Eötvös Loránd Tudományegyetem

Természettudományi Kar

Szőke Tamás

Exponenciális összegek

Matematika BSc, Matematikus szakirány

Szakdolgozat

Témavezető:

Tóth Árpád, egyetemi docens

Analízis Tanszék

Budapest, 2018

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőnek, Tóth Árpádnak a sok segítéségért, a konzultációkért és a dolgozat átnézéséért.

Tartalomjegyzék

Bevezető

A dolgozat az exponenciális összegek elméletébe nyújt betekintést, azon belül is főleg a Kloosterman-összegek témakörébe. Ezen összegeket először Poincaré írta fel a moduláris formák vizsgálata során a [8] cikkben , de nem sokkal később Kloosterman ezen összegeket alkalmazta az $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2 = n$ diofantikus egyenlet megoldásszámának tanulmányozásához a [7] cikkben. Az ehhez használt klasszikus Kloosterman-összegekről belátunk néhány állítást a dolgozat elején, utána pedig ezek algebrai számtestek feletti általánosítását fogjuk vizsgálni. A Kloosterman-összegek ma is fontos szerepet töltenek be a moduláris formák elméletében, a harmadik fejezetben megmutatjuk majd, hogy hogyan kapcsolódik egymáshoz a két terület.

Az első fejezet elején találhatóak számelméletből és algebrai számelméletből azon ismeretek, amik szükségesek lesznek a Kloosterman-összegek és azok számtestek feletti általánosításának vizsgálatához. Ezután definiáljuk a klasszikus Kloosterman-összegeket és belátunk róluk néhány alapvető állítást, majd egy nagyságrendi becslést is.

A második fejezetben áttérünk a számtestek feletti Kloosterman-összegek vizsgálatára, és megnézzük, hogy hogyan mondható ki a Selberg-féle azonosság ebben az esetben, azután pedig ezt be is bizonyítjuk, speciális esetként kapva a klasszikus összegekre vonatkozó Selberg-azonosságot.

A harmadik fejezetben definiáljuk a moduláris formákat, az Eisenstein-sorokkal példát is adunk rájuk, azután pedig megkonstruáljuk a Poincaré-sorokat és meglátjuk, hogy hogyan jönnek elő a Kloosterman-összegek ennek kapcsán.

1. fejezet

Előismeretek és klasszikus eredmények

1.1. Karakterek véges Abel-csoportok felett

Az exponenciális összegek tanulmányozásához elengedhetetlen a karakterek ismerete, ebben a részben gyűjtjük össze a hozzájuk kötődő alapvető állításokat. Ezek megtalálhatóak a [3] könyvben.

A továbbiakban G mindig egy véges Abel-csoportot fog jelölni.

1.1.1. Definíció. *Azt mondjuk, hogy a $\chi : G \to \mathbb{C}^\times$ függvény G-nek karaktere, ha minden $g, h \in G$ esetén $\chi(g+h) = \chi(g)\chi(h)$. (Vagyis, ha χ G-ből a komplex számok multiplikatív csoportjába menő homomorfizmus).*

Mivel a karakter egy homomorfizmus, ezért G egységelemét az 1-be kell vinnie. G végessége miatt minden elem rendje véges, ebből ezután könnyen látható, hogy egy χ karakter csak komplex egységgyököket vesz fel.

Karakterek szorzatát is definiálhatjuk a megszokott módon: ha χ_1, χ_2 karakterek, akkor $\chi_1 \cdot \chi_2(g) := \chi_1(g) \cdot \chi_2(g)$. Az erre vonatkozú tulajdonságokat a következő állítás foglalja össze:

1.1.2. Állítás. *A karakterek a fenti műveletre nézve egy véges Abel-csoportot alkotnak, melynek elemszáma megegyezik G-nek az elemszámával. Ezt a csoportot $\widehat{G}$-vel jelöljük.*

Bizonyítás. Könnyen ellenőrizhető, hogy karakterek szorzata ismét karakter lesz, hogy az azonosan 1-et felvevő karakter (az ún. triviális karakter) egységelem lesz, és hogy egy χ karakter inverze az a χ^{-1} karakter lesz, amire $\chi^{-1}(g) = \overline{\chi(g)}$ minden $g \in G$-re.

Az elemszámra vonatkozó állítást először abban az esetben bizonyítjuk be, amikor $G = C_n$ az n elemű ciklikus csoport. Legyen ekkor g egy generátoreleme G-nek. Mivel $g^n = 1$, ezért $\chi(g)^n = \chi(g^n) = 1$, vagyis $\chi(g)$-nek egy n-edik komplex egységnek kell lennie. Viszont tetszőleges n-edik komplex egységgyököt választva $\chi(g)$-nek, az egyértelműen meg fog határozni egy karaktert G-n, és mivel n darab n-edik egységgyök van, így n különböző karakterünk lesz.

Tetszőleges G véges Abel-csoport esetén használjuk a véges Abel-csoportok alaptételét, ami szerint G felírható ciklikus csoportok direkt szorzataként: $G = C_{n_1} \times C_{n_2} \times ... \times C_{n_k}$. Legyenek C_{n_1}, C_{n_2}, ..., C_{n_k} generetárelemei rendre g_1, g_2, ..., g_k! Világos, hogyha g_1, g_2, ..., g_k-n megadjuk egy karakter értékeit, azzal egyértelműen meghatározzuk G-nek egy karakterét. De a fentiek szerint g_1-n n_1-féleképpen, g_2-n n_2-féleképpen, ..., g_k-n n_k-féleképpen adhatjuk meg egy karakter értékét, így összesen $n_1 \cdot n_2 \cdot ... \cdot n_k$ darab karakter van G-n, ami éppen megegyezik G elemszámával. $\square$

1.1.3. Állítás. *Ha H részcsoportja G-nek, akkor H minden karaktere kiterjed G karakterévé.*

Bizonyítás. A $G : H$ index szerinti teljes indukcióval fogjuk bizonyítani az állítást. Ha $G : H = 1$, akkor $G = H$, és nincs mit bizonyítanunk. Tegyük fel, hogy $G : H > 1$, és legyen x olyan, hogy $x \in G$, de $x \notin H$. Legyen továbbá n az a legkisebb pozitív egész, amire $nx \in H$ (ilyen nyilván létezik, hiszen x-et a G csoport rendjeszer összeadva az egységelemet kapjuk, és $x \notin H$ miatt $n > 1$).

