Приметимо да је претходно дефинисано дејство *транзитивно*. У односу на њега природно се индукује значајна подгрупа групе G, описана наредном дефиницијом.

Дефиниција 2.5.1. *Нека је $\mathfrak{p}$ прост број у K и $\mathfrak{P}$ прост број у L који га проширује. Група*

$$G(\mathfrak{P}) = \{\sigma \in G(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \subseteq G(L/K)$$

се назива ***групом декомпозиције*** *за $\mathfrak{P}$.*

Приметимо да смо претходном дефиницијом убацили већ приличан број различитих концепата и конструкција у интеракцију. Међутим, од посматрања такве интеракције нема никакве користи ако она нема смисла, односно ако не успева да очува природне односе и хармонију између објеката на које делује. Зато поред изградње нових објеката треба видети и оправдање за њихову егзистеницију. Наредна теорема даје оправдање за наставак излагања у правцу којим смо се до сада кретали, илуструјући савршену хармонију између групе декомпозиције и комплетирања поља у одговарајућим простим бројевима.

Теорема 2.5.2. *Нека је $\mathfrak{p}$ прост број у бројевном пољу K и $\mathfrak{P}$ његово проширење у пољу L које је Галуаово над K. Означимо са $G(\mathfrak{P})$ групу декомпозиције за $\mathfrak{P}$. Тада је*

комплетирање $L_{\mathfrak{P}}$ поља L у $\mathfrak{P}$ Галуаово раширење над комплетирањем $K_{\mathfrak{p}}$ поља K у $\mathfrak{p}$ са Галуаовом групом $G(\mathfrak{P})$,

$$G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \cong G(\mathfrak{P}).$$

Доказ. Приказаћемо веома кратку скицу која илуструје главну идеју доказа ове теореме.
Означимо са $\mathfrak{P}_i, 1 \leq i \leq r$ сва раширења простог броја $\mathfrak{p}$ у бројевно поље L. Први део доказа теореме је општије природе, и састоји се у показивању да важи изоморфизам поља

$$K_{\mathfrak{p}} \otimes_K L \cong L_{\mathfrak{P}_1} \oplus \cdots \oplus L_{\mathfrak{P}_r}. \tag{2.11}$$

Дејство Галуаове групе $G = G(L/K)$, идентификовано као дејство $1 \otimes G$, тада пермутује суманде на десној страни релације (2.11) и на сваком од тих сумандa индукује аутоморфизме. Од интереса је испитати дејство сваке од група инерције $G(\mathfrak{P}_i) \subseteq G$. Лако се види да дејство групе $G(\mathfrak{P}_i)$ фиксира цело поље $L_{\mathfrak{P}_i}$ (посматрано као скуп, не тачку по тачку), па треба испитати оставља ли $G(\mathfrak{P}_i)$ фиксним још неки скуп поред $L_{\mathfrak{P}_i}$. Сврха таквог испитивања је у показивању да је $G(\mathfrak{P}_i)$ Галуаова група за $L_{\mathfrak{P}_i}$ над $K_{\mathfrak{p}}$. Последња чињеница, уз установљени изоморфизам (2.11) онда лако завршава доказ.

□

2.5.3 Група инерције

Претпоставимо сада да је $\mathfrak{p}$ коначан прост број у K. Означимо са $\mathscr{O}$ прстен валуације који одговара $\mathfrak{p}$, идентификујмо $\mathfrak{p}$ као максимални идеал прстена $\mathscr{O}$ и означимо са $\overline{\mathscr{O}}$ интегрално затворење од $\mathscr{O}$ у L. Нека је $\mathfrak{P}$ прост идеал прстена $\overline{\mathscr{O}}$ који садржи $\mathfrak{p}$. Како за произвољно $\sigma \in G(\mathfrak{P})$ важи $\sigma(\mathfrak{P}) = \mathfrak{P}$, једнакошћу

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}, \quad x \in \overline{\mathscr{O}}$$

је дефинисан аутоморфизам $\bar{\sigma}$ количника $\mathscr{O}_{\mathfrak{P}} = \overline{\mathscr{O}}/\mathfrak{P}$. Ако означимо $\mathscr{O}_{\mathfrak{p}} = \mathscr{O}/\mathfrak{p}$, онда је $\bar{\sigma}$ елемент Галуаове групе $\mathscr{O}_{\mathfrak{P}}$ над $\mathscr{O}_{\mathfrak{p}}$. Према томе, придруживање

$$G(\mathfrak{P}) \to G(\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}}), \quad \sigma \to \bar{\sigma}$$

је хомоморфизам из групе $G(\mathfrak{P})$ у Галуаову групу $G(\mathscr{O}_{\mathfrak{P}}/\mathscr{O}_{\mathfrak{p}})$. Његово језгро представља значајну подгрупу групе $G(\mathfrak{P})$ (па самим тим и Галуаове групе $G(L/K)$) која се назива **група инерције** за $\mathfrak{P}$ и обележава са $I(\mathfrak{P})$. Та група је уско везана са индексом рамификације $e(\mathfrak{P} \mid \mathfrak{p})$, што приказује следећа тврђење.

Тврђење 2.5.1. *Нека је $\mathfrak{p}$ прост идеал у $\mathscr{O}$ и $\mathfrak{P}$ прост идеал у $\overline{\mathscr{O}}$ изнад $\mathfrak{p}$. Тада важи:*

1. *Придруживање $\sigma \to \bar{\sigma}$ је сурјективно.*

2. Ред групе инерције $I(\mathfrak{P})$ једнак је индексу рамификације $e(\mathfrak{P} \mid \mathfrak{p})$.

Доказ. Погледати [8]. □

Тврђењем 2.5.1 установљено је да је хомоморфизам $\sigma \to \bar{\sigma}$ сурјективан. Одатле, на основу прве теореме о изоморфизму група и дефиниције групе инерције добијамо

$$G(\mathfrak{P})/I(\mathfrak{P}) \cong G\left(\frac{\mathscr{O}_{\mathfrak{P}}}{\mathscr{O}_{\mathfrak{p}}}\right). \tag{2.12}$$

Изоморфизам установљен релацијом (2.12) представљаће једно од полазишта приликом дефинисања Артинових L-функција, којим ћемо се, како је већ напоменуто, бавити мало касније.

2.6 Фробенијусов аутоморфизам и Артиново пресликавање

2.6.1 Фробенијусов аутоморфизам

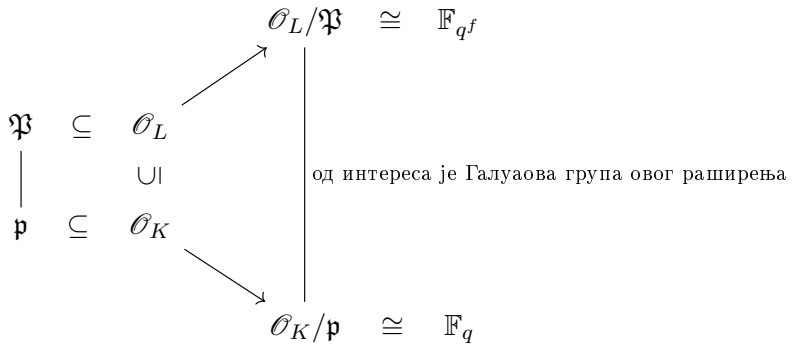
Нека је $\mathfrak{p}$ коначан прост број у K, чији је прстен целих $\mathscr{O}_K$ и L/K Галуаово раширење бројевних поља. Посматрајмо раширење $\mathfrak{P}$ простог броја $\mathfrak{p}$ у поље L. Ако означимо $q = \mathfrak{N}(\mathfrak{p})$, имамо да је

$$\mathscr{O}_K/\mathfrak{p} \cong \mathbb{F}_q$$

и

$$\mathscr{O}_L/\mathfrak{P} \cong \mathbb{F}_{q^f},$$

за неки природан број f.
Ситуацију коју разматрамо осликава наредни дијаграм.



За свако $\sigma \in G(\mathfrak{P})$ важи $\sigma(\mathfrak{P}) = \mathfrak{P}$, па је на потпуно исти начин као у пододељку 2.5.3, формулом

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}, \;\; x \in \mathscr{O}_L$$

дефинисан један аутоморфизам $\bar{\sigma}$ количника $\mathscr{O}_L/\mathfrak{P}$. Додатно, $\bar{\sigma}$ можемо видети и као елемент Галуаове групе $G\left(\frac{\mathscr{O}_L/\mathfrak{P}}{\mathscr{O}_K/\mathfrak{p}}\right)$.

Одатле закључујемо да је група $G\left(\frac{\mathscr{O}_L/\mathfrak{P}}{\mathscr{O}_K/\mathfrak{p}}\right)$ циклична и генерисана

$$y \to y^q, \;\; y \in \mathscr{O}_L/\mathfrak{P},$$

па постоји јединствени косет $\sigma I(\mathfrak{P}) \subset G(\mathfrak{P})$ чији сви елементи испуњавају

$$\sigma(x) \equiv x^q \mod \mathfrak{P}, \;\; x \in \mathscr{O}_L. \tag{2.13}$$

Сваки елемент τ тог косета назива се **Фробенијусовим аутоморфизмом** придруженом $\mathfrak{P}$ и означава се са

$$\tau = \left(\frac{L/K}{\mathfrak{P}}\right)$$

да би се нагласила његова зависност од простог броја $\mathfrak{P}$ и раширења L/K. Ако се $\mathfrak{p}$ не рамификује у L, према Теореми 2.5.1 је $|I(\mathfrak{P})| = e(\mathfrak{P} \mid \mathfrak{p}) = 1$, што значи да је косет $\sigma I(\mathfrak{P})$ једночлан. Одатле добијамо да за проширење нерамификованог идеала $\mathfrak{p}$ у L постоји јединствени њему придружени Фробенијусов аутоморфизам.

Тврђење које следи показује независност Фробенијусовог аутоморфизма од дејства Галуаове групе $G(L/K)$ и омогућава да додатно изоштримо овај појам.

Тврђење 2.6.1. *Нека је $\tau \in G(L/K)$, $\mathfrak{p}$ прост број у K који се не рамификује у L и $\mathfrak{P}$ неко његово проширење у L. Претпоставимо да је група $G(L/K)$ Абелова. Тада је $G(\tau(\mathfrak{P})) = G(\mathfrak{P})$ и*

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Доказ. Сваки елемент прстена целих $\mathscr{O}_L$ се може записати као $\tau^{-1}(x)$ за неко $x \in \mathscr{O}_L$. Из једнакости (2.13) имамо

$$\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}(x) \equiv \tau^{-1}(x)^q \mod \mathfrak{P}.$$

Применом τ добијамо

$$\tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}(x) \equiv x^q \mod \tau(\mathfrak{P}), \tag{2.14}$$

одакле из чињенице да је Галуаова група $G(L/K)$ Абелова следи

$$\left(\frac{L/K}{\mathfrak{P}}\right)(x) \equiv x^q \mod \tau(\mathfrak{P}).$$

Из последње релације по дефиницији Фробенијусовог аутоморфизма одмах следи тражено тврђење. □

Напомена. *За неабелова раширења важи*

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1},$$

као и

$$G(\tau(\mathfrak{P})) = \tau G(\mathfrak{P})\tau^{-1}$$

што следи директно из (2.14). Такође, поред установљеног односа група декомпозиције за $\tau(\mathfrak{P})$ *и* $\mathfrak{P}$*, и за њихове групе инерције важи да су* τ*-конјуговане,*

$$I(\tau(\mathfrak{P})) = \tau I(\mathfrak{P})\tau^{-1}.$$

Доказ тог тврђења је у великој мери попут овде приказаног доказа Тврђења 2.6.1, следећи дефиницију групе инерције.

Тврђење 2.6.1 показује да за нерамификовани прост број $\mathfrak{p}$ у K, одговарајући Фробенијусов аутоморфизам је исти за сваки $\mathfrak{P}$ који проширује $\mathfrak{p}$ у L. У складу са том чињеницом уводимо ознаку

$$(L/K, \mathfrak{p}) = \left(\frac{L/K}{\mathfrak{P}}\right) \in G(\mathfrak{P})$$

за било који прост број $\mathfrak{P}$ који проширује $\mathfrak{p}$ у поље L. Поред наведене ознаке, користићемо и још краћу ознаку $\mathrm{Fr}_{\mathfrak{p}}$ уместо $(L/K, \mathfrak{p})$, када је јасно о којим се бројевним пољима L и K ради. За $(L/K, \mathfrak{p})$ кажемо да је Фробенијусов аутоморфизам који одговара $\mathfrak{p}$. На тај начин добијамо везу између простих идеала у K који се не рамификују у L и елемената комутативне Галуаове групе $G(L/K)$.

2.6.2 Артиново пресликавање

Претходно установљену везу између простих идеала у K који су нерамификовани у L и елемената комутативне Галуаове групе $G(L/K)$ проширујемо и на идеале који нису прости на следећи начин. Означимо са S *коначан* скуп простих идеала у K, при чему захтевамо да тај скуп садржи све оне просте идеале који се рамификују у L и посматрајмо подгрупу J^S групе I_K генерисану свим ненула простим идеалима који су *изван* скупа S. Сваки елемент групе J^S је облика

$$\mathfrak{A} = \prod_{\substack{\mathfrak{p} \text{ прост} \\ \mathfrak{p} \notin S}} \mathfrak{p}^{a(\mathfrak{p})}, \tag{2.15}$$

при чему су $a(\mathfrak{p})$ цели бројеви којих је само коначно много различито од нула. Ова карактеризација произвољног елемента групе J^S нам омогућава да на њој дефинишемо пресликавање

$$\varphi_{L/K} : J^S \to G(L/K)$$

релацијом

$$\varphi_{L/K}(\mathfrak{A}) = \prod_{\substack{\mathfrak{p} \text{ прост} \\ \mathfrak{p} \nmid S}} (L/K, \mathfrak{p})^{a(\mathfrak{p})},$$

где су $a(\mathfrak{p})$ цели бројеви одређени репрезентацијом (2.15) елемента $\mathfrak{A}$. Из већ наглашене чињенице да је само коначно много бројева $a(\mathfrak{p})$ различито од нуле, као и због комутативности групе $G(L/K)$ следи да је пресликавање $\varphi_{L/K}$ коректно дефинисано. Оно представља изузетно значајан објекат алгебарске теорије бројева и назива се **Артиново пресликавање**.

Може се показати да је Артиново пресликавање сурјективно. О томе ће бити речи касније. Тренутно нам је од интереса да кажемо нешто више о његовом језгру, односно да га доведемо у везу са зраком по неком модулу. Нека је $\mathfrak{m}$ произвољан модул у бројевном пољу K. Артиново пресликавање је дефинисано на $J^{\mathfrak{m}}$ под условом да је $\mathfrak{m}$ дељив сваким коначним простим бројем у K који се рамификује у L. Тада има смисла разматрати у каквом је односу његово језгро са подгрупама групе $J^{\mathfrak{m}}$. Случај који се може догодити и од нарочитог је значаја истакнут је наредном дефиницијом.

Дефиниција 2.6.1. *За тројку $(L, K, \mathfrak{m})$ важи* ***закон реципроцитета*** *ако је L комутативно Галуаово раширење поља K и $\mathfrak{m}$ је модул у K за кога је испуњено $\varsigma(K_{\mathfrak{m},1}) \subseteq \ker \varphi_{L/K}$.*

Напомена. *За више о разлозима зашто се закон установљен претходном дефиницијом назива законом реципроцитета, погледати напомену после Теореме 2.6.1.*

Комбиновање закона реципроцитета са појмовима групе идеала и њеног кодуктора доводе до занимљивог резултата који представља још једну значајну карактеристику Абеловог раширења L/K. Наиме, претпоставимо да је поље L Галуаово над K, при чему је одговарајућа Галуаова група комутативна и нека је $\mathfrak{m}$ модул у K такав да важи закон реципроцитета за $(L, K, \mathfrak{m})$. Тада је језгро Артиновог пресликавања $\varphi_{L/K}$ дефинисаног на $J^{\mathfrak{m}}$ конгруентна подгрупа коју ћемо означавати са $H^{\mathfrak{m}}(L/K)$. Ако је $\mathfrak{m}'$ други модул у K такав да важи закон реципроцитета за $(L, K, \mathfrak{m}')$ онда је

$$\ker(\varphi_{L/K}|J^{\mathfrak{m}}) \cap J^{\mathfrak{m}\mathfrak{m}'} = \ker(\varphi_{L/K}|J^{\mathfrak{m}\mathfrak{m}'}) = \ker(\varphi_{L/K}|J^{\mathfrak{m}'}) \cap J^{\mathfrak{m}\mathfrak{m}'},$$

одакле следи да $H^{\mathfrak{m}}(L/K)$ и $H^{\mathfrak{m}'}(L/K)$ имају заједничку рестикцију на $J^{\mathfrak{m}\mathfrak{m}'}$. Закључујемо да све конгруентне подгрупе $H^{\mathfrak{m}}(L/K)$ такве да закон реципроцитета важи за $(L, K, \mathfrak{m})$ леже у једној групи идеала коју означавамо са $H(L/K)$. Због њеног изузетног значаја истакнимо је и формално следећом дефиницијом.

Дефиниција 2.6.2. *Нека је L Абелово раширење поља бројевног поља K. Група идеала $H(L/K)$ чији су елементи све конгруентне подгрупе $H^{\mathfrak{m}}(L/K) = \ker(\varphi_{L/K}|J^{\mathfrak{m}})$, при чему је $\mathfrak{m}$ модул у K такав да важи закон реципроцитета за $(L, K, \mathfrak{m})$, се назива* ***група класа*** *раширења L/K. Поље L се назива* ***пољем класа*** *групе $H(L/K)$, док се њен кондуктор означава са $f(L/K)$ и назива* ***кондуктором*** *раширења L/K.*

Претходна дефиниција представља почетак теорије поља класа, која је централна у алгебарској теорији бројева. Међутим, пратећи начин нашег досадашњег излагања, није у потпуности јасно да је та теорија коректно заснована. Наиме, можемо приметити да у дефиницији поља класа кључну улогу игра претпоставка важења закона реципроцитета за тројку $(L, K, \mathfrak{m})$. Проблем настаје у томе што до сада нисмо дали никакве услове када тај закон важи. Зато не можемо у потпуности искључити случај да за раширење L/K не постоји нетривијални модул $\mathfrak{m}$ такав да закон реципроцитета важи за $(L, K, \mathfrak{m})$. Такође, чак и у случају да постоје такви нетривијални модули, њихова евентуална малобројност би произвела сиромашност теорије поља класа. Наведене проблеме решава *Артинова теорема о реципроцитету*, коју многи (с правом) сматрају основном теоремом теорије поља класа. Грубо говорећи, она показује да за $(L, K, \mathfrak{m})$ важи закон реципроцитета уколико су експоненти простих бројева који деле модул $\mathfrak{m}$ у K довољно велики. Њен формалан исказ нам овде није од значаја и нећемо га наводити, већ ћемо дати формулацију једне њене директне последице која ће нам бити од значаја касније.

Теорема 2.6.1. *Означимо са* $\mathfrak{f}$ *кондуктор раширења* L/K *и са* $H^{\mathfrak{f}}$ *његову групу класа. Тада је* $J^{\mathfrak{f}}/H^{\mathfrak{f}} \cong G(L/K)$ *и изоморфизам се остварује пресликавањем*

$$\mathfrak{p} \to \left(\frac{L/K}{\mathfrak{p}}\right).$$

Наредно тврђење је помало техничке природе, али је карактеризација коју даје веома згодна, нарочито у конјукцији са Тврђењем 2.5.1.

Тврђење 2.6.2. *Нека је* L/K *Абелово раширење и* $\mathfrak{f}$ *његов кондуктор. Тада је за прост број* $\mathfrak{p}$ *у* K *испуњено*

$$\mathfrak{p} \text{ } \textit{се рамификује у } L \textit{ ако и само ако } \mathfrak{p} | \mathfrak{f}.$$

Доказ. Видети [14]. □

Завршимо ово поглавље једном историјском дигресијом са циљем да додатно објаснимо закон реципроцитета, као и улогу коју је он имао у развоју теорије поља класа.

Дигресија (Кратка историја закона реципроцитета)**.**
У овој дигресији укратко ћемо приказати историју закона реципроцитета са циљем разјашњавања зашто закон описан дефиницијом 2.6.1 дугује себи баш тај назив.

Закон квадратног реципроцитета дуго је фасцинирао умове математичара као први суштински дубок и нетривијалан резултат у вези са простим бројевима. Подсећања ради, тај закон је доказао Гаус почетком XIX века и од тог периода почиње потрага за његовим формулацијама у све општијим контекстима. Колике је размере та потрага добила најбоље описује чињеница да је њој било посвећен један од чувена 23 проблема која је поставио Давид Хилберт на Међународном конгресу математичара у Паризу 1900. године. Наведен као девети по реду, тај проблем гласи:

Наћи општи закон реципроцитета који генерализује квадратни закон реципроцитета у контекст произвољног бројевног поља.

Чињеницу да је најутицајнији математичар тог времена сврстао закон реципроцитета међу најважније задатке који остају математици XX века говори о томе колико је сам проблем еволуирао од времена Гауса. Такође, валидација коју је закон реципроцитета добио од стране Давида Хилберта много је помогла развоју теорије поља класа. Наиме, неки од утицајних математичара тог доба, међу њима истакнути Кронекер и Вебер[3], теорију поља класа нису видели као ништа друго до средство за уопштење Дирихлеове теореме о простим бројевима у аритметичкој прогресији. Хилберт је имао много шире видике и он је теорију поља класа видео као теорију **Абелових** проширења бројевних поља. Управо под Хилбертовим утицајем, подстакнута његовим Деветим (и Дванаестим) проблемом, развијала се теорија поља класа до значаја и статуса који има данас.

Опишимо сада прецизније на шта се мисли под општим законом реципроцитета. Посматрајмо моничан и иредуцибилан полином $f(X) \in \mathbb{Z}[X]$ и означимо са K_f коренско поље полинома f над $\mathbb{Q}$. Тада је $K_f/\mathbb{Q}$ коначно Галуаово проширење.

Уочимо произвољан рационалан прост број p и редукујмо све коефицијенте полинома $f(X)$ по модулу p. На тај начин добијамо полином $f_p(X)$ над коначним пољем $\mathbb{F}_p$. Уколико се f_p може раставити на различите линеарне факторе над $\mathbb{F}_p$ кажемо да се f потпуно цепа по модулу p. Дефинишемо

$$\mathrm{Spl}(f) = \{p \text{ прост} \mid f \text{ се потпуно цепа по модулу } p\}\,.$$

Оно што је од значаја је питање описа факторизације полинома $f_p(X)$ у функцији од простог броја p. Понекад можемо поставити и једноставније питање одређивања правила на основу кога се може знати који прости бројеви припадају скупу $\mathrm{Spl}(f)$. Међутим, у случају оба питања крије се одређена непрецизност. На шта се тачно мисли под појмом „функције" односно „правила"? Управо је то питање којим се баве општи закони реципроцитета.

Претпоставимо да је проширење $K_f/\mathbb{Q}$ **Абелово**, односно да је Галуаова група G тог проширење комутативна. Тада се често каже и за полином f да је Абелов, а група G се назива Галуаовом групом за $f(X)$. Као што смо видели у претходном пасусу, један од задовољавајућих начина дефинисања закона реципроцитета, у оваквом, **Абеловом** случају, је давање услова на основу којих се може описати скуп $\mathrm{Spl}(f)$. Артинов закон реципроцитета се онда у траженом контексту реформулише у:

[3] у алгебарској теорији бројева веома је позната Теорема Кронекер-Вебера по којој је свако Абелово проширење поља $\mathbb{Q}$ садржано у неком циклотомичном проширењу од $\mathbb{Q}$

Тврђење 2.6.3. Ако је полином $f(X)$ Абелов, онда се $\mathrm{Spl}(f)$ може описати помоћу конгруенција у односу на модуле који зависе само од $f(X)$.

Тврђење 2.6.3 се може још додатно продубити показивањем да оно важи и у обратном смеру. На тај начин долазимо до познате **Теореме о Абеловом полиному**.

Теорема 2.6.2 (о Абеловом полиному)**.** Скуп $\mathrm{Spl}(f)$ се може описати помоћу конгруенција у односу на модуле који зависе само од $f(X)$ ако и само ако је полином $f(X)$ Абелов.

Из претходне теореме закључујемо да Артинов закон реципроцитета представља одговор на Девети Хилбертов проблем у случају **Абелових** раширења. Нагласимо да је у општем случају Девети проблем остао нерешен.
За много више о закону реципроцитета у једноставнијим случајевима, као и много више о Артиновом закону реципроцитета и Теореми о Абеловом полиному, погледати [19] и [4].

ГЛАВА 3

L-функције

3.1 Уопштене Дирихлеове L-функције. Дедекиндова зета функција

У овом одељку бавићемо се дефинисањем *уопштених Дирихлеових L-функција* које ће представљати значајан искорак у односу на L-функције дефинисане у одељку 1.3.

Нека је $\mathfrak{m}$ произвољан модул у бројевном пољу K. Означимо стандардно као и до сада са $J^{\mathfrak{m}}$ подгрупу групе I_K свих ненула размољених идеала прстена целих $\mathscr{O}_K$ генерисану простим идеалима који не деле коначни део модула $\mathfrak{m}$. Такође, под

$$J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$$

ћемо као и у досадашњем излагању подразумевати групу класа зрака у односу на модул $\mathfrak{m}$. Дефиниција уопштене Дирихлеове L-функције ослањаће се на коначност групе $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$, установљене Теоремом 2.3.1. Због те чињенице можемо посматрати карактер ψ коначне Абелове групе $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$ кога називамо *уопштеним Дирихлеовим карактером по модулу* $\mathfrak{m}$. Њега можемо видети и као карактер групе $J^{\mathfrak{m}}$ који има $\varsigma(K_{\mathfrak{m},1})$ у језгру и означавати са $\psi(\mathfrak{a})$ његову вредност у косету $\mathfrak{a}\,\varsigma(K_{\mathfrak{m},1})$. Зато има смисла уопштеном Дирихлеовом карактеру по модулу $\mathfrak{m}$ придружити L-функцију која је дефинисана аналогно L-функцији датој дефиницијом 1.3.1,

$$L(s,\psi)=\sum_{\mathfrak{a}\in J^{\mathfrak{m}}}\frac{\psi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}$$

и коју називамо *уопштена Дирихлеова L-функција* придружена карактеру ψ и модулу $\mathfrak{m}$.

Једно од основних питања везано за уопштене Дирихлеове L-функције је питање области (у $\mathbb{C}$) на којој су оне дефинисане. Приметимо да аналогно као у Теореми 1.3.1

имамо да је произвољна уопштена Дирихлеова L-функција $L(s,\psi)$ коректно дефинисана и аналитичка на домену $\Re(s) > 1$. Поставља се питање да ли се та област може проширити. У случају да је одговор на то питање потврдан, интересује нас и која је највећа област у $\mathbb{C}$ на коју се $L(s,\chi)$ може аналитички проширити. Одговоре на ова питања пружа *аналитичко проширење* уопштених Дирихлеових L-функција.

У својој потпуности, извођење аналитичког проширења уопштених Дирихлеових L-функција је прилично дуготрајан и технички веома захтеван поступак који превазилази оквире нашег излагања. Због тога ћемо овде приказати само изузетно кратку скицу са циљем илустрације како се тај поступак може извести. Детаљно извођење аналитичког проширења уопштених Дирихлеових L-функција може се пронаћи у [14].

Посматрајмо уопштену Дирихлеову L-функцију

$$L(s,\psi) = \sum_{\mathfrak{a}\in J^{\mathfrak{m}}} \frac{\psi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}$$

придружену карактеру ψ и модулу $\mathfrak{m}$ у бројевном пољу K. Први корак аналитичког проширења уопштене Дирихлеове L-функције $L(s,\psi)$ је прилично једноставан и своди се на њену декомпозицију на такозване парцијалне L-функције. Разбијањем групе класа зрака у односу на модул $\mathfrak{m}$ на појединачне класе добијамо да се функција $L(s,\psi)$ може записати у облику суме

$$L(s,\psi) = \sum_{\mathfrak{k}} L(\mathfrak{k},s,\psi),$$

узете по свим класама $\mathfrak{k}$ у $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$, при чему је

$$L(\mathfrak{k},s,\psi) = \sum_{\mathfrak{a}\in\mathfrak{k}} \frac{\psi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}.$$

Функције $L(\mathfrak{k},s,\psi)$ називамо *парцијалним L-функцијама.* Сврха овакве декомпозиције уопштене Дирихлеове L-функције $L(s,\psi)$ на суму парцијалних L-функција $L(\mathfrak{k},s,\psi)$ се огледа у томе што се на тај начин проблем аналитичког проширење функције $L(s,\psi)$ редукује на проблем аналитичког проширења функција $L(\mathfrak{k},s,\psi)$. Према томе, све што је још потребно урадити је извести аналитичко проширење за парцијалну L-функцију $L(\mathfrak{k},s,\psi)$. Такав поступак у себи садржи комбиновање великог броја фундаменталних објеката како алгебарске тако и аналитичке теорије бројева. Ми ћемо само у најкраћим цртама навести кључне кораке.

- Прво што треба урадити је записати парцијалну L-функцију $L(\mathfrak{k},s,\psi)$ у погоднијем облику за аналитичке манипулације. У ту сврху користе се важни објекти алгебарске теорије бројева познати под називом *идеални бројеви.* Грубо говорећи, идеални бројеви су алгебарски цели бројеви који на погодан начин представљају идеале прстена целих бројевног поља.

- Кључни и технички најзахтевнији део доказа се састоји у показивању да је парцијална L-функција $L(\mathfrak{k}, s, \psi)$ Мелинова трансформација неке аналитичке функције $f(t)$. У сврху дефинисања функције $f(t)$ се користи θ-функција везана за бројевно поље K, као и одговарајућа θ-трансформациона формула.

- Када је добијена веза са функцијом $f(t)$, аналитичко проширење парцијалне L-функције $L(\mathfrak{k}, s, \psi)$ следи на основу чињенице да се Мелинове трансформације могу аналитички проширити (ово чињеница се често назива *Мелинов принцип*).

Напомена. *Претходни поступак аналитичког проширења имплицитно претпоставља да је модул $\mathfrak{m}$ или карактер ψ нетривијалан. У случају да ти услови нису испуњени, аналитичко проширење одговарајуће L-функције постоји и изводи се потпуно аналогно, уз разлику да проширена функција има прост пол у тачки $s = 1$. Више о том специјалном случају приказано је наредним примером.*

Пример 3.1. Посматрајмо тривијалан случај када је $\mathfrak{m} = 1$ и $\psi = \psi_0$ тривијалан карактер. Уопштена Дирихлеова L-функција придружена њима изражава се као сума реда

$$L(s, \psi_0) = \sum_{\mathfrak{a} \in J \setminus \{0\}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}$$

или еквивалентно у облику Ојлеровог производа

$$L(s, \psi) = \prod_{\mathfrak{p} \in M_K} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}}$$

и назива се *Дедекиндова зета функција* бројевног поља K. Означаваћемо је са $\zeta_K(s)$. Приметимо да је $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ тј. да Дедекиндова зета функција поља $\mathbb{Q}$ није ништа друго до Риманова зета функција. Дакле, Дедекиндова зета функција неког бројевног поља је природно уопштење Риманове зета функције на том пољу[1].
Наведимо две особине Дедекиндове зета функције које ће нам бити од значаја приликом дефинисања појма Дирихлеове густине.

- Дедекиндова зета функција има аналитичко проширење на цео скуп $\mathbb{C} \setminus \{1\}$, док у тачки $s = 1$ има прост пол. Користећи конвенцију по којој се за две комплексне функције f и g пише $f(s) \sim g(s)$ ако је $f(s) - g(s)$ аналитичка функција у тачки $s = 1$, ту чињеницу можемо записати и као

$$\zeta_K(s) \sim \frac{1}{s - 1}.$$

  За прецизан опис резидуума функције $\zeta_K(s)$ у тачки $s = 1$ погледати [14].

[1] приметимо како је и разматрање најтривијалније L-функције донело доста нетривијалног

- Из Ојлеровог производа Дедекиндове зета функције логаритмујући и развијајући у Тејлоров ред добијамо

$$\log \zeta_K(s) = \sum_{\mathfrak{p} \in M_K} \sum_{m=1}^{\infty} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p} \in M_K} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} + \sum_{\mathfrak{p} \in M_K} \sum_{m \geq 2} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}}.$$

Како сума

$$\sum_{\mathfrak{p} \in M_K} \sum_{m \geq 2} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}}$$

очигледно дефинише аналитичку функцију у тачки $s = 1$, добијамо

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p} \in M_K} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}}.$$

Приметимо још да комбинујући две претходне особине добијамо

$$\sum_{\mathfrak{p} \in M_K} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} \sim \log \frac{1}{s-1}$$

□

Аналитичко проширење уопштених Дирихлеових L-функција се може схватити као генерализација аналитичког проширења („обичних") Дирихлеових L-функција. Имајући то у виду, од интереса је да испитамо да ли уопштене Дирихлеове L-функције имају још неку особину у аналогији са класичним.

Подсетимо се да у случају класичних Дирихлеових L-функција важи $L(1, \chi) \neq 0$. Управо је то својство есенцијално у доказу Дирихлеове теореме о простим бројевима. Наредна теорема показује да се и уопштене Дирихлеове L-функције не анулирају у тачки $s = 1$, што ће бити кључно доказу Дирихлеове теореме о густини.

Теорема 3.1.1. *Нека је ψ нетривијалан карактер по модулу $\mathfrak{m}$, односно нетривијалан карактер групе класа зрака $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$. Тада важи*

$$L(1, \psi) \neq 0.$$

На овом месту, користећи само технике уопштених Дирихлеових L-функција нисмо у стању да прикажемо доказ Теореме 3.1.1. Ипак, од доказа нећемо одустати, већ ћемо немогућност приказивања доказа једне тако значајне теореме схватити као знак да је потребно да контекст који разматрамо обогатимо додатним објектима. Из тог разлога, кренућемо путем дефинисања још једне врсте L-функција, познате као *Артинове L-функције*.