Vegyük most egy tetszőleges χ karakterét H-nak, és legyen $t = \chi(nx)$. Ekkor létezik egy olyan $w \in \mathbb{C}^\times$ szám, amire $w^n = t$ (hiszen t egy $|H|$-adik egységgyök, így w-nak jó lesz egy megfelelő $n \cdot |H|$-adik egységgyök).

Vegyük az x és H által generált H' részcsoportot G-ben, a χ karaktert ki fogjuk terjeszteni erre a részcsoportra, és ha már azt tudjuk, akkor utána az indukciós feltevés maitt készen leszünk. H' minden h' eleme felírható $h' = h + ax$ alakban, ahol $h \in H$, és $a \in \mathbb{Z}$, hiszen G egy Abel-csoport. Definiáljuk a χ' karaktert H'-n úgy, hogy egy adott $h' \in H'$ elemet írjunk fel az előbbi módon, és legyen $\chi'(h') = \chi(h)w^a$.

Először is be kell látnunk, hogy χ' jóldefiniált, azaz nem függ h'-nak a felírásától. Tegyük fel, hogy felírtuk h'-t kétféleképpen: $h' = h_1 + a_1 x = h_2 + a_2 x$, h_1, $h_2 \in H$, a_1, $a_2 \in \mathbb{Z}$. Ekkor $h_2 - h_1 = (a_1 - a_2)x$, de a baloldal nyilvánvalóan eleme H-nak, így n definíciója miatt $n | a_1 - a_2$. Ezek alapján:
$\overline{\chi(h_1)w^{a_1}}\chi(h_2)w_2^a = \chi(h_2 - h_1)w^{a_2 - a_1} = \chi(h_2 - h_1)(w^n)^{\frac{a_2 - a_1}{n}} = \chi(h_2 - h_1)t^{\frac{a_2 - a_1}{n}} =$

$= \chi(h_2-h_1)(\chi(nx))^{\frac{a_2-a_1}{n}} = \chi(h_2-h_1)\chi((a_2-a_1)x) = \chi(h_2+a_2x-(h_1+a_1x)) = \chi(0) = 1$, és ezt átrendezve $\chi(h_1)w^{a_1} = \chi(h_2)w^{a_2}$ adódik, tehát χ' valóban jóldefiniált.

χ' karakter lesz H'-n, hiszen világos, hogy $\mathbb{C}^\times$-ba képez, és a defiinicó alapján könnyen kiszámítható, hogy homomorfizmus is lesz. Az is teljesül, hogy H-ra megszorítva éppen χ-t kapjuk vissza, mert egy $h \in H$ elemet írhatunk $h + 0 \cdot x$ alakban, és így $\chi'(h) = \chi(h) \cdot 1 = \chi(h)$. Tehát χ kiterjed H'-re, és így az indukciós feltevés miatt készen vagyunk. □

1.1.4. Lemma. $\widehat{\widehat{G}} \cong G$

Bizonyítás. Legyen $g \in G$. Ekkor definiálhaunk $\widehat{G}$ felett egy karaktert a következő módon:

$$f_g : \widehat{G} \to \mathbb{C}^\times, \chi \mapsto \chi(g)$$

Ez karakter, hiszen ha $\chi_1, \chi_2 \in \widehat{G}$, akkor $f_g(\chi_1\chi_2) = \chi_1\chi_2(g) = \chi_1(g)\chi_2(g) = f_g(\chi_1)f_g(\chi_2)$. Tekintsük a $G \to \widehat{\widehat{G}}, g \mapsto f_g$ leképezést. Ez csoporthomomorfizmus, hiszen ha $g, h \in G$, akkor $f_{gh}(\chi) = \chi(gh) = \chi(g)\chi(h) = f_g(\chi)f_h(\chi)$ minden $\chi \in \widehat{G}$-re, tehát $f_{gh} = f_g f_h$.

Az előbbiek szerint G és $\widehat{\widehat{G}}$ két véges csoport, amiknek megegyezik az elemszáma. Ezért elég belátnunk, hogy a fenti homomorfizmus injektív, mert akkor már izomorfizmus lenne.

Tegyük fel, hogy létezik $g \neq 0$ elem, amire f_g az azonosan 1 karakter $\widehat{G}$ felett. Ez f_g definíciója miatt azt jelenti, hogy G-nek minden karaktere g-n egyet vesz fel. Mi viszont konstruálhatunk egy olyan karaktert, ami g-n nem egyet vesz fel a következő módon: tekintsük a g által generált részcsoportot G-ben, aminek legyen az elemszáma n. Ez ciklikus, és $g \neq 0$ miatt n>1 . Így ezen a részcsoporton definiálhatunk egy karaktert úgy, hogy g-n legyen egy primitív n-edik egységgyök, a ciklikusság miatt ez kiterjed az egész részcsoportra egyértelműen. Az előző állítás szerint ez a karakter kiterjed G-nek egy karakterévé, ami tehát olyan karakter, ami g-n nem egyet vesz fel. Tehát ellentmondásra jutottunk, így csak a 0 van benne a fenti homomorfizmus magjában, ami így tehát injektív. □

A most következő két állítást ortogonalitási relációknak szokás hívni.

1.1.5. Állítás. *Legyen $\chi \in \widehat{G}$. Ekkor*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{ha } \chi = 1. \\ 0, & \text{ha } \chi \neq 1. \end{cases}$$

Bizonyítás. Ha $\chi = 1$, akkor az állítás nyilvánvaló. Ha $\chi \neq 1$, akkor létezik olyan $h \in G$, amire $\chi(h) \neq 1$. Ebben az esetben

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(h+g) = \sum_{g \in G} \chi(g)$$

ezért

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$$

és mivel $\chi(h) \neq 1$, így ebből adódik az állítás. □

1.1.6. Állítás. *Legyen $g \in G$. Ekkor*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G|, & ha\ g = 0. \\ 0, & ha\ g \neq 0. \end{cases}$$

Bizonyítás. Az állítás azonnal következik a lemmából és az előző állításból, hiszen

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} f_g(\chi)$$

ahol f_g a lemmában definiált $\widehat{G}$ feletti karakter. □

1.2. Algebrai számelméleti tudnivalók

A következőekben áttekintjük a dolgozatban felmerülő algebrai számelméleti fogalmakat és fontosabb állításokat, bizonyítás nélkül. Ezen állítások és bizonyításuk megtalálhatóak az [5] jegyzetben.

1.2.1. Definíció. *A racionális számok testének egy véges algebrai $\mathbb{Q} \leq \mathbb{F}$ bővítését algebrai számtestnek nevezzük.*
Azt mondjuk, hogy az $a \in \mathbb{F}$ elem algebrai egész, ha gyöke egy $\mathbb{Q}$-beli egész együtthatós, 1 *főegyütthatós polinomnak.*

A továbbiakban $\mathbb{F}$ mindig egy számtestet fog jelölni, $\mathcal{O}$ pedig benne az algebrai egészek halmazát.

1.2.2. Állítás.

(i) $\mathcal{O}$ gyűrű az $\mathbb{F}$-ből örökölt összeadásra és szorzásra nézve.

(ii) Ha I tetszőleges nemnulla ideál $\mathcal{O}$-ban, akkor az $\mathcal{O}/I$ faktorgyűrű véges sok elemből áll.

1.2.3. Definíció. *Legyen I nemnulla ideál $\mathcal{O}$-ban, ekkor az $N(I) = |\mathcal{O}/I|$ mennyiséget az I ideál normájának nevezzük.*

1.2.4. Állítás. *Az ideálnorma teljesen multiplikatív, tehát ha I és J nemnulla ideálok $\mathcal{O}$-ban, akkor $N(I \cdot J) = N(I)N(J)$.*

1.2.5. Tétel. *(egyértelmű prímfaktorizációs tétel ideálokra): Legyen I nemnulla valódi ideál $\mathcal{O}$-ban, ekkor I egyértelműen előáll nemnulla prímideálok szorzataként: $I = P_1^{n_1} P_2^{n_2} ... P_k^{n_k}$, ahol $P_1, P_2, ..., P_k$ prímideálok, $n_1, n_2, ..., n_k$ pedig pozitív egész számok.*

1.2.6. Definíció. *Legyenek I, J nemnulla ideálok $\mathcal{O}$-ban, ekkor azt mondjuk, hogy I és J relatív prímek, ha $I + J = \mathcal{O}$, ahol az összeg a komplexusösszeget jelenti.*
Azt monjuk, hogy J osztja I-t , ha J tartalmazza I-t, és ezt $J|I$-vel jelöljük.

Két ideál relatív prímségét, iletve az oszthatóságot a prímfelbontásukból is megállapíthatjuk az egész számok körében megszokott módon: I és J pontosan akkor relatív prímek, ha a prímfelbontásukban különböző prímtényezők szerepelnek, J pontosan akkor osztja I-t, ha a prímfelbontásukban ugyanazon prímtényezők szerepelnek, és J-nél mindegyiknek kisebb a hatványkitevője, mint I-nél.

1.2.7. Tétel. *(kínai maradéktétel): Legyenek A, B relatív prím, nemnulla ideálok $\mathcal{O}$-ban, ekkor $\mathcal{O}/AB \cong \mathcal{O}/A \times \mathcal{O}/B$.*

1.2.8. Következmény. Ha I nemnulla ideál $\mathcal{O}/I$-ben, $I = P_1^{n_1} P_2^{n_2} ... P_k^{n_k}$ pedig a prímfelbontása, akkor $\mathcal{O}/I \cong \mathcal{O}/P_1^{n_1} \times \mathcal{O}/P_2^{n_2} \times ... \times \mathcal{O}/P_k^{n_k}$.

1.3. A klasszikus Kloosterman-összegekről

Az ebben a részben levő állítások és még sok más ismerete az exponenciális összegekkel kapcsolatban megtalálhatóak a [2] jegyzetben.

A dolgozat további részében élni fogunk a következő jelöléssel: $e(x) = e^{2\pi i x}$.

Legyen c egy pozitív egész szám. Exponenciális összegen általában egy $\sum e(\frac{1}{c}\frac{f(x)}{g(x)})$ alakú összeget értünk, ahol f és g egész együtthatós polinomok, g nem azonosan nulla

mod c, és x azon *mod* c maradékosztályokon fut, amikre $g(x) \neq 0$ *mod* c. Kloosterman-összegen a következő, speciális alakú exponenciális összeget értjük:

$$S(n,m,c) = \sum_{\substack{0<x<c \\ (x,c)=1}} e\left(\frac{nx + m\bar{x}}{c}\right)$$

ahol n, $m \in \mathbb{Z}$, és $\bar{x}$ az x inverzét jelöli *mod* c. Ebben a fejezetben nem teljesen ilyen alakú Kloosterman-összegekkel fogunk foglalkozni, hanem egy véges testek feletti változattal. Azoknak speciális eseteként visszakapjuk prím c-kre a klasszikus Kloosterman-összegeket, ami a legfontosabb eset.