3.2 Репрезентације коначне групе

Имајући у виду циљ најављен у претходном одељку, оно ћему тежимо у наставку нашег излагања је дефинисање нове врсте L-функција, које су комплексније од до сада посматраних уопштених Дирихлеових L-функција. Значајно својство које карактерише уопштене Дирихлеове L-функције је њихова везаност за фиксирано бројевно поље K. Према томе, оно што можемо урадити у циљу потребног богаћења контекста у коме радимо је да уместо фиксираног бројевног поља K посматрамо Галуаово раширење L/K. Тражене компликованије L-функције онда дефинишемо као L-функције које су везане за само раширење L/K. Основне информације о том раширењу носи Галуаова група $G(L/K)$. Стога је природно да L-функција коју желимо да дефинишемо зависи од њених елемената тј. од K-аутоморфизама поља L. Међутим, управо у тој природној претпоставци се крије и један не баш занемарљив проблем. Наиме, значај L-функција је у томе што се аналитички могу испитати њихове особине, које се онда импресивно рефлектују на решавање проблема теорије бројева[2]. Због тога је директан рад са групом $G = G(L/K)$ приликом дефинисања L-функције прилично непожељан; у мањој мери зато што и та сама група може бити компликована, а у већој мери зато што је директан рад са њеним елементима рад са аутоморфизмима поља, што вишеструко отежава примену анализе. Решење тог проблема је у представљању Галуаове групе G у облику погоднијем за аналитичко разматрање. Смернице како да то урадимо налазимо у наредном примеру.

Пример 3.2. Нека је m природан број, χ Дирихлеов карактер модуло m и

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

њему придружена L-функција. Посматрајмо циклотомично раширење $\mathbb{Q}(\mu_m)/\mathbb{Q}$. За сваки $\mathbb{Q}$-аутоморфизам поља $\mathbb{Q}(\mu_m)$ важи да је облика

$$\alpha_t : x \to x^t, \text{ за } x \in \mu_m,$$

при чему је $t \in (\mathbb{Z}/m\mathbb{Z})^*$. Због тога пресликавање

$$\Theta : (\mathbb{Z}/m\mathbb{Z})^* \to G, \ \Theta(t) = \alpha_t$$

представља изоморфизам Галуаове групе $G = G(\mathbb{Q}(\mu_m)/\mathbb{Q})$ и групе $(\mathbb{Z}/m\mathbb{Z})^*$. Захваљујући том изоморфизму, карактер χ можемо интерпретирати и као карактер Галуаове групе G односно као хомоморфизам

$$\chi : G \to \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C}).$$

[2]нпр. Дирихлеова теорема о простим бројевима је есенцијално последица чињенице да се L-функције придружене нетривијалном Дирихлеовом карактеру не анулирају у 1, што је особина која се проверава аналитички

Користећи ту интерпертацију, L-функција придружена карактеру χ може се написати у облику

$$L(s,\chi) = \prod_{p \nmid m} \frac{1}{1-\chi(\alpha_p)p^{-s}}, \tag{3.1}$$

који у потпуности изражен преко елемената Галуаове групе G. Дакле, формулом (3.1) дефинисана је L-функција везана за Галуаово раширење $\mathbb{Q}(\mu_m)/\mathbb{Q}$.
□

Како претходно описану L-функцију везану за једно конкретно раширење бројевних поља можемо искористити за проширивање приче у општи контекст? Пре свега, уочимо колико је значајна чињеница да смо могли да конструишемо хомоморфизам између Галуаове групе G и групе $\mathrm{GL}_1(\mathbb{C})$. Другим речима, сваком, за анализу неприступачном елементу групе G, односно $\mathbb{Q}$-аутоморфизму поља $\mathbb{Q}(\mu_m)$ смо успели да придружимо комплексну матрицу 1×1, односно комплексан број, што је објекат веома приступачан за примену анализе. Егзистенција L-функције у наведеном облику одатле онда следи прилично једноставно.

Идеју придруживања комплексних бројева елементима Галуаове групе ћемо покушати да применимо и у много општијој ситуацији од оне разматране у примеру тј. у случају произвољног Галуаовог раширења L/K бројевних поља. Међутим, у таквој, значајно компликованијој ситуацији аутоморфизмима ћемо придруживати квадратне комплексне матрице чија димензија може бити већа од 1, а не искључиво комплексне бројеве. Тако долазимо да појма *репрезентације* Галуаове групе G раширења L/K. Овај одељак посвећен је управо дефинисању тог појма, као и приказивању неких његових основних особина. При томе ћемо у целокупном излагању разматрати општи случај произвољне коначне групе G, имајући у виду да нам је од интереса ситуација када је та група баш Галуаова група Галуаовог раширења L/K бројевних поља.

Дефиниција 3.2.1. ***Репрезентација*** *коначне групе G је дејство те групе на коначно димензиони комплексни векторски простор V, односно хомоморфизам*

$$\rho : G \to \mathrm{GL}(V) = Aut_{\mathbb{C}}(V).$$

По конвенцији ћемо репрезентацију групе G означавати са (ρ, V), где су ρ хомоморфизам и V комплексни векторски простор дати претходном дефиницијом. Такође, ако је (ρ, V) репрезентација групе G, дејство елемента $\sigma \in G$ на вектор $v \in V$ ћемо означавати скраћено са σv, уместо пуне нотације $\rho(\sigma)v$. Неколико основних карактеристика репрезентације групе уводимо наредним дефиницијама.

Дефиниција 3.2.2. ***Степен*** *репрезентације (ρ, V) коначне групе G је димензија векторског простора V над $\mathbb{C}$.*

Дефиниција 3.2.3. *Нека су (ρ, V) и (ρ', V') две репрезентације коначне групе G. За линеарно пресликавање $T : V \to V'$ кажемо да* ***преводи*** *ρ у ρ' уколико за свако $g \in G$ важи*

$$\rho'(g) \circ T = T \circ \rho(g).$$

Приметимо да претходна дефиниција значи ништа друго до комутативност наредног дијаграма за свако $g \in G$.

$$\begin{array}{ccc} V & \xrightarrow{T} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{T} & V' \end{array}$$

Дефиниција 3.2.4. *За две репрезентације (ρ, V) и (ρ', V') коначне групе G кажемо да су* ***еквивалентне*** *ако постоји бијективно линеарно пресликавање $T : V \to V'$ које преводи ρ у ρ'.*

Дефиниција 3.2.5. *Репрезентација (ρ, V) коначне групе G је* ***иредуцибилна*** *ако V нема ниједан прави G-инваријантан потпростор.*

Дефиниција 3.2.6. *Ако су (ρ, V) и (ρ', V') две репрезентације коначне групе G њихова* ***директна сума*** *$(\rho \oplus \rho', V \oplus V')$ је такође репрезентација групе G дефинисана са*

$$\rho \oplus \rho' : G \to \mathrm{GL}(V \oplus V'), \;\; (\rho \oplus \rho')(g)(v, v') = (\rho(g)(v), \rho'(g)(v')),$$

за произвољне $g \in G, v \in V$ и $v' \in V'$.

Значај иредуцибилних репрезентација је у томе што се свака друга репрезентација може изразити као њихова коначна директна сума. Дакле, ако је (ρ, V) репрезентација групе G, онда постоји коначно много иредуцибилних репрезентација (ρ_α, V_α) те групе, међу којима може бити и међусобно еквивалентних и за које важи

$$(\rho, V) = (\oplus_\alpha \rho_\alpha, \oplus_\alpha V_\alpha). \tag{3.2}$$

За неку фиксирану иредуцибилну репрезентацију $(\rho_{\alpha_0}, V_{\alpha_0})$ групе G кажемо да има *вишеструкост* једнаку r_{α_0} у (ρ, V), ако је еквивалентна са тачно r_{α_0} иредуцибилних репрезентација које учествују у декомпозицији (3.2). Релацију (3.2) онда можемо записати и скраћено као

$$\rho \sim \sum r_\alpha \rho_\alpha,$$

где се сума узима по свим међусобно нееквивалентним иредуцибилним репрезентацијама (ρ_α, V_α) групе G вишеструкости r_α у (ρ, V).

Ако је (ρ, V) репрезентација групе G, за произвољно $\sigma \in G$ је онда $\rho(\sigma)$ елемент групе $\mathrm{GL}(V)$, па има коректно дефинисан траг. Због тога је и наредна дефиниција карактера репрезентације коректна.

Дефиниција 3.2.7. ***Карактер*** *репрезентације* (ρ, V) *коначне групе* G *је пресликавање*

$$\chi_\rho : G \to \mathbb{C}$$

дефинисано са

$$\chi_\rho(\sigma) = \operatorname{Tr} \rho(\sigma).$$

Специјално, ако је репрезентација (ρ, V) *иредуцибилна, онда се и карактер* χ *назива* ***иредуцибилним****.*

Наредним примером описано је неколико основних примера репрезентација коначне групе, као и њихови карактери.

Пример 3.3. Нека је G коначна група.

- Репрезентација (ρ, V) групе G, где је $\dim V = 1$ и $\rho : G \to \mathrm{GL}(V)$, $\rho(\sigma) = 1$ за све $\sigma \in G$ назива се *тривијалном*. Карактер тривијалне репрезентације је константно пресликавање $1_G : G \to \mathbb{C}$, $1_G(\sigma) = 1$ за све $\sigma \in G$.

- Уочимо комплексни векторски простор

$$V = \mathbb{C}[G] = \left\{ \sum_{\tau \in G} x_\tau \tau \mid x_\tau \in \mathbb{C} \right\}$$

  и означимо са ρ дејство множењем слева групе G на V. Тада је (ρ, V) репрезентација групе G коју називамо *регуларном* репрезентацијом. Карактер придружен регуларној репрезентацији означавамо са r_G.

- Комплексни векторски простор

$$W = \left\{ \sum_{\sigma \in G} x_\sigma \sigma \mid x_\sigma \in \mathbb{C}, \sum_{\sigma \in G} x_\sigma = 0 \right\}$$

  заједно са дејством множењем слева групе G на њега дефинишу *аугментовану* репрезентацију групе Г. Карактер придружен аугментованој репрезентацији означавамо са u_G.

- Однос три претходно наведене репрезентације групе G је прилично интересантан. Наиме, важи да је регуларна репрезентација директна сума тривијалне и аугментоване. Стога и за њима придружене карактере важи $r_G = u_G + 1_G$.

□

Карактер прецизно одређује репрезентацију у смислу да су две репрезентације еквивалентне ако и само ако су њима одговарајући карактери једнаки. Такође, ако је χ_ρ карактер репрезентације (ρ, V) коначне групе G, онда важи $\chi_\rho(1) = \dim V$, као и $\chi_\rho(\sigma\tau\sigma^{-1}) = \chi_\rho(\tau)$ за све $\sigma, \tau \in G$. Последње наведена особина карактере репрезентације сврстава у ширу групу пресликавања описаних наредном дефиницијом.

Дефиниција 3.2.8. *Пресликавање*

$$f : G \to \mathbb{C}$$

је ***централно*** *или* ***класно*** *у* G *ако важи*

$$f(\sigma\tau\sigma^{-1}) = f(\tau)$$

за све $\sigma, \tau \in G$.

Из претходне дефиниције је јасно да су карактери репрезентација централна пресликавања који узимају вредност једнаку степену репрезентације у неутралу групе G. Због таквог истакнутог места који у простору свих централних функција заузимају карактери, може се наслутити да га они на неки начин генеришу. Такво размишљање води у добром правцу; свако централно пресликавање φ се на јединстен начин може написати као $\mathbb{C}$-линеарна комбинација иредуцибилних карактера. При томе се карактери од произвољних централних пресликавања истичу по томе што су сви коефицијенти у њиховој декомпозицији на суму иредуцибилних карактера позитивни цели бројеви. Последње тврђење можемо и експлицитно видети, јер за карактер χ_ρ придружен репрезентацији (ρ, V) коначне групе G, $\rho \sim \sum r_\alpha \rho_\alpha$, важи

$$\chi_\rho = \sum r_\alpha \chi_{\rho_\alpha},$$

где се сума узима по свим каракактерима међусобно нееквивалентних иредуцибилних репрезентација (ρ_α, V_α) групе G вишеструкости r_α у (ρ, V).

Веома интересантна и значајна особина простора централних функција је што се тај простор може снабдети ермитским скаларним производом. Централним пресликавањима φ и ψ у G придружимо комплексан број $\langle \varphi, \psi \rangle$ на следећи начин:

$$\langle \varphi, \psi \rangle = \frac{1}{g} \sum_{\sigma \in G} \varphi(\sigma)\bar{\psi}(\sigma), \tag{3.3}$$

где је $\bar{\psi}$ комплексно конјугована функција функције ψ и g ред групе G. Тада за два иредуцибилна карактера χ и χ' важи

$$\langle \chi, \chi' \rangle = \begin{cases} 1, & \text{ако је } \chi = \chi' \\ 0, & \text{ако је } \chi \neq \chi', \end{cases}$$

што значи да једнакост (3.3) дефинише ермитски скаларни производ на простору централних пресликавања, при чему једну ортонормирану базу у односу на тај скаларни производ чини управо скуп иредуцибилних карактера.

Овако богата структура простора свих централних пресликавања има одјека и значења у контексту репрезентација коначне групе G. Уочимо произвољну репрезентацију (ρ, V) те групе и напишимо је као директну суму иредуцибилних репрезентација $(\rho_1, V_1), (\rho_2, V_2), \ldots, (\rho_s, V_s)$,

$$(\rho, V) = (\rho_1, V_1) \oplus (\rho_2, V_2) \oplus \cdots \oplus (\rho_s, V_s).$$

Означимо са χ карактер придружен репрезентацији (ρ, V) и са χ_i карактер придружен презентацији $(\rho_i, V_i), 1 \leq i \leq s$. Тада важи

$$\chi = \chi_1 + \chi_2 + \cdots + \chi_s.$$

Ако је (ρ', V') још једна произвољна презентација групе G са карактером χ' одатле имамо да је

$$\langle \chi, \chi' \rangle = \langle \chi_1, \chi' \rangle + \langle \chi_2, \chi' \rangle + \cdots + \langle \chi_s, \chi' \rangle.$$

Како су репрезентације $(\rho_1, V_1), (\rho_2, V_2), \ldots, (\rho_s, V_s)$ иредуцибилне, имамо да је за све $1 \leq i \leq s$

$$\langle \chi_i, \chi' \rangle = \begin{cases} 1, & \text{ако су } V_i \text{ и } V' \text{ изоморфни} \\ 0, & \text{ако } V_i \text{ и } V' \text{ нису изоморфни.} \end{cases}$$

Закључујемо да вредност скаларног производа $\langle \chi, \chi' \rangle$ није ништа друго до вишеструкост репрезентације (ρ', V') у (ρ, V).

Погледајмо у каквом је односу скаларни производ дефинисан релацијом (3.3) са хомоморфизмима коначне групе G. Нека је H нека коначна група и $h : H \to G$ хомоморфизам. Тада је једнакошћу

$$h^*(\varphi) = \varphi \circ h$$

за произвољну централну функцију φ у G дефинисана централна функција $h^*(\varphi)$ у H. Занимљиво је да хомоморфизам h индукује и пресликавање h_* између централних функција у H и оних у G. Пресликавања h^* и h_* су у изузетној хармонији са скаланим производом одређеним једнакошћу (3.3). Она веома подсећа на однос линеарног оператора и њему адјунгованог оператора на Хилбертовог простору и описана је следећом теоремом.

Теорема 3.2.1 (Фробенијусов реципроцитет)**.** *Нека је $h : H \to G$ хомоморфизам коначних група G и H. Тада за свако централно пресликавање ψ у H постоји јединствено централно пресликавање $h_*(\psi)$ у G такво да важи*

$$\langle \varphi, h_*(\psi) \rangle = \langle h^*(\varphi), \psi \rangle,$$

за свако централно пресликавање φ у G.

Доказ. Погледати [17]. □

Основне две ситуације примене Фробенијусовог реципроцитета приказане су наредним примером.

Пример 3.4.

- *H је подгрупа од G и h је инклузија*

У овом случају пишемо $\varphi|H$ или чак само φ уместо $h^*(\varphi)$ и ψ_* уместо $h_*(\psi)$. Пресликавање ψ_* називамо *индукованим* пресликавањем (централног пресликавања ψ у H). Ако је φ карактер репрезентације (ρ, V) групе G, онда је $\varphi|H$ карактер репрезентације $(\rho|H, V)$ подгрупе X. Уз репрезентацију (ρ, V) групе H посматрамо и репрезентацију $(\mathrm{Ind}(\rho), \mathrm{Ind}_G^H V)$ групе G коју називамо *индукованом* репрезентацијом. Дефинишемо је на следећи начин: $\mathbb{C}$-векторски простор $\mathrm{Ind}_G^H V$ је одређен са

$$\mathrm{Ind}_G^H V = \{f : G \to V \mid f(\tau x) = \tau f(x), \text{ за све } \tau \in H, x \in G\},$$

а $\mathrm{Ind}(\rho)$ је дејство групе G на тај простор дефинисано са

$$(\sigma f)(x) = f(x\sigma),$$

за све $\sigma, x \in G$, $f \in \mathrm{Ind}_G^H V$.
Индуковано централно пресликавање ψ_* карактера ψ репрезентације (ρ, V) групе H природно је везано са индукованом репрезентацијом $(\mathrm{Ind}(\rho), \mathrm{Ind}_G^H V)$ групе G тиме што представља карактер те репрезентације.

- *G се може изразити као неки количник H/N групе H и h је пројекција*

У овом случају пишемо $\psi_\natural$ уместо $h_*(\psi)$ и важи

$$\psi_\natural(\sigma) = \frac{1}{|N|} \sum_{\tau + N = \sigma} \psi(\tau)$$

за све $\sigma \in G$. Такође, ако је φ карактер репрезентације (ρ, V) групе G, $h^*(\varphi)$ представља карактер репрезентације $(\rho \circ h, V)$ групе H.
□

Подсетимо се да је степен репрезентације (ρ, V) коначне групе G димензија $\mathbb{C}$-векторског простора V. Ову дефиницију проширујемо и на карактере, па кажемо степен карактера χ мислећи на степен њему придружене репрезентације (ρ, V). Приметимо да карактер χ степена 1 групе G није ништа друго до хомоморфизам

$$\chi : G \to \mathbb{C}^*.$$

Узимајући у обзир њихову једноставност, за очекивати је да карактери степена 1 имају некакву генераторну/базну улогу међу осталим карактерима. У оправданост таквог очекивања уверава нас наредна теорема Брауера.

Теорема 3.2.2 (Брауер). *Нека су $H_1, H_2, \ldots, H_s$ све подгрупе коначне групе G и χ_i њима придружени карактери степена 1. Тада се сваки карактер χ придружен некој репрезентацији коначне групе G може представити као $\mathbb{Z}$-линеарна комбинација индукованих карактера χ_{i*}.*

Доказ. Приказаћемо кратку скицу доказа Брауерове теореме. Прво што је потребно је разматрање неколико чињеница из теорије група, које ћемо сада навести.

Елемент x коначне групе G се назива *p-унипотентим* ако је његов ред у G степен простог броја p. Са друге стране, елемент x коначне групе G се назива *p-регуларним* ако прост број p не дели његов ред. Додатно, може се показати да се сваки $x \in G$ може записати у облику

$$x = x_u x_r,$$

где је x_u p-унипотентан, а x_r p-регуларан и x_u и x_r комутирају.

Следеће што је потребно је претходно разматрање са нивоа елемената групе G пребацити на ниво погрупа од G. Тако за подгрупу H групе G кажемо да је *p-елементарна* ако се може записати као директан производ

$$H = C \times P,$$

где је p прост број, C циклична група реда узајамно простог са p и P p-група тј. група у којој је ред сваког елемента неки степен броја p. Показује се да је свака p-елементарна подгрупа нилпотента, као и да је композиција $H = C \times P$ јединствена; C је скуп свих p-регуларних елемената групе H, а P скуп свих p-унипотентих елемената те групе.

Наредни корак је дефинисање конкретне групе на коју се могу применити претходно приказана општа тврђења теорије група. Нека је G коначна група (из исказа теореме). Са $R(G)$ ћемо означавати слободну Абелову групу генерисану свим иредуцибилним карактерима придруженим подгрупама те групе. Дакле, ако су $\chi_1, \chi_2, \ldots, \chi_s$ сви такви карактери, важи

$$R(G) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_s.$$

За прост број p означимо са V_p погрупу од $R(G)$ генерисану карактерима индукованим карактерима придруженим p-елементарним погрупама од G. Кључни део доказа теореме Брауера је у доказивању да је индекс подгрупе V_p у групи $R(G)$ коначан и узајамно прост са p. Одатле се онда показује да је

$$\bigoplus_{p \text{ прост}} V_p = R(G).$$

Другим речима, добијамо да је сваки карактер придружен некој репрезентацији групе G се може представити као $\mathbb{Z}$-линеарна комбинација карактера индукованих карактерима придруженим елементарним подгрупама групе G.[3] Одавде онда лако следи тврђење које треба доказати. □

[3] често се и ово тврђење наводи као теорема Брауера

3.3 Артинове L-функције

Појам репрезентације коначне групе омогућава да се елементи Галуаове групе $G = G(L/K)$ Галуаовог раширења L/K бројевних поља представе као симетрије коначно димензионог комплексног векторског простора. На тај начин се често неприступачан директан рад са K-аутоморфизмима поља L замењује радом са квадратним матрицама, за кога постоје развијене технике линеарне алгебре. Тако је одређен и терен на коме ћемо дефинисати *Артинове L-функције*– тај појам неће бити везан директно за Галуаову групу G раширења L/K, већ за неку њену репрезентацију (ρ, V). Поред репрезентације (ρ, V) групе G посматрајмо прост идеал $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ заједно са простим идеалом $\mathfrak{P}$ у $\mathscr{O}_L$ који је изнад њега. Означимо стандардно као и до сада са $G(\mathfrak{P})$ групу декомпозиције за $\mathfrak{P}$ и са $I(\mathfrak{P})$ групу инерције за $\mathfrak{P}$. У пододељку 2.5.3 установили смо изоморфизам

$$G(\mathfrak{P})/I(\mathfrak{P}) \cong G\left(\frac{\mathscr{O}_L/\mathfrak{P}}{\mathscr{O}_K/\mathfrak{p}}\right),$$

као и чињеницу да је група $G(\mathfrak{P})/I(\mathfrak{P})$ циклична, генерисана косетом чији су елементи Фробенијусови аутоморфизми придружени $\mathfrak{P}$. Фиксирајмо један Фробенијусов аутоморфизам $\varphi_{\mathfrak{P}}$ придружен $\mathfrak{P}$. Тада је карактеристични полином

$$\det(I_n - \rho(\varphi_{\mathfrak{P}})t)$$

коректно дефинисан (I_n је јединична квадратна матрица димензије једнаке степену репрезентације (ρ, V)). Такође, тај полином зависи само од избора простог идеала $\mathfrak{p}$, па је следећа дефиниција коректна.

Дефиниција 3.3.1. *Нека је L/K Галуаово раширење бројевних поља и (ρ, V) репрезентација одговарајуће Галуаове групе.* ***Артинова L-функција*** *придружена тој репрезентацији дефинисана је као Ојлеров производ*

$$\mathfrak{L}(L/K, \rho, s) = \prod_{\mathfrak{p} \in M_K} \frac{1}{\det(I_n - \rho(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s})}$$

узет по скупу M_K свих простих идеала прстена целих $\mathscr{O}_K$ бројевног поља K.

Следећи аналоган пут као у доказу Теореме 1.3.1 показује се да производ којим се дефинише Артинова L-функција конвергира апсолутно и униформно у области $\Re(s) \geq 1 + \delta$, за све $\delta > 0$. Одатле закључујемо да је Артинова L-функција аналитичка у полуравни $\Re(s) > 1$. Приметимо да у случају да је репрезентација (ρ, V) Галуаове групе G тривијална, њој придружена Артинова L-функција једнака је Дедекиндовој зета функцији $\zeta_K(s)$ бројевног поља K.

У претходном одељку видели смо да еквивалентне репрезентације коначне групе имају једнаке карактере. Због тога можемо Артинову L-функцију придружити карактеру χ репрезентације (ρ, V), па ћемо надаље уместо $\mathfrak{L}(L/K, \rho, s)$ писати

$$\mathfrak{L}(L/K, \chi, s) = \prod_{\mathfrak{p} \in M_K} \frac{1}{\det(I_n - \rho(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s})}.$$

Основне особине Артинових L-функција показане су наредном теоремом.

Теорема 3.3.1. *За произвољно Галуаово раширење L/K бројевних поља је испуњено:*

1. *Ако су χ и χ' карактери придружени двема репрезентацијама Галуаове групе $G(L/K)$ тада је*

$$\mathfrak{L}(L/K, \chi + \chi', s) = \mathfrak{L}(L/K, \chi, s)\mathfrak{L}(L/K, \chi', s).$$

2. *Нека је L' Галуаово раширење поља K такво да је $L' \supseteq L \supseteq K$ и χ карактер придружен некој репрезентацији Галуаове групе $G(L/K)$. Тада се χ може посматрати и као карактер придружен репрезентацији Галуаове групе $G(L'/K)$ и важи*

$$\mathfrak{L}(L'/K, \chi, s) = \mathfrak{L}(L/K, \chi, s).$$

3. *За међуполе M, $L \supseteq M \supseteq K$ и карактер χ придружен некој репрезентацији Галуаове групе $G(L/M)$ важи*

$$\mathfrak{L}(L/M, \chi, s) = \mathfrak{L}(L/K, \chi_*, s),$$

где је χ_* индукован карактер карактера χ.

Доказ за 1. и 2.
1. Нека су (ρ, V) и (ρ', V') репрезентације Галуаове групе $G(L/K)$ степена n и n' којима су редом придружени карактери χ и χ'. Тада је директној суми $(\rho \oplus \rho', V \oplus V')$ тих репрезентација придружен карактер $\chi + \chi'$ и важи

$$\det(I_{n+n'} - (\rho \oplus \rho')(\varphi_{\mathfrak{P}})t) = \det(I_n - \rho(\varphi_{\mathfrak{P}})t)\det(I_{n'} - \rho'(\varphi_{\mathfrak{P}})t).$$

Из те релације на основу дефиниције Артинове L-функције одмах следи тражено тврђење.
2. Уочимо прост идеал $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ бројевног поља K, као и просте идеале $\mathfrak{P}$ и $\mathfrak{P}'$ који су у $\mathscr{O}_L$ односно $\mathscr{O}'_L$ и за које важи да је $\mathfrak{P}'|\mathfrak{P}|\mathfrak{p}$ (другим речима, идеал прстена целих већег поља се налази изнад идеала прстена целих мањег поља). Означимо са (ρ, V) репрезентацију Галуаове групе $G(L/K)$ којој одговара карактер χ. Композиција пројекције $G(L'/K) \to G(L/K)$ Галуаових група са пресликавањем ρ представља дејство ρ' групе $G(L'/K)$ на векторски простор V. То дејство индукује епиморфизме

$$G(\mathfrak{P}') \to G(\mathfrak{P}),\ I(\mathfrak{P}') \to I(\mathfrak{P}),\ G(\mathfrak{P}')/I(\mathfrak{P}') \to G(\mathfrak{P})/I(\mathfrak{P})$$

одговарајућих група декомпозиције и инерције, као и њихових количника. Последње наведени епиморфизам слика Фробенијусов аутоморфизам $\varphi_{\mathfrak{P}'}$ придружен $\mathfrak{P}'$ у Фробенијусов аутоморфизам $\varphi_{\mathfrak{P}}$ придружен $\mathfrak{P}$, при чему важи

$$\det(I_n - \rho'(\varphi_{\mathfrak{P}'})t) = \det(I_n - \rho(\varphi_{\mathfrak{P}})t).$$

На основу последње релације уз коришћење дефиниције Артинове L-функције одмах следи тражено тврђење.

□

Доказ трећег дела претходне теореме ћемо, због његове компликованости, извести постепено у неколико етапа. Уведимо прво неке конвенције које ћемо користити, а које омогућавају растерећење уобичајене нотације.

За репрезентацију (ρ, V) степена n неке коначне групе G и произвољно $\varphi \in G$ писаћемо

$$\det(\mathrm{Id} - \varphi X; V) \text{ уместо } \det(I_n - \rho(\varphi)X).$$

Ако је G' нормална подгрупа групе G са $V^{G'}$ ћемо означавати потпростор комплексног векторског простора V који је G'-инваријантан у односу на дејство ρ. Означимо са ρ' пресликавање дефинисано на количнику G/G' са

$$\rho' : G/G' \to V^{G'},\ \ \rho'(gG') = \rho(g), g \in G.$$

Тада $(\rho', V^{G'})$ представља репрезентацију количничке групе G/G'. У оваквом специјалном случају репрезентације ћемо у складу са претходно уведеним записом писати као

$$\det(\mathrm{Id} - \varphi X; V^{G'}).$$

Доказ дела 3. Теореме 3.3.1.

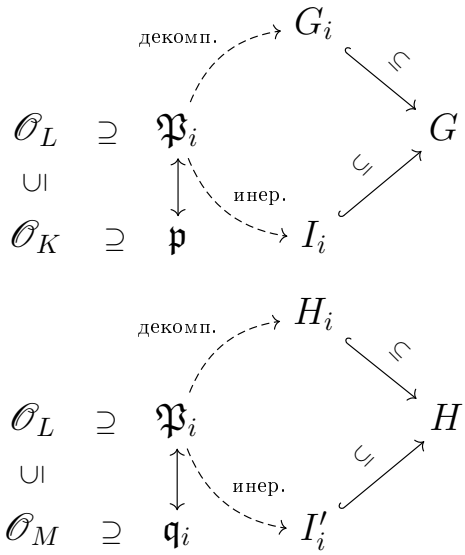
1.корак– Одабир ознака

Нека је $G = G(L/K)$ и $H = G(L/M)$. За прост идеал $\mathfrak{p}$ у $\mathscr{O}_K$ уочимо све просте идеале $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ у $\mathscr{O}_M$ који су изнад њега, као и по један прост идеал $\mathfrak{P}_i$ у $\mathscr{O}_L$ изнад $\mathfrak{q}_i, 1 \leq i \leq r$, као на наредном дијаграму.

$$\begin{array}{ccccc} L & \supseteq & \mathscr{O}_L & \supseteq & \mathfrak{P}_i \\ | & & \cup | & & \vdots \text{ изнад} \\ M & \supseteq & \mathscr{O}_M & \supseteq & \mathfrak{q}_i \\ | & & \cup | & & \vdots \text{ изнад} \\ K & \supseteq & \mathscr{O}_K & \supseteq & \mathfrak{p} \end{array}$$

Означимо са G_i групу декомпозиције, а са I_i групу инерције идеала $\mathfrak{P}_i$ посматраног као проширење простог идеала $\mathfrak{p}$ у прстен целих $\mathscr{O}_L$. Групе декомпозиције и инерције

идеала $\mathfrak{P}_i$ посматраног као проширење простог идеала $\mathfrak{q}_i$ у прстен целих $\mathscr{O}_L$ ћемо означавати редом са H_i и I_i' :



У складу са наведеним ознакама, испуњено је

$$H_i = G_i \cap H \text{ и } I_i' = I_i \cap H.$$

2.корак– Успостављање веза између одговарајућих група декомпозиције и инерције

Подсетимо се на кратко теорије рамификације идеала, према којој се степен инерције f_i идеала $\mathfrak{q}_i$ над идеалом $\mathfrak{p}$ по дефиницији изражава као степен раширења резидуалног поља $\mathscr{O}_M/\mathfrak{q}_i$ над резидуалним пољем $\mathscr{O}_K/\mathfrak{p}$,

$$f_i = [\mathscr{O}_M/\mathfrak{q}_i : \mathscr{O}_K/\mathfrak{p}].$$

Како је раширење $\mathscr{O}_M/\mathfrak{q}_i$ поља $\mathscr{O}_K/\mathfrak{p}$ Галуаово, одатле следи да се f_i може изразити и као

$$f_i = \#G\left(\frac{\mathscr{O}_M/\mathfrak{q}_i}{\mathscr{O}_K/\mathfrak{p}}\right). \tag{3.4}$$

Позивајући се на изоморфизам (2.12) установљен у пододељку 2.5.3 добијамо да важи

$$\#G\left(\frac{\mathscr{O}_M/\mathfrak{q}_i}{\mathscr{O}_K/\mathfrak{p}}\right) = [G(\mathfrak{q}_i) : I(\mathfrak{q}_i)].$$

Из једнакости (3.4), у складу са ознакама које смо увели, онда имамо да је

$$f_i = [G_i : H_i I_i].$$

Погледајмо како се претходно установљене везе рефлектују у Галуаовој групи G. Пре свега, за сваки прост идеал $\mathfrak{P}_i$ у $\mathscr{O}_L$ постоји елемент $\tau_i \in G$ такав да је $\tau_i(\mathfrak{P}_i) = \mathfrak{P}_1$. Због тога[4] је $G_i = \tau_i^{-1} G_1 \tau_i$ и $I_i = \tau_i^{-1} I_1 \tau_i$. Нека је $\varphi \in G_1$ такав да му у количнику G_1/I_1 одговара Фробенијусов аутоморфизам $\varphi_{\mathfrak{P}_1}$ придружен идеалу $\mathfrak{P}_1$. Означимо са φ_i пресликавања у G_i која су τ_i-конјугована пресликавању φ,

$$\varphi_i = \tau_i^{-1} \varphi \tau_i.$$

Сваком од φ_i тада у количнику G_i/I_i одговара Фробенијусов аутоморфизам $\varphi_{\mathfrak{P}_i}$ придружен $\mathfrak{P}_i$ (изнад простог идеала $\mathfrak{p}$). Поред тога, Фробенијусовом аутоморфизму у H_i/I_i', који је придружен $\mathfrak{P}_i$ посматраном као идеал изнад простог идеала $\mathfrak{q}_i$, одговара пресликавање $\varphi_i^{f_i}$.