Legyen tehát q egy prímhatvány, $\mathbb{F}_q$ pedig a q elemű véges test. Vegyük észre, hogy az $x \mapsto e(\frac{nx}{p})$ leképezés egy karaktere $\mathbb{F}_p$ additív csoportjának, ha p prím. Ez alapján véges testek felett természetesen adódik a Kloosterman-összegek következő definíciója: ha φ, ψ karakterei $\mathbb{F}_q$ additív csoportjának, akkor legyen

$$S(\varphi,\psi) = \sum_{x \in \mathbb{F}_q^\times} \varphi(x)\psi(x^{-1})$$

Amikor $q = p$ prím, ez klasszikus Kloosterman-összeget ad.

Ha $q = p$ prím, akkor ismerjük $\mathbb{F}_q$ additív karaktereit, de igazából az általános esetben is karakterizálhatóak. Legyen $q = p^n$, p prím. Ekkor az algebrából ismert nyom leképezés:

$$Tr_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p, a \mapsto a + a^p + ...a^{p^{n-1}}$$

egy szürjektív $\mathbb{F}_p$-lineáris leképezés. Ennek segítségével, ha $a \in \mathbb{F}_q$, akkor deifiniálhatjuk $\mathbb{F}_q$ egy ψ_a karakterét a következő módon:

$$\psi_a(x) = e\left(\frac{Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax)}{p}\right)$$

ahol ezt úgy értjük, hogy egy $b \in \mathbb{F}_p$ elemet azonosítunk egy $_beta \in \mathbb{Z}_p$-beli elemmel a természetes izomorfizmus mentén (az egységelemet az egységelembe küldjük). A nyom tulajdonságai miatt könnyen látható, hogy a fenti ψ_a leképezés jóldefiniált és karaktere $\mathbb{F}_q$ additív csoportjának. A következő állítás azt mondja, hogy más karakter nincs is ezeken kívül.

1.3.1. Állítás. *Ha* χ *karaktere* $\mathbb{F}_q$ *additív csoportjának, akkor* $\chi = \psi_a$ *egy alkalmas* $a \in \mathbb{F}_q$*-ra.*

Bizonyítás. Tudjuk, hogy F_q additív csoportja felett éppen q darab karakter létezik, ezért ha belátjuk, hogy ha $a, b \in \mathbb{F}_q$ és $a \neq b$, akkor $\psi_a \neq \psi_b$, akkor azzal belátjuk az állítást.

Tegyük fel tehát, hogy $a \neq b$ és $\psi_a = \psi_b$. Ez azt jelenti, hogy minden $x \in \mathbb{F}_q$-ra $e\left(\frac{Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax)}{p}\right) = e\left(\frac{Tr_{\mathbb{F}_q/\mathbb{F}_p}(bx)}{p}\right)$. Ezt rendezve és a nyom linearitását kihasználva adódik, hogy $e\left(\frac{Tr_{\mathbb{F}_q/\mathbb{F}_p}((b-a)x)}{p}\right) = 1$ minden $x \in \mathbb{F}_q$-ra, vagyis $Tr_{\mathbb{F}_q/\mathbb{F}_p}((b-a)x) = 0$.
Tudjuk, hogy a nyom szürjektív, így létezik olyan $c \in \mathbb{F}_q$, amire $Tr_{\mathbb{F}_q/\mathbb{F}_p}(c) \neq 0$. Mivel $b-a \neq 0$, így létezik inverze, ezért $x = (b-a)^{-1}c$-t helyettesítve a fent kapott összefüggésbe az adódik, hogy $Tr_{\mathbb{F}_q/\mathbb{F}_p}(c) = 0$, ami ellentmondás. Így ezzel beláttuk az állítást. □

A végs testek feletti Kloosterman-összegek definíciójából leolvashatunk néhány egyszerű tulajdonságot.

1.3.2. Állítás.

(i) $S(\varphi, \psi)$ *valós szám*

(ii) $b \in \mathbb{F}_q^\times$ *esetén* $S(\varphi, \psi) = S(\varphi_b, \psi_{b^{-1}})$, *ahol* $\varphi_b(x) = \varphi(bx)$ *és* $\psi_{b^{-1}}(x) = \psi(b^{-1}x)$.

Bizonyítás.

(i)

$$\overline{S(\varphi,\psi)} = \overline{\sum_{x\in\mathbb{F}_q^\times} \varphi(x)\psi(x^{-1})} = \sum_{x\in\mathbb{F}_q^\times} \varphi(x^{-1})\psi(x) = \sum_{y\in\mathbb{F}_q^\times} \varphi(y)\psi(y^{-1}) = S(\varphi,\psi)$$

az $y = x^{-1}$ bijektív változócserével. Tehát $S(\varphi, \psi)$ megegyezik a konjugáltjával, azaz valós szám.

(ii) Az $y = b^{-1}x$ bijektív változócserével könnyen adódik.

□

Az exponenciális összegek tanulmányozásánál nagy szerepe van az abszolútértékre vonatkozó becsléseknek, hiszen pontos formulát egy adott összegre, a legegyszerűbb esetektől eltekintve, nem várhatunk.
Egy $\mathbb{F}_q$ feletti Kloosterman-összeg esetén a triviális felső becslés q, ha háromszög-egyenlőtlenséggel becsülünk, minden tag abszolútértéke 1. Ez éles, ha φ és ψ mindketten a triviális karakterek, de ha egyikük sem triviális, akkor ennél lényegesen jobb eredmény is igaz. Weil algebrai geometriai eszközöket használva belátta a [4] cikkben, hogy ha φ,

ψ nem főkarakterek, akkor $|S(\varphi,\psi)| \leq 2q^{\frac{1}{2}}$. Mi most egy $2q^{\frac{3}{4}}$-es korlátot fogunk igazolni, elemi módszerekkel.