3.корак– Посматрање репрезентације којој одговара индуковани карактер χ_* и декомпозиција комплексног векторског простора на коме је дефинисана њему одговарајућа репрезентација

Уочимо сада репрезентацију (ρ, W) Галуаове групе H којој је придружен карактер χ. Индуковани карактер χ_* је онда карактер индуковане репрезентације $(\mathrm{Ind}(\rho), V), V = \mathrm{Ind}_G^H W$ групе G. Имајући у виду ознаке које смо до сада увели, оно што треба да докажемо је да важи

$$\det(\mathrm{Id} - \varphi X; V^{I_1}) = \prod_{i=1}^{r} \det(\mathrm{Id} - \varphi_i^{f_i} X^{f_i}; W^{I_i'}).$$

Довољно је посматрати тај проблем у редукованом случају када је $G = G_1$. Конјугујући са τ_i добијамо да је

$$\det(\mathrm{Id} - \varphi_i^{f_i} X^{f_i}; W^{I_i'}) = \det(Id - \varphi^{f_i} X^{f_i}; (\tau_i W)^{I_1 \cap \tau_i H \tau_i^{-1}})$$

и

$$f_i = [G_1 : (G_1 \cap \tau_i H \tau_i^{-1}) I_1].$$

Уочимо да за свако i група $G_1 \cap \tau H \tau^{-1}$ чини једну партицију групе G_1 на косете, као њега погрупа. Означимо за свако i елементе трансверзале такве партиције са $\{\sigma_{ij}\}$. Тада скуп $\{\sigma_{ij}\tau_i\}$ чини једну трансверзалу партиције групе G на косете њене подгрупе H. Због тога за векторске просторе V и W важи[5]

$$V = \bigoplus_{i,j} \sigma_{ij} \tau_i W.$$

Стављајући $V_i = \bigoplus_j \sigma_{ij} \tau_i W$ добијамо декомпозицију комплексног векторског простора V на потпросторе V_i на које све делује G_1.

[4] погледати напомену после доказа Тврђења 2.6.1

[5] у вези са овим тврђењем видети опширније у [14]

4.корак– Редукција проблема

Из декомпозиције комплексног векторског V установљене у претходном кораку, закључујемо да је

$$\det(\mathrm{Id} - \varphi X; V^{I_1}) = \prod_{i=1}^{r} \det(\mathrm{Id} - \varphi X; V_i^{I_1}).$$

Одатле следи да је довољно доказати да је

$$\det(\mathrm{Id} - \varphi X; V_i^{I_1}) = \det(\mathrm{Id} - \varphi^{f_i} X^{f_i}; (\tau_i W)^{I_1 \cap \tau_i H \tau_i^{-1}}).$$

Упростимо сада ознаке тако што ћемо надаље писати G уместо G_1, I уместо I_1, H уместо $G_1 \cap \tau_i H \tau_i^{-1}$, f уместо f_i, V уместо V_i и W уместо $\tau_i W$. Приметимо да је при овим ознакама и даље $V = \mathrm{Ind}_G^H W$. Наредно што ћемо показати је да можемо сматрати да је група I тривијална, што ће нам увелико олакшати посао.

Означимо са $\bar{G} = G/I$ и са $\bar{H} = H/I \cap H$. Ако покажемо да је $V^I = \mathrm{Ind}_{\bar{G}}^{\bar{H}} W^{I \cap H}$, коректно је редукујемо ситуацију $(\mathrm{mod}\ I)$ или ради једноставности записа да сматрамо да је група I тривијална. Посматрајмо хоморфизам $f : G \to W$. Тада је слика пресликавања f садржана у V^I ако и само ако је испуњено

$$f(x\tau) = f(x), \text{ за све } \tau \in I,$$

односно ако и само ако је f константна на косетима групе G/I сдесна. Тада је она константна и слева на косетима исте групе, што значи да је f пресликавање количничке групе $\bar{G} = G/I$. Како је испуњено

$$\tau f(x) = f(\tau x) = f(x), \text{ за све } \tau \in I \cap H,$$

закључујемо да је f узима вредности у векторском простору $W^{I \cap H}$. Одатле на основу дефиниције индуковане репрезентације следи тражено $V^I = \mathrm{Ind}_{\bar{G}}^{\bar{H}} W^{I \cap H}$.

5.корак– Завршетак доказа

Када смо се уверили у оправданост таквог корака, сматрајмо надаље да је група I тривијална. Тада је група G генерисана пресликавањем φ, $f = [G : H]$ и важи

$$V = \bigoplus_{i=0}^{f-1} \varphi^i W.$$

Фиксирајмо неку базу $\{w_1, w_2, \ldots, w_d\}$ векторског простора W. Означимо са A матрицу пресликавања φ^f у тој бази и са E јединичну матрицу димензије d. Тада матрица

$$\begin{bmatrix} 0 & E & 0 & \ldots & 0 \\ 0 & 0 & E & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & E \\ A & 0 & 0 & \ldots & 0 \end{bmatrix}$$

представља матрицу пресликавања φ у бази $\varphi^i w_j$ векторског простора V. Одатле налазимо да је

$$\det(\mathrm{Id} - \varphi X; V) = \det \begin{bmatrix} E & -XE & 0 & \dots & 0 \\ 0 & E & -XE & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -XE \\ -XA & 0 & 0 & \dots & E \end{bmatrix}. \tag{3.5}$$

Множећи прву колону матрице у формули (3.5) са X и додајући другој колони, затим множећи другу колону са X и додајући трећој и тако надаље закључно са множењем претпоследње колоне са X и додавањем последњој добијамо

$$\det(\mathrm{Id} - \varphi X; V) = \det(\mathrm{Id} - \varphi^f X^f; W),$$

чиме се коначно завршава доказ теореме.

□

Нека је L/K Галуаово раширење бројевних поља. Посматрајмо тривијалну подгрупу Галуаове групе $G(L/K)$. Очигледно је једини карактер који се може придружити репрезентацији такве тривијалне подгрупе тривијалан карактер $\chi = 1$. Њему индуковани карактер 1_* је тада једнак карактеру r_G регуларне репрезентације групе $G(L/K)$. На основу Теореме 3.3.1 (делови 1. и 3.), онда непосредно добијамо следећу значајну последицу.

Теорема 3.3.2. *Нека је L/K Галуаово раширење бројевних поља. Тада важи*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} \mathfrak{L}(L/K, \chi, s)^{\chi(1)},$$

при чему се производ узима по свим нетривијалним иредуцибилним карактерима χ придруженим репрезентацијама Галуаове групе $G(L/K)$, а $\chi(1)$ представља вредност карактера χ у неутралу групе $G(L/K)$.

Претходно приказана теорема представља први есенцијални састојак за испуњење нашег циља, а то је доказивање да се уопштене Дирихлеове L-функције не анулирају у тачки $s = 1$. Пут ка проналаску другог (и последњег) састојка започећемо једним малим историјским осврtом.

3.3.1 Артинова хипотеза (AHC)

Аустријско-амерички математичар Емил Артин започео је своје истраживање L-функција питајући се да ли за произвољно Галуаово раширење L/K бројевних поља

количник њихових Дедекиндових зета функција $\zeta_L(s)/\zeta_K(s)$ дефинише целу функцију у $\mathbb{C}$. Решавањем тог проблема дошао је до нове врсте L-функција, а то су управо L-функције назване по њему које смо посматрали у овом одељку. Откривањем тврђења приказаним у Теореми 3.3.2, Артин је закључио да се на питање да ли је функција $\zeta_L(s)/\zeta_K(s)$ цела одговор може дати у терминима новооткривених Артинових L-функција. Прецизније, наведени количник ће дефинисати целу функцију ако важи

Артинова хипотеза. *Артинова L-функција $\mathfrak{L}(L/K, \chi, s)$ придружена иредуцибилном нетривијалном карактеру χ неке репрезентације Галуаове групе $G(L/K)$ Галуаовог раширења L/K бројевних поља је цела функција у $\mathbb{C}$.*

Из саме чињенице да је претходно тврђење под називом „хипотеза" можемо закључити да Артин није успео да га докаже. Штавише, оно је у пуној општости остало недоказано до данас. Овде ће бити приказан доказ валидности хипотезе у специјалном случају када је раширење L/K Абелово. При томе, важнији од саме чињенице да Артинова хипотеза важи у случају комутативних Галуаових раширења, биће нам начин на који ћемо то доказати. Разлог таквог става крије се у чињеници да ћемо приликом доказа Артинове хипотезе за Абелова раширења довести у везу Артинове L-функције са уопштеним Дирихлеовим L-функцијама. Управо та веза ће представљати други есенцијални састојак за доказ Теореме 3.1.1.

Посматрајмо Абелово раширење L/K бројевних поља и означимо са $\mathfrak{f}$ његов кондуктор. Према Теореми 2.6.1 важи $J^{\mathfrak{f}}/H^{\mathfrak{f}} \cong G(L/K)$, при чему се изоморфизам остварује пресликавањем

$$\mathfrak{p} \to \left(\frac{L/K}{\mathfrak{p}}\right). \tag{3.6}$$

Посматрајмо иредуцибилни карактер χ Абелове групе $G(L/K)$, који је подсећања ради, хомоморфизам

$$\chi : G(L/K) \to \mathbb{C}^*.$$

Тада композиција карактера χ са изоморфизмом (3.6) представља карактер групе класа зрака по модулу $\mathfrak{f}$ тј. уопштени Дирихлеов карактер по модулу кондуктора $\mathfrak{f}$. Означимо тај индуковани карактер са $\tilde{\chi}$. Искористимо још исту ознаку коју смо користили пре формулисања дефиниције Артинове L-функције: за произвољан прост идеал $\mathfrak{p}$ у прстену целих $\mathscr{O}_K$ ознака $\varphi_{\mathfrak{P}}$ ће представљати Фробенијусов аутоморфизам придружен простом идеалу $\mathfrak{P}$ у прстену целих $\mathscr{O}_L$ који је изнад $\mathfrak{p}$. Такође, за такво $\mathfrak{P}$ групе декомпозиције и инерције ћемо означавати стандардно са $G(\mathfrak{P})$ и $I(\mathfrak{P})$. При овако дефинисаним ознакама важи следећа теорема.

Теорема 3.3.3. *Нека је L/K Абелово раширење бројевних поља, $\mathfrak{f}$ кондуктор тог расхирења, χ иредуцибилан карактер Галуаове групе $G(L/K)$ и $\tilde{\chi}$ њиме индукован уопштени Дирихлеов карактер по модулу $\mathfrak{f}$. Тада су Артинова L-функција придружена*

карактеру χ *и уопштена Дирихлеова* L*-функција придружена карактеру* $\bar{\chi}$ *повезане релацијом*

$$\mathfrak{L}(L/K,\chi,s)=L(s,\tilde{\chi})\prod_{\mathfrak{p}\in S}\frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}},$$

где је $\Re(s)>1$ *и* $S=\{\mathfrak{p}\mid \mathfrak{p}$ *је прост идеал у* $\mathscr{O}_K$ *и важи* $\mathfrak{p}\mid\mathfrak{f},\chi(I_{\mathfrak{P}})=1\}$.

Доказ. Ради што прегледнијег записа, уведимо и овде конвенцију коришћену приликом доказа Теореме 3.3.1, део3.
Репрезентација Галуаове групе $G(L/K)$ којој је придружен иредуцибилан нетривијалан карактер χ одређена је векторским простором $V=\mathbb{C}$ на кога $G(L/K)$ делује множењем са χ,

$$\sigma v=\chi(\sigma)v,\ \text{за све}\ \sigma\in G(L/K),v\in V.$$

Посматрајмо произвољан прост идеал $\mathfrak{p}$ у $\mathscr{O}_K$. Због чињенице да је $\mathfrak{f}$ кондуктор Абеловог раширења L/K, на основу Тврђења 2.6.2 следи да ако $\mathfrak{p}|\mathfrak{f}$, онда је идеал $\mathfrak{p}$ рамификован у $\mathscr{O}_L$. Одатле на основу Теореме 2.5.1 следи да група инерције $I(\mathfrak{P})$ простог идеала $\mathfrak{P}$ који је изнад $\mathfrak{p}$ у $\mathscr{O}_L$ не може бити тривијална. Због тога имамо раздвајање на два случаја:

- $\chi(I_{\mathfrak{P}})\neq\{1\}$
  Тада је $V^{I_{\mathfrak{P}}}=\{0\}$, па одговарајући члан за $\mathfrak{p}$ не постоји у Ојлеровом производу који дефинише Артинову L-функцију $\mathfrak{L}(L/K,\chi,s)$.
- $\chi(I_{\mathfrak{P}})=\{1\}$
  У овом случају је $V^{I_{\mathfrak{P}}}=\mathbb{C}$, па важи

$$\det(\mathrm{Id}-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{p})^{-s};V^{I_{\mathfrak{P}}})=1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}.$$

Сумирањем како се ова два случаја заједно са случајем када $\mathfrak{p}\nmid\mathfrak{f}$ одражавају на Артинову L-функцију придружену карактеру χ добијамо

$$\mathfrak{L}(L/K,\chi,s)=\prod_{\mathfrak{p}\mid\mathfrak{f}}\frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}}\prod_{\mathfrak{p}\in S}\frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}}.\tag{3.7}$$

Са друге стране, за уопштену Дирихлеову L-функцију придружену карактеру $\tilde{\chi}$ дефинисаном по модулу $\mathfrak{f}$ важи

$$L(s,\tilde{\chi})=\prod_{\mathfrak{p}\mid\mathfrak{f}}\frac{1}{1-\tilde{\chi}(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}.\tag{3.8}$$

Коначно, за $\mathfrak{p}\nmid\mathfrak{f}$ важи

$$\left(\frac{L/K}{\mathfrak{p}}\right)=\varphi_{\mathfrak{P}},$$

па имамо $\tilde{\chi}(\mathfrak{p})=\chi(\varphi_{\mathfrak{P}})$, одакле на основу једнакости (3.7) и (3.8) следи тражено тврђење. □

Из чињенице да се уопштене Дирихлеове L-функције могу аналитички проширити на целу комплексну раван, на основу Теореме 3.3.3 следи да се исто може урадити и за Артинове L-функције придружене карактерима репрезентација Галуаове групе *Абеловог* раширења бројевних поља L/K. Другим речима, Артинова хипотеза је тачна за комутативна раширења L/K бројевних поља. Међутим, једно је установити да аналитичко проширење неке функције или фамилије функција постоји, а сасвим друго је наћи експлицитан начин како да се оно изведе. Што се тиче Артинових L-функција, успостављање експлицититних једначина којима се оне проширују холоморфно до целе комплексне равни води путем који захтева дефинисање појма *Артиновог кондуктора*. Ипак, и поред изузетне интригантности коју нуди, наше даље излагање се неће кретати тим правцем. Уместо тога, извешћемо дуго очекивани доказ Теореме 3.1.1 за кога коначно имамо сав потребан алат.

3.3.2 Доказ Теореме 3.1.1

Пре извођења самог доказа најављеног у наслову пододељка подсетимо се укратко контекста у коме је она формулисана. Нека је K бројевно поље и $\mathfrak{m}$ модул у K. Карактер по модулу $\mathfrak{m}$, односно карактер групе класе зрака $J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})$ назива се уопштеним Дирихлеовим карактером. Њему придружени генераторни Дирихлеов ред

$$L(s,\chi) = \sum_{\mathfrak{a}\in J^{\mathfrak{m}}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}$$

називамо уопштеном Дирихлеовом L-функцијом придруженој карактеру χ. Пређимо сада на доказ Теореме 3.1.1 која тврди да се уопштена Дирихлеова L-функција придружена нетривијалном карактеру χ по модулу $\mathfrak{m}$ не анулира у тачки $s = 1$.

Доказ Теореме 3.1.1. Нека је бројевно поље L Абелово раширење бројевног поља K такво да је група класа зрака по модулу $\mathfrak{m}$ изоморфна Галуаовој групи $G(L/K)$ (за овакво поље L се каже да је *поље класа по модулу* $\mathfrak{m}$). Тада можемо χ интерпретирати као карактер Галуаове групе $G(L/K)$, па на основу Теореме 3.3.3 добијамо везу између уопштене Дирихлеове L-функције $L(s,\chi)$ и Артинове L-функције $\mathfrak{L}(L/K,\chi,s)$. Из те везе, због чињенице да функције $L(s,\chi)$ и $\mathfrak{L}(L/K,\chi,s)$ немају пол у тачки $s = 1$ закључујемо да је довољно показати да важи $\mathfrak{L}(L/K,\chi,1) \neq 0$.

Према Теореми 3.3.2 важи

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi\neq 1} \mathfrak{L}(L/K,\chi,s)^{\chi(1)}, \tag{3.9}$$

при чему је производ узет по свим нетривијалним иредуцибилним карактерима придруженим репрезентацијама Галуаове групе $G(L/K)$ и $\chi(1)$ вредност коју узима карактер χ у неутралу групе $G(L/K)$.

У примеру 3.1 установили смо да Дедекиндова зета функција придружена произвољном бројевном пољу има прост пол у тачки $s = 1$. Због тога функција са леве стране једнакости (3.9) има прост пол у тачки $s = 1$, па је такав и пол функције са десне стране те једнакости. Одатле следи да је испуњено

$$\prod_{\chi \neq 1} \mathfrak{L}(L/K, \chi, s)^{\chi(1)} \neq 0,$$

што значи да је $\mathfrak{L}(L/K, \chi, 1) \neq 0$, за све нетривијалне карактере χ. Тиме је доказ завршен. □

Напомена. *Приметимо да је приказани доказ Теореме 3.1.1 на који смо дуго чекали на крају испао веома једноставан. Разлог те једноставности поред употребе моћног алата Артинових L-функција персонификованог у применама Теореме 3.3.2 и Теореме 3.3.3 треба потражити и у самим доказима тих теорема. Наиме, приликом извођења наведених доказа, често смо се позивали на различите теореме и канонске изоморфизме који у одређеној мери чине саму срж веома велике и значајне теорије поља класа. Дакле, у доказу Теореме 3.1.1 сакривено је много, много изузетно узбудљиве и нетривијалне математике.*

ГЛАВА 4

Теореме о густини– Дирихлеа и Чеботарева

4.1 Појам Дирихлеове густине. Дирихлеова теорема о густини

Главни циљ овог поглавља је да се дефинише појам густине, као и да се докажу теореме о њеној егзистенцији. Као што смо већ рекли, интуитивно густину можемо видети као „меру простора"који у неком скупу идеала заузимају прости идеали. У складу са том интуитивном представом, природно се јавља идеја за посматрањем функције облика

$$\kappa_S(s) = \frac{\sum\limits_{\mathfrak{p}\in S} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum\limits_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}, \tag{4.1}$$

где је $s \in \mathbb{C}, \Re(s) > 1$, M скуп свих простих идеала прстена целих $\mathscr{O}_K$ бројевног поља K, а $S \subset M$ неки скуп простих идеала чија нас густина занима. При томе, од интереса нам је понашање функције κ_S кад се промењива s приближава вредности 1. Таквим разматрањем долазимо до следеће дефиниције Дирихлеове густине.

Дефиниција 4.1.1. *Нека је K бројевно поље, M скуп свих простих идеала његовог прстена целих и $S \subset M$ неки скуп простих идеала. Граничну вредност*

$$d(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}, \tag{4.2}$$

под условом да постоји, називамо ***Дирихлеовом густином*** *скупа S.*

Приметимо да због $\sum\limits_{\mathfrak{p}\in M} \frac{1}{\mathfrak{N}(\mathfrak{p})^s} \sim \log \frac{1}{s-1}$ показаног у примеру 3.1, Дирихлеову густину можемо записати и у облику

$$d(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathfrak{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}}.$$

Генерално говорећи, теореме густине се баве доказивањем егзистенције густине различитих скупова простих идеала. Користећи уопштене Дирихлеове L-функције, доказаћемо уопштену Дирихлеову теорему о густини, која разматра (прилично општи) контекст група класа зрака по неком модулу.

Теорема 4.1.1 (Уопштена Дирихлеова теорема о густини). *Нека је K бројевно поље, $\mathfrak{m}$ модул у K и $H^{\mathfrak{m}}$ група идеала таква да је*

$$\varsigma(K_{\mathfrak{m},1}) \subseteq H^{\mathfrak{m}} \subseteq J^{\mathfrak{m}}.$$

Тада за сваку класу $\mathfrak{k} \in J^{\mathfrak{m}}/H^{\mathfrak{m}}$ скуп $P(\mathfrak{k})$ простих идеала у $\mathfrak{k}$ има Дирихлеову густину

$$d(P(\mathfrak{k})) = \frac{1}{[J^{\mathfrak{m}} : H^{\mathfrak{m}}]}.$$

Доказ. Нека је χ уопштени Дирихлеов карактер по модулу $\mathfrak{m}$ и $L(s,\chi)$ одговарајућа уопштена Дирихлеова L-функција. Логаритмујући и развијајући у Тејлоров ред функцију $L(s,\chi)$ добијамо слично као у примеру 3.1

$$\log L(s,\chi) = \sum_{\mathfrak{p}\in M}\sum_{m=1}^{\infty} \frac{\chi(\mathfrak{p})}{m\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}\in M} \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{s}} + \sum_{\mathfrak{p}\in M}\sum_{m\geq 2} \frac{\chi(\mathfrak{p})}{m\mathfrak{N}(\mathfrak{p})^{ms}}.$$

Како је функција дефинисана сумом

$$\sum_{\mathfrak{p}\in M}\sum_{m\geq 2} \frac{\chi(\mathfrak{p})}{m\mathfrak{N}(\mathfrak{p})^{ms}}$$

очигледно аналитичка у тачки $s = 1$, имамо да важи

$$\log L(s,\chi) \sim \sum_{\mathfrak{p}\in M} \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{s}} = \sum_{\mathfrak{k}'\in J^{\mathfrak{m}}/H^{\mathfrak{m}}} \chi(\mathfrak{k}') \sum_{\mathfrak{p}\in\mathfrak{k}'} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}}.$$

Множећи са $\chi(\mathfrak{k}^{-1})$ и сумирајући по свим карактерима χ добијамо

$$\log \zeta_K(s) + \sum_{\chi\neq\chi_0} \chi(\mathfrak{k}^{-1}) \log L(s,\chi) \sim \sum_{\mathfrak{k}'\in J^{\mathfrak{m}}/H^{\mathfrak{m}}} \sum_{\chi} \chi(\mathfrak{k}'\mathfrak{k}^{-1}) \sum_{\mathfrak{p}\in\mathfrak{k}'} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}}.$$

За све $\chi \neq \chi_0$ важи $L(1,\chi) \neq 0$, па је $\log L(s,\chi)$ аналитичка у тачки $s = 1$. Како је испуњено

$$\sum_{\chi} \chi(\mathfrak{k}'\mathfrak{k}^{-1}) = \begin{cases} 0, & \text{ако је } \mathfrak{k}' \neq \mathfrak{k} \\ [J^{\mathfrak{m}} : H^{\mathfrak{m}}], & \text{ако је } \mathfrak{k}' = \mathfrak{k}, \end{cases}$$

добијамо коначно

$$\log \frac{1}{s-1} \sim \log \zeta_K(s) \sim [J^{\mathfrak{m}} : H^{\mathfrak{m}}] \sum_{\mathfrak{p} \in \mathfrak{k}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s},$$

чиме је теорема доказана.

□

Напомена. *Приметимо да је у претходном доказу од кључног значаја чињеница да је* $L(1, \chi) \neq 0$ *за све* $\chi \neq \chi_0$ *установљена Теоремом 3.1.1. Без ње се може доказати слабија верзија теореме, по којој густина ниједне од класа* $\mathfrak{k} \in J^{\mathfrak{m}}/H^{\mathfrak{m}}$ *не може бити већа од* $\frac{1}{[J^{\mathfrak{m}}:H^{\mathfrak{m}}]}$*. За доказ тог тврђења погледати [8].*

Уопштена Дирихлеова теорема о густини показује да је густина простих идеала једнака у свим класама од $J^{\mathfrak{m}}/H^{\mathfrak{m}}$. Другим речима, прости идеали су равномерно распоређени по свим класама. Специјални случај примене теореме у једноставном, али ипак значајном контексту приказан је следећим кратким примером.

Пример 4.1. Искористимо исте ознаке као у исказу Теореме 4.1.1 и применимо је у специјалног случају када је $H^{\mathfrak{m}} = \varsigma(K_{\mathfrak{m},1})$. Тада је $J^{\mathfrak{m}}/H^{\mathfrak{m}}$ ништа друго до група класа зрака по модулу $\mathfrak{m}$ и свака класа те групе представља класу зрака по модулу $\mathfrak{m}$. Онда из Теореме 4.1.1 добијамо да је густина простих идеала у свакој од класа зрака по модулу $\mathfrak{m}$ једнака и износи $\frac{1}{|J^{\mathfrak{m}}/\varsigma(K_{\mathfrak{m},1})|}$.
□

У наредном примеру видећемо једну ефективну примену теореме у контексту већ разматраном Примером 2.4 да бисмо открили чему она дугује свој назив Уопштена Дирихлеова теорема о густини, фокусирајући се пре свега на атрибут „уопштена".

Пример 4.2. Посматрајмо бројевно поље $K = \mathbb{Q}$ и главни идеал $\langle m \rangle$ његовог прстена целих $\mathscr{O}_K = \mathbb{Z}$ за неки позитиван цео број m. У примеру 2.4 установили смо да је група класа зрака по модулу $\langle m \rangle$ изоморфна са $(\mathbb{Z}/m\mathbb{Z})^*$, као и да класе зрака по модулу $\langle m \rangle$ можемо видети као аритметичке прогресије $a + m\mathbb{Z}, (a, m) = 1$. Са друге стране, на основу примера 4.1 знамо је да у свакој од класа зрака по модулу $\langle m \rangle$ густина простих идеала иста и износи $\frac{1}{|J^{\langle m \rangle}/\varsigma(K_{\langle m \rangle,1})|} = \frac{1}{|(\mathbb{Z}/m\mathbb{Z})^*|} = \frac{1}{\varphi(m)}$. Користећи чињеницу да је прстен целих $\mathbb{Z}$ поља $\mathbb{Q}$ које посматрамо главноидеалски, просте идеале прстена $\mathbb{Z}$ идентификујемо са његовим простим елементима. Дакле, у свакој класи зрака по модулу $\langle m \rangle$, односно артиметничкој прогресији $a + m\mathbb{Z}, (a, m) = 1$ има бесконачно много простих идеала, односно рационалних простих бројева и њихова густина је $\frac{1}{\varphi(m)}$. Закључујемо да смо применом Уопштене Дирихлеове теореме о густини добили Дирихлеову теорему о простим бројевима у аритметичкој прогресији, али и више него што класична Дирихлеова теорема тврди, а то је информација о густини простих бројева у одговарајућој аритметичкој прогресији. Управо то је разлог због

чега Теорема 4.1.1 представља уопштење Дирихлеове теореме о простим бројевима и објашњење откуда њено име.
□

4.2 Теорема Чеботарева о густини

Сада прелазимо на доказивање још једне теореме о густини, нарочито интересантне због тога што се бави произвољним Галуавим проширењима бројевних поља (не обавезно Абеловим). Пре саме формулације теореме, наведимо неколико лема које ће нам бити потребне за њено доказивање.

Лема 4.2.1. *Ако је S коначан скуп простих идеала у прстену целих $\mathscr{O}_K$ бројевног поља K тада S има Дирихлеову густину једнаку нули.*

Доказ. Тврђење следи одмах из чињенице да је

$$\sum_{\mathfrak{p}\in S} \frac{1}{\mathfrak{N}(p)^s} \sim 0$$

за коначан скуп простих идеала S и дефиниције Дирихлеове густине. □

Лема 4.2.2. *Означимо са S_1 скуп свих простих идеала прстена целих $\mathscr{O}_K$ бројевног поља K који имају релативни степен 1 над $\mathbb{Q}$. Претпоставимо да скуп S простих идеала у $\mathscr{O}_K$ има Дирихлеову густину $d(S)$. Тада је $d(S) = d(S \cap S_1)$.*

Доказ. За доказ ове леме погледати [8]. □

Лема 4.2.3. *Нека су S_1 и S_2 два дисјунктна скупа простих идеала прстена целих $\mathscr{O}_K$ бројевног поља K и нека је*

$$S = S_1 \amalg S_2.$$

Тада, ако постоји Дирихлеова густина барем од два скупова S, S_1, S_2, постоји и Дирихлеова густина трећег скупа и важи

$$d(S) = d(S_1) + d(S_2).$$

Доказ. Како је $S = S_1 \amalg S_2$, важи

$$\sum_{\mathfrak{p}\in S} \frac{1}{\mathfrak{N}(p)^s} = \sum_{\mathfrak{p}\in S_1} \frac{1}{\mathfrak{N}(p)^s} + \sum_{\mathfrak{p}\in S_2} \frac{1}{\mathfrak{N}(p)^s}. \tag{4.3}$$

Претпоставимо да постоје Дирихлеове густине скупова S и S_1. Тада је

$$\sum_{\mathfrak{p}\in S} \frac{1}{\mathfrak{N}(p)^s} \sim d(S) \log \frac{1}{s-1}$$

и

$$\sum_{\mathfrak{p}\in S_1}\frac{1}{\mathfrak{N}(p)^s}\sim d(S_1)\log\frac{1}{s-1}.$$

Последње уз формулу (4.3) даје

$$d(S)\log\frac{1}{s-1}\sim d(S_1)\log\frac{1}{s-1}+\sum_{\mathfrak{p}\in S_2}\frac{1}{\mathfrak{N}(p)^s},$$

одакле је

$$\sum_{\mathfrak{p}\in S_2}\frac{1}{\mathfrak{N}(p)^s}\sim (d(S)-d(S_1))\log\frac{1}{s-1},$$

што према дефиницији повлачи да је Дирихлеова густина скупа S_2 једнака

$$d(S_2)=d(S)-d(S_1).$$

Тиме је доказ завршен у једном случају, преостала два се показују аналогно. □

Лема 4.2.4. *Нека је L/K коначно раширење бројевних поља и $\mathscr{O}_L\supseteq\mathscr{O}_K$ њихови прстени целих. Онда постоји само коначно много простих идеала $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ који се гранају у прстену $\mathscr{O}_L$.*

Доказ. Погледати [5]. □

Вратимо се сада најављеној формулацији и доказивању још једне теореме о густини. Нека је L/K Галуаово раширење бројевних поља са Галуаовом групом $G=G(L/K)$. За свако $\sigma\in G$ посматрајмо скуп

$$P_{L/K}(\sigma)$$

свих нерамификованих простих идеала $\mathfrak{p}$ у K за које постоји прост идеал $\mathfrak{P}$ у L такав да $\mathfrak{P}\mid\mathfrak{p}$ и важи

$$\left(\frac{L/K}{\mathfrak{P}}\right)=\sigma,$$

где је $\left(\frac{L/K}{\mathfrak{P}}\right)$ Фробенијусов аутоморфизам за $\mathfrak{P}$ над K. Очигледно је да скуп $P_{L/K}(\sigma)$ зависи само од класе конјугације $[\sigma]$ аутоморфизма σ у групи G. На питање колика је његова густина одговор даје наредна теорема Чеботарева.

Теорема 4.2.1 (Чеботарев)**.** *Нека је L/K Галуаово раширење бројевних поља са Галуаовом групом $G=G(L/K)$. Онда за сваки аутоморфизам $\sigma\in G$ скуп*

$$P_{L/K}(\sigma)$$

има Дирихлеову густину која је одређена са

$$d(P_{L/K}(\sigma))=\frac{\#[\sigma]}{\#G}.$$

Доказ. Претпоставимо прво да је група G циклична и генерисана са σ. Нека је $\mathfrak{f}$ кондуктор раширења L/K и $H^{\mathfrak{f}}$ његова група класа. Онда према Теореми 2.6.1 важи $J^{\mathfrak{f}}/H^{\mathfrak{f}} \cong G(L/K)$. Означимо са $\mathfrak{k}$ класу у $J^{\mathfrak{f}}/H^{\mathfrak{f}}$ која одговара σ при том изоморфизму. Тада скуп $P_{L/K}(\sigma)$ чине тачно прости идеали $\mathfrak{p}$ који су у $\mathfrak{k}$. Користећи Дирихлеову теореми о густини, густину тог скупа рачунамо као

$$d(P_{L/K}(\sigma)) = \frac{1}{[J^{\mathfrak{f}} : H^{\mathfrak{f}}]} = \frac{1}{\#G} = \frac{\#[\sigma]}{\#G}.$$

Посматрајмо сада општи случај. Означимо са Σ фиксно поље аутоморфизма σ. Тада имамо ситуацију као на следећем дијаграму.

$$\begin{array}{c} L \\ | \\ \Sigma \\ | \\ K \end{array}$$

Ако је l ред од σ у G, онда из претходно показаног имамо да је

$$d(P_{L/\Sigma}(\sigma)) = \frac{1}{l}.$$

Дефинишимо два скупа идеала која ћемо посматрати:

- Означимо са $\mathfrak{P}$ прост идеал у L за кога постоји прост идеал $\mathfrak{p}$ из скупа $P_{L/K}(\sigma)$ такав да је испуњено $\mathfrak{P}|\mathfrak{p}$ и $\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma$. Скуп свих таквих простих идеала $\mathfrak{P}$ означимо са $\bar{P}(\sigma)$.

- Означимо са $\mathfrak{q}$ прост идеал који припада скупу $P_{L/\Sigma}(\sigma)$ и за кога је испуњено да су комплетирања $\Sigma_{\mathfrak{q}}$ и $K_{\mathfrak{p}}$ поља Σ, односно K, једнака, при чему је $\mathfrak{p}$ прост идеал из скупа $P_{L/K}(\sigma)$ и $\mathfrak{q}|\mathfrak{p}$. Скуп свих таквих простих идеала $\mathfrak{q}$ означимо са $P'_{L/\Sigma}(\sigma)$.

Приметимо да су претходно дефинисани скупови простих идеала $\bar{P}(\sigma)$ и $P'_{L/\Sigma}(\sigma)$ у обострано једнозначној кореспонденцији.