Jelöljük χ_0-al a $\mathbb{F}_q$ additív csoportja feletti triviális karaktert. A bizonyításhoz az ötlet az, hogy egyszerre próbáljuk megérteni a vizsgált összegeket. Ha ugyanis be tudnánk látni, hogy $\sum^* |S(\varphi,\psi)|^{2k} \leq M$ valamilyen k pozitív egészre és M pozitív konstansra ($\sum^*$ azt jelzi, hogy csak olyan (φ,ψ) karakterpárokra összegzünk, hogy $\varphi \neq \chi_0$, $\psi \neq \chi_0$ karakterekre összegzünk), akkor az előző állítás (ii) pontját felhasználva

$$(q-1)|S(\varphi,\psi)|^{2k} = \sum_{b\neq 0} |S(\varphi_b, \psi_{b^{-1}})|^{2k} \leq M$$

és így $|S(\varphi,\psi)| \leq (\frac{M}{q-1})^{\frac{1}{2k}}$ adódna. (Vegyük észre, hogy a fenti egyenlőtlenség tényleg helytálló, ugyanis ha φ nemtriviális karakter, b invertálható elem, $b \neq 1$, akkor φ_b szintén nemtriviális karakter és $\varphi_b \neq \varphi$, hiszen ellenkező esetben φ_{b-1} főkarakter lenne, de az csak $b = 1$ esetben lehetséges.)

A továbbian legyen $q, \mathbb{F}_q$ rögzített. Jelölje $M_k = \frac{1}{(q-1)^2} \sum^* |S(\varphi,\psi)|^{2k}$ a fenti összegből képzett átlagot (ez valóban átlag, hiszen $\mathbb{F}_q$ felett összesen q darab additív karakter van). A következő állításban belátjuk, hogy $M_2 = \frac{2q^3-3q^2-3q-1}{q-1}$. Ebből már adódik a felső korlátunk: $|S(\varphi,\psi)| \leq ((q-1)M_2)^{\frac{1}{4}} < 2q^{\frac{3}{4}}$. Ezt először Kloosterman látta be [7]-ben.

1.3.3. Tétel. $M_2 = \frac{2q^3-3q^2-3q-1}{q-1}$

Bizonyítás. Először egy általános formulát adunk meg M_k kiszámítására: tetszőleges k pozitív egész szám esetén

$$M_k = \frac{q^2}{(q-1)^2}|A_k| - \frac{2}{q-1} - (q-1)^{2k-2}$$

ahol

$$A_k = \left\{ (x,y) \in (\mathbb{F}_q^\times)^{k+k} \mid \sum_{1\leq i\leq k} x_i = \sum_{1\leq i\leq k} y_i \ , \ \sum_{1\leq i\leq k} x_i^{-1} = \sum_{1\leq i\leq k} y_i^{-1} \right\}$$

Ez visszavezeti a kérdéses összeg kiszámolását egy F_q feletti leszámlálási problémára: bizonyos polinomiális egyenletrendszerek megoldásszámát kell meghatároznunk. A fenti képletet úgy láthatjuk be, hogy az összegünkhöz hozzárakjuk a triviális karakterekből származó tagokat, hogy alkalmazni tudjuk az ortogonalitási relációt a karakterekre, majd levonjuk azokat. Ezt könnyen meg tudjuk tenni, hiszen

$$S(\chi_0,\psi) = \sum_{x\in\mathbb{F}_q^\times} \psi(x^{-1}) = \sum_{y\in\mathbb{F}_q^\times} \psi(y) = -1$$

ha $\psi \neq \chi_0$, az első ortogonális reláció alapján. Hasonlóan adódik, hogy ha $\varphi \neq \chi_0$, akkor $S(\varphi, \chi_0) = -1$, továbbá nyilvánvaló, hogy $S(\chi_0, \chi_0) = q - 1$. Így

$$(q-1)^2 M_k = \sum_{\varphi,\psi} |S(\varphi,\psi)|^{2k} - 2(q-1) - (q-1)^{2k}$$

Ezután kifejtjük a Kloosterman-összegeket és átírjuk konjugálással az abszolútértéket:

$$(q-1)^2 M_k = \sum_{\varphi,\psi)} \sum_{x=(x_1,\ldots,x_k)\in(\mathbb{F}_q^\times)^k} \sum_{y=(y_1,\ldots,y_k)\in(\mathbb{F}_q^\times)^k} \varphi(x_1+\ldots+x_k-y_1-\ldots-y_k)\times$$

$$\times\psi(x_1^{-1}+\ldots+x_k^{-1}-y_1^{-1}-\ldots-y_k^{-1}) - 2(q-1) - (q-1)^{2k}$$

Az ortogonalitást alkalmazva a karakterekre:

$$(q-1)^2 M_k = \sum_{x,y} \left(\sum_{\varphi} \varphi(T(x)-T(y)) \right) \times \left(\sum_{\psi} \psi(U(x)-U(y)) \right) - 2(q-1) - (q-1)^{2k} =$$

$$= q^2 |A_k| - 2(q-1) - q^{2k}$$

ahol $x \in (\mathbb{F}_q^\times)^k$ esetén $T(x) = x_1 + \ldots + x_k$ és $U(x) = x^{-1} + \ldots + x_k^{-1}$. Így tehát beláttuk a fenti formulát.

Az állítás igazolásához már csak A_2 elemszámát kell meghatároznunk, ami pedig a következő egyenletrendszer megoldásszáma:

$$\begin{cases} x_1 + x_2 = y_1 + y_2 \\ x_1^{-1} + x_2^{-1} = y_1^{-1} + y_2^{-1} \end{cases}$$

Ha (y_1, y_2) egy permutációja (x_1, x_2)-nek, akkor ez a számnégyes nyilvánvalóan megoldása a fenti egyenletrendszernek. Ilyen alakú megoldásokból $2(q-1)^2 - (q-1)$ darab van (x_1-et és x_2-t is $q-1$-féleképpen választhatjuk, minden ilyen párhoz két darab (y_1, y_2) pár tartozik, kivéve akkor, amikor $x_1 = x_2$).

Most megvizsgáljuk, hogy milyen feltételek esetén határozza meg $x_1 + x_2$ és $x_1^{-1} + x_2^{-1}$ értéke permutáció erejéig az $\{x_1, x_2\}$ párt, ezekhez a párokhoz ugyanis csak a fenti alakú megoldások léteznek.

Az elemi szimmetrikus polinomok elméletéből tudjuk, hogy $(x_1 + x_2, x_1 x_2)$ egyértelműen meghatározza az $\{x_1, x_2\}$ párt. Vegyük észre, hogy $x_1^{-1} + x_2^{-1} = \frac{x_1+x_2}{x_1 x_2}$, ezért ha $x_1 + x_2 \neq 0$, akor ezt átrendezve $x_1 + x_2$ és $x_1^{-1} + x_2^{-1}$ meghatározza $x_1 x_2$-t, és így magát az (x_1, x_2) párt is permutáció erejéig.

Tehát csak abban az esetben kaphatunk új megoldásokat, mikor $x_1 + x_2 = 0$, de ebben az esetben csak $(x_1, -x_1, y_1, -y_1)$ alakú számnégyesek jöhetnek szóba, de ezek valóban

megoldásai is az eredeti egyenletrendszernek. Ilyenekből $(q_1)^2$ darab van (x_1-et és y_1-et is $(q-1)$-féleképpen választhatjuk), de az $(x_1, -x_1, x_1, -x_1)$ és $(x_1, -x_1, -x_1, x_1)$ alakúakat már korábban leszámoltuk, ezekből $2(q-1)$ darab van.

Összeségében tehát azt kaptuk, hogy $|A_2| = 2(q-1)^2 - (q-1) + (q_1)^2 - 2(q-1) = = 3(q-2)(q-1)$, és innen, a formulát használva $M_2 = \frac{2q^3-3q^2-3q-1}{q-1}$ adódik, és éppen ezt akartuk belátni. $\square$

Egy Kloosterman-összeg kiszámítását vissza lehet vezetni egyszerűbb Kloosterman-összegek kiszámítására a Selberg-azonosság segítségével:

$$S(n,m,c) = \sum_{d|(n,m,c)} dS\left(1, \frac{nm}{d^2}, \frac{c}{d}\right)$$

Ezt először Selberg írta fel. A következő fejezetben ennek egy általánosítását fogjuk felírni és bebizonyítani, speciális esetként ez az azonosság is be lesz bizonyítva.

2. fejezet

Algebrai számtestek feletti Kloosterman-összegek

Ebben a fejezetben a klasszikus Kloosterman-összegeket általánosítani fogjuk algebrai számtestek felett. Megvizsgáljuk az alapvető tulajdonságait, azután pedig belátjuk a Selberg-féle azonosság általánosítását. Ez a [1] cikkben lett kimondva és bizonyítva, ez a fejezet is az ottani gondolatmenetet és bizonyítást követi.

2.1. Az általánosított Kloosterman-összegek értelmezése

Legyen $\mathbb{F}$ egy tetszőleges algebrai számtest, azaz $\mathbb{Q}$-nak egy véges algebrai bővítése, $\mathcal{O}$ pedig legyen $\mathbb{F}$-ben az egészek gyűrűje. A klasszikus Kloosterman-összegeket a következőképpen definiáltuk:

$$S(n,m,c) = \sum_{\substack{0<x<c \\ (x,c)=1}} e\left(\frac{nx+m\bar{x}}{c}\right)$$

ahol n, m, $c \in \mathbb{Z}$, $c > 0$ és $\bar{x}$ az x inverze mod c. Ha $\mathbb{F}$ felett szeretnénk értelmezni hasonló összegeket, akkor kézenfekvő, hogy $\mathbb{Z}$ helyét $\mathcal{O}$ fogja átvenni, c pedig egy modulus szerepét tölti be tulajdonképpen, így az is természetes, hogy c helyét egy I nemnulla ideál veszi át $\mathcal{O}$-ban, hiszen minden ilyen ideálra $\mathcal{O}/I$ véges. A véges testek feletti általánosításkor pedig már láttuk, hogy igazából az exponenciális rész a $\varphi_{\frac{n}{c}}$ és $\varphi_{\frac{m}{c}}$ $\mathbb{Z}/c\mathbb{Z}$ feletti karakterek szorzata, az egyiket az x, a másikat pedig a $\bar{x}$ helyen kiértékélve. Ezeket összerakva már adódik is a következő definíció számtestek feletti Kloosterman-összegre:

$$S(\varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^\times} \varphi(x)\psi(x^{-1})$$

ahol I nemnulla ideál $\mathcal{O}$-ban, φ, ψ karakterei $\mathcal{O}/I$-nek és x^{-1} az x inverze mod I.

A fentiek alapján nyilvánvaló, hogy $\mathbb{F} = \mathbb{Q}$ esetén a klasszikus Kloosterman-összegeket kapjuk vissza.