Направимо једну кратку дигресију у виду подсећања на теорију рамификације идеала. Нека је L/K коначно раширење бројевних поља. Прост идеал $\mathfrak{p}$ у $\mathscr{O}_K$ се потпуно цепа у прстену целих $\mathscr{O}_L$ бројевног поља L ако је

$$\mathfrak{p}\mathscr{O}_L = \mathfrak{P}_1\mathfrak{P}_2, \ldots, \mathfrak{P}_r,$$

где су $\mathfrak{P}_i, 1 \leq i \leq r$ међусобно различити прости идеали у $\mathscr{O}_L$, чији су степени инерције $f_i = [\mathscr{O}_L/\mathfrak{P}_i : \mathscr{O}_K/\mathfrak{p}]$ над $\mathfrak{p}$ сви једнаки 1 и $1 \leq r \leq [L : K]$.

Вратимо се сада доказу. Скуп $P'_{L/\Sigma}(\sigma)$ је очигледно подскуп скупа $P_{L/\Sigma}(\sigma)$ и садржи све идеале тог скупа који се потпуно цепају. Због тога за идеале који припадају скупу $P_{L/\Sigma}(\sigma) \setminus P'_{L/\Sigma}(\sigma)$, уколико таквих идеала има, важи да се или рамификују или имају степен инерције већи од 1. Међутим, имајући у виду четири леме којима смо започели овај одељак, такви идеали не утичу на густину, чиме добијамо

$$d(P'_{L/\Sigma}(\sigma)) = d(P_{L/\Sigma}(\sigma)) = \frac{1}{l}.$$

Посматрајмо сада сурјективно пресликавање

$$\rho : P'_{L/\Sigma}(\sigma) \to P_{L/K}(\sigma), \;\; \rho(\mathfrak{q}) = \mathfrak{q} \cap K.$$

Како је $P'_{L/\Sigma}(\sigma) \cong \bar{P}(\sigma)$, добијамо да за свако $\mathfrak{p} \in P_{L/K}(\sigma)$ важи

$$\rho^{-1}(\mathfrak{p}) = \{\mathfrak{P} \in \bar{P}(\sigma) \mid \mathfrak{P}|\mathfrak{p}\} \cong Z(\sigma)/\langle\sigma\rangle,$$

где је $Z(\sigma) = \{\theta \in G \mid \theta\sigma = \sigma\theta\}$ централизатор за σ у G. Коначно, одатле добијамо

$$d(P_{L/K}(\sigma)) = \frac{1}{[Z(\sigma) : (\sigma)]} d(P'_{L/\Sigma}(\sigma)) = \frac{l}{\#Z(\sigma)} \frac{1}{l} = \frac{\#[\sigma]}{\#G},$$

чиме је доказ завршен. □

4.3 Примери примена теореме Чеботарева

4.3.1 Природна густина и њен однос са Дирихлеовом густином

У овом одељку бавићемо се приказивањем неких интересантних примена теореме Чеботарева о густини доказане у претходном одељку. Ипак, пре преласка на саме примере, погледајмо прво алтернативну дефиницију густине и у каквом је она односу са Дирихлеовом густином.

Дефиниција 4.3.1. *Нека је S неки скуп простих идеала у прстену целих $\mathcal{O}_K$ бројевног поља K. Гранична вредност*

$$\delta(S) = \lim_{n\to\infty} \frac{\#\{\mathfrak{p} \in S \mid \mathfrak{N}(\mathfrak{p}) \leq n\}}{\#\{\mathfrak{p} \in M \mid \mathfrak{N}(\mathfrak{p}) \leq n\}},$$

под условом да постоји, назива се ***природном густином*** *скупа S.*

Из саме дефиниције претходне густине, јасно је да је она, посматрано у духу теорије вероватноће, веома природна. Отуда потиче и њен назив. Са друге стране, постоји и Дирихлеова густина, која је дефинисана у претходном одељку. Основна питања које се онда јављају у вези те две густине су питања њиховог односа, или прецизније:

- Да ли егзистеницијa једне густине повлачи егзистенцију друге?
- У случају да постоје обе врсте густине, да ли су њихове вредности једнаке?

Прве одговоре на та два важна питања пружа следећа теорема, чији ћемо доказ пружити у у потпуности у случају када је $K = \mathbb{Q}$, највише као илустрацију интересантне примене Теореме о простим бројевима.

Теорема 4.3.1. *Нека је S скуп простих идеала у прстену целих $\mathcal{O}_K$ бројевног поља K. Ако постоји природна густина $\delta(S)$ тог скупа, онда постоји и његова Дирихлеова густина $d(S)$ и важи*

$$\delta(S) = d(S).$$

Доказ Теореме 4.3.1 за поље рационалних бројева. Како разматрамо поље рационалних бројева, просте идеале његовог прстена целих $\mathbb{Z}$ можемо идентификовати са рационалним простим бројевима. Означимо скуп свих простих рационалних бројева са $\mathbb{P}$. Тада скуп S можемо видети као неки подскуп скупа $\mathbb{P}$. Уведимо ознаке

$$\begin{aligned} S(x) &= \#\{p \in S \mid p \leq x\}, \\ \pi(x) &= \#\{p \in \mathbb{P} \mid p \leq x\}, \\ p_n &= \begin{cases} 1, & \text{ако } n \in S \\ 0, & \text{ако } n \notin S \end{cases}, n \in \mathbb{N}. \end{aligned}$$

Приметимо прво да за сваки број $n \in \mathbb{N}$ важи

$$p_n = S(n) - S(n-1).$$

Чињеница да постоји природна густина скупа S значи егзистенцију граничне вредности

$$\lim_{x \to \infty} \frac{S(x)}{\pi(x)} = \delta. \tag{4.4}$$

На основу Теореме о простим бројевима важи

$$\pi(x) \sim \frac{x}{\log x}, \ x \to \infty,$$

па се релација (4.4) може записати као

$$\lim_{x \to \infty} \frac{S(x) \log x}{x} = \delta$$

или еквивалентно

$$S(x) \sim \frac{\delta x}{\log x}, \ x \to \infty \tag{4.5}$$

Са друге стране је

$$\begin{aligned}
\sum_{\substack{p\in S\\ p\le x}} \frac{1}{p^s} &= \sum_{1\le n\le x} \frac{p_n}{n^s} \\
&= \sum_{1\le n\le x} \frac{S(n)-S(n-1)}{n^s} \\
&= \sum_{1\le n\le x} \frac{S(n)}{n^s} - \sum_{1\le n\le x-1} \frac{S(n)}{(n+1)^s} \\
&= \frac{S(x)}{x^s} + \sum_{1\le n\le x-1} S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) \\
&= \frac{S(x)}{x^s} + \sum_{1\le n\le x-1} S(n)\int_n^{n+1} s\frac{1}{t^{s+1}}dt \\
&= \frac{S(x)}{x^s} + s\sum_{1\le n\le x-1} \int_n^{n+1} S(t)\frac{1}{t^{s+1}}dt, (\text{ јер је } S(x) \text{ константна на } [n,n+1)) \\
&= \frac{S(x)}{x^s} + s\int_1^x S(t)\frac{1}{t^{s+1}}dt.
\end{aligned}$$

Одатле следи да се Дирихлеова густина скупа S може израчунати као

$$d(S) = \lim_{s\to 1^+} \frac{\sum_{p\in S} \frac{1}{p^s}}{\log\frac{1}{s-1}} = \lim_{s\to 1^+} \frac{\lim_{x\to\infty}(\frac{S(x)}{x^s} + s\int_1^x S(t)\frac{1}{t^{s+1}}dt)}{\log\frac{1}{s-1}}.$$

Из релације (4.5) примењене на бројилац последње граничне вредности добијамо

$$d(S) = \lim_{s\to 1^+} \frac{\lim_{x\to\infty}\frac{\delta x}{x^s\log x} + s\int_1^\infty \frac{S(t)}{t^{s+1}}dt}{-\log(s-1)} = \lim_{s\to 1^+} \frac{\lim_{x\to\infty}\frac{\delta}{x^{s-1}\log x} + s\int_1^\infty \frac{S(t)}{t^{s+1}}dt}{-\log(s-1)}. \quad (4.6)$$

Како је при $s\to 1^+$ испуњено $s-1\ge 0$ важи

$$\lim_{x\to\infty} \frac{\delta}{x^{s-1}\log x} = 0,$$

па се на основу једнакости (4.6) Дирихлеова густина скупа S изражава као

$$d(S) = \lim_{s\to 1^+} \frac{s\int_1^\infty \frac{S(t)}{t^{s+1}}dt}{-\log(s-1)} = \lim_{s\to 1^+} \frac{\int_1^\infty \frac{S(t)}{t^{s+1}}dt}{-\log(s-1)}. \quad (4.7)$$

Поново користећи (4.5) добијамо да при $s\to 1^+$ важи

$$\int_1^\infty \frac{S(t)}{t^{s+1}}dt \sim \int_1^\infty \frac{\delta t}{t^2\log t}dt \sim \int_1^\infty \frac{1}{t\log t}dt = \infty,$$

што значи да је последња гранична вредност у (4.7) облика $\frac{\infty}{\infty}$, па се на њу може применити Лопиталова теорема. После примене Лопиталове теореме на последњу граничну вредност у (4.7) добијамо

$$d(S) = \lim_{s\to 1^+}(s-1)\int_1^\infty \frac{S(t)\log t}{t^{s+1}}dt.$$

Још једном применом (4.5) одатле следи

$$\begin{aligned} d(S) &= \lim_{s\to 1^+}(s-1)\int_1^\infty \frac{\delta t\log t}{t^{s+1}\log t}dt \\ &= \lim_{s\to 1^+}\delta(s-1)\int_1^\infty \frac{1}{t^s}dt \\ &= \lim_{s\to 1^+}\delta(s-1)(-\frac{1}{s-1}\frac{1}{t^{s-1}})\Big|_1^\infty \\ &= \lim_{s\to 1^+} -\delta(0-1^{s-1}) \\ &= \delta, \end{aligned}$$

што значи не само да постоји Дирихлеова густина скупа S, већ и да је онда једнака његовој природној густини, чиме је доказ теореме завршен. □

Теоремом 4.3.1 установљено је да сваки скуп простих идеала прстена целих бројевног поља који има природну густину мора имати и Дирихлеову густину, при чему су оне обавезно једнаке. Уколико би важила и обрнута веза тј. уколико би сваки скуп простих идеала који има Дирихлеову густину имао и једнаку природну густину, између појмова природне и Дирихлеове густине не би било суштинске разлике. Међутим, то није случај– постоје скупови простих идеала прстена целих бројевних поља који имају Дирихлеову густину, али чија природна густина не постоји. Један од најпознатијих примера таквог скупа је скуп P_1 свих рационалних простих бројева чија је прва цифра у декадном запису једнака 1. Бомбијери је показао да скуп P_1 нема природну густину, као и да је његова Дирихлеова густина једнака $\log_{10} 2$. За детаљније о овом примеру, као и објашњење дубљих аритметичких феномена који се иза њега крију погледати [1].

4.3.2 Артиново пресликавање је сурјективно

Приликом рада на дефинисању Артиновог пресликавања споменули смо да то пресликавање има особину сурјективности. На овом месту позабавићемо се доказивањем те значајне особине Артиновог пресликавања. При томе, основно средство у доказу неће бити директно Теорема Чеботарева, већ једна њена директна последица позната и као *Фробенијусова теорема о густини*. За њено формулисање неопходни су неки појмови из опште теорије група којима је посвећено наредних неколико дефиниција.

Дефиниција 4.3.2. *За два елеменента a и b групе G кажемо да су* ***квази-конјуговани*** *уколико су конјуговане цикличне групе њима генерисане.*

Дефиниција 4.3.3. ***Раздор*** *елемента a групе G је скуп свих елемената те групе који су квази-конјуговани са a.*

Претпоставимо да је a елемент реда n у групи G. Уочимо неки $b \in G$ који је квази-конјугован са a. По дефиницији, тада постоји неки елемент $\tau \in G$ такав да је

$$\langle b \rangle = \tau^{-1} \langle a \rangle \tau.$$

Последње је еквивалентно са чињеницом да постоји неки природан број m који је узајамно прост са n и за кога је испуњено

$$b = \tau^{-1} a^m \tau.$$

Према томе, раздор елемента a реда n у групи G можемо видети и као скуп свих елемената те групе који су конјуговани са неким a^m, при чему је m произвољан природан број који је узајамно прост са n.

После овог кратког излета у дефинисање неколико појмова из опште теорије група можемо прећи на формулисање Фробенијусове теореме о густини.

Теорема 4.3.2 (Фробенијус). *Нека је L/K Галуаово раширење бројевних поља и $G = G(L/K)$ одговарајућа Галуаова група. Уочимо произвољан аутоморфизам $\sigma \in G$ који има тачно t елемената у свом раздору. Означимо са $S(\sigma)$ скуп свих нерамификованих простих идеала $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ за које постоји прост идеал $\mathfrak{P}$ прстена целих $\mathscr{O}_L$ такав да $\mathfrak{P}|\mathfrak{p}$ и одговарајући Фробенијусов аутоморфизам $\left(\frac{L/K}{\mathfrak{P}}\right)$ припада раздору елемента σ. Тада скуп $S(\sigma)$ има Дирихлеову густину и она је једнака*

$$d(S(\sigma)) = \frac{t}{\#G}.$$

Напомена. *Приметимо да је Фробенијусова теорема о густини идентична Теореми Чеботарева у којој је услов „конјугован"замењен са „квази-конјугован". Према томе, теорема Фробенијуса је директна последица теореме Чеботарева. Међутим, начин излагања кога смо се држали није у складу са историјским токовима развоја теорије-теорема Фробенијуса била је позната много времена пре теореме Чеботарева. Штавише, није погрешно рећи да је доказ теореме Чеботарева представљао својеврстан историјски помак, јер је користио до тада непознате технике, пре свега Артинов закон реципроцитета.*[1]
Добар приказ директног доказа теореме Фробенијуса се може наћи у [8].

Користећи Теорему Фробенијуса о густини прилично једноставно и брзо доказујемо сурјективност Артиновог пресликавања.

[1] у оригиналном доказу своје теореме Чеботарев није користио овде приказане технике L-функција

Теорема 4.3.3. *Нека је L/K Абелово раширење бројевних поља и S произвољан коначан скуп простих идеала прстена целих $\mathscr{O}_K$ који садржи све просте идеале који су рамификовани у L. Означимо са I^S подгрупу групе I_K свих разломењих идеала прстена целих $\mathscr{O}_K$, генерисану свим ненула простим идеалима који су* ***изван*** *скупа S. Тада Артиново пресликавање $\varphi_{L/K}$ слика I^S сурјективно у Галуаову групу $G = G(L/K)$.*

Доказ. Уочимо произвољан елемент $\sigma \in G$. Како је раширење L/K Абелово, таква је и одговарајућа Галуаова група G, па се раздор елемента σ састоји тачно од генератора цикличне групе $\langle\sigma\rangle$. Према Фробенијусовој теореми о густини следи да скуп свих простих идеала $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ за које постоји прост идеал $\mathfrak{P}$ прстена целих $\mathscr{O}_L$ такав да $\mathfrak{P}|\mathfrak{p}$ и одговарајући Фробенијусов аутоморфизам $\left(\frac{L/K}{\mathfrak{P}}\right)$ припада раздору елемента σ има густину. Специјално, то значи да постоји бесконачно много простих идеала у $\mathscr{O}_L$ чији придружени Фробенијусов аутоморфизам генерише $\langle\sigma\rangle$. Због тога, како је скуп S коначан, можемо наћи прост идеал $\mathfrak{P}$ прстена целих $\mathscr{O}_L$ такав да Фробенијусов аутоморфизам $\left(\frac{L/K}{\sigma}\right)$ генерише $\langle\sigma\rangle$ и идеал $\mathfrak{p} = \mathfrak{P} \cap \mathscr{O}_K$ не припада скупу S. Према дефиницији Артиновог пресликавања, онда следи да $\varphi_{L/K}(\mathfrak{p})$ генерише $\langle\sigma\rangle$ или другим речима σ припада слици $\varphi_{L/K}(I^S)$ групе I^S при Артиновом пресликавању. Према томе, за произвољно $\sigma \in G$ смо показали да је у слици Артиновог пресликавања, што доказује сурјективност тог пресликавања.

□

4.3.3 Карактеризација Галуаових раширења бројевних поља помоћу простих идеала који се у њима цепају

У овом пододељку приказаћемо прилично директну и веома значајну примену теореме Чеботарева која ће се огледати у давању једне карактеризације Галуаових раширења бројевних поља. Поступак примене ћемо изводити поступно, у неколико раздвојених теорема и започињемо га са неким ознакама које ћемо користити.

1. За два скупа простих идеала S и T прстена целих бројевног поља K писаћемо

$$S \preceq T$$

уколико је сваки, осим евентуално коначно много елемената скупа S садржан у скупу T. Додатно, уколико је $S \preceq T$ и $T \preceq S$ писаћемо $S \approx T$.

2. Скуп свих простих идеала прстена целих $\mathscr{O}_K$ бројевног поља K означавамо са M_K.

3. Нека је L/K коначно раширење бројевних поља и $\mathfrak{p}$ произвољан прост идеал у прстену целих $\mathscr{O}_K$ бројевног поља K. Прост идеал $\mathfrak{p}$ се потпуно цепа у прстену целих $\mathscr{O}_L$ бројевног поља L ако је

$$\mathfrak{p}\mathscr{O}_L = \mathfrak{P}_1\mathfrak{P}_2, \ldots, \mathfrak{P}_r,$$

где су $\mathfrak{P}_i, 1 \leq i \leq r$ међусобно различити прости идеали у $\mathscr{O}_L$, чији су степени инерције $f_i = [\mathscr{O}_L/\mathfrak{P}_i : \mathscr{O}_K/\mathfrak{p}]$ над $\mathfrak{p}$ сви једнаки 1. Означимо са $P(L/K)$ скуп свих простих идеала $\mathfrak{p}$ у $\mathscr{O}_K$ таквих да постоји прост идеал $\mathfrak{P}$ у $\mathscr{O}_L$ који је степена 1 над $\mathfrak{p}$. Приметимо да у случају да је раширење L/K Галуаово, $P(L/K)$ није ништа друго до скуп свих простих идеала у $\mathscr{O}_K$ који се потпуно цепају у $\mathscr{O}_L$.

4. Подсетимо се још и ознаке већ коришћене у исказу Теореме Чеботарева о густини. Нека је L/K Галуаово раширење бројевних поља са Галуаовом групом $G = G(L/K)$ и $\sigma \in G$ произвољан аутоморфизам. Тада скуп свих нерамификованих простих идеала $\mathfrak{p}$ у $\mathscr{O}_K$ за које постоји прост идеал $\mathfrak{P}$ у $\mathscr{O}_L$ такав да $\mathfrak{P} \mid \mathfrak{p}$ и важи
$$\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma,$$
где је $\left(\frac{L/K}{\mathfrak{P}}\right)$ Фробенијусов аутоморфизам за $\mathfrak{P}$ над K обележавамо са $P_{L/K}(\sigma) \subseteq M_K$.

Тврђење које следи је техничке природе и даје значајну везу између скупова идеала уведених у 1. и 2. при Галуаовим раширењима $N/L/K$ бројевних поља.

Тврђење 4.3.1. *Нека је N/K Галуаово раширење бројевних поља и L међуполе, $K \subseteq L \subseteq N$. Означимо са $G = G(N/K)$ и $H = G(N/L)$ одговарајуће Галуаове групе. Тада је, при ознакама уведеним пре исказа теореме,*
$$P(L/K) \approx \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} P_{N/K}(\sigma),$$
при чему је $\coprod$ ознака за дисјунктну унију, а $[\sigma]$ представља класу конјугације аутоморфизма σ у групи G.

Доказ. Уочимо произвољан прост идеал у $\mathscr{O}_K$ који је нерамификован у L. Тада је $\mathfrak{p} \in P(L/K)$ ако и само ако постоји прост идеал $\mathfrak{P}$ у прстену целих $\mathscr{O}_N$ такав да $\mathfrak{P}|\mathfrak{p}$ и класа конјугације одговарајућег Фробенијусовог аутоморфизма $\left(\frac{N/K}{\mathfrak{P}}\right)$ у G садржи неки елемент који припада групи H. Другим речима, $\mathfrak{p}$ припада скупу $P(L/K)$ ако и само ако је $\mathfrak{p} \in P_{N/K}(\sigma)$ за неко $\sigma \in G$ такво да је $[\sigma] \cap H \neq \emptyset$. Одатле, уз Лему 4.2.4, одмах следи тврђење које треба доказати. □

Користећи Тврђење 4.3.1 у комбинацији са Теоремом Чеботарева можемо добити прилично прецизну оцену о густини скупа $P(L/K)$, као што показује наредно тврђење.

Тврђење 4.3.2. *Нека је L/K коначно раширење бројевних поља степена n. Тада за Дирихлеову густину скупа $P(L/K)$ важи*
$$d(P(L/K)) \geq \frac{1}{n}.$$

Додатно, важи еквиваленција

$$d(P(L/K)) = \frac{1}{n} \text{ ако и само ако је раширење } L/K \text{ Галуаово.}$$

Доказ. Нека је N/K Галуаово раширење бројевног поља K такво да је $K \subseteq L \subseteq N$ и нека су $G = G(N/K)$, $H = G(N/L)$ одговарајуће Галуаове групе. Према Тврђењу 4.3.1 важи

$$P(L/K) \approx \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} P_{N/K}(\sigma),$$

Одатле, према Теореми 4.2.1 Чеботарева, уз коришћење Леме 4.2.1 и Леме 4.2.3, добијамо

$$d(P(L/K)) = \sum_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} \frac{\#[\sigma]}{\#G} = \frac{1}{\#G} \#\Big(\coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} [\sigma] \Big). \tag{4.8}$$

Због чињенице да је

$$H \subseteq \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} [\sigma]$$

следи[2]

$$d(P(L/K)) \geq \frac{\#H}{\#G} = \frac{1}{n},$$

чиме је доказан први део тврђења.

Да бисмо доказали други део тврђења уочимо да је раширење L/K Галуаово ако и само ако је H нормална подгрупа групе G. Чињеница да је $H \lhd G$ еквивалентна је са затвореношћу те групе за конјуговање или другачије говорећи $H \lhd G$ ако и само ако за сваку класу конјугације $[\sigma]$ у G такву да је $[\sigma] \cap H \neq \emptyset$ важи $[\sigma] \subseteq H$. Због тога закључујемо и да је $H \lhd G$ ако и само се може написати као дисјунктна унија

$$H = \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} [\sigma].$$

Пратећи низ еквиваленција који смо извели добијамо да важи

$$L/K \text{ је Галуаово ако и само ако је } H = \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} [\sigma],$$

што уз једнакост (4.8) завршава доказ другог дела тврђења. □

[2] наравно, важи очигледно: ако је $A \preceq B$ тада је $d(A) \leq d(B)$.

Имајући у виду дефиницију скупа $P(L/K)$, Тврђење 4.3.2 можемо искористити да покажемо да не постоје коначна раширења бројевних поља у којима се скоро сви прости идеали потпуно цепају.

Тврђење 4.3.3. *Ако се L/K коначно раширење бројевних поља, такво да се скоро сваки прост идеал из $\mathscr{O}_K$ потпуно цепа у $\mathscr{O}_L$, онда је $L = K$.*

Доказ. Означимо са N нормално затворење поља L тј. најмање Галуаово раширење поља K које садржи L. У таквој ситуацији, ослањајући се на особине рамификације идеала, важи да се прост идеал $\mathfrak{p}$ у $\mathscr{O}_K$ потпуно цепа у раширењу L/K ако и само ако се тај идеал потпуно цепа у раширењу N/K.[3] Одатле закључујемо да за густине скупова $P(L/K)$ и $P(N/K)$ важи

$$d(P(L/K)) = d(P(N/K)).$$

Како се по претпоставци тврђења скоро сваки прост идеал из $\mathscr{O}_K$ потпуно цепа у $\mathscr{O}_L$, добијамо да је $d(P(L/K)) = 1$. Са друге стране, због тога што је раширење N/K Галуаово, на основу Тврђења 4.3.2 добијамо да важи $d(P(N/K)) = \frac{1}{[N:K]}$. Коначно, из једнакости густина скупова $P(L/K)$ и $P(N/K)$ онда следи да је

$$[N : K] = 1,$$

што значи да је $K = L = N$, чиме је тврђење доказано. □

Другачијом применом Тврђења 4.3.2 добијамо карактеризацију Галуаовог раширења L/K помоћу скупа $P(L/K)$. Она је описана наредном теоремом.

Тврђење 4.3.4. *Коначно раширење L/K бројевних поља је Галуаово ако и само ако се сваки прост идеал у скупу $P(L/K)$ потпуно цепа у L.*

Доказ. Ако је раширење L/K Галуаово онда се, као што смо приметили у приликом дефиниције скупа $P(L/K)$ у делу 2. на почетку овог пододељка, сваки прост идеал у $P(L/K)$ потпуно цепа у L. Дакле, једна импликација еквиваленције коју треба показати важи, само треба још доказати другу.

Претпоставимо да се сваки прост идеал у скупу $P(L/K)$ потпуно цепа у L и означимо са N нормално затворење поља L. Из потпуно истих разлога као у доказу Тврђења 4.3.3, имамо да се скуп $P(N/K)$ састоји тачно од простих идеала прстена целих $\mathscr{O}_K$ који се потпуно цепају у L. Из претпоставке о идеалима скупа $P(L/K)$ којом смо започели наше разматрање онда следи да је $P(N/K) = P(L/K)$, па су специјално и густине та два скупа једнаке. Из Тврђења 4.3.2, пошто је раширење N/K Галуаово имамо

$$d(P(N/K)) = \frac{1}{[N : K]},$$

[3] упутство како доказати то тврђење може се наћи у [14]

док применом истог тврђења за коначно раширење L/K закључујемо да је

$$d(P(L/K)) \geq \frac{1}{[L:K]}.$$

Тада, због установљене једнакости густина скупова $P(L/K)$ и $P(N/K)$ добијамо да је

$$[N:K] \leq [L:K],$$

одакле закључујемо да је $L = N$, што значи по дефиницији поља N да је L Галуаово над K. Тиме је доказана и друга импликација еквиваленције коју је требало доказати. □

Наредно тврђење приказује карактеризацију односа произвољног коначног и Галуаовог раширења бројевног поља у терминима одговарајућих скупова идеала које смо дефинисали у делу 2. на почетку овог пододељка.

Тврђење 4.3.5. *Нека је L/K Галуаово, а M/K коначно раширење бројевног поља K. Тада важи еквиваленција*

$$P(L/K) \succeq (M/K) \text{ ако и само ако је } L \subseteq M.$$

Доказ. Ако је $L \subseteq M$, онда их дефиниције скупова $P(L/K)$ односно $P(M/K)$, одмах следи $P(L/K) \succeq P(M/K)$. Према томе, потребно је доказати само обратну импликацију да би се завршио доказ тврђења.

Претпоставимо да је $P(L/K) \succeq P(M/K)$. Уочимо Галуаово раширење N/K које садржи поља L и M и означимо са $G = G(N/K), H = G(N/L)$ и са $H' = G(N/M)$ одговарајуће Галуаове групе. Пошто су раширења N/K и L/K Галуаова, због $L \subseteq N$ важи да је $H \triangleleft G$. Такође је

$$P(M/K) \approx \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H' \neq \emptyset}} P_{N/K}(\sigma) \preceq P(L/K) \approx \coprod_{\substack{\sigma \in G \\ [\sigma] \cap H \neq \emptyset}} P_{N/K}(\sigma).$$

Уочимо произвољно $\sigma \in H'$. Тада је према Теореми 4.2.1 Чеботарева скуп $P_{N/K}(\sigma)$ бесконачан, па постоји $\mathfrak{p} \in P_{N/K}(\sigma)$ такво да је $\mathfrak{p} \in P_{N/K}(\tau)$, за $\tau \in G$ такво да је $[\tau] \cap H \neq \emptyset$. Тада је елемент σ конјугован са τ, па како је H нормална подгрупа групе G, налазимо да је $[\sigma] = [\tau] \subseteq H$. Одатле је $H' \subseteq H$, па је и $L \subseteq M$, чиме је доказ завршен. □

Све до сада показано у овом пододељку сумирано је у облику наредне теореме.

Теорема 4.3.4. *Галуаово раширење бројевних поља L/K јединствено одређује скуп $P(L/K)$ простих идеала који се у њему потпуно цепају.*

Теорема 4.3.4 представља почетно тврђење знатно већег програма чији је циљ карактеризација Галуаових раширења произвољног бројевног поља K, заједно са свим алгебарским и аритметичким својствима која она имају, преко простих идеала прстена целих $\mathscr{O}_K$. Наредни корак на развијању овог програма било би давање карактеризације скупа простих идеала $P(L/K)$ искључиво у терминима идеала прстена целих базног поља K. У случају да је раширење L/K Абелово, тражену карактеризацију пружа теорија поља класа. Међутим, за неабелова раширења L/K она есенцијално није позната. Решење тог проблем само по себи представља делић много дубљег и за теорију бројева веома значајног програма који се назива *Лангландски програм*.

4.3.4 Лежандров симбол и Дирихлеова густина

Нека је p прост непаран рационалан број и $a \in \mathbb{Z}$ цео број. Тада се *Лежандров симбол* за a и p, у ознаци $\left(\frac{a}{p}\right)$, дефинише у зависности од тога да ли конгруенција

$$x^2 \equiv a \pmod{p} \tag{4.9}$$

има решења у пољу $\mathbb{Z}/p\mathbb{Z}$, на следећи начин

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако } p \nmid a \text{ и конгруенција (4.9) има решења у пољу } \mathbb{Z}/p\mathbb{Z} \\ -1, & \text{ако } p \nmid a \text{ и конгруенција (4.9) нема решења у пољу } \mathbb{Z}/p\mathbb{Z} \\ 0, & \text{ако } p \mid a. \end{cases}$$

Поред дефиниције Лежандровог симбола подсетимо се у каквој је он вези са рамификацијом рационалних простих бројева у квадратним бројевним пољима. Посматрајмо поље рационалних бројева $\mathbb{Q}$ и његово квадратно раширење $K = \mathbb{Q}(\sqrt{D})$, где је $D \in \mathbb{Z}$ бесквадратан цео број. Тада за произвољан прост број $p \in \mathbb{Q}$, због $[K : \mathbb{Q}] = 2$, постоје само три следеће могућности:

1. $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}'$,
   где су $\mathfrak{p}$ и $\mathfrak{p}'$ различити прости идеали у прстену целих $\mathscr{O}_K$. У овом случају се p (идеал $p\mathbb{Z}$) потпуно цепа у прстену целих $\mathscr{O}_K$.

2. $p\mathscr{O}_K$ је прост идеал у прстену целих $\mathscr{O}_K$. У овом случају је p (идеал $p\mathbb{Z}$) инертан у прстену целих $\mathscr{O}_K$.

3. $p\mathscr{O}_K = \mathfrak{p}^2$,
   за неки прост идеал $\mathfrak{p}$ прстена целих $\mathscr{O}_K$. У овом случају се p (идеал $p\mathbb{Z}$) рамификује у прстену целих $\mathscr{O}_K$.

Три претходно наведена случаја могу се окарактерисати помоћу Лежандровог симбола за D и p и то на следећи начин:

$$\left(\frac{D}{p}\right) = \begin{cases} 1, & \text{ако и само ако је случај 1.} \\ -1, & \text{ако и само ако је случај 2.} \\ 0, & \text{ако и само ако је случај 3.} \end{cases}$$

Имајући у виду шта је експлицитно случај 1. добијамо одмах наредно тврђење.

Тврђење 4.3.6. *Нека је K квадратно бројевно поље, $K = \mathbb{Q}(\sqrt{D})$, где је $D \in \mathbb{Z}$ бесквадратан цео број. Тада, за сваки рационалан прост број p, прост идеал $p\mathbb{Z}$ се потпуно цепа у прстену целих $\mathscr{O}_K$ ако и само ако је испуњено*

$$\left(\frac{D}{p}\right) = 1.$$

Претходна теорема има у конјукцији са Тврђењем 4.3.2 из претходног пододељка једну прилично интересантну директну последицу. Посматрајмо квадратно бројевно поље $K = \mathbb{Q}(\sqrt{D})$. Тада је очигледно K Галуаово над $\mathbb{Q}$.[4] Због тога се скуп $P(K/\mathbb{Q})$ састоји тачно од простих идеала у прстену $\mathbb{Z}$ који се потпуно цепају у $\mathscr{O}_K$. Користећи Тврђење 4.3.6, због чињенице да је $K/\mathbb{Q}$ Галуаово добијамо

$$d(P(K/\mathbb{Q})) = \frac{1}{[K:\mathbb{Q}]} = \frac{1}{2}.$$

Са друге стране, Тврђење 4.3.6 елементе скупа $P(K/\mathbb{Q})$, односно просте идеале у прстену $\mathbb{Z}$ који се потпуно цепају у $\mathscr{O}_K$, идентификује као рационалне просте бројеве p за које је

$$\left(\frac{D}{p}\right) = 1.$$

Одатле директно добијамо следеће тврђење.

Тврђење 4.3.7. *Нека је D бесквадратан цео број. Тада скуп свих простих бројева p таквих да је*

$$\left(\frac{D}{p}\right) = 1$$

има Дирихлеову густину једнаку $\frac{1}{2}$.

[4] раширење поља степена 2 је Галуаово, осим евентуално у случају поља карактеристике 2. Наравно, K је као бројевно поље карактеристике 0

ГЛАВА 5

Асимптотски поглед на теорему Чеботарева

На самом почетку поглавља уведимо стандардне ознаке за неколико различитих асимптотских релација које ћемо користити како у овом поглављу, тако и у току нашег даљег излагања.

Нека су f и g две реалне функције променљиве x, дефинисане на скупу $D \subseteq \mathbb{R}$, који садржи неку околину тачке $+\infty$.

- Пишемо $f(x) = O\left(g(x)\right)$, или еквивалентно, $f(x) \ll g(x)$, односно $g(x) \gg f(x)$, ако постоји позитиван реалан број M такав да је

  $$|f(x)| \leq Mg(x),$$

  за све $x \in D$. Додатно, писаћемо $f(x) = O_C\left(g(x)\right)$, или еквивалентно, $f(x) \ll_C g(x)$, односно $g(x) \gg_C f(x)$, уколико је M функција која зависи од неке величине C.