Az eddigiekhez hasonlóan könnyen belátható, hogy $S(\varphi, \psi, I)$ mindig egy valós szám lesz, valamint hogy $S(\varphi, \psi, I) = S(\psi, \varphi, I)$. A következőekben a Selberg-féle azonosság általánosítását szeretnénk megfogalmazni, azután a fejezet legnagyobb részét annak bizonyítására fogjuk szentelni. Emlékeztetőül, klasszikus Kloosterman-összegek esetén a Selberg-féle azonosság a következő volt:

$$S(n, m, c) = \sum_{d|(n,m,c)} dS\left(1, \frac{nm}{d^2}, \frac{c}{d}\right)$$

Az általánosítás során néhány dolog bonyolultabb lesz, tekintve, hogy $\mathcal{O}/I$ nem feltétlenül főideálgyűrű. A d-k megfelelői nyilvánvalóan ideálok lesznek, de nem teljesen tiszta, hogy a $d|(n, m, c)$ hogyan íródik át. Ezt a feltételt másképp úgy mondhatjuk, hogy $d|n$, $d|m$ és $d|c$. Ezekből a $d|c$ feltétel könnyen átmegy számtestekre, hiszen ott c és d ideálok, és ideálok között tudtunk oszthatóságot értelmezni, így az összegzésnek majd I-t osztó J ideálok között kell történnie.

Ez még mindig nem teljesen jó így, hiszen az utolsó argumentum, $\frac{c}{d}$ azt szeretnénk, ha egy ideál lenne, de jelenleg ezt így nem tudjuk ideálként értelmezni, de tudjuk, hogy ha $d|c$, akkor $\frac{c}{d}|d$, ezért az eredeti összegzést átírhatjuk úgy, hogy d'-kre összegzünk, melyekre $c = dd'$,és $d|(n, m)$, és akkor ideálokra átírva így már $\frac{c}{d}$ helyett írhatunk J-t.

A $d|(n, m)$ feltétel megértéséhez nézzünk rá az összegben szereplő Kloosterman-összegek második argumentumára: $\frac{nm}{d^2} = \frac{n}{d} \cdot \frac{m}{d}$, a d'-s átírásban $\frac{n}{d'} \cdot \frac{m}{d'}$ szerepel, ahol $d'|n, m$. Ha n-re, m-re, mint $\varphi_{\frac{n}{c}}$ és $\varphi_{\frac{m}{c}}$ $\mathbb{Z}/c\mathbb{Z}$ karaterekre gondoltunk az eredeit Kloosterman-összegnél, akkor ezek helyét veszik át $\frac{n}{d'}$ és $\frac{m}{d'}$, mint valami $\mathbb{Z}/d\mathbb{Z}$ feletti karakterek. Tehát az általánosított esetben φ és ψ $\mathcal{O}/I$ feletti karakterekből kellene $\mathcal{O}/J$ feletti karaktereket csinálnunk. Ez bizonyos esetekben könnyen megy: ugyanis, egy $\mathcal{O}/I$ feletti karakterre gondolhatunk úgy, mint egy $\mathcal{O} \to S^1$ leképezésre (ahol S^1 a komplex egységkört jelöli), aminek a magjának részhalmaza I. Így ezek alapján, ha ezen leképezés magjának még J is része, ahol $J|I$, akkor ez a leképezés természetes módon indukál egy karaktert $\mathcal{O}/J$-n. Ennek példáján úgy írjuk át a $d|(n, m)$ feltételt, hogy $J \subseteq ker\varphi \cap ker\psi$ (a dolgozat to-

vábbi részében ugyanúgy φ, ψ-vel fogjuk jelölni a $\mathcal{O}/I$ feletti karaktert, annak $\mathcal{O}$-ra való kiterjesztését és a $\mathcal{O}/J$-re való megszorítását is, ez nem fog félreértést okozni). Tehát az összegzést olyan J ideálokra fogjuk végezni, amikre $J|I$, $J \subset ker\varphi \cap ker\psi$,és $\frac{c}{d}$ helyét J veszi át.

Ahhoz, hogy $\frac{n}{d'} \cdot \frac{m}{d'}$ megfelelőjét megtaláljuk az általánosításban, jobban meg kell értenünk $\mathcal{O}/J$-t, hiszen tudjuk, hogy $\frac{n}{d'}$ és $\frac{m}{d'}$ helyett $\mathcal{O}/J$ feletti karakterek lesznek, de ezek szorzatát még nem tudjuk értelmezni, hiszen az alapesetben ez nem a karakterek pontonkénti szorzásának felel meg, hanem egy $\mathbb{Z}$-ből örökölt szorzásnak, esetünkben is hasonlót kellene találnunk.Ehhez ki kell bővítenünk a $\widehat{\mathcal{O}/J}$ karaktercsoport struktúráját.

Első körben egy $\mathcal{O}$-modulussá tudjuk tenni $\widehat{\mathcal{O}/J}$-t a következő művelettel:
$r \cdot \varphi : x \mapsto \varphi(rx)$, ha $r \in \mathcal{O}$ és $\varphi \in \widehat{\mathcal{O}/J}$. Ez tényleg egy $\mathcal{O}$-modulus lesz, és a természetes módon $\mathcal{O}/J$-modulussá válik, sőt az is kiderül, hogy ciklikus $\mathcal{O}/J$-modulus lesz, ezen állításokat a következő részben látjuk majd be.

Ezeket elfogadva, vegyük egy λ_J generátorát $\mathcal{O}/J$-nek. Ekkor

$$\mathcal{O}/I \to \widehat{\mathcal{O}/I}, r \mapsto r \cdot \lambda_I$$

egy modulusizomorfizmus lesz, és ennek segítségével már tudunk definiálni egy gyűrűstruktúrát is $\widehat{\mathcal{O}/I}$-n úgy, hogy az előbbi izomorfizmus mentén lemásoljuk a $\mathcal{O}/I$-beli szorzást (így $\widehat{\mathcal{O}/I}$-n az összeadás a "régi", pontonként szorzás lesz, a szorzás pedig a most bevezetett). Ha φ, $\psi \in \widehat{\mathcal{O}/J}$, akkor jelöljük ezt a szorzatukat $\varphi * \psi$-vel. Tehát, ha $\varphi = r \cdot \lambda_J$, $\psi = r' \cdot \lambda_J$, akkor $\varphi * \psi = rr' \cdot \lambda_J$. Ezekből már azt is sejthetjük, hogy a jobb oldali Kloosterman-összegek első argumentumában a λ_J generátorelemnek kell állnia, hiszen az 1-es ott a $\varphi_{1/d}$ karakternek felel meg, ami valóban generálja a $\widehat{\mathbb{Z}/d\mathbb{Z}}$ modulust.