- Пишемо $f(x) \asymp g(x)$ уколико је

  $$f(x) \ll g(x) \quad \text{и} \quad g(x) \ll f(x).$$

- Пишемо $f(x) = o\left(g(x)\right)$ ако је

  $$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

- Пишемо $f(x) \sim g(x)$ ако је

  $$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

- Са $\operatorname{li} x$ ћемо означавати логаритамски интеграл,

  $$\operatorname{li} x = \int_2^x \frac{1}{\log t} dt.$$

Када су уведене претходне значајне ознаке, можемо кренути на пут посматрања Теореме Чеботарева о густини другачијим, „асимптотским" очима. Подсетимо се прво контекста у коме је та теорема дефинисана.

5.1 Ефективна верзија теореме Чеботарева о густини

Посматрајмо Галуаово раширење L/k бројевних поља са Галуаовом групом G. Нека је $\sigma \in G$ произвољан $k-$аутоморфизам поља L. Означимо са

$$P_{L/k}(\sigma)$$

скуп свих нерамификованих простих идеала $\mathfrak{p}$ у k за које постоји прост идеал $\mathfrak{P}$ у L такав да $\mathfrak{P} \mid \mathfrak{p}$ и важи

$$\sigma = \mathrm{Fr}_{\mathfrak{p}}\,.$$

Теорема 4.2.1 показује да скуп $P_{L/k}(\sigma)$ има Дирихлеову густину, која је једнака $\frac{|[\sigma]|}{|G|}$, где је $[\sigma]$ ознака за класу конјугације аутоморфизма σ у Галуаовој групи G. Наравно, уместо само једне класе конјугације, можемо посматрати произвољан скуп $C \subseteq G$ који је инваријантан за конјуговање, и тада је одговарајућа Дирихлеова густина једнака $\frac{|C|}{|G|}$.

Тиме је приказан класичан облик Теореме Чеботарева, на начин изведен у претходној глави. Оно што нам је од интереса у овом поглављу је да теорему гледамо у другачијем светлу, као асимптотску релацију неке за ту сврху дефинисане функције (отуди и најава „асимптотског" погледа). Задржимо C за ознаку подскупа од G који је стабилан у односу на конјугацију и дефинишимо за све реалне x

$$\pi_C(x, L/k) = \#\left\{\mathfrak{p} \mid \mathfrak{p} \in P_{L/k}(\sigma) \text{ за неко } \sigma \in C \text{ и } \mathfrak{N}(\mathfrak{p}) \leq x\right\}.$$

Смисао функције $\pi_C(x, L/k)$ је у следећем: у њеној дефиницији остају садржана сва алгебарско/аритметичка својства скупа $P_{L/k}(\sigma)$ на који се примењује Теорема Чеботарева (управо та добро сложена својства дају значај теореми Чеботарева и од њих не одустајемо), али за разлику од скупа $P_{L/k}(\sigma)$ више не посматрамо све просте идеале са наведеним својствима, него само оне чија норма не прелази x. На тај начин, реалну променљиву x од које зависи реална функција $\pi_C(x, L/k)$ можемо видети и као параматер чијим варирањем можемо на посредан начин, испитујући функцију $\pi_C(x, L/k)$, да откривамо особине иначе не лако приступачног скупа идеала, попут $P_{L/k}(\sigma)$. Једна од најзначајнијих особина функције $\pi_C(x, L/k)$ је њена асимптотика, односно понашање те функције када x постаје неограничено велики реалан број. Управо је то особина о којој нам теорема Чеботарева може дати информацију и која представља „асимптотски" поглед на саму теорему. Наиме, имајући у виду дефиницију Дирихлеове густине, као и дефиницију функције $\pi_C(x, L/k)$, на основу Теореме Чеботарева имамо да када $x \to \infty$ важи

$$\pi_C(x, L/k) \sim \frac{|C|}{|G|} \operatorname{li} x. \tag{5.1}$$

Последња релација омогућава да за довољно велике вредности променљиве x вредности функције $\pi_C(x, L/k)$ које је тешко рачунати, апроксимирамо вредношћу интеграла $\operatorname{li} x$ (скалираног константом $\frac{|C|}{|G|}$). Наравно, приликом такве апроксимације чинимо одређену грешку, па се сасвим природно намеће питање давања оцене те грешке. Другим речима, заинтересовани смо за верзију релације (5.1) која поред саме апроксимације функције $\pi_C(x, L/k)$ пружа и оцену грешке приликом те апроксимације. Такву верзију називамо *ефективном*. Имајући у виду да релација (5.1) није ништа друго до теорема Чеботарева, оно чиме ћемо се бавити је давање *ефективне верзије теореме Чеботарева*. Битно је нагласити да постоји више различитих ефективних верзија теореме Чеботарева у зависности од тога које додатне хипотезе претпоставимо. Претпоставке које ћемо ми користити су:

- Генерализована Риманова хипотеза (GRH)
- Артинова Хипотеза (AHC)
- Хипотеза о корелацији парова (PCC)

О Артиновој хипотези речено је нешто у пододељку 3.3.1; за више везано за Хипотезу о корелацији парова погледати Додатак који се налази на крају овог рада, после целокупног главног тока излагања, док се више о Генерализованој Римановој хипотези може пронаћи у [7].

5.1.1 Оцена дискриминанте бројевног поља

Пре приказивања првог облика ефективне верзије теореме Чеботарева, наведимо неколико оцена везаних за дискриминанте бројевних поља које ћемо користити. Пре самог почетка излагања, нагласимо да су оцене које ћемо извести *глобалне*. Поред њих, постоје и *локалне* оцене, чији се детаљан приказ може пронаћи у [16].

Означимо са d_k, односно d_L апсолутне вредности дискриминанти бројевних поља k и L. Степене k и L над $\mathbb{Q}$ означимо редом са n_k и n_L. Под $\mathcal{P}(L/k)$ ћемо подразумевати скуп свих рационалних простих бројева p за које постоји прост број $\mathfrak{p}$ у k такав да $\mathfrak{p} \mid p$ и $\mathfrak{p}$ је рамификован у раширењу L/k. Приметимо да је скуп $\mathcal{P}(L/k)$ коначан. Уз претходно наведене ознаке дефинишимо

$$M(L/k) = |G| d_k^{1/n_k} \prod_{p \in \mathcal{P}(L/k)} p.$$

Даље, означимо са $\partial_{L/k}$ релативну дискриминанту раширења L/k. Тада из алгебарске теорије бројева знамо да је $\partial_{L/k}$ један ненула идеал прстена целих $\mathscr{O}_k$, као и да важи

$$d_L = (d_k)^n \mathfrak{N}(\partial_{L/k}), \tag{5.2}$$

при чему је $n = [L : k] = n_L/n_k$. Оно чиме ћемо се бавити је давање оцене вредности норме $\mathfrak{N}(\partial_{L/k})$ релативне дискриминанте $\partial_{L/k}$ раширења L/k, као и апсолутних вредности дискриминанти d_k и d_L самих бројевних поља L и k.

У ту сврху, приметимо прво да логаритмујући формулу (5.2) добијамо релацију

$$\log d_L = n \log d_k + \log \mathfrak{N}(\partial_{L/k}), \tag{5.3}$$

која на једноставан, стога и веома значајан начин, повезује вредности d_k, d_L и $\partial_{L/k}$. Уз наведене ознаке важи следећа теорема.

Теорема 5.1.1. *Имајући у виду претходне ознаке важи оцена*

$$\log \mathfrak{N}(\partial_{L/k}) \leq n_L \left(1 - \frac{1}{n}\right) \sum_{p \in \mathcal{P}(L/k)} \log p + n_L \left|\mathcal{P}(L/k)\right| \log n.$$

Доказ. Приказаћемо кратку скицу доказа теореме. Нагласимо прво да се сам доказ у великој мери ослања на *локалне* оцене дискриминанти бројевних поља.
Уочимо неки коначан прост број $\mathfrak{p}$ у бројевном пољу k. Подсећања ради, $\mathfrak{p}$ је тада класа еквиваленције релације еквивалентности на скупу свих валуација на k; означимо једног представника те класе са v. Приметимо да је, због тога што је прост број $\mathfrak{p}$ коначан, v једна неархимедова валуација на k. Са друге стране, прост број $\mathfrak{p}$ можемо видети и као један идеал прстена целих $\mathscr{O}_k$ бројевног поља K. Резидуално поље

$$\mathscr{O}_k/\mathfrak{p}$$

је коначно; означимо његову карактеристику са p_v и број елемената са $\mathfrak{N}_v$. Тада важи

$$\mathfrak{N}_v = \mathfrak{N}(\mathfrak{p}) = (p_v)^{f_v},$$

где је f_v број који се назива *резидуални степен* валуације v. Додатно, дефинишимо индекс рамификације e_v за v са

$$e_v = v(p_v).$$

Највећи део доказа теореме се састоји у примени једне од локалних оцена дискриминанти бројевних поља да се добије оцена

$$\log \mathfrak{N}(\partial_{L/k}) \leq \sum_{v \in V(L/k)} \left((n-1) f_v \log p_v + n f_v e_v \log n\right), \tag{5.4}$$

где је $V(L/k)$ скуп свих међусобно нееквивалентних, неархимедових валуација на k за које је $v(\partial_{L/k}) > 0$. Даље, за све просте бројеве p важи да

$$\sum_{p_v = p} f_v e_v = n_k,$$

као и

$$\sum_{p_v=p} f_v \leq n_k.$$

Коришћењем последње две чињенице у комбинацији са формулом (5.4) добијамо

$$\log \mathfrak{N}(\partial_{L/k}) \leq n_k\,(n-1) \sum_{p\in\mathcal{P}(L/k)} \log p + nn_k\,|\mathcal{P}(L/k)|\log n,$$

одакле због $n_L = nn_k$ следи тражено тврђење. □

Директним коришћењем формуле (5.3) претходна теорема добија следећи облик.

Последица 5.1.1. *Уз исте ознаке као у Теореми 5.1.1 важи оцена*

$$\log d_L \leq n\log d_k + n_L\left(1-\frac{1}{n}\right)\sum_{p\in\mathcal{P}(L/k)} \log p + n_L\,|\mathcal{P}(L/k)|\log n.$$

Поред приказаног општег случаја када је раширење L/k коначно, можемо разматрати и случај када је то раширење Галуаово. Одговарајућа оцена у наведеној ситуацији је описана наредном теоремом.

Теорема 5.1.2. *Уз исте ознаке као у Теореми 5.1.1, ако је раширење L/k Галуаово, важи оцена*

$$\log \mathfrak{N}(\partial_{L/k}) \leq n_L\left(1-\frac{1}{n}\right)\sum_{p\in\mathcal{P}(L/k)} \log p + n_L\log n.$$

Доказ. Доказ ове теореме је у великој мери аналоган доказу Теореме 5.1.1 и изводи се коришћењем одговарајуће локалне оцене. Детаљи се могу пронаћи у [16]. □

Још једна ствар коју можемо приметити је да се цео контекст у коме је посматрана Теорема 5.1.1 може лако сузити на једноставнији контекст једног бројевног поља. У ту сврху довољно је посматрати случај када је $k = \mathbb{Q}$. Тада свака од претходних теорема добија своју верзију у контексту само једног бројевног поља (оно може, али не мора бити Галуаово над $\mathbb{Q}$), од којих ћемо само ми навести само верзију која ће бити од значаја касније, приликом рада на Фробенијусовом пољу елиптичих кривих.

Последица 5.1.2. *Нека је L бројевно поље степена n_L над $\mathbb{Q}$ такво да је $L/\mathbb{Q}$ Галуаово. Нека је d_L апсолутна вредност дискриминанте од L и $\mathcal{P}(L/\mathbb{Q})$ скуп рационалних бројева који се рамификују у $L/\mathbb{Q}$. Тада је*

$$\log d_L \leq (n_L-1)\sum_{p\in\mathcal{P}(L/\mathbb{Q})} \log p + n_L\log n_L.$$

За крај овог пододељка, погледајмо још један занимљив пример у коме је приказан случај када се у неједнакости одређеној Последицом 5.1.2 достиже једнакост.

Пример 5.1. Нека је p прост рационалан број и m цео број, $m \geq 1$. Нека је π такво да је $\pi^{p^m} = p$ и $L = \mathbb{Q}(\pi)$. Тада важи (у ознакама истим као код Теореме 5.1.1) да је $n_L = p^m$ и $\mathcal{P}(L/\mathbb{Q}) = \{p\}$. Због тога, ако означимо стандардно са d_L апсолутну вредност дискриминанте од L, на основу Теореме 5.1.1 имамо да је

$$\log d_L \leq (p^m - 1)\log p + p^m \log p^m,$$

што је еквивалентно са

$$\log d_L \leq (p^m(m+1) - 1)\log p. \tag{5.5}$$

Са друге стране, краћи рачун показује да за дискриминанту d_L бројевног поља L важи

$$d_L = p^{mp^m + p^m - 1} = p^{p^m(m+1)-1}.$$

Логаритмујући последњу једнакост добијамо да је

$$\log d_L = (p^m(m+1) - 1)\log p,$$

што показује да се формули 5.5, потеклој од Теореме 5.1.1, достиже једнакост.

5.1.2 Приказ неколико ефективних верзија теореме Чеботарева о густини

Први облик ефективне верзије теореме Чеботарева, даћемо под претпоставком GRH. Он је описан наредном теоремом.

Теорема 5.1.3. *Претпоставимо да за Дедекиндову зета функцију бројевног поља L важи* GRH. *Тада, при $x \to \infty$ важи*

$$\pi_C(x, L/k) = \frac{|C|}{|G|}\operatorname{li} x + O\left(|C|x^{\frac{1}{2}}\left(\frac{\log|d_L|}{n_L} + \log x\right)\right).$$

Притом је апсолутна O-константа апсолутна.

Доказ. Погледати [16]. □

Ако уз GRH претпоставимо и AHC, можемо извести бољу оцену за грешку у ефективној верзији теореме Чеботарева него што је она дата претходном теоремом. Таква, другачија ефективна верзија теореме Чеботарева се суштински базира на једном тврђењу чије је формулисање и доказивање у неким сегментима изван граница овог рада. Ипак, због његовог изузетног значаја, приказаћемо формулацију и скицу доказа наведеног тврђења.

Кренимо прво са неким ознакама које су од значаја, а нисмо их користили до сада. Нека је χ карактер Галуаове групе $G = G(L/k)$ и $\chi(1)$ вредност коју тај карактер узима

у неутралу групе G. Означимо са $\delta(\chi)$ вишеструкост коју има тривијални карактер у χ. Карактеру χ можемо придружити један идеал који се назива *Артинов кондуктор* и обележава са $\mathfrak{f}_\chi$. Детаљно о Артиновом кондуктору може се пронаћи у [14]; оно што је овде од значаја је вредност

$$A_\chi = d_K^{\chi(1)} \mathfrak{N}(\mathfrak{f}_\chi).$$

Уз A_χ посматрамо и функцију $\pi(x, \chi)$ независно промењиве x, дефинисану као суму

$$\pi(x, \chi) = \sum_{\mathfrak{N}(\mathfrak{p}) \leq x} \chi(\mathrm{Fr}_\mathfrak{p}),$$

узету по свим простим бројевима $\mathfrak{p}$ у k, норме мање од x. Користећи претходно уведене ознаке имамо наредно тврђење.

Тврђење 5.1.1. *Претпоставимо да је Артинова L-функција придружена карактеру χ аналитичка за све $s \neq 1$ и ненула за $\Re(s) \neq \frac{1}{2}, 0 < \Re(s) < 1$. Тада је*

$$\pi(x, \chi) = \delta(\chi) \operatorname{li} x + O\left(x^{\frac{1}{2}} \left(\log A_\chi + \chi(1) n_k \log x\right)\right) + O\left(\chi(1) n_k \log M(L/k)\right).$$

Доказ. Прикажимо детаљну скицу доказа. Иницијална поставка се састоји у посматрању функције

$$\Lambda(s, \chi) = A_\chi^{\frac{s}{2}} \gamma(s) \mathfrak{L}(s, \chi)$$

комплексно промењиве s, при чему је $\gamma(s)$ одређена функција која се изражава као производ степена π и $\Gamma-$функција. Кључне за доказ тврђења су особине које поседује функција $\Lambda(s, \chi)$. Прва од њих је функционална једначина коју је показао Артин:

$$\Lambda(s, \chi) = W(\chi) \Lambda(1 - s, \bar{\chi}), \tag{5.6}$$

где је $W(\chi) \in \mathbb{C}, |W(\chi)| = 1$ и $\bar{\chi}$ комплексни конјугат од χ.

Приметимо да из претпоставке тврђења следи да је функција

$$(s(s-1))^{\delta(\chi)} \Lambda(s, \chi)$$

цела. Захваљујући тој чињеници добијамо значајну особину функције $\Lambda(s, \chi)$ познату као Адамарова факторизација:

$$\Lambda(s, \chi) = e^{a(\chi) + b(\chi) s} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} \cdot (s(s-1))^{-\delta(\chi)}, \tag{5.7}$$

при чему су $a(\chi), b(\chi) \in \mathbb{C}$, а производ је узет по свим нулама ρ функције $\Lambda(s, \chi)$.

Трећа особина функције $\Lambda(s, \chi)$ која је од значаја је једноставно својство

$$\overline{\Lambda(s, \chi)} = \Lambda(\bar{s}, \bar{\chi}), \tag{5.8}$$

из кога одмах следи

$$\overline{\frac{\Lambda'}{\Lambda}(s,\chi)} = \frac{\Lambda'}{\Lambda}(\bar{s},\bar{\chi}). \tag{5.9}$$

Сада, користећи функционалну једначину (5.6) добијамо да важи и

$$\frac{\Lambda'}{\Lambda}(s,\chi) = -\frac{\Lambda'}{\Lambda}(1-s,\bar{\chi}).$$

Последња релација, у комбинацији са (5.9), омогућава да донесемо закључак да важи

$$\Re\left(\frac{\Lambda'}{\Lambda}\left(\frac{1}{2},\chi\right)\right) = 0.$$

Даље, комбинујући (5.6) и (5.8) закључујемо да за сваку нулу ρ функције $\Lambda(s,\chi)$ и $1-\bar{\rho}$ јесте нула те функције. Одатле следи да је

$$\Re\left(\sum_{\rho}\left(\frac{1}{2}-\rho\right)^{-1}\right) = 0.$$

Узимајући логаритамски извод у Адамаровој факторизацији (5.7) и проналажењем реалног дела у $s=\frac{1}{2}$, добијамо и

$$\Re\left(b(\chi)+\sum_{\rho}\frac{1}{\rho}\right) = 0.$$

Користећи последње две релације, добијамо следећу значајну формулу за реални део логаритамског извода функције $\Lambda(s,\chi)$,

$$\Re\left(\frac{\Lambda'}{\Lambda}(s,\chi)\right) = \sum_{\rho}\Re\left(\frac{1}{s-\rho}\right) - \delta(\chi)\Re\left(\frac{1}{2}+\frac{1}{s-1}\right). \tag{5.10}$$

Остатак доказа тврђења се базира на давању оцена за факторе у формули (5.10). У сврху давања тих оцена, уводимо ознаку $N(t,\chi)$ за број нула $\rho=\beta+i\gamma$ функције $\mathfrak{L}(s,\chi)$ у региону $0<\beta<1, |\gamma-t|\leq 1$. Приметимо прво да важи једноставна оцена

$$\Re\left(\frac{1}{2+it-\rho}\right) = \frac{2-\beta}{(2-\beta)^2+(t-\gamma)^2}\begin{cases}\geq 0, \text{ за све } \rho\\ \geq \frac{1}{5}, \text{ ако је } |t-\delta|\leq 1.\end{cases}$$

Из те оцене, стављајући $s=2+it$ у (5.10), закључујемо да је

$$N(t,\chi) \ll \Re\left(\frac{\Lambda'}{\Lambda}(2+it,\chi)\right).$$

Због тога што $\mathfrak{L}(s,\chi)$ конвергира у $2+it$, десна страна последње релације се релативно лако оцењује. При томе, главни допринос долази од $\log A_\chi$ и броја $\Gamma-$фактора. Прецизније, важи

$$N(t,\chi) \ll \log A_\chi + \chi(1) n_k \log(|t|+5). \tag{5.11}$$

Формулом (5.11) је есенцијално завршен допринос који даје претпоставка о аналитичности функције $\mathfrak{L}(s,\chi)$. Доказ теореме се приводи крају добијањем експлицитне формуле

$$\sum_{\mathfrak{N}(\mathfrak{p})<x}{}' \chi(\mathrm{Fr}_\mathfrak{p}) \log \mathfrak{N}(\mathfrak{p}) = \delta(\chi)x - \sum_{|\gamma|<x} \frac{x^\rho}{\rho} + O(\chi(1) n_k \log M(L/k)) + \\ + O(x^{\frac{1}{2}} (\log x)\,(\log A_\chi + \chi(1) n_k \log x)),$$

при чему $\sum'$ означава да је сума узета по свим нерамификованим простим бројевима у L. Коначно, коришћењем једноставне оцене

$$\sum_{|\gamma|<x} \frac{1}{\rho} \ll \sum_{j<x} \frac{N(j,\chi)}{j},$$

формуле (5.11) и метода парцијалне сумације, добија се тврђење које треба доказати. □

Лема која следи је директна последица претходно приказаног тврђења, али у детаље исписивања њеног доказа нећемо залазити. Они се могу пронаћи у [13].

Лема 5.1.1. *Нека је L/k Галуаово раширење бројевних поља чија је Галуаова група G. Нека је $C \subseteq G$ подскуп који је стабилан у односу на конјугацију. Претпоставимо да важе AHC и GRH за Артинове L-функције придружене иредуцибилним карактерима групе G. Тада је, при $x \to \infty$*

$$\sum_{[\sigma]\in C} \frac{1}{|[\sigma]|} \left(\pi_{[\sigma]}(x, L/k) - \frac{|[\sigma]|}{|G|} \operatorname{li} x \right)^2 \ll x n_k^2 (\log M(L/k) x)^2,$$

где је сума узета по свим класама конјугације $[\sigma]$ у C.

На основу претходне леме, лако се добија тражена ефективна верзија теореме Чеботарева о густини, уз претпоставку GRH.

Теорема 5.1.4. *Нека је L/k Галуаово раширење бројевних поља чија је Галуаова група G. Нека је $C \subseteq G$ подскуп који је стабилан у односу на конјугацију. Претпоставимо да важе* AHC *и* GRH *за Артинове L-функције придружене иредуцибилним карактерима групе G. Тада је, при $x \to \infty$*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{li} x + O\left(|C|^{\frac{1}{2}} x^{\frac{1}{2}} n_k \log(M(L/k)x) \right).$$

Имплицитна O-константа је апсолутна.

Доказ. Посматрајмо разлику

$$\pi_C(x, L/k) - \frac{|C|}{|G|} \operatorname{li} x$$

и приметимо да је можемо представити у облику суме

$$\sum_{[\sigma]\in C} \left(\pi_{[\sigma]}(x, L/k) - \frac{|[\sigma]|}{|G|} \operatorname{li} x \right), \tag{5.12}$$

узету по свим класама конјугације $[\sigma]$ у C. Сада, применом неједнакости Коши-Шварца на (5.12) добијамо

$$\sum_{[\sigma]\in C} \left| \pi_{[\sigma]}(x, L/k) - \frac{|[\sigma]|}{|G|} \operatorname{li} x \right| \ll \left(\sum_{[\sigma]\in C} |[\sigma]| \right)^{\frac{1}{2}} \left(\sum_{[\sigma]\in C} \frac{1}{|[\sigma]|} \left| \pi_{[\sigma]}(x, L/k) - \frac{|[\sigma]|}{|G|} \operatorname{li} x \right|^2 \right)^{\frac{1}{2}}.$$

На основу Леме 5.1.1 следи да за десну страну последње релације важи да је једнака

$$O\left(|C|^{\frac{1}{2}} \left(x n_k^2 (\log M(L/k)x)^2 \right)^{\frac{1}{2}} \right) = O\left(|C|^{\frac{1}{2}} x^{\frac{1}{2}} n_k \log(M(L/k)x) \right),$$

одакле одмах следи тражено тврђење. □

Наредном теоремом описана је ефективна верзија теореме Чеботарева уз претпоставке GRH, AHC и PCC, дакле уз још једну додатну претпоставку у односу на верзију описану Теоремом 5.1.4.

Теорема 5.1.5. *Нека је L/k Галуаово раширење бројевних поља чија је Галуаова група G. Нека је $C \subseteq G$ подскуп који је стабилан у односу на конјугацију. Претпоставимо да важе* AHC, PCC *и* GRH *за Артинове L-функције придружене иредуцибилним карактерима групе G. Тада је, при $x \to \infty$*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{li} x + O\left(|C|^{\frac{1}{2}} x^{\frac{1}{2}} \left(\frac{|\tilde{G}|}{|G|} \right)^{\frac{1}{4}} n_k \log(M(L/k)x) \right),$$

где је $|\tilde{G}|$ ознака за број класа конјугације у G. Имплицитна O-константа је апсолутна.

Доказ. Погледати [12]. □

Напомена. *Приметимо да оцени грешке датој Теоремом 5.1.5 фигурише фактор $\left(\frac{|\tilde{G}|}{|G|} \right)^{\frac{1}{4}}$ који ту оцену разликује од оне дате Теоремом 5.1.4. Имајући у виду да $|\tilde{G}|$ представља број класа конјугације у G, имамо да је*

$$\left(\frac{|\tilde{G}|}{|G|} \right)^{\frac{1}{4}} < 1.$$

То значи да је оцена грешке коју даје Теорема 5.1.5 боља од оне коју даје Теорема 5.1.4. Дакле, добили смо очекивани исход по коме додатна претпоставка даје прецизнију оцену грешке.

Значај Теорема 5.1.4 и 5.1.5 је у томе што се понекад могу применити у *Абеловим* проширењима бројевних поља, пошто је познато да у њима важи АНС. Управо је то један од важних механизама које ћемо користити у каснијем излагању, приликом рада на Фробенијусовом пољу елиптичких кривих. Притом ћемо користити благо модификоване верзије Теорема 5.1.4 и 5.1.5, које описује наредна теорема.

Теорема 5.1.6. *Претпоставимо да важи* GRH *за Артинове L-функције. Нека је D непразан скуп који се састоји од класа конјугације у G и нека је H нормална подгрупа од G таква да је $HD \subseteq H$.*

1. *Претпоставимо да важи* АНС *за Артинове L-функције придружене иредуцибилним карактерима групе G/H. Тада је*

$$\pi_D(x, L/k) = \frac{|D|}{|G|} \operatorname{li} x + O\left(\left(\frac{|D|}{|H|}\right)^{\frac{1}{2}} x^{\frac{1}{2}} n_k \log(M(L/k)x)\right).$$

2. *Претпоставимо да важе* АНС *и* РСС *за Артинове L-функције придружене иредуцибилним карактерима групе G/H. Тада је*

$$\pi_D(x, L/k) = \frac{|D|}{|G|} \operatorname{li} x + O\left(\left(\frac{|D|}{|H|}\right)^{\frac{1}{2}} x^{\frac{1}{2}} \left(\frac{|\tilde{G}|}{|G|}\right)^{\frac{1}{4}} n_k \log(M(L/k)x)\right),$$

   где је $|\tilde{G}|$ ознака за број класа конјугације у G.

Имплицитне O-константе су апсолутне.

Доказ. 1. Приказаћемо кратку скицу доказа овог дела теореме. Означимо са $\bar{D}$ слику скупа D у G/H, а са k' фиксно поље подгрупе H од G. Тада применом Теореме 5.1.4 на $\bar{D}$ добијамо да важи

$$\pi_{\bar{D}}(x, L/k) = \frac{|\bar{D}||H|}{|G|} \operatorname{li} x + O\left(|\bar{D}|^{\frac{1}{2}} x^{\frac{1}{2}} n_k \log(M(k'/k)x)\right). \tag{5.13}$$

Како је по претпоставци $HD \subseteq D$, следи да је $|\bar{D}||H| = |D|$. Додатно, може се показати[1] да важи

$$\pi_D(x, L/k) = \pi_{\bar{D}}(x, L/k) + O\left(\frac{\log d_L}{|G|}\right),$$

[1] у вези са извођењем наведених тврђења погледати [13], а нешто више ће бити речено и на крају овог поглавља

као и

$$M(k'/k) \ll M(L/k).$$

Последње две релације, уз (5.13) одмах дају тражено тврђење.
2. Овај део теореме следи директно из дела *1.* и Теореме 5.1.5. □

5.2 Неколико значајних тврђења општијег карактера уз ефективне верзије теореме Чеботарева

У овом одељку приказаћемо још неколико тврђење општијег карактера која имају значај уз ефективне верзије теореме Чеботарева. Њихов значај је у томе што омогућавају редукцију посматрања функције $\pi_c(x, L/\mathbb{Q})$ на посматрање функције $\pi_D(x, L/k)$ за неко бројевно поље k, $\mathbb{Q} \subseteq k \subseteq L$ такво да је L/k Абелово. Приметимо да је управо у таквим, Абеловим проширењима важи AHC, што отвара простор за употребу Теореме 5.1.6.

Почимо од неколико значајних ознака и дефиниција. Користићемо уобичајене ознаке $G(\mathfrak{P})$ и $I(\mathfrak{P})$ за групу декомпозиције, односно инерције простог броја $\mathfrak{P}$ у L. Означимо са $\mathfrak{p}$ прост број p у k такав да $\mathfrak{P} \mid \mathfrak{p}$. Нека је φ класна функција . За цео број $m \geq 1$ дефинишемо

$$\varphi(\mathrm{Fr}_{\mathfrak{p}}^m) = \frac{1}{|I(\mathfrak{P})|} \sum_{\substack{g \in G(\mathfrak{P}) \\ g \cong \mathrm{Fr}_{\mathfrak{p}}^m \bmod I(\mathfrak{P})}} \varphi(g),$$

$$\tilde{\pi}_\phi(x) = \sum_{\mathfrak{N}(\mathfrak{p}^m) \leq x} \frac{1}{m} \varphi(\mathrm{Fr}_{\mathfrak{p}}^m),$$

$$\pi_\phi(x) = \sum_{\mathfrak{N}(\mathfrak{p}) \leq x} \varphi(\mathrm{Fr}_{\mathfrak{p}}).$$

Као и раније, са C ћемо означавати скуп $C \subseteq G$ који је инваријантан у односу на конјугацију, а сада уводимо ознаку δ_C за карактеристичну функцију тог скупа. За елемент $s \in G$ ћемо са $C_G(s)$ означавати одговарајућу класу конјугације у G, а са $C_H(s)$ одговарајућу конјугације у подгрупи $H \subseteq G$, ако је $s \in H$.

Теорема 5.2.1. *Уз нотацију описану у овом одељку имамо следеће:*

1. *Ако је ϕ класна функција на G, важи*

$$\tilde{\pi}_\phi(x) = \pi_\phi(x) + O\left(\|\phi\| \left\{ \frac{1}{|G|} \log d_L + [k : \mathbb{Q}] x^{\frac{1}{2}} \right\} \right),$$

где је $\|\phi\| = \sup_{s \in G} |\phi(s)|$. При томе је имплицитна O-константа апсолутна.

2. *Ако је* $s \in H$ *дефинишимо*

$$\tilde{\pi}_{C_H(s)}(x, L/L^H) = \tilde{\pi}_{\delta_{C_H(s)}}(x)$$

и

$$\tilde{\pi}_{C_G(s)}(x, L/k) = \tilde{\pi}_{\delta_{C_G(s)}}(x).$$

Тада је

$$\tilde{\pi}_{C_H(s)}(x, L/L^H) = \lambda \cdot \tilde{\pi}_{C_G(s)}(x, L/k),$$

где је

$$\lambda = \frac{|C_H(s)|/|H|}{|C_G(s)|/|G|}.$$

Доказ. За доказ ове теореме и више детаља о реченом у овом одељку погледати [16], као и [13].

□

ГЛАВА 6

Елиптичке криве

У нашем досадашњем излагању приказан је велики број различитих моћних теорема и објеката како алгебарске, тако и аналитичке теорије бројева, кулминирајући у претходној глави приказивањем ефективних верзија теореме Чеботарева о густини. При томе, приказана теорија има значај и сама по себи, али се њена пуна моћ и смисао огледа у томе што се може примењивати у различитим контекстима, дајући притом интересантне и значајне резултате. Због тога се фокус даљег излагања окреће ка дефинисању једног таквог, нама значајног контекста. Он је одређен појмом *елиптичке криве*, што је управо објекат коме је посвећена ова глава. Нагласимо да је наш циљ да поред давања дефиниције елиптичких кривих, прикажемо и неке њихове значајне особине. При томе, докази тврђења која будемо формулисали неће бити приказивани. Заинтересовани читалац их све може пронаћи у [18].

6.1 Дефиниција елиптичке криве

Изучавање *Диофантових једначина* датира још из периода Старе Грчке. Диофантове једначине су полиномијалне једначине за које тражимо цела или рационална решења. Најједноставнија таква једначина је линеарна,

$$aX + bY = c, \quad a, b, c \in \mathbb{Z}, ab \neq 0. \tag{6.1}$$

Оваква једначина увек има рационална решења. Додатно, она има целобројна решења ако и само ако $\gcd(a, b) \mid c$ и у том случају се сва решења једначине могу пронаћи користећи Еуклидов алгоритам. На тај начин, користећи одређена аритметичко-алгебарска својства можемо добити доста информација о једначини (6.1). Са друге стране, приметимо да је једначином (6.1) одређена права у $\mathbb{R}^2$. Тако добијамо и геометријски поглед на саму једначину. Управо оваква дуалност геометријског и аритметичко-алгебарског погледа на алгебарску једначину представља објекат истраживања *Диофантске геометрије*. Због једноставности једначине (6.1) моћ ове спреге

се не може добро видети, али је она веома јака– аритметика криве дефинисане алгебарском једначином утиче на њене геометријске особине и обратно, изучавањем геометријских особина криве може се сазнати више о њеним аритметичким својствима. Имајући у виду ту чињеницу, ми ћемо приступити дефинисању елиптичке криве у оба духа и показати да се такве две дефиниције поклапају. Наравно, алгебарска једначина која дефинише елиптичку криву је компликованија од једначине (6.1), па ће и један и други поглед пружати своје предности, у смислу већ поменуте геометријско-аритметичко-алгебарске спреге. Такође, учинићемо и још један корак више у односу на једначину (6.1) тако што нећемо посматрати само елиптичке криве над пољем $\mathbb{Q}$, већ ће контекст бити одређен произвољним пољем K и његовим алгебарским затворењем $\bar{K}$.

6.1.1 Алгебарска дефиниција елиптичке криве

Прикажимо прво алгебарски поглед на појам елиптичке криве. Он се огледа у томе да је свака елиптичка крива одређена једначином која се назива *Вајерштрасова једначина*. Следећом дефиницијом описане су Вајерштрасове једначине над алгебарским затворењем $\bar{K}$ поља K.

Дефиниција 6.1.1. *Нека је K поље, чије је алгебарско затворење $\bar{K}$ и $a_1, a_2, \ldots, a_6 \in \bar{K}$. (Хомогена) једначина облика*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{6.2}$$

назива се ***Вајештрасовом једначином***.

Наредном дефиницијом, користећи појам Вајерштрасове једначине дефинише се појам елиптичке криве.

Дефиниција 6.1.2. *Елиптичка крива E је крива одређена Вајерштрасовом једначином (6.2) са фиксираном базном тачком $O = [0, 1, 0]$. Додатно, уколико у једначини (6.2) која дефинише криву E важи $a_1, a_2, \ldots, a_6 \in K$ кажемо да је крива E дефинисана над пољем K и пишемо E/K.*

Приметимо да су Вајерштрасове једначине, па самим тим и одговарајуће елиптичке криве задате хомогеним полиномима. Оне се, наравно, могу дехомогенизовати, користећи у једначини (6.2) нехомогене координате $x = X/Z$ и $y = Y/Z$. На тај начин елиптичке криве добијају једначине

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{6.3}$$

при чему базна тачка $O = [0, 1, 0]$ постаје тачка „у бесконачности".

Уколико је поље $\bar{K}$ карактеристике различите од 2, једначина (6.3) се може додатно упростити допуном до квадрата. Довољно је извршити смену

$$y \to \frac{1}{2}\left(y - a_1x - a_3\right),$$

после које једначина (6.3) добија облик

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{6.4}$$

где је

$$b_2 = a_1^2 + 4a_4,$$
$$b_4 = 2a_4 + a_1a_3$$

и

$$b_6 = a_3^2 + 4a_6.$$

Дефинишимо још и вредности

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

и

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{6.5}$$

Због значаја вредности Δ издвојимо је у посебну дефиницију.

Дефиниција 6.1.3. *Вредност Δ одређена формулом (6.5) назива се* ***дискриминанта*** *елиптичке криве E.*

Који је тачно значај дискриминанте елиптичке криве видећемо ускоро, а за крај алгебарског уводног разматрања везаног за елиптичке криве, приметимо да уколико је карактеристика бројевног поља $\bar{K}$ различита и од 3, једначина (6.4) се може додатно упростити до облика

$$y^2 = x^3 + Ax + B,$$

где су $A, B \in \bar{K}$. Последње наведни облик Вајерштрасове једначине је значајно имати на уму, јер њега, између осталог, имају елиптичке криве над бројевним пољима, дакле, над изузетно широком и значајном класом поља.

6.1.2 Геометријска дефиниција елиптичке криве

Погледајмо сада како изгледа геометријски поглед на појам елиптичке криве. Пре свега, да бисмо уопште разматрали елиптичке криве потребно је знати шта је уопште крива. Тај појам описан је наредном дефиницијом.

Дефиниција 6.1.4. ***Крива*** *је пројективни варијетет димензије један.*

Као и код осталих варијетета, и међу кривама се истиче класа оних које су глатке, што значи да имају тангентни простор у свакој тачки. Такве криве се поред глатких називају и *несингуларним*. Други значај појам везан за криве је појам *рода*. Он је установљен фундаменталног теоремом алгебарске геометрије која је позната као теорема Риман-Роха. У сам исказ теореме, као и објашњење свих појмова везаних за

њу нећемо залазити, па стога упућујемо заинтересованог читаоца да детаље везане за теорему Риман-Роха, укључујући и њен доказ, потражи на [18], односно [10]. Једино што ћемо издвојити везано за појам рода криве је такозвана *формула степена* која омогућава његово релативно једноставно рачунање и описана је наредном теоремом.

Теорема 6.1.1. *Нека је $F(X,Y,Z) \in K[X,Y,Z]$ хомогени полином степена $d, d \geq 1$. Претпоставимо да је крива C дефинисана једначином $F(X,Y,Z) = 0$ несингуларна. Тада је род криве C једнак*

$$\frac{(d-1)(d-2)}{2}.$$

Следећа кључна ствар везана за појам рода састоји се у показивању да за сваки цео број $m \geq 1$ постоји крива рода m. Користећи то својство, можемо извршити класификацију кривих према њиховом роду. Специјално, нама ће од интереса бити (несингуларне) криве рода један, које ћемо називати *елиптичким кривама*. Прецизније, имамо следећу дефиницију.

Дефиниција 6.1.5. ***Елиптичка крива*** *је уређени пар (E,O) где је E несингуларна крива рода 1 и $O \in E$ базна тачка.*

Сада имамо и геометријску, знатно апстрактнију дефиницију елиптичке криве од оне одређене Вајерштрасовом једначином. Какав је однос ових дефиниција показује наредни пододељак.

6.1.3 Однос геометријске и алгебарске дефиниције

Приметимо прво да се код геометријске дефиниције елиптичке криве захтева да она буде несингуларна, док дефиниција помоћу Вајерштрасових једначина не поставља такав захтев. Због тога, за почетак, погледајмо какав је услов несингуларности за Вајерштрасове једначине. У њему ће кључну улогу имати појам дискриминанте елиптичке криве, описан дефиницијом 6.1.3. Како прецизно изгледа та улога описује наредна теорема.

Теорема 6.1.2. *Нека је E елиптичка крива одређена Вајерштрасовом једначином (6.3), чија је дискриминанта Δ. Тада је E несингуларна ако и само ако је $\Delta \neq 0$.*[1]

Иако постоји развијена теорија кривих рода 1 које нису глатке, надаље ћемо се ограничити само на рад са оним кривама које су несингуларне, било да их посматрамо геометријски или дефинисане помоћу Вајерштрасових једначина.

[1] приметимо да се већ на овом месту може добро видети један пример аритметичко-алгебарске и геометријске интеракције. Дискриминанта је појам који је у потпуности алгебарски и зависи само од коефицијената одговарајуће Вајерштрасове једначине, а на основу ње можемо добити информацију о чисто геометријском појму какав је појам глаткости, односно егзистенције тангентног простора елиптичке криве у свакој њеној тачки.

Наредно што ћемо приказати је да су два различита погледа, односно два различита приступа појму елиптичких кривих које смо видели у досадашњем излагању сагласна, односно да одређују исти објекат. Таква чињеница даје оправданост и једном и другом погледу, што је веома значајно у већ више пута поменутом коришћењу алгебарско-геометријске спреге.

Теорема 6.1.3. *1. Нека је E несингуларна крива одређена Вајерштрасовом једначином (6.2). Тада је E генуса један, што је уз одабир тачке $O = [0, 1, 0]$ за базну чини елиптичком кривом у смислу дефиниције 6.1.5.*

2. Обратно, ако је E несингуларна крива генуса један са базном тачком O, тада постоји Вајерштрасова једначина (6.2) која одређује криву E, таква да тачка O при таквом избору једначине има хомогене координате $[0, 1, 0]$, што значи да је E елиптичка крива у смислу дефиниције 6.1.2.

6.2 Групни закон на елиптичкој кривој и изогеније

Подсетимо се да је инспирација за посматрање елиптичких кривих потекла од Диофантових једначина и размотримо како се поглед у таквом, Диофантовом духу, може осликати на саме елиптичке криве. Нека је E елиптичка крива над пољем K одређена Вајерштрасовом једначином

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Претходну једначину, поред тога што је једначина која дефинише криву E, можемо посматрати и једноставније, као полиномијалну једначину над пољем K. Имајући у виду такав поглед, природно се, у Диофантовом духу, поставља питање K-рационалних решења те једначине, односно оних уређених парова $(x, y) \in K^2$ који је задовољавају. Поново се враћајући на геометријски поглед, такве уређене парове (x, y) можемо видети као тачке елиптичке криве E чије су обе координате у пољу K. Због тога их називамо *K-рационалним тачкама*. Скуп свих K-рационалних тачака на елиптичкој кривој E означавамо са $E(K)$.

Оно што желимо је да одемо корак даље и да скуп $E(K)$ не видимо само као скуп, већ да на њему дефинишемо и правилну алгебарску структуру, каква је структура групе. Управо у ту сврху ћемо се још једном ослонити на геометријски поглед, јер ће, дефиниција групног закона на скупу $E(K)$ бити индукована геометријом саме криве E. При том, геометријска особина елиптичке криве E на коју ћемо се ослањати је прилично једноставна, али и даље од фундаменталног значаја:

Права која пролази кроз две тачке на елиптичкој кривој сече ту криву у тачно још једној тачки (рачунајући притом и вишеструкост).

Претходна чињеница гарантује коректност наредне дефиниције групног закона на елиптичкој кривој E.

Дефиниција 6.2.1. *Нека је E елиптичка крива чија је базна тачка O и нека су P и Q две тачке на E. Означимо са L праву која пролази кроз P и Q, а са R трећу тачку пресека праве L са кривом E (у случају да је $P = Q$, L је тангента на криву E у тачки P). Нека је L' права која пролази кроз R и O. Трећу тачку пресека праве L' са елиптичком кривом E називамо* ***композицијом*** *или* ***збиром*** *тачака P и Q и означавамо са $P + Q$.*

Раније смо већ напоменули, а из претходне дефиниције постаје потпуно јасно да је групни закон на елиптичкој кривој дефинисан геометријски. Наравно, он може добити и своју алгебарску репрезентацију, у виду експлицитних формула за композицију две тачке на елиптичкој кривој којој је фиксирана Вајерштрасова једначина. Саме формуле се изводе уз релативно дуг рачун и елементарно познавање аналитичке геометрије, али нам овде нису од интереса, па неће бити наведене.

Оно што јесте од интереса је давање оправдања употреби појма „групни закон"у вези са дефиницијом операције композиције тачака на елиптичкој кривој. Тражено оправдање пружа наредна теорема.

Теорема 6.2.1. *Нека је E елиптичка крива чија је базна тачка O. Тада крива E у односу на операцију композиције тачака има структуру Абелове групе чији је неутрал тачка O. Додатно, ако је елиптичка крива E дефинисана над пољем K, скуп*

$$E(K) \cup \{O\}$$

чини једну подгрупу од E.

Претходна теорема, дакле, успоставља структуру групе како на целој елиптичкој кривој E, тако и специјално на скупу $E(K)$. Већ та чињеница чини велики помак приликом испитивања скупа $E(K)$ у односу на пуко виђење тог скупа као колекције свих K-рационалних решења одговарајуће полиномијалне једначине. Даљи помак би ишао путем стицања увида у структуру $E(K)$ посматраног као групе. Тај пут води до једне од најзначајних теорема у теорији елиптичких кривих, познате као Мордел-Вејлова теорема. Нажалост, подухват приказивања те теореме превазилази оквире овог рада и ми ћемо излагање наставити наредном дефиницијом која уводи појам *изогеније*.

Дефиниција 6.2.2. *Нека су (E_1, O_1) и (E_2, O_2) елиптичке криве.* ***Изогенија*** *између E_1 и E_2 је морфизам кривих*

$$\phi : E_1 \to E_2$$

који задовољава $\phi(O_1) = O_2$.

Скуп свих изогенија између елиптичких кривих E_1 и E_2 означимо са $\mathrm{Hom}(E_1, E_2)$. На том скупу можемо задати операцију сабирања на стандардан начин,

$$(\phi + \psi)(P) = \phi(P) + \psi(P), \tag{6.6}$$

за све изогеније $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ и тачке P на кривој E. Додатно, када је $E_1 = E_2$ можемо вршити и композицију изогенија. Прецизније, за елиптичку криву E означимо са

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

прстен на коме је сабирање дефинисано помоћу (6.6), а множење као композиција изогенија,

$$(\phi\psi)(P) = \phi\left(\psi(P)\right),$$

за све изогеније $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ и тачке P на кривој E. Прстен $\mathrm{End}(E)$ се назива *прстеном ендоморфизама* елиптичке криве E. Пре даљег испитивања прстена $\mathrm{End}(E)$ погледајмо основни пример изогенија које постоје на свакој елиптичкој кривој.

Пример 6.1. Нека је (E, O) произвољна елиптичка крива. За свако $m \in \mathbb{Z}$ дефинишемо пресликавање множења са m, у ознаци $[m]$ на следећи начин:

1. Ако је $m = 0$, имамо за све тачке P криве E, $[0](P) = O$.
2. Ако је $m > 0$, дефинишемо за све тачке P криве E, $[m](P) = P + P + \cdots + P$ (m пута).
3. Ако је $m < 0$, дефинишемо за све тачке P криве E, $[m](P) = [-m](-P)$.

Имајући у виду да операција сабирања тачака на елиптичкој кривој јесте морфизам те криве, лако се индукцијом показује да је за свако $m \in \mathbb{Z}$, $[m]$ један морфизам елиптичке криве E. Такође, очигледно је да за све $m \in \mathbb{Z}$ важи

$$[m](O) = O,$$

одакле следи да су пресликавања $[m]$ елементи прстена ендоморфизама $\mathrm{End}(E)$ елиптичке криве E. Више о њиховој улози показује наредна теорема.
□

Теорема 6.2.2. *1. Нека је E елиптичка крива. Прстен ендоморфизама $\mathrm{End}(E)$ те криве је (не обавезно комутативни) прстен карактеристике 0, без делитеља нуле.*

2. Нека је E/K елиптичка крива и $m \in \mathbb{Z}$, уз $m \neq 0$. Тада је изогенија множења са m,

$$[m] : E \to E$$

неконстантна.

Претпоставимо да је карактеристика поља K једнака 0 (на пример, нека је K бројевно поље) и E/K елиптичка крива. Претходна теорема онда показује да уобичајено важи

$$\mathrm{End}(E) \cong \mathbb{Z},$$

односно да за криву E не постоји других изогенија осим оних множења са m, $m \in \mathbb{Z}$. За такве криве се каже да су *без комплексног множења*. У супротном, ако је $\mathrm{End}(E)$ строго већи од $\mathbb{Z}$, за криву E кажемо да је *са комплексним множењем*. Елиптичке криве са комплексним множењем поседују многа посебна својства; следећим примером приказаћемо једну такву криву.

Пример 6.2. Нека је K поље карактеристике различите од 2 и $i \in \bar{K}$ примитивни четврти корен јединице,

$$i^2 = -1.$$

Посматрајмо елиптичку криву E/K одређену једничином

$$y^2 = x^3 - x.$$

Приметимо да је прстен $\mathrm{End}(E)$ строго већи од $\mathbb{Z}$, пошто њему припада пресликавање које ћемо означити са $[i]$, а које је дефинисано са

$$[i](x, y) = (-x, iy)$$

за све тачке (x, y) криве E. То значи да је E један пример елиптичке криве са комплексним множењем.
□

6.3 Елиптичке криве над коначним пољима и редукција елиптичке криве

Нека је p прост рационалан број и q неки степен броја p. Означимо стандардно као и до сада са $\mathbb{F}_q$ коначно поље са q елемената, а са $\bar{\mathbb{F}}_q$ алгебарско затворење тог поља. Посматрајмо елиптичку криву $E/\mathbb{F}_q$ дефинисану над коначним пољем $\mathbb{F}_q$. Оно што нам је од интереса је давање процене за број елеменената скупа $E(\mathbb{F}_q)$ или еквивалентно, фиксирајући Вајерштрасову једначину за криву E, број решења једначине

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

у $\mathbb{F}_q^2$. Пре свега, пошто свака вредност за x може дати највише две вредности за y, одмах добијамо тривијалну горњу оцену

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

Међутим, пошто је „случајно изабрана"квадратна једначина решива над $\mathbb{F}_q$ у 50% случајева, оно што интуитивно очекујемо је да је кардиналност скупа $E(\mathbb{F}_q)$ реда q, а не $2q$ како тврди тривијална оцена. Исправност таквог интуитивног очекивања показује наредна значајна теорема Хасеа.

Теорема 6.3.1 (Хасе). *Нека је $E/\mathbb{F}_q$ елиптичка крива дефинисана над коначним пољем $\mathbb{F}_q$. Тада је*

$$|\#E(\mathbb{F}_q) - q - 1| < 2\sqrt{q}.$$

Претходну теорему можемо посматрати и као илустрацију чињенице да рад са елиптичким кривама над коначим пољима није претерано компликован. Наиме, теорема Хасеа пружа увид у кардиналност скупа $E(\mathbb{F}_q)$ за све елиптичке криве E над произвољним коначим пољем $\mathbb{F}_q$, што је информација коју немамо за елиптичке криве над произвољним пољем K. Због тога се јасно намеће потреба за постојањем механизма који омогућава прелазак са посматрања елиптичке криве над компликованијим, апстрактнијим пољем на посматрање криве над једноставнијим, по могућности коначним пољем. Такав механизам постоји и назива се *редукција* елиптичке криве. У наставку излагања ћемо приказати како изгледа редукција елиптичких кривих над пољем рационалних бројева $\mathbb{Q}$.

Нека је $E/\mathbb{Q}$ елиптичка крива над пољем $\mathbb{Q}$ чија је Вајерштрасова једначина

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{6.7}$$

Како је крива дефинисана над пољем $\mathbb{Q}$, важи да су $a_1, a_2, \ldots, a_6$ рационални бројеви. Увођењем смене

$$(x, y) \to (u^{-2}x, u^{-3}y)$$

претходна Вајерштрасова једначина добија облик

$$y^2 + ua_1xy + u^3a_3y = x^3 + u^2a_2x^2 + u^4a_4x + u^6a_6.$$

Одатле следи да можемо изабрати довољно велики број u тако да сви коефицијенти у Вајерштрасовој једначини (6.7) буду цели бројеви. Због тога ћемо надаље претпостављати да у једначини (6.7) важи $a_1, a_2, \ldots, a_6 \in \mathbb{Z}$.

Уочимо сада произвољан прост рационалан број p и посматрајмо све Вајерштрасове једначине елиптичке криве E са коефицијентима у прстену целих бројева. Међу свим таквим једначинама постоји (бар једна) једначина која има минималну дискриминанту, по модулу p. Називамо је *минималном Вајерштрасовом једначином*. Фиксирајмо једну минималну Вајерштрасову једначину елиптичке криве E,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

и редукујмо све коефицијенте те једначине по модулу p. На тај начин добијамо (не обавезно глатку) криву E_p дефинисану над коначим пољем $\mathbb{F}_p$ коју називамо *редукција елиптичке криве E по модулу p*. У вези са кривом E_p имамо два значајна питања: питање њене јединствености и питање њене сингуларности.

Јединственост редукције E_p криве E по модулу p регулисана је јединственошћу минималне Вајерштрасове једначине. Наиме, може се показати да је минимална Вајерштрасова једначина, па самим тим и крива E_p, јединствена до на одређену стандардну

промену координата која не утиче на природу криве одређене једначином. У том смислу, није превелики губитак општости ако сматрамо да је крива E_p јединствена.

Са друге стране, питање сингуларности криве E_p је доста компликованије. Да бисмо га размотрили, потребно је прво рећи нешто опште о сингуларним елиптичким кривама. Пре свега, уколико је елиптичка крива сингуларна, онда има сингуларитет у само једној тачки. На основу броја тангентних праваца у тој тачки сингуларна тачка може бити

- **чвор**: ако постоје тачно два различита тангента правца у тој тачки.
- **касп**: ако постоји само један тангенти правац у тој тачки.

Као што само већ напоменули, редукција E_p криве E по модулу p може бити сингуларна крива. Због тога, претходну класификацију сингуларних тачака можемо искористити да дамо прецизан опис могућих редукција криве E који је дат наредном дефиницијом.

Дефиниција 6.3.1. *Нека је $E/\mathbb{Q}$ елиптичка крива и E_p редукција те криве по модулу p. Кажемо да E има*

1. ***добру или стабилну редукцију*** *ако је E_p несингуларна.*
2. ***мултипликативну или полустабилну редукцију*** *ако E_p има чвор.*
3. ***адитивну или нестабилну редукцију*** *ако E_p има касп.*

У случајевима 1. и 2. кажемо да крива E има ***лошу редукцију****.*

У вези простих бројева за које елиптичка крива има лошу редукцију, дефинише се објекат који их све кодира на елегантан начин. Он је познат под називом *кондуктор* елиптичке криве и описан је наредном дефиницијом.

Дефиниција 6.3.2. *Нека је $E/\mathbb{Q}$ елиптичка крива над пољем $\mathbb{Q}$.* ***Кондуктор*** *елиптичке криве E, у ознаци N_E, је производ*

$$N_E = \prod_{p\text{-прост}} p^{f_p(E)},$$

где је

$$f_p(E) = \begin{cases} 0, & \text{ако } E \text{ има добру редукцију у } p, \\ 1, & \text{ако } E \text{ има мултипликативну редукцију у } p, \\ 2, & \text{ако } E \text{ има адитивну редукцију у } p. \end{cases}$$

ГЛАВА 7

Фробенијусова поља елиптичких кривих

7.1 Уводно разматрање

Посматрајмо елиптичку криву $E/\mathbb{Q}$ над пољем рационалних бројева $\mathbb{Q}$ без комплексног множења, чији је кондуктор N. За рационалан прост број p такав да $p \nmid N$, означимо са E_p редукцију криве E по модулу p. Крива E_p је дефинисана над коначним пољем $\mathbb{F}_p$, па има смисла посматрати скуп $E(\mathbb{F}_p)$ свих $\mathbb{F}_p-$рационалних тачака те криве. На основу теореме Хасеа важи

$$\left|\#E_p(\mathbb{F}_p) - p - 1\right| < 2\sqrt{p}.$$

Одатле, ако означимо са

$$a_p(E) = p + 1 - \#E_p(\mathbb{F}_p), \tag{7.1}$$

одмах имамо и релацију

$$|a_p(E)| < 2\sqrt{p}. \tag{7.2}$$

Редукција E_p елиптичке криве E је дефинисана над пољем $\mathbb{F}_p$, које је карактеристике p. Због тога је за криву E_p коректно дефинисан *Фробенијусов ендоморфизам* Φ_p, одређен са

$$\Phi_p(x, y) = (x^p, y^p), \text{ за све } (x, y) \in E_p.$$

Посматраћемо полином

$$P_{E,p}(X) = X^2 - a_p(E)X + p, \tag{7.3}$$

који је значајан због тога што представља карактеристични полином пресликавања Φ_p. Из неједнакости (7.2) следи да $P_{E,p}(X)$ има два комплексно-конјугована корена која ћемо означавати са $\pi_p(E)$ и $\overline{\pi_p(E)}$, па Фробенијусов аутоморфизам Φ_p можемо идентификовати са комплексним бројем $\pi_p(E)$. Оваква идентификација је веома згодна, због тога што омогућава да се интеракција Фробенијусовог аутоморфизма Φ_p редукције E_p и поља $\mathbb{Q}$ дефиниције криве E изрази елегантно као раширење поља $\mathbb{Q}$. Прецизније, имамо следећу дефиницију.

Дефиниција 7.1.1. *Нека је E елиптичка крива над $\mathbb{Q}$ без комплексног множења чији је кондуктор N. Посматрајмо рационалан прост број p такав да $p \nmid N$ и означимо са E_p редукцију криве E по модулу p. Нека је $a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$ и $\pi_p(E)$ један корен карактеристичног полинома одређеног формулом (7.3). Тада раширење $\mathbb{Q}(\pi_p(E))$ поља рационалних бројева $\mathbb{Q}$ називамо* ***Фробенијусовим пољем*** *по модулу p за елиптичку криву E.*

Претходно дефинисани појам Фробенијусовог поља придруженог елиптичкој кривој биће један од централних објеката које ћемо посматрати у овој глави. Прецизније објашњење како ће изгледати то посматрање дато је наредним редовима.

Нека је $\pi_p(E)$ корен полинома (7.3) и $\mathbb{Q}(\pi_p(E))$ одговарајуће Фробенијусово поље по модулу p елиптичке криве E. Приметимо да смо раније установили да је $\pi_p(E)$ комплексан број, па из чињенице да је полином (7.3) степена 2, одмах можемо поље $\mathbb{Q}(\pi_p(E))$ окарактерисати као квадратно имагинарно бројевно поље.

Подсетимо се да смо претпоставили да је крива E без комплексног множења. Због тога, како p пролази све рационалне просте бројеве такве да не деле кондуктор N елиптичке криве E, међу одговарајућим квадратним имагинарним бројевним пољима $\mathbb{Q}(\pi_p(E))$ постојаће бесконачно много међусобно различитих. На овом месту се онда природно јавља питање квантификовања броја рационалних простих бројева p таквих да је $\mathbb{Q}(\pi_p(E)) = K$ за неко фиксирано квадратно имагинарно бројевно поље K. Имајући у виду интуицију коју смо већ неколико пута видели у досадашњем излагању, наведено квантификовање извршићемо посматрањем функције

$$\Pi_E(K; x) = \#\{p \leq x \mid p \nmid N, \mathbb{Q}(\pi_p(E)) = K\},$$

дефинисане за сваки реалан број x. Наравно, од интереса ће бити понашање функције $\Pi_E(K; x)$ како број x расте или другим речима, бавићемо се испитивањем асимптотике те функције при $x \to \infty$.

Као последње међу уводним разматрањима ове главе наведимо још хипотезу Ленг-Тротера о асимптотици функције $\Pi_E(K; x)$. Наведена хипотеза претпоставља доста прецизнију оцену о асимптотском понашању функције $\Pi_E(K; x)$ при $x \to \infty$ од оне које ћемо ми показати и представља још увек отворено питање у теорији елиптичких кривих.

Хипотеза (Ленг-Тротер). *Нека је $E/\mathbb{Q}$ елиптичка крива без комплексног множења са кондуктором N и K квадратно имагинарно бројевно поље. Тада постоји позитивна константа $c(E, K)$ која зависи од криве E и поља K таква да је*

$$\Pi_E(K; x) \sim c(E, K) \frac{\sqrt{x}}{\log x},$$

када $x \to \infty$.

7.2 Комбиноване Галуаове репрезентације

У овом одељку бавићемо се извођењем комбинованих Галуаових репрезентација придружених истовремено елиптичкој кривој и фиксираном имагинарном квадратном бројевном пољу. Приметимо да за произвољну елиптичку криву E дефинисану над бројевним пољем L, чије је алгебарско затворење $\bar{L}$, имамо Галуаову ℓ-адичну репрезентацију дефинисану као хомоморфизам

$$\rho_\ell : G_{\bar{L}/L} \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

индукован дејством Галуаове групе $G_{\bar{L}/L}$ на ℓ^n-торзионе тачке те криве, за свако $n \in \mathbb{N}$ и неки фиксирани рационални прост број ℓ. Према томе, оно што је потребно да урадимо је да ту репрезентацију везану за елиптичку криву додефинишемо и проширимо тако да може да обухвати и репрезентацију неког фиксираног квадратног имагинарног бројевног поља K.

Нека је $E/\mathbb{Q}$ елиптичка крива без комплексног множења, чији је кондуктор N и K квадратно имагинарно бројевно поље, чији је класни број једнак h. На основу примера 2.1 имамо да је група инвертибилних елемената бројевног поља K коначна. Означимо број елемената те групе са w.

Нека је ℓ рационалан прост број који се потпуно цепа у K тј. рационалан прост број такав да је

$$\ell\mathscr{O}_K = \mathfrak{L} \cdot \overline{\mathfrak{L}},$$

за нека два различита, међусобно конјугована идеала $\mathfrak{L}$ и $\overline{\mathfrak{L}}$ прстена целих $\mathscr{O}_K$ бројевног поља K.

7.2.1 Репрезентација везана за елиптичку криву $E/\mathbb{Q}$

Са једне стране, посматрамо Галуаову ℓ-адичну репрезентацију придружену елиптичкој кривој E, дефинисану као дејство Галуаове групе $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ на групу $E[\ell]$ сачињену од ℓ-торзионих тачака криве E:

$$\rho_{\ell,E} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Можемо сматрати да је ℓ довољно велико, тако да је репрезентација $\rho_{\ell,E}$ сурјективна и да је $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, при чему је $\mathbb{Q}(E[\ell])$ бројевно поље ℓ-торзионих тачака елиптичке криве E. Подсетимо се да је раширење $\mathbb{Q}(E[\ell])/\mathbb{Q}$ рамификовано само у простим делитељима од ℓN, као и да за просте бројеве p такве да $p \nmid \ell N$ важи

$$\mathrm{Tr}\, \rho_{\ell,E}(\mathrm{Fr}_p) \equiv a_p(E) \pmod{\ell} \tag{7.4}$$

и

$$\det \rho_{\ell,E}(\mathrm{Fr}_p) \equiv p \pmod{\ell}, \tag{7.5}$$

при чему је Fr_p скраћени запис за Фробенијусов аутоморфизам $\left(\overline{\mathbb{Q}}/\mathbb{Q}, p\right)$ који одговара p у Галуаовој групи $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, а a_p је број одређен формулом (7.1).

Уз репрезентацију $\rho_{\ell,E}$ посматрамо и њену пројекцију у $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ да бисмо на тај начин добили репрезентацију:

$$\hat{\rho}_{\ell,E} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Уочимо да репрезентација $\hat{\rho}$ није бијективна, али сечењем по њеном језгру добијамо бијективну репрезентацију, коју ћемо исто означавати и за коју важи

$$\hat{\rho}_{\ell,E} : \mathrm{Gal}(F_{\ell,E}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

при чему је $F_{\ell,E}$ раширење поља $\mathbb{Q}$ настало сечењем по одговарајућем језгру, тако да је гарантована инјективност пресликавања $\hat{\rho}_{\ell,E}$.

7.2.2 Репрезентација везана за квадратно имагинарно бројевно поље K

Наредна ствар коју дефинишемо је репрезентација придружена квадратном имагинарном бројевном пољу K. Уочимо произвољни ненула идеал $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ бројевног поља K, напишимо $\mathfrak{p}^h = \alpha\mathscr{O}_K$ за неко $\alpha \in K^*$ и дефинишимо

$$\pi_{\mathfrak{p}}(K) = \alpha^w,$$

где је w (коначна) кардиналност групе инвертибилних елемената у K. Приметимо да уколико уочимо неко друго $\beta \in K^*$ такво да је $\mathfrak{p}^h = \beta\mathscr{O}_K$, важи да је

$$\alpha = j\beta,$$

при чему j припада групи инвертибилних елемената у K. Због тога, према дефиницији броја w важи да је

$$\alpha^w = \beta^w.$$

Последња чињеница показује да је $\pi_{\mathfrak{p}}(K)$ коректно дефинисано, у смислу да не зависи од избора α.

Посматрајмо пресликавање

$$\chi_\ell = (\chi_{\mathfrak{L}}, \chi_{\bar{\mathfrak{L}}}) : \mathrm{Gal}(\bar{K}, K) \to (\mathscr{O}_K/\mathfrak{L})^* \times \left(\mathscr{O}_K/\bar{\mathfrak{L}}\right)^* \cong (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*,$$

дефинисано са

$$\chi_\ell(\mathrm{Fr}_{\mathfrak{p}}) = \left(\pi_{\mathfrak{p}}(K) (\mathrm{mod}\, \mathfrak{L}), \pi_{\mathfrak{p}}(K) (\mathrm{mod}\, \bar{\mathfrak{L}})\right),$$

где је $\mathrm{Fr}_{\mathfrak{p}}$ скраћени запис за Фробенијусов аутоморфизам $\left(\bar{K}/K, \mathfrak{p}\right)$ који одговара $\mathfrak{p}$ у Галуаовој групи $\mathrm{Gal}(\bar{K}, K)$. Дејство компоненте $\chi_{\mathfrak{L}}$ са групе $\mathrm{Gal}(\bar{K}, K)$ у групу $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ индукује репрезентацију везану за бројевно поље K коју желимо да дефинишемо.

Пре свега, приметимо да је због $[K:\mathbb{Q}]=2$, подгрупа $\mathrm{Gal}(\bar{K},K)$ индекса 2 у групи $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Због тога, ако уочимо нетривијалан $\mathbb{Q}$-аутоморфизам θ поља K имамо да је

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Gal}(\bar{K},K) \oplus \mathrm{Gal}(\overline{K^\theta},K^\theta).$$

Захваљујући овој особини Галуаове групе $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ можемо дефинисати индуковану репрезентацију

$$\rho_{\ell,K} : \mathrm{Gal}(\overline{\mathbb{Q}},\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

као

$$\rho_{\ell,K}(\sigma) = \begin{cases} \begin{bmatrix} \chi_{\mathfrak{L}}(\sigma) & 0 \\ 0 & \chi_{\mathfrak{L}}(\theta\sigma\theta) \end{bmatrix}, & \text{ако је } \sigma \in \mathrm{Gal}(\bar{K},K) \\ \\ \begin{bmatrix} 0 & \chi_{\mathfrak{L}}(\sigma\theta) \\ \chi_{\mathfrak{L}}(\theta\sigma) & 0 \end{bmatrix} & \text{ако је } \sigma \notin \mathrm{Gal}(\bar{K},K), \end{cases}$$

за све $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}},\mathbb{Q})$. За овако дефинисану репрезентацију $\rho_{\ell,K}$ кажемо да је *придружена квадратном имагираном бројевном пољу* K.[1] Слично као и у случају репрезентације $\rho_{\ell,E}$ везане за елиптичку криву E и за репрезентацију $\rho_{\ell,K}$ придружену квадратном имагинарном бројевном пољу K посматрамо пројекцију у $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ да бисмо добили репрезентацију

$$\hat{\rho}_{\ell,K} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Наредна теорема пружа потпун увид у структуру слике репрезентације $\rho_{\ell,K}$, као и репрезентације $\hat{\rho}_{\ell,K}$.

Теорема 7.2.1. *Означимо са N_ℓ слику репрезентације $\rho_{\ell,K}$ и са PN_ℓ слику репрезентације $\hat{\rho}_{\ell,K}$ у $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Тада је*

$$N_\ell = \left\{ \begin{bmatrix} a^{hw} & 0 \\ 0 & b^{hw} \end{bmatrix}, \begin{bmatrix} 0 & a^{hw} \\ b^{hw} & 0 \end{bmatrix} \middle| a,b \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}$$

и

$$PN_\ell = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & b^{hw} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ b^{hw} & 0 \end{bmatrix} \middle| b \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\},$$

[1] приметимо колико је пресликавање $\rho_{\ell,K}$ суптилно дефисано; из његове саме дефиниције није на први поглед јасно у каквој је вези са пољем K. Због тога конструкција пресликавања $\rho_{\ell,K}$ може деловати помало неприродно, односно не толико блиска самом пољу K. Такве сумње руши посматрање помоћних пресликавања која се користе у дефиницији репрезентације $\rho_{\ell,K}$; у њиховим дејствима фигуришу, између осталог, класни број, кардиналност групе инвертибилних елемената и аутоморфизам бројевног поља K, дакле неке од основних карактеристика тог поља.

при чему су h и w редом класни број, односно кардиналност групе инвертибилних елемената квадратног имагинарног бројевног поља K. Специјално, за кардиналности слика N_ℓ и PN_ℓ важи

$$|N_\ell| = 2\left(\frac{\ell-1}{\gcd(\ell-1,hw)}\right)^2 \text{ и } |PN_\ell| = \frac{2(\ell-1)}{\gcd(\ell-1,hw)}.$$

Доказ. Означимо са $S(\ell)$ групу класа зрака по модулу $\ell\mathscr{O}_K$ у бројевном пољу K. За сваки зрак $C \in S(\ell)$ постоји бесконачно много простих идеала $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ који су конјуговани са C у групи $S(\ell)$, што ћемо скраћено писати са $\mathfrak{p} \sim C$. Због тога, ако уочимо произвољно $\gamma \in (\mathscr{O}_K/\ell\mathscr{O}_K)^*$, постоји бесконачно много простих идеала $\mathfrak{p}$ прстена целих $\mathscr{O}_K$ таквих да је $\mathfrak{p} \sim \langle\gamma\rangle$. Имајући у виду дефиницију $\pi_\mathfrak{p}(K)$ добијамо да за све такве просте идеале $\mathfrak{p}$ важи

$$\pi_\mathfrak{p}(K) \equiv \gamma^{hw} \pmod{\ell\mathscr{O}_K}. \tag{7.6}$$

На основу Кинеске теореме о остацима имамо да $\gamma(\mathrm{mod}\ell)$ одговара пар (α,β) по модулима $\mathfrak{L}$ и $\bar{\mathfrak{L}}$ редом. Захваљујући оваквој вези, релацију (7.6) можемо записати у еквивалентном облику

$$\pi_\mathfrak{p}(K) \equiv \alpha^{hw}(\mathrm{mod}\mathfrak{L}) \text{ и } \overline{\pi_\mathfrak{p}(K)} \equiv \bar{\beta}^{hw}(\mathrm{mod}\overline{\mathfrak{L}}). \tag{7.7}$$

Нека је сада p рационалан прост број који се потпуно цепа у бројевном пољу K, као

$$p = \mathfrak{p}\cdot\bar{\mathfrak{p}}.$$

Означимо са Fr_p Фробенијусов аутоморфизам $\left(\overline{\mathbb{Q}}/\mathbb{Q},p\right)$ који одговара p у Галуаовој групи $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Користећи особине Фробенијусовог аутоморфизма, као и дефиницију репрезентације $\rho_{\ell,K}$ имамо да важи

$$\rho_{\ell,K}(\mathrm{Fr}_p) = \begin{bmatrix} \pi_\mathfrak{p}(K)(\mathrm{mod}\mathfrak{L}) & 0(\mathrm{mod}\mathfrak{L}) \\ 0(\mathrm{mod}\mathfrak{L}) & \overline{\pi_\mathfrak{p}(K)}(\mathrm{mod}\mathfrak{L}) \end{bmatrix}.$$

Одатле, на основу релација датих у (7.7), добијамо да је за рационалне просте бројеве p који се цепају у K слика $\rho_{\ell,K}(\mathrm{Fr}_p)$ дијагонална матрица чији су елементи hw-ти степени у $(\mathbb{Z}/\ell\mathbb{Z})^*$.

Треба још погледати каква је слика Фробенијусових аутоморфизама придружених рационалним простим бројевима који су инертни у K, односно рационалним простим бројевима p за које је $p\mathscr{O}_K$ прост идеал у K. Нека је θ нетривијалан $\mathbb{Q}$-аутоморфизам поља K. Приметимо да, на основу дефиниције репрезентације $\rho_{\ell,K}$, аутоморфизму θ у групи $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ одговара матрица

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Такође, за све $a, b \in (\mathbb{Z}/\ell\mathbb{Z})^*$ очигледно важи,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix},$$

што је, поново у сагласности са дефиницијом репрезентације $\rho_{\ell,K}$, довољно да утврдимо да је слика Фробенијусовог аутоморфизма придруженог произвољном рационалном простом броју који је инертан у K при пресликавању $\rho_{\ell,K}$ квадратна матрица облика

$$\begin{bmatrix} 0 & a^{hw} \\ b^{hw} & 0 \end{bmatrix},$$

за неке $a, b \in (\mathbb{Z}/\ell\mathbb{Z})^*$. Тиме је завршен доказ за N_ℓ; из њега директно следи и тврђење везано за PN_ℓ . Сами редови група N_ℓ и PN_ℓ добијају се пребројавањем елемената који су hw-ти степени у $(\mathbb{Z}/\ell\mathbb{Z})^*$. □

Слично као и за пројективну репрезентацију везану за елиптичку криву E, и за репрезентацију $\hat{\rho}_{\ell,K}$ придружену бројевном пољу K можемо урадити сечење по одговарајућем језгру, добијајући тако бијективну репрезентацију

$$\hat{\rho}_{\ell,K} : \mathrm{Gal}(F_{\ell,K}/\mathbb{Q}) \to PN_\ell,$$

при чему је $F_{\ell,K}$ раширење поља рационалних бројева такво да је гарантована инјективност пресликавања $\hat{\rho}_{\ell,K}$.

7.2.3 Дефиниција комбиноване Галуаове репрезентације

У досадашњем току излагања овог одељка видели смо да се елиптичкој кривој E и фиксираном квадратном имагинарном бројевном пољу K могу придружити бијективне пројективне репрезентације које смо редом означавали са $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$. При томе, репрезентације $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$ су дефинисане на раширењима поља $\mathbb{Q}$, која смо означавали редом са $F_{\ell,E}$ и $F_{\ell,K}$ и која су одабрана тако да је гарантована инјективност одговарајућих репрезентација. Подсетимо се да је циљ целокупног овог одељка проналажење начина да се две репрезентације- $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$, споје у једну репрезентацију која ће у себи носити особине обе своје компоненте, дакле која ће бити везана и за елиптичку криву E и бројевно поље K. Према томе, очигледно је да рад на остварењу тог циља изискује истовремено посматрање репрезентација $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$, па је потребно знати нешто о њиховом односу. Неопходну информацију о њему пружа теорема која следи, и то не изражену директно, него преко односа поља $F_{\ell,E}$ и $F_{\ell,K}$ на којима су репрезентације $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$ дефинисане. Пре саме формулације теореме, уведимо ознаке које ћемо користити у њеном исказу:

- ζ_ℓ је примитивни ℓ-ти корен из јединице
- $\mathbb{Q}(\zeta_\ell)$ је ℓ-то циклотомично раширење поља $\mathbb{Q}$

- $\mathbb{Q}(\sqrt{\ell^*})$ је квадратно раширење поља $\mathbb{Q}$ садржано у $\mathbb{Q}(\zeta_\ell)$

Теорема 7.2.2. *Нека су $F_{\ell,E}$ и $F_{\ell,K}$ поља на којима су дефинисане репрезентације $\hat{\rho}_{\ell,E}$ и $\hat{\rho}_{\ell,K}$. Тада важи:*

1. $F_{\ell,E} \cap F_{\ell,K} \subseteq \mathbb{Q}(\sqrt{\ell^*})$.
2. $F_{\ell,E} \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\sqrt{\ell^*})$.

Доказ. 1. Подсетимо се избора рационалног простог броја ℓ са самог почетка одељка, кога се држимо у току целокупног излагања: ℓ се потпуно цепа у K и довољно је велик број, тако да важи $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, при чему је $\mathbb{Q}(E[\ell])$ бројевно поље ℓ-торзионих тачака елиптичке криве E. Због таквог избора броја ℓ важи $K \cap F_{\ell,E} = \mathbb{Q}$, при чему још и раширење $KF_{\ell,E}/K$ има Галуаову групу $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Како је раширење $F_{\ell,K}$ Абелово, поље $KF_{\ell,E} \cap F_{\ell,K}$ представља једно Абелово раширење поља K. Међутим, приметимо да група $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ има само два количника који су Абелове групе, један реда 1 и други реда 2. Због тога је

$$[KF_{\ell,E} \cap F_{\ell,K} : K] \leq 2.$$

Из последње неједнакости имамо одмах, због $[K : \mathbb{Q}] = 2$ и неједнакост

$$[KF_{\ell,E} \cap F_{\ell,K} : \mathbb{Q}] \leq 4,$$

која директно повлачи неједнакост

$$[F_{\ell,E} \cap F_{\ell,K} : \mathbb{Q}] \leq 2. \tag{7.8}$$

Коначно, због претпоставке да важи $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$ следи да се $F_{\ell,E} \cap F_{\ell,K}/\mathbb{Q}$ рамификује само у ℓ. Одатле, уз неједнакост (7.8), следи $F_{\ell,E} \cap F_{\ell,K} \subseteq \mathbb{Q}(\sqrt{\ell^*})$, чиме је доказан први део теореме.
2. По својој дефиницији поље $F_{\ell,E}$ је једно потпоље поља $\mathbb{Q}(E[\ell])$ које је фиксно у односу на дејство свих скаларних матрица. Приметимо да је дејство произвољне скаларне матрице

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \ a \in \bar{\mathbb{Q}}$$

на примитивни ℓ-ти корен јединице ζ_ℓ одређено са

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \zeta_\ell = \zeta_\ell^{a^2}.$$

Из две претходно наведене чињенице, имајући у виду дефиницију поља $\mathbb{Q}(\sqrt{\ell^*})$, одмах следи да је

$$F_{\ell,E} \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\sqrt{\ell^*}),$$

чиме је завршен доказ другог дела теореме. □

Теорема 7.2.2 имаће значајну улогу приликом доказивања постојања једне особине комбинованих Галуаових репрезентација, која је од великог оперативног значаја. Пре самог извођења поменутог доказа, прикажимо коначно дефиницију *комбинованих Галуаових репрезентација.*

Дефиниција 7.2.1. *Нека је E елиптичка крива и K квадратно имагинарно бројевно поље, којима су придружене бијективне пројективне репрезентације $\hat{\rho}_{\ell,E}$, односно $\hat{\rho}_{\ell,K}$ дефинисане редом на пољима $F_{\ell,E}$ и $F_{\ell,K}$.* ***Комбинована Галуаова репрезентација*** *придружена истовремено елиптичкој кривој E и бројевном пољу K, у ознаци $\hat{\rho}_\ell$, дефинисана је као производ-репрезентација:*

$$\hat{\rho}_\ell : \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell,$$

$$\hat{\rho}_\ell(\sigma) = (\hat{\rho}_{\ell,E}(\sigma), \hat{\rho}_{\ell,K}(\sigma)),$$

при чему је PN_ℓ слика репрезентације $\hat{\rho}_{\ell,K}$, детаљно описана Теоремом 7.2.1, и $\sigma \in \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q})$ произвољан аутоморфизам.

Напоменимо да ћемо често писати скраћено $F_\ell/\mathbb{Q}$ уместо $F_{\ell,E}F_{\ell,K}/\mathbb{Q}$.

Нека је $\hat{\rho}_\ell$ комбинована Галуаова репрезентација везана истовремено за елиптичку криву E и квадратно имагирно бројевно поље K. Означимо са G_ℓ слику те репрезентације. Нагласимо још једном да сматрамо да је ℓ рационалан прост број који се цепа у K и довољно је велик , тако да важи $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, при чему је $\mathbb{Q}(E[\ell])$ бројевно поље ℓ-торзионих тачака елиптичке криве E. Приметимо да ако уз наведене претпоставке претпоставимо и $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$, имамо да важи

$$G_\ell \cong \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell.$$

На овом месту се природно јавља питање егзистенције и бројности рационалних простих бројева ℓ са траженим својствима. Теорема која следи пружа одговор на то питање, у виду гарантовања егзистенције бесконачно много простих бројева ℓ који имају наведена својства и који се јављају у аритметичких прогресијама по модулу у зависности од квадратног имагинарног бројевног поља K. Пре саме формулације и доказа теореме, напоменимо да ознаке које ћемо при том користити имају исто значење које су имале до сада.

Теорема 7.2.3. *1. Нека је $K = \mathbb{Q}(i)$. Ако је $\ell \equiv 5 (\mathrm{mod}\ 8)$, рационалан прост број ℓ се цепа у K и важи $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.*
2. Нека је $K = \mathbb{Q}(\sqrt{-D})$, где је $D > 1$ бесквадратан цео број. Запишимо D у облику $D = 2^k D'$ за непаран број D' и $k \in \{0, 1\}$. Тада:

а) *Ако је $D' \equiv 1 (\mathrm{mod}\ 4)$, за сваки рационалан прост број ℓ такав да је*

$$\ell \equiv 7 (\mathrm{mod}\ 8) \text{ и } \left(\frac{\ell}{D'}\right) = -1,$$

важи да се ℓ цепа у K и $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.

б) *Ако је* $D' \equiv 3 (\mathrm{mod}\ 4)$, *за сваки рационалан прост број* ℓ *такав да је*

$$\ell \equiv 7 (\mathrm{mod}\ 8) \text{ и } \left(\frac{\ell}{D'}\right) = 1,$$

важи да се ℓ *цепа у* K *и* $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.

Доказ. Подсетимо се да смо са h означавали класни број, а са w кардиналност групе инвертибилних елемената квадратног имагинарног бројевног поља K.
1. Ако је $K = \mathbb{Q}(i)$, тада је $hw = 4$. Претпоставимо да је $\ell \equiv 5 (\mathrm{mod}\ 8)$, као у исказу теореме. Користећи Теорему 7.2.1 онда добијамо да важи

$$[F_{\ell,K} : K] = \frac{|PN_\ell|}{2} = \frac{\ell - 1}{4}. \tag{7.9}$$

Приметимо да је $\frac{\ell-1}{4}$ непаран цео број, па на основу (7.9) закључујемо да $F_{\ell,K}/K$ нема потпоље реда 2. Због тога је $\mathbb{Q}(\sqrt{\ell^*}) \not\subseteq F_{\ell,K}$. Како је на основу Теореме 7.2.2 гарантовано

$$F_{\ell,E} \cap F_{\ell,K} \subseteq \mathbb{Q}(\sqrt{\ell^*})$$

и због тога што је по дефиницији поље $\mathbb{Q}(\sqrt{\ell^*})$ степена 2 над $\mathbb{Q}$, из последње чињенице закључујемо

$$F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q},$$

чиме је доказан први део теореме.
2. За произвољно квадратно имагинарно бројевно поље важи $2 \mid hw$. Одатле, користећи Теорему 7.2.1, добијамо да је

$$[F_{\ell,K} : K] = \frac{|PN_\ell|}{2} = \left(\frac{\ell - 1}{\gcd(hw, \ell - 1)}\right)^2, \text{ што дели } \left(\frac{\ell - 1}{2}\right)^2.$$

Приметимо да се и у случају а) и у случају б) у исказу теореме претпоставља $\ell \equiv 7 (\mathrm{mod}\ 8)$. За такве ℓ је број $\left(\frac{\ell-1}{2}\right)^2$ непаран, па следи да да $F_{\ell,K}/K$ нема потпоље реда 2. Због тога је $\mathbb{Q}(\sqrt{\ell^*}) \not\subseteq F_{\ell,K}$, одакле на основу Теореме 7.2.2, на потпуно исти начин као у доказу дела *1.* закључујемо

$$F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}.$$

Да бисмо завршили доказ теореме потребно је још да покажемо да се рационалан прост број ℓ цепа у $K = \mathbb{Q}(\sqrt{-D})$ под претпостављеним условима. Користећи Теорему 4.3.6 добијамо да је чињеница коју треба доказати еквивалентна са

$$\left(\frac{-D}{\ell}\right) = 1. \tag{7.10}$$

Користећи основне особине Лежандровог симбола имамо

$$\begin{aligned}\left(\frac{-D}{\ell}\right) &= \left(\frac{-2^k D'}{\ell}\right)\\ &= \left(\frac{-1}{\ell}\right)\left(\frac{2^k}{\ell}\right)\left(\frac{D'}{\ell}\right)\\ &= (-1)^{\frac{\ell-1}{2}}\left(\frac{2^k}{\ell}\right)\left(\frac{D'}{\ell}\right)\\ &= (-1)^{\frac{\ell-1}{2}}\left(\frac{2^k}{\ell}\right)\left(\frac{\ell}{D'}\right)(-1)^{\frac{\ell-1}{2}\frac{D'-1}{2}}\\ &= (-1)^{\ell-1}\left(\frac{2^k}{\ell}\right)\left(\frac{\ell}{D'}\right)(-1)^{\frac{D'-1}{2}}\\ &= (-1)\left(\frac{2}{\ell}\right)^k\left(\frac{\ell}{D'}\right)(-1)^{\frac{D'-1}{2}},\end{aligned}$$

што значи да се формула (7.10) може записати у еквивалентном облику

$$(-1)\left(\frac{2}{\ell}\right)^k\left(\frac{\ell}{D'}\right)(-1)^{\frac{D'-1}{2}} = 1. \tag{7.11}$$

Ако је $D' \equiv 1 (\mathrm{mod}\ 4)$, као у случају а), имамо да међу свим $\ell \equiv 7 (\mathrm{mod}\ 8)$, бројеви за које је

$$\left(\frac{\ell}{D'}\right) = -1,$$

задовољавају формулу (7.11). Имајући у виду низ еквиваленција који је претходио формули (7.11) закључујемо да се такви рационални прости бројеви ℓ цепају у K.

Са друге стране, ако је $D' \equiv 3 (\mathrm{mod}\ 4)$, као у случају б), имамо да међу свим $\ell \equiv 7 (\mathrm{mod}\ 8)$, бројеви за које је

$$\left(\frac{\ell}{D'}\right) = 1,$$

задовољавају формулу (7.11). Идентично као у случају а), закључујемо да се такви рационални прости бројеви ℓ цепају у K. На тај начин су доказана оба случаја дела *2.* теореме, чиме је њен доказ завршен. □

Теорема 7.2.3 омогућава примењивост комбинованих Галуаових репрезентација, које ћемо користити приликом извођења асимптотске релације за $\Pi_E(K; x)$ у одељку који следи. За рационалан прост број ℓ ћемо надаље претпостављати да испуњава услове неког од случајева Теореме 7.2.3 (ово је могуће јер наведена теорема гарантује егзистенцију *бесконачно много* таквих бројева). Тада је

$$G_\ell = \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell.$$

Специјално, важи

$$|G_\ell| = |PGL_2(\mathbb{Z}/\ell\mathbb{Z})| \cdot |PN_\ell| = \frac{2\ell(\ell-1)^2(\ell+1)}{\gcd(\ell-1, hw)} \asymp_K \ell^4, \tag{7.12}$$

при чему константа у $\asymp_K$ зависи од квадратног имагинарног бројевног поља K.

7.3 Асимптотска формула за $\Pi_E(K;x)$

Нека је $E/\mathbb{Q}$ елиптичка крива са кондуктором N и без комплексног множења. Уз криву E посматрамо и фиксирано квадратно имагинарно бројевно поље $K = \mathbb{Q}(\sqrt{-D})$ ($D > 0-$ бесквадратан цео број) чији је класни број h, а кардиналност групе инвертибилних елемената w. У Одељку 7.1 дефинисали смо функцију $\Pi_E(K;x)$ као

$$\Pi_E(K;x) = \#\{p \leq x \mid p \nmid N, \mathbb{Q}(\pi_p(E)) = K\},$$

при чему је $\pi_p(E)$ одређен као корен карактеристичног полинома (7.3). Циљ овог одељка је извођење асимптотске формуле за функцију $\Pi_E(K;x)$, када $x \to +\infty$.

Као први корак на пут ка извођењу поменуте асимптотске формуле, приметимо да је довољно да посматрамо просте бројеве $p \nmid N$ за које је $a_p \neq 0$. Наиме, у случају да је $a_p = 0$, карактеристични полином (7.3) је

$$P_{E,p}(X) = X^2 + p,$$

па је очигледно $\pi_p(E) = \sqrt{-p}$. Због тога је $\mathbb{Q}(\pi_p(E)) = \mathbb{Q}(\sqrt{-p})$, што значи да посматрани прости бројеви тј. они прости бројеви p за које је $a_p = 0$, доприносе вредности функције $\Pi_E(K;x)$ са највише 1 и то ако је баш $K = \mathbb{Q}(\sqrt{-p})$.

Једно од основних средстава које ћемо користити приликом извођења асимптотске формуле за функцију $\Pi_E(K;x)$ биће ефективне верзије Теореме Чеботарева, приказане у Поглављу 5. Лема која следи је елементарна по својој природи, али ће бити од великог значаја приликом дефинисања контекста у које ћемо примењивати наведене теореме, чиме ћемо се детаљно бавити после њеног доказа.

Лема 7.3.1. *Нека су a и b међусобно независне променљиве и n позитиван цео број. Тада постоји полином $P_n(X) \in \mathbb{Z}[X]$ такав да је*

$$\frac{(a^n + b^n)^2}{(ab)^n} = P_n\left(\frac{(a+b)^2}{ab}\right).$$

Доказ. Приметимо прво да важи

$$\frac{(a+b)^2}{ab} = \frac{a^2 + 2ab + b^2}{ab} = \frac{a}{b} + 2 + \frac{b}{a},$$

као и

$$\frac{(a^n+b^n)^2}{(ab)^n} = \frac{a^{2n}+2a^nb^n+b^{2n}}{(ab)^n} = \frac{a^n}{b^n} + 2 + \frac{b^n}{a^n}.$$

Због тога, ако уведемо смену $t = \frac{a}{b}$, добијамо да се доказ леме своди на доказивање егзистенције полинома $P_n(X) \in \mathbb{Z}[X]$ таквог да је

$$t^n + 2 + \frac{1}{t^n} = P_n\left(t + 2 + \frac{1}{t}\right).$$

Приметимо да је за доказ тог тврђења довољно доказати да важи

$$\left(t + 2 + \frac{1}{t}\right)^n = t^n + 2 + \frac{1}{t^n} + Q_n\left(t + 2 + \frac{1}{t}\right) \tag{7.13}$$

за неки полином $Q_n(X) \in \mathbb{Z}[X]$, јер тада можемо дефинисати

$$P_n(X) = X^n - Q_n(X).$$

Дакле, све што треба да урадимо је да докажемо тачност формуле (7.13), што ћемо урадити индукцијом по природном броју n.

Приметимо да за $n = 1$ и $n = 2$ имамо очигледно $Q_1(X) = 0$ и $Q_2(X) = 4X - 4$.

Претпоставимо да тврђење важи за све $k \leq n-1$. Тада за $k = n$ имамо:

$$\begin{aligned}
\left(t+2+\frac{1}{t}\right)^n &= \left(t+2+\frac{1}{t}\right)^{n-1}\left(t+2+\frac{1}{t}\right) \\
&= \left(t^{n-1}+2+\frac{1}{t^{n-1}}+Q_{n-1}\left(t+2+\frac{1}{t}\right)\right)\left(t+2+\frac{1}{t}\right) \\
&= \left(t+2+\frac{1}{t}\right)Q_{n-1}\left(t+2+\frac{1}{t}\right)+2\left(t+2+\frac{1}{t}\right) \\
&+ t^{n-1}\left(t+2+\frac{1}{t}\right)+\frac{1}{t^{n-1}}\left(t+2+\frac{1}{t}\right) \\
&= \left(t+2+\frac{1}{t}\right)Q_{n-1}\left(t+2+\frac{1}{t}\right)+2\left(t+2+\frac{1}{t}\right) \\
&+ \left(t^n+2+\frac{1}{t^n}\right)+2\left(t^{n-1}+\frac{1}{t^{n-1}}\right)+t^{n-2}+\frac{1}{t^{n-2}}-2 \\
&= \left(t^n+2+\frac{1}{t^n}\right)+\left(t+2+\frac{1}{t}\right)Q_{n-1}\left(t+2+\frac{1}{t}\right)+2\left(t+2+\frac{1}{t}\right) \\
&+ 2\left(t^{n-1}+2+\frac{1}{t^{n-1}}\right)+\left(t^{n-2}+2+\frac{1}{t^{n-2}}\right)-8 \\
&= \left(t^n+2+\frac{1}{t^n}\right)+\left(t+2+\frac{1}{t}\right)Q_{n-1}\left(t+2+\frac{1}{t}\right)+2\left(t+2+\frac{1}{t}\right) \\
&+ 2\left(\left(t+2+\frac{1}{t}\right)^{n-1}-Q_{n-1}\left(t+2+\frac{1}{t}\right)\right)+\left(t+2+\frac{1}{t}\right)^{n-2} \\
&- Q_{n-2}\left(t+2+\frac{1}{t}\right)-8 \\
&= \left(t^n+2+\frac{1}{t^n}\right)+\left(t+2+\frac{1}{t}\right)Q_{n-1}\left(t+2+\frac{1}{t}\right)+2\left(t+2+\frac{1}{t}\right) \\
&+ 2\left(t+2+\frac{1}{t}\right)^{n-1}-2Q_{n-1}\left(t+2+\frac{1}{t}\right)+\left(t+2+\frac{1}{t}\right)^{n-2} \\
&- Q_{n-2}\left(t+2+\frac{1}{t}\right)-8.
\end{aligned}$$

Из последње једнакости одмах следи да полином $Q_n(X) \in \mathbb{Z}[X]$, дефинисан са

$$Q_n(X) = XQ_{n-1}(X) + 2X + 2X^{n-1} - 2Q_{n-1}(X) + X^{n-2} - Q_{n-2}(X) - 8$$

задовољава формулу (7.13), чиме је завршен индукцијски корак, а тиме и доказ леме. □

Оквир који ћемо посматрати у даљем излагању одређен је комбинованим Галуаовим репрезентацијама, дефинисаним у одељку 7.2. Нагласимо да за рационалан прост број ℓ задржавамо претпоставке којих смо се држали у наведеном одељку. Такође, у поменутом одељку могу се пронаћи дефиниције објеката које ћемо користити у наставку нашег излагања, а не буду експлицитно поновљене.

Пређимо сада на дефинисање скупа C_ℓ у групи G_ℓ, који ће бити један од централних објеката у нашем даљем излагању. Значај скупа C_ℓ је у томе што пружа карактеризацију простих бројева p таквих да је $\mathbb{Q}(\pi_p(E)) = K$.

Дефиниција 7.3.1. *Означимо за произвољну матрицу* $g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

$$t(g) = \frac{(\operatorname{Tr} g)^2}{\det g}.$$

Дефинишемо $C_\ell \subseteq G_\ell$ *са*

$$C_\ell = \left\{ (\hat{g_1}, \hat{g_2}) \in G_\ell \mid t(g_2) = P_{hw}(t(g_1)), g_2 = \begin{bmatrix} 1 & 0 \\ 0 & b^{hw} \end{bmatrix} \ u \ \left(\frac{(\operatorname{Tr} g_1)^2 - 4 \det g_1}{\ell} \right) = 1 \right\}.$$

У контексту претходне дефиниције приметимо да су $t(g)$, као и услов везан за Лежандров симбол у дефиницији C_ℓ коректно дефинисани за матрице у $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Теорема 7.3.1. *Нека је* ℓ *прост број који се потпуно цепа у квадратном бројевном пољу* K *и нека је* $C_\ell \subset G_\ell$ *скуп одређен дефиницијом 7.3.1. Тада је*

$$\Pi_E(K; x) \leq \Pi_{C_\ell}(x, F_\ell/\mathbb{Q}).$$

Доказ. Нека је p прост број који је нерамификован у раширењу $F_\ell/\mathbb{Q}$ и такав да је $a_p(E) \neq 0$ и $\mathbb{Q}(\pi_p(E)) = K$. Са једне стране, p се потпуно цепа у $\mathbb{Q}(\pi_p(E)) = K$ и то као

$$p\mathscr{O}_K = (\pi_p(E))\overline{(\pi_p(E))} =: \mathfrak{p} \cdot \bar{\mathfrak{p}}.$$

Са друге стране, нека је $\pi_p(K)$ један од $\pi_{\mathfrak{p}}(K)$ или $\pi_{\bar{\mathfrak{p}}}(K)$. Из дефиниције $\pi_p(K)$ онда имамо

$$p^{hw}\mathscr{O}_K = (\pi_p(E))\overline{(\pi_p(E))}$$

и

$$\hat{\rho}(\mathrm{Fr}_p) = \begin{bmatrix} \pi_p(K) \pmod{\mathfrak{L}} & 0 \pmod{\mathfrak{L}} \\ 0 \pmod{\mathfrak{L}} & \overline{\pi_p(K)} \pmod{\mathfrak{L}} \end{bmatrix}.$$

Комбинацијом претходних запажања, уз евентуално претходно преименовање корена, добијамо

$$\pi_p(E)^{hw} = \pi_p(K). \tag{7.14}$$

Коришћењем Леме 7.3.1, из формуле (7.14) добијамо

$$\frac{\left(\pi_p(K)+\overline{\pi_p(K)}\right)^2}{\pi_p(K)\overline{\pi_p(K)}}=\frac{\left(\pi_p(E)^{hw}+\overline{\pi_p(E)}^{hw}\right)^2}{\pi_p(E)^{hw}\overline{\pi_p(E)}^{hw}}=P_{hw}\left(\frac{\left(\pi_p(E)+\overline{\pi_p(E)}\right)^2}{\pi_p(E)\overline{\pi_p(E)}}\right).$$

Сада редукцијом по модулу ℓ леве и десне стране последње једнакости (која је коректна због тога што су обе стране елементи поља $\mathbb{Q}$ са имениоцима узајамно простим са ℓ) и коришћењем дефиниције $\hat{\rho}_{\ell,K}(\mathrm{Fr}_p)$ за просте бројеве p који се потпуно цепају у K добијамо

$$t(\hat{\rho}_{\ell,K}(\mathrm{Fr}_p))\equiv P_{hw}(t(\hat{\rho}_{\ell,E}(\mathrm{Fr}_p)))\pmod{\ell}.$$

Коначно, приметимо да претпоставка да се ℓ потпуно цепа у $K=\mathbb{Q}(\pi_p(E))$ имплицира да се карактеристични полином $P_{E,p}=X^2-a_p(E)X+p$ за $\pi_p(E)$ потпуно цепа у $\mathbb{F}_\ell[X]$. Одатле следи да је

$$\left(\frac{(\operatorname{Tr}\hat{\rho}_{\ell,K}(\mathrm{Fr}_p))^2-4\det\hat{\rho}_{\ell,K}(\mathrm{Fr}_p)}{\ell}\right)=1,$$

чиме је доказ завршен. □

Уз скуп C_ℓ, чији значај показује претходна теорема, дефинишемо још неколико значајних скупова на следећи начин:

- $B_\ell=\left\{(\hat{g_1},\hat{g_2})\in G_\ell \mid g_1=\begin{bmatrix}a_1 & b_1\\ 0 & d_1\end{bmatrix} \text{ и } g_2=\begin{bmatrix}a_2 & 0\\ 0 & b_2\end{bmatrix}\right\}$. Приметимо да B_ℓ није само скуп, већ је и група у односу на уобичајену операцију множења матрица.

- Дефинишемо $\Gamma\subseteq B_\ell\cap C_\ell$ као максимални скуп елемената $\gamma=(\hat{\gamma_1},\hat{\gamma_2})$ који нису међусобно конјунговани у G_ℓ.

  Приметимо да за $g=(\hat{g_1},\hat{g_2})\in C_\ell$ важи

  $$\left(\frac{(\operatorname{Tr} g_1)^2-4\det g_1}{\ell}\right)=1,$$

  што значи да је g конјугат неког елемента из B_ℓ. Због тога, ако са $C_{G_\ell}(\gamma)$ означимо класу конјугације елемента γ у групи G_ℓ, имамо да је

  $$C_\ell=\cup_{\gamma\in\Gamma}C_{G_\ell}(\gamma).$$

- Означимо слично као у претходној тачки са $C_{B_\ell}(\gamma)$ класу конјугације елемента γ у групи B_ℓ. Онда дефинишемо скуп D_ℓ као

  $$D_\ell=\cup_{\gamma\in\Gamma}C_{B_\ell}(\gamma).$$

Наредна теорема показује нека основна својства претходно дефинисаних скупова.

Теорема 7.3.2. *Нека су B_ℓ, D_ℓ и Γ претходно дефинисани скупови. Тада важи*

1. $|B_\ell| = \frac{\ell(\ell-1)^2}{\gcd(\ell-1,hw)} \asymp_K \ell^3$.
2. $|\Gamma| \asymp \ell$.
3. *Нека је $\gamma \in \Gamma$. Тада је*
$$|C_{G_\ell}(\gamma)| \asymp \ell^2$$
и
$$|C_{B_\ell}(\gamma)| \asymp \ell.$$
4. *Важи*
$$|C_\ell| \asymp \ell^3$$
и
$$|D_\ell| \asymp \ell^2.$$
5. *Нека је $\gamma \in \Gamma$. Тада је*
$$\frac{|C_{B_\ell}(\gamma)|/|B_\ell|}{|C_{G_\ell}(\gamma)|/|G_\ell|} = 1 + \underline{o}(1).$$

Доказ. 1. Следи директно бројањем матрица у B_ℓ.
2. Нека је $(\hat{g_1}, \hat{g_2}) \in C_\ell$. Из дефиниције скупа C_ℓ имамо да је

$$\left(\frac{(\operatorname{Tr} g_1)^2 - 4\det g_1}{\ell}\right) = 1,$$

што значи да је g_1 конјугована у групи $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ дијагоналној матрици

$$\gamma_1 = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}, \text{ уз услов } \alpha \neq \beta. \tag{7.15}$$

Такође, било које две дијагоналне матрице су конјуговане у $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ ако и само ако имају исте елементе на дијагонали. Одатле добијамо да за број класа конјугације за $\hat{g_1}$ важи да је $\asymp \ell$. Како је из дефиниције C_ℓ матрица g_2 дијагонална и $\hat{g_2}$ је потпуно одређена са $\hat{g_1}$, добијамо да је $|\Gamma| \asymp \ell$.
3. Да бисмо проценили $|C_{G_\ell}(\gamma)|$, приметимо прво да се класа конјугације дијагоналне матрице облика (7.15) у $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ састоји од свих матрица чији је траг једнак $\alpha+\beta$, а детерминанта $\alpha\beta$. За број таквих матрица важи да је асимптотски $\asymp \ell^2$. Додатно, никоје две такве матрице нису еквиваленте у $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Одатле, имајући у виду да за $\gamma = (\gamma_1, \gamma_2)$, где је γ_1 дијагонална матрица облика (7.15), класа конјугације за γ_2 у PN_ℓ има највише 2 елемента, добијамо тражену процену за $|C_{G_\ell}(\gamma)|$.

Што се тиче процене за $|C_{G_\ell}(\gamma)|$, она се изводи потпуно аналогно, када знамо да конјуговање матрицама из B_ℓ се изводи као

$$\frac{1}{d}\begin{bmatrix}1 & b\\ 0 & d\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & \beta\end{bmatrix}\begin{bmatrix}d & -b\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & \frac{b(\beta-1)}{d}\\ 0 & \beta\end{bmatrix}.$$

4. Следи одмах из делова *2.* и *3.*
5. Следи одмах из (7.12) и делова *1.* и *3.* □

Теорема 7.3.1 гарантује да је за извођење асимптотске формуле за $\Pi_E(K;x)$, што је, подсетимо се, циљ овог одељка, довољно направити процену за $\pi_{C_\ell}(x, F_\ell/\mathbb{Q})$. Да бисмо то урадили, користићемо метод редукције, који омогућава да применимо ефективне верзије теореме Чеботарева о густини у *Абеловом* раширењу бројевних поља, дакле управо у оном раширење где важи АНС.

Први корак ка најављеном циљу је редукција Галуаове групе коју посматрамо са G_ℓ на B_ℓ. То ћемо учинити у неколико етапа. Прво, коришћењем Теореме 5.2.1 и Теореме 7.3.2, део*5.* закључујемо да за све $\gamma \in \Gamma$ важи

$$\tilde{\pi}_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q}) = (1+\underline{o}(1))\tilde{\pi}_{C_{B_\ell}(\gamma)}(x, F_\ell/{F_\ell}^{B_\ell}).$$

Одатле следи да је

$$\begin{aligned}\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) = \sum_{\gamma\in\Gamma}\pi_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q}) &\le \sum_{\gamma\in\Gamma}\tilde{\pi}_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q})\\ &\ll \sum_{\gamma\in\Gamma}\tilde{\pi}_{C_{B_\ell}(\gamma)}(x, F_\ell/{F_\ell}^{B_\ell}) = \tilde{\pi}_\phi(x), \qquad (7.16)\end{aligned}$$

где је $\phi : B_\ell \to \{0,1\}$ карактеристична функција скупа $D_\ell = \cup_{\gamma\in\Gamma} C_{B_\ell}(\gamma)$.

Даље, користећи први део Теореме 5.2.1 за $L = F_\ell$, $k = F_\ell^{B_\ell}$ и $G = \mathrm{Gal}(F_\ell/F_\ell^{B_\ell})$ заједно са Последицом 5.1.2 добијамо да је

$$\tilde{\pi}_\phi(x) = \pi_\phi(x) + O\left(\ell\log(\ell d_K N) + \ell x^{\frac{1}{2}}\right). \qquad (7.17)$$

При томе је имплицитна O-константа апсолутна. Због тога, све што остаје да се уради у циљу процењивања $\pi_{C_\ell}(x, F_\ell/\mathbb{Q})$ је да се процени $\pi_\phi(x)$, где је ϕ карактеристична функција скупа D_ℓ. У сврху те процене дефинишемо

$$H_\ell = \left\{(\hat{g_1}, \hat{g_2}) \in B_\ell \mid g_1 = \begin{bmatrix}a_1 & b_1\\ 0 & a_1\end{bmatrix}, g_2 = \begin{bmatrix}a_2 & 0\\ 0 & a_2\end{bmatrix}\right\} \qquad (7.18)$$

Очигледно је да је H_ℓ подгрупа од B_ℓ, а њена даља својства показује наредна теорема.

Теорема 7.3.3. *Нека је H_ℓ подгупа дефинисана са (7.18). Тада важи:*

1. *H_ℓ је нормална подгрупа од B_ℓ и количничка група B_ℓ/H_ℓ је Абелова.*

2. *$H_\ell D_\ell \subseteq D_\ell$.*

3. *$|H_\ell| \asymp l$.*

Доказ. 1. Овај део теореме следи одмах ако приметимо да је H_ℓ језгро хомоморфизма група

$$\Theta : B_\ell \to (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*$$

одређеног са

$$\Theta\left(\widehat{\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}}, \widehat{\begin{bmatrix} a_2 & 0 \\ 0 & d_2 \end{bmatrix}}, \right) \to (a_1^{-1}d_1, a_2^{-1}d_2),$$

где су $a_1, b_1, d_1, d_2 \in \mathbb{Z}/\ell\mathbb{Z}$.
2. Нека је $(\hat{g_1}, \hat{g_2}) \in G_\ell$. Како је $\hat{g_2}$ јединична матрица, довољно је видети како се прва компонента у D_ℓ понаша при множењу са g_1. Имамо да је

$$\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & b \\ 0 & \beta \end{bmatrix} = \begin{bmatrix} \alpha & b + \beta b_1 \\ 0 & \beta \end{bmatrix}.$$

што је и даље матрица у истој класи конјугације у D_ℓ као и

$$\begin{bmatrix} \alpha & b \\ 0 & \beta \end{bmatrix},$$

чиме је доказ овог дела теореме завршен.
3. Овај део следи одмах тривијалним пребројавањем. □

Претходна теорема омогућава даљу редукцију на групу B_ℓ/H_ℓ. Штавише, имамо гаранцију да је поменута група *Абелова* и управо та чињеница је кључна за наставак пута ка нашем циљу, а то је извођење асимптотске формуле за $\Pi_E(K; x)$. Наиме, како је група B_ℓ/H_ℓ Абелова, АНС важи за Артинове L-функције придружене иредуцибилним карактерима те групе. Због тога је оправдана примена Теореме 5.1.6, на основу које, уз претпоставку GRH добијамо

$$\begin{aligned} \pi_\phi(x) = \pi_{D_\ell}(x; F_\ell/F_\ell^{B_\ell}) &\ll \frac{|D_\ell|}{|C_\ell|} \operatorname{li} x + \left(\frac{|D_\ell|}{|H_\ell|}\right)^{\frac{1}{2}} \left[F_\ell^{B_\ell} : \mathbb{Q}\right] x^{\frac{1}{2}} \log M(F_\ell/F_\ell^{B_\ell}) \\ &\ll \frac{\gcd(\ell - 1, hw)}{\ell} \cdot \frac{x}{\log x} + \ell^{\frac{3}{2}} x^{\frac{1}{2}} \log(\ell d_K N x) \\ &\ll \frac{hwx}{\ell \log x} + \ell^{\frac{3}{2}} x^{\frac{1}{2}} \log(\ell d_K N x), \end{aligned} \tag{7.19}$$

при чему смо још у оценама користили Теореме 7.3.2, 7.3.3, Последицу 5.1.2, као и формулу (7.12). Коначно, комбинујући добијено у формулама (7.16), (7.17) и (7.19), уз претпоставку GRH имамо да важи

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hwx}{\ell \log x} + \ell^{\frac{3}{2}} x^{\frac{1}{2}} \log(\ell d_K N x) + \ell \log(\ell d_K N). \tag{7.20}$$

Нагласимо да је имплицитна $\ll$-константа апсолутна. Такође, приметимо да је $w \leq 4$ и да можемо сматрати да је $d_K \leq 4x$, јер је иначе $\Pi_E(K; x) = 0$. Користећи те напомене, формула (7.20) добија облик

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hw}{\ell \log x} + \ell^{\frac{3}{2}} x^{\frac{1}{2}} \log(\ell N x) + \ell \log(\ell N) \tag{7.21}$$

са апсолутном $\ll$-константом.

Наредни циљ који имамо је да додатно побољшамо формулу (7.21). То ћемо учинити на веома суптилан начин, који је већ најављен на почетку овог одељка приликом формулисања услова за прост број ℓ. Тада је речено да ће ℓ имати параметарску улогу и да ће у погодном тренутку бити изабран оптимално у односу на x. Тај тренутак је управо дошао и бирамо ℓ такво да је

$$\ell \asymp \frac{h^{\frac{2}{5}} x^{\frac{1}{5}}}{(\log x)^{\frac{4}{5}}}. \tag{7.22}$$

Уз такав избор параметра ℓ формула (7.21) добија облик

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{h^{\frac{3}{5}} x^{\frac{4}{5}}}{(\log x)^{\frac{1}{5}}} + \frac{h^{\frac{3}{5}} x^{\frac{4}{5}} \log(hNx)}{(\log x)^{\frac{6}{5}}}.$$

Због тога је и

$$\Pi_E(K; x) \ll_{N,h} \frac{x^{\frac{4}{5}}}{(\log x)^{\frac{1}{5}}}, \tag{7.23}$$

при чему имплицитна $\ll$-константа зависи од N и h.

Наравно, асимптотска формула (7.23) је у потпуној зависности од егзистенције простог броја ℓ који задовољава услове Теореме 7.2.3 (што је есенцијално за егзистенцију комбинованих Галуавих репрезентација и сматрамо да ℓ испуњава током целокупног излагања) и има величину одређену са (7.22). Због тога је значајно показати да такав прост број постоји, што ће следити из *Теореме о простим бројевима за просте бројеве у аритметичким прогресијама*, под претпоставком GRH.

Наиме, ако означимо

$$y = \frac{h^{\frac{2}{5}} x^{\frac{1}{5}}}{(\log x)^{\frac{4}{5}}}$$

онда GRH гарантује да постоји прост број ℓ који задовољава услове Теореме 7.2.3 и лежи у сегменту $[y, y+u]$ за свако u такво да је

$$y^{\frac{1}{2}}(\log y)^{2+\varepsilon} \leq u \leq y.$$

Тада, једино што је још остало да урадимо је да одаберемо довољно велико x такво да је репрезентација $\rho_{E,\ell}$ сурјективна и да важи $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$ (што је био последњи од есенцијалних захтева за прост број ℓ са почетка овог одељка), чиме је показана егзистенција простог броја ℓ, а тиме и асимптотске формуле (7.23).[2]

Горња асимптотска оцена (7.23) добијена је уз помоћ оцене за $\pi_\phi(x)$ на основу првог дела Теореме 5.1.6. Ако уз GRH претпоставимо и PCC, можемо применити други део те теореме и тако добити прецизнију оцену.

Заиста, примена другог дела Теореме 5.1.6 уз претпоставке GRH и PCC уводи додатни фактор $\frac{1}{\sqrt{\ell}}$ у грешку, што доводи до формуле

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell x^{\frac{1}{2}} \log(\ell N x) + \ell \log(\ell N), \tag{7.24}$$

при чему је имплицитна $\ll$-константа апсолутна. Сада бирамо оптимално параметар ℓ тако да важи

$$\ell \asymp \frac{h^{\frac{1}{2}} x^{\frac{1}{4}}}{\log x}.$$

Оправданост оваквог избора ℓ важи потпуно аналогно као оправнданост избора (7.22). Формула (7.24) овим избором добија облик

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll h^{\frac{1}{2}} x^{\frac{3}{4}} + h^{\frac{1}{2}} x^{\frac{3}{4}} \frac{\log(hNx)}{\log x},$$

одакле је и

$$\Pi_E(K; x) \ll_{N,h} x^{\frac{3}{4}}, \tag{7.25}$$

при чему имплицитна $\ll$-константа зависи од N и h.

[2] на овом месту није лоше приметити колико је значајан и интересантан механизам који је примењен у последњем делу извођења асимптотске формуле (7.23). Грубо говорећи, он се састоји из два дела од којих сваки има своју посебну виртуозност. Прво, током целокупног извођења, ℓ се чува као слободан параметар, остављајући тако „простора слободе", који се онда „искористити"у најпогоднијем тренутку. Друго, барем иницијално изгледа очигледно да се (слободан) параметар може изабрати на одговарајући начин, али мало детаљнија анализа показује да то уопште није тако једноставно (приметимо колико се озбиљна теорија крије иза оправдања егзистенције избора (7.22) простог броја ℓ).

Коначно, асимптотске формуле (7.23) и (7.25) изведене у овом одељку сумирајмо у облику наредне теореме.

Теорема 7.3.4. *Нека је $E/\mathbb{Q}$ елиптичка крива са кондуктором N и без комплексног множења. Нека је K квадратно имагинарно бројевно поље класног броја h.*

1. *Претпоставимо да важи* GRH. *Тада је*

$$\Pi_E(K;x) \ll_{N,h} \frac{x^{\frac{4}{5}}}{(\log x)^{\frac{1}{5}}}.$$

2. *Претпоставимо да важе* GRH *и* PCC. *Тада је*

$$\Pi_E(K;x) \ll_{N,h} x^{\frac{3}{4}}$$

Имплицитне $\ll_{N,h}$-константе зависе од N и h.

Додатак: Хипотеза о корелацији парова (PCC)

У овом додатку даћемо кратак приказ хипотезе о корелацији парова (PCC), фокусирајући се притом на Риманову зета функцију $\zeta(s)$. Почнимо прво са уводним описивањем размака између нула функције $\zeta(s)$.

О размацима између нула Риманове зета функције

Претпоставимо да важи Риманова хипотеза, што је претпоставка које ћемо се држати до краја овог додатка. Тада се све нетривијалне нуле функције $\zeta(s)$ налазе на критичној оси $\Re(s) = \frac{1}{2}$, па њихове имагинарне делове можемо поређати у растући низ

$$\cdots \leq \gamma_{-2} \leq \gamma_{-1} < 0 < \gamma_1 \leq \gamma_2 \leq \cdots,$$

при чему важи да је $\gamma_{-n} = -\gamma_n$. Означимо са $N(T)$ функцију бројања нула Риманове зета функције,

$$N(T) = \#\left\{n \in \mathbb{N} \mid 0 < \gamma_n \leq T\right\},$$

дефинисану за све $T > 0$. У вези са функцијом $N(T)$ се показује да важи

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi e} + O(\log T)$$

за $T \geq 2$. Одатле следи да је хеуристички

$$\gamma_n \sim 2\pi n (\log n)^{-1}, \text{ када } n \to \infty,$$

па се нормализоване вредности

$$\zeta_n = \frac{1}{2\pi} \gamma_n \log |\gamma_n| \tag{7.26}$$

понашају као

$$\zeta_n \sim n, \text{ када } |n| \to \infty.$$

Међутим, поред значаја који има последња релација, персонификованог у опису понашања бројева ζ_n, она не пружа увид у суптилиније аспекте описа нула γ_n Риманове

зета функције, мислећи ту пре свега на опис размака између две узастопне нуле. Риманова хипотеза, сама по себи, једноставно не пружа одговор на то питање.

Ипак, нека информација о размаку између узастопних нула Риманове зета функције може се добити анализирањем статистике низа бројева ζ_n. Питање које се може поставити је да ли низ узастопних размака

$$\delta_n = \zeta_{n+1} - \zeta_n$$

чине потпуно случајни бројеви или међу њима постоји одређена правилност. На шта се тачно мисли под том правилношћу описује наредна општа дефиниција.

Дефиниција. *За низ бројева*

$$0 < \zeta_1 \leq \zeta_2 \leq \dots$$

кажемо да има ***Гаусов***[3] ***унитарни положај*** *ако је испуњено*

$$\frac{1}{N} \sum_{1 \leq n \leq N} f(\delta_n) \sim \int_0^\infty f(s) P(s) ds$$

за сваку довољно „лепу" функцију[4]

$$f : \mathbb{R}^+ \to \mathbb{C},$$

при чему је $\delta_n = \zeta_{n+1} - \zeta_n$, *а* $P(s)$ *је гранична густина расподеле узастопних размака сопствених вредности случајних унитарних матрица.*

Годин и Мехта су показали да низ ζ_n одређен формулом (7.26), који је нама од интереса, има Гаусов унитарни положај. При томе је функција $P(s)$ одређена са

$$P(s) = \det(I - Q_s),$$

где је Q_s интегрални оператор на $L^2([-1, 1])$, чије је језгро дато са

$$k_s(x, y) = \frac{\sin \frac{\pi s}{2}(x - y)}{\pi(x - y)}.$$

Посебно, тражена густина се може изразити у облику бесконачног производа

$$P(s) = \prod_{j=0}^{\infty} (1 - \lambda_j(s)),$$

[3] енг. Gaussian unitary ensemble

[4] Најчешће се захтева да је f Шварцове класе на $\mathbb{R}^+$, што значи да је бесконачно пута диференцијабилна и да за све целе бројеве $m, n > 0$ важи $\sup_{x \in \mathbb{R}^+} |x^m f^{(n)}(x)| < \infty$.

при чему су

$$1 \geq \lambda_0(s) \geq \lambda_1(s) \geq \lambda_2(s) \geq \dots$$

сопствене вредности интегралног оператора Q_s.

У случају да разматрамо L-функцију која је компликованија од Риманове зета функције, веома је тешко утврдити да ли одговарајући низ ζ_n, конструисан аналогно као низ одређен формулом (7.26) који смо посматрали, има Гаусов унитарни положај. Разлог томе лежи у чињеници да хармонијска анализа, као основно средство за рад са L-функцијама, не може да контролише узастопне тачке низа ζ_n. Међутим, оно што је могуће радити помоћу хармонијске анализе је детектовати тачке на малим скуповима (доменима). Управо због тога су проблеми корелације скупова тачака доста приступачинији и на њих су дати много потпунији одговори. У наредном одељку дајемо кратак приказ корелације парова нула Риманове зета функције.

Корелација парова нула Риманове зета функције

Основно средство које се користи за решавање проблема корелације парова нула Риманове зета функције је Риманова експлицитна формула (или евентуално неке варијанте те формуле) која повезује одређену суму узету свим нулама функције $\zeta(s)$ са неком сумом узетом по свим рационалним простим бројевима. Конкретније, нека је $\Gamma_R(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, где је $\Gamma(s)$ гама функција и још за функцију $g \in C_c^\infty(\mathbb{R})$ означимо са

$$h(r) = \int_{-\infty}^{+\infty} g(u)e^{iur}du$$

одговарајућу Фуријеову трансформацију.
Тада је испуњено

$$\sum_\gamma h(\gamma) = h\left(\frac{i}{2}\right) + h\left(-\frac{i}{2}\right) + \frac{1}{2\pi}\int_{-\infty}^{+\infty} h(r)\left(\frac{\Gamma_R'}{\Gamma_R}\left(\frac{1}{2}+ir\right) + \frac{\Gamma_R'}{\Gamma_R}\left(\frac{1}{2}-ir\right)\right)dr -$$
$$- \sum_{n=1}^{\infty}\frac{\Lambda(n)}{\sqrt{n}}\left(g(\log n) + g(-\log n)\right),$$

при чему је сума са леве стране узета по свим имагинарним деловима нула $\rho = \frac{1}{2} + i\gamma$ Риманове зета функције, а $\Lambda(n)$ је *фон Манголтова функција*, одређена са

$$\Lambda(n) = \begin{cases} \log p, \text{ ако је } n = p^\alpha, \text{ за } \alpha \geq 1 \\ 0, \text{ ако } n \text{ није степен простог броја.} \end{cases}$$

Стратегија испитивања корелације парова нула Риманове зета функције је онда у следећем. Прво се локализују γ-чланови избором погодне тест функције $h(r) = h(r,t)$, где је t параметар који имамо на располагању. Притом, $h(r)$ мора бити цела функција.

Због *принципа неодређености* хармонијске анализе, наведена локализација не може бити потпуно тачна, односно када се r налази у близини t, оно се не може видети на растојању мањем од $\frac{c}{\log t}$, где је c нека позитивна константа. Када је извршена локализација, пажљивим варирањем параметра t добија се сума по паровима γ, γ' нула Риманове зета функције, при чему је $\gamma - \gamma'$ мало. Одатле, коришћењем одређених апроксимација или увођењем још једног параметра у дефиницију тест функције стиже се до суме чији су чланови тражена функција од разлика $\gamma - \gamma'$.

Први који је претходно наведени план успешно спровео је амерички математичар Хју Монтгомери. Он је користио веома природну тест функцију $F(\alpha, T)$, која представља Фуријеову трансформацију размака између нула функције $\zeta(s)$ и одређена је са

$$F(\alpha, T) = \frac{2\pi}{T \log T} \sum_{0<\gamma,\gamma' \leq T} \sum w(\gamma - \gamma') T^{i\alpha(\gamma-\gamma')}$$

за све реалне бројеве α, $T \geq 2$, при чему је $w(u)$ функција локализације, дата са

$$w(u) = 4(4 + u^2)^{-1}.$$

Наведимо неколико основних особина тест функције $F(\alpha, T)$.

- $F(\alpha, T)$ је реална и ненегативна.
- За све $\alpha \in \mathbb{R}$ и све $T \geq 2$ важи $F(\alpha, T) = F(-\alpha, T)$.
- За $\alpha \in \mathbb{R}$ и све $T \geq 2$ важи $F(\alpha, T) \leq F(0, T) \ll \log T$.

Поред наведених особина, за функцију $F(\alpha, T)$ је кључна одговарајућа асимптотска формула, при $T \to \infty$, која је униформна за вредности $0 \leq \alpha \leq 1$. Ту формулу описује наредна теорема.

Теорема (Монтгомери). *За све* $0 \leq \alpha \leq 1$ *и све* $T \geq 2$ *важи*

$$F(\alpha, T) = \alpha + T^{-2\alpha} \log T + O\left(\alpha T^{\alpha-1} + T^{-\alpha} \log 2T^{\alpha} + (\log T)^{-1}\right). \tag{7.27}$$

Имплицитна O-константа је апсолутна.

Претходна теорема има велики број значајних последица. Ми ћемо овде навести само једну од њих, која се истиче својом занимљивошћу.
Означимо са $N_1(T)$ функцију која броји просте нуле Риманове зета функције[5],

$$N_1(T) = \#\left\{0 < \gamma \leq T \mid \rho = \frac{1}{2} + i\gamma \text{ је проста нула функције } \zeta(s)\right\}.$$

Асимптотика функције $N_1(T)$ када $T \to \infty$ има изузетно интересантну импликацију, као што показује наредна теорема.

[5]подсећања ради, и даље је на снази претпоставка важења Риманове хипотезе са почетка додатка

Теорема. *При $T \to \infty$, уз Риманову хипотезу, важи оцена*

$$N_1(T) > \left(\frac{2}{3} + o(1)\right) \frac{T}{2\pi} \log T.$$

Другим речима, баре̄м $\frac{2}{3}$ нула Риманове зета функције су просте.

Вратимо се сада још кратко на посматрање асимптотске формуле (7.27). Јасно је да та формула важи униформно за $\varepsilon \leq \alpha \leq 1 - \varepsilon$, где је $\varepsilon > 0$ довољно мали број. Уз одређени напор претходни закључак се поправити, показивањем да формула (7.27) важи униформно за $\varepsilon \leq \alpha \leq 1$. Међутим, оно што остаје нејасно је какво је понашање функције $F(\alpha, T)$ за $\alpha > 1$. Монтгомери је показао да у том случају не важи формула (7.27). Такође, он је пружио одређене хеуристичке аргументе који сугеришу да је

$$F(\alpha, T) \sim 1, \text{ при } T \to \infty, \tag{7.28}$$

униформно на ограниченим сегментима облика $1 \leq \alpha \leq A$. Даљим размишљањима, Монтгомери је дошао до познате *Хипотезе о корелацији парова.*

Хипотеза (О корелацији парова (PCC))**.** *За позитивне бројеве α и β такве да је $\alpha < \beta$ дефинишимо*

$$N(\alpha, \beta; T) = \# \left\{ m \neq n \mid 0 < \gamma_m, \gamma_n \leq T, \frac{2\pi\alpha}{\log T} < \gamma_m - \gamma_n < \frac{2\pi\beta}{\log T} \right\}.$$

Тада, при $T \to \infty$ имамо

$$N(\alpha, \beta; T) \sim N(T) \int_\alpha^\beta \left(1 - \left(\frac{\sin \pi u}{\pi u}\right)^2\right) du. \tag{7.29}$$

Напомена. *Монтгоријева експлицитна формула (7.27) за $0 \leq \alpha \leq 1$ и претпоставка (7.28) суштински су еквиваленте формули (7.29) коју предвиђа* PCC*. Према томе,* PCC *даје асимптотску формулу, при $T \to \infty$, која је униформна за вредности $\alpha \geq 0$.*

Литература

[1] Daniel I.A. Cohen, Talbot M Katz, *Prime numbers and the first digit phenomenon*, Journal of Number Theory, volume 18, issue 3, (1984), p. 261-268

[2] Alina C. Cojocaru, Chantal David, *Frobenius fields for elliptic curves*, American Journal of Mathematics, volume 130, issue 6, (2008), p. 1535-1560

[3] Alina C. Cojocaru, Chantal David, *Frobenius fields for Drinfeld modules of rank 2*, Compositio Mathematica, volume 144, (2008), p. 827-848

[4] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication* (2nd edition), Wiley, New Jersey, 2013

[5] Goran Đanković, *Teorija brojeva*, Matematički fakultet, Beograd, 2013

[6] Fernando Q. Gouvêa, *P-adic numbers: an introduction* (2nd edition), Springer-Verlag, Berlin, Heidelberg, 1997

[7] Henryk Iwaniec, Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society, Providence, Rhode Island, 2004

[8] Gerald J. Janusz, *Algebraic number fields* (2nd edition), American Mathematical Society, Providence, Rhode Island, 1996

[9] Serge Lang, *Algebraic number theory* (2nd edition), Springer-Verlag, New York, 1994

[10] Serge Lang, *Introduction to algebraic and abelian funcions* (2nd edition), Springer-Verlag, New York, 1982

[11] M. Ram Murty, Jody Esmonde, *Problems in algebraic number theory* (2nd edition), Springer-Verlag, New York, 2005

[12] M. Ram Murty, V. Kumar Murty, *Pair Correlation conjecture and the Chebotarev density theorem*, preprint, 2004

[13] M. Ram Murty, V. Kumar Murty, N. Saradha, *Modular forms and the Chebotarev density theorem*, American Journal of Mathematics, volume 110, issue 2, (1988), p. 253-281

[14] Jürgen Neukirch, *Algebraic number theory* (translated from the German by Norbert Schappacher), Springer, Berlin, 1999

[15] Jean-Pierre Serre, *A course in arithmetics*, Springer-Verlag, New York, 1973

[16] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques, volume 54, issue 1, (1981), p. 123-201

[17] Jean-Pierre Serre, *Linear representations of finite groups* (translated from the French by Leonard L. Scott), Springer-Verlag, New York, 1977

[18] Joseph H. Silverman, *The arithmetic of elliptic curves* (2nd edition), Springer, Providence, Rhode Island, 2008

[19] B.F. Wyman, *What is a reciprocity law?*, The American Mathematical Monthly, volume 79, issue 6, (1972), p. 571-586

Листа симбола и ознака

$\lvert\cdot\rvert_p$	p-адична валуација на $\mathbb{Q}$
$\lvert\cdot\rvert_\infty$	валуација у бесконачности на $\mathbb{Q}$
$\mathbb{C}$	поље комплексних бројева
$C_c^\infty(\mathbb{R})$	простор свих бесконачно диференцијабилних функција на $\mathbb{R}$ са компактним носачем
$d(s)$	Дирихлеова густина скупа S
d_K	апсолутна вредност дискриминанте бројевног поља K
Δ	дискриминанта елиптичке криве
$\delta(s)$	природна густина скупа S
$E[m]$	група m-торзионих тачака елиптичке криве E
E_p	редукција елиптичке криве E по модулу простог броја p
F^*	мултипликативна група поља F
$\mathrm{Fr}_\mathfrak{P}$, $\left(\frac{L/K}{\mathfrak{P}}\right)$	Фробенијусов аутоморфизам који одговара простом броју $\mathfrak{P}$
$F_\mathfrak{p}$	комплетирање поља F у простом броју $\mathfrak{p}$
$\mathbb{F}_q$	коначно поље са q елемената
$\bar{F}$	алгебарско затворење поља F
$\varphi_{L/K}$	Артиново пресликавање које одговара раширењу L/K бројевних поља
$G(\mathfrak{P})$	група декомпозиције за прост број $\mathfrak{P}$
$G(L/K)$, $\mathrm{Gal}(L/K)$	Галуаова група раширења поља L/K
$I(\mathfrak{P})$	група инерције за прост број $\mathfrak{P}$
I_K	група свих ненула идеала разломака прстена целих бројевног поља K
$J^\mathfrak{m}/\varsigma(K_{\mathfrak{m},1})$	група класа зрака по модулу $\mathfrak{m}$
$K_{\mathfrak{m},1}$	зрак по модулу $\mathfrak{m}$
$\mathrm{li}\, x$	логаритамски интеграл
$L(s,\psi)$	уопштена Дирихлеова L-функција
$\mathfrak{L}(L/K,\chi,s)$	Артинова L-функција
$\Lambda(n)$	фон Манголтова функција
$[m]$	изогенија множења са $m \in \mathbb{Z}$

M_K	скуп свих ненула простих идеала прстена целих бројевног поља K
$\mathfrak{m}_0$	коначни део модула $\mathfrak{m}$
$\mathfrak{m}_\infty$	бесконачни део модула $\mathfrak{m}$
μ_F	група корена из јединице који се налазе у пољу F
N_E	кондуктор елиптичке криве E
$\mathfrak{N}(\mathfrak{a})$	норма идеала $\mathfrak{a}$
$\mathscr{O}_K$	прстен целих бројевног поља K
$\mathrm{ord}_\mathfrak{p}$	нормализована валуација у коначном простом броју $\mathfrak{p}$
$\left(\frac{\cdot}{p}\right)$	Лежандров симбол
$\mathbb{Q}$	поље рационалних бројева
$\mathbb{Q}_p$	поље p-адичних бројева
$\mathbb{R}$	поље реалних бројева
$\hat{\rho}_\ell$	комбинована ℓ-адична Галуаова репрезентација
$\rho_{\ell,E}$	ℓ-адична репрезентација везана за елиптичку криву E
$\rho_{\ell,K}$	ℓ-адична репрезентација везана за квадратно имагинарно бројевно поље K
$\mathbb{S}^1$	јединична кружница у комплексној равни
$\mathbb{Z}$	прстен целих бројева
$\mathbb{Z}_p$	прстен p-адичних целих бројева
$\zeta(s)$	Риманова зета функција
$\zeta_K(s)$	Дедекиндова зета функција бројевног поља K

Индекс

Артинова хипотеза, 58, 60
Артиново пресликавање, 35, 73

Дискриминанта елиптичке криве, 95

Фробенијусов аутоморфизам, 33
Функција
  $\Pi_E(K;x)$, 104
  Артинова L-, 51, 52
  Дедекиндова зета $\zeta_K(s)$, 41
  Дирихлеова L-, 5
  фон Манголтова, 127
  најједноставнија уопштена L-, 6
  Риманова зета $\zeta(s)$, 4
  уопштена Дирихлеова L-, 39

Група
  декомпозиције, 30
  идеала, 27
  инерције, 31
  класа, 35
  класа зрака по модулу $\mathfrak{m}$, 23
Густина
  Дирихлеова, 62
  природна, 68

Хипотеза
  Ленг-Тротера, 104
  о корелацији парова, 129

Изогенија, 98

Карактер
  репрезентације, 46
  уопштени Дирихлеов, 39
Комплетирање поља, 11
Кондуктор
  елиптичке криве, 102
  групе идеала, 27
  раширења бројевних поља, 35
Конгруентна подгрупа, 25
Крива, 95

Лежандров симбол, 78

Модул, 19

Норма идеала, 5

Поље
  p-адичних бројева $\mathbb{Q}_p$, 16
  класа, 35
Прост број у пољу, 10
Прстен p-адичних целих бројева $\mathbb{Z}_p$, 17

Репрезентација
  аугментована, 46
  групе, 44
  индукована, 49
  комбинована Галуаова, 111
  придружена квадратном имагинарном бројевном пољу, 107
  регуларна, 46
  тривијална, 46

везана за елиптичку криву, 105
Род криве, 95

Теорема
Брауера, 50
Чеботарева о густини, 66
Дирихлеа о густини, 63
Дирихлеа о инвертибилним елементима, 18
Дирихлеа о простим бројевима, 3, 64
Фробенијуса о густини, 72
Хасеа, 101
Монтгомерија, 128
Островског о валуацијама на $\mathbb{Q}$, 16
Тривијални модул, 25

Вајерштрасова једначина, 94
Валуација
p-адична на $\mathbb{Q}$, 15
архимедова, 9
на пољу, 9
неархимедова, 9
у бесконачности на $\mathbb{Q}$, 12

Закон реципроцитета, 35, 36
Зрак по модулу $\mathfrak{m}$, 22