Az előbbi meggondolásokkal szemben egy probléma léphet fel: a karakterek szorzása, ahogy bevezettük, függ attól, hogy melyik generátorelemet választottuk ki. Szerencsére ez a Kloosterman-összegekre nem lesz hatással: később be fogjuk látni, hogy ha λ_J, λ'_J generátorai a $\widehat{\mathcal{O}/J}$ modulusnak, $*$, $*'$ pedig az általuk indukált szorzások, akkor

$$S(\lambda_J, \varphi * \psi, J) = S(\lambda'_J, \varphi *' \psi, J)$$

Már csak a d-s szorzó megfelelője hiányzik a Kloosterman-összegek előtt, ennek ideálokon nézve a norma egy kézenfekvő megfelelője. Vigyázni kell azonban, mert a d'-s átírásunk miatt nem $N(J)$ fog ott állni, hanem $N(I) \cdot N(J)^{-1}$. Összerakva mindezt, azt kaptuk, hogy

a Selberg-azonosságot így írhatjuk át számtestek felett:

$$S(\varphi,\psi,I)=N(I)\sum_{\substack{J|I\\ J\subseteq ker\varphi\cap ker\psi}}N(J)^{-1}S(\lambda_J,\varphi*\psi,J)$$

Ellenőrizzük le, hogy ez valóban általánosítja a régi formulát. Legyen tehát $\mathbb{F}=\mathbb{Q}$, ekkor minden nemnulla ideál $c\mathbb{Z}$ alakú, $\mathbb{Z}/c\mathbb{Z}$ karakterei éppen a

$$\varphi_{\frac{n}{c}}:x\mapsto e\left(\frac{nx}{c}\right)$$

leképezések, $n=0,1,...,c-1$.Mivel $n\cdot\varphi_{\frac{m}{c}}(x)=\varphi_{\frac{m}{c}}(nx)=\varphi_{\frac{nm}{c}}(x)$, így $n\cdot\varphi_{\frac{m}{c}}=\varphi_{\frac{nm}{c}}$. Ezekből már adódik, hogy $\varphi_{\frac{1}{c}}$ generátora $\widehat{\mathbb{Z}/c\mathbb{Z}}$-nek. Ezzel a szorzás a $\mathbb{Z}$-n megszokott szorzás lesz, tehát $\varphi_{\frac{n}{c}}*\varphi_{\frac{m}{c}}=\varphi_{\frac{nm}{c}}$.

Ha $(c)=(d)(d)'$, akkor $d\in ker\varphi_{\frac{n}{c}}$ akkor és csak akkor, ha d' osztja n-t.Ebben az esetben, a fent meggondoltak szerint $\varphi_{\frac{n}{c}}\in\mathbb{Z}/d\mathbb{Z}$, és $\varphi_{\frac{n}{c}}=\frac{n}{d'}\cdot\varphi_{\frac{1}{d}}$, ez könnyen kiszámolható.Így tehát $I=(c)$, $\varphi=\varphi_{\frac{n}{c}}$, $\psi=\varphi_{\frac{m}{c}}$ választással a formulánkban, a következőt kapjuk:

$$S(n,m,c)=c\sum_{\substack{c=dd'\\ d'|(n,m)}}d^{-1}S\left(\varphi_{\frac{1}{d}},\frac{nm}{d'^2}\cdot\varphi_{\frac{1}{d}},(d)\right)=\sum_{\substack{c=dd'\\ d'|(n,m)}}d'S\left(1,\frac{nm}{d'^2},d\right)=$$

$$=\sum_{d|(n,m,c)}dS\left(1,\frac{nm}{d^2},\frac{c}{d}\right)$$

az utolsó egyenlőségnél a d' helyére d-t helyettesítve. Tehát valóban visszakapjuk az eredeti azonosságot.

A következőekben belátjuk, hogy $\widehat{\mathcal{O}/I}$ valóban ciklikus $\mathcal{O}/I$-modulus, a megfelelő Kloosterman-összeg független a választott generátorelemtől, és aztán rátérünk a Selberg-féle azonosság bizonyítására.

2.2. $\widehat{\mathcal{O}/I}$, mint ciklikus modulus

A Selberg-féle azonosság általánosításának már a kimondásához szükségünk van $\widehat{\mathcal{O}/I}$ egy generátorára, ehhez ebben a részben belátjuk, hogy $\widehat{\mathcal{O}/I}$ valóban ciklikus $\mathcal{O}/I$-modulus. Emlékeztetőül, a $\widehat{\mathcal{O}/I}$ karaktercsoporton először is egy $\mathcal{O}$-modulusstruktúrát adtunk meg: $r\in\mathcal{O},\varphi\in\widehat{\mathcal{O}/I}$ esetén $r\cdot\varphi:x\mapsto\varphi(rx)$ legyen. (A fejezetben mostantól végig $r\in\mathcal{O}$, $\varphi\in\widehat{\mathcal{O}/I}$.) Azt, hogy ez valóban jó definíció, és hogy ez a természetes módon ad egy $\widehat{\mathcal{O}/I}$-modulusstruktúrát is, a következő állítás foglalja össze.

2.2.1. Állítás.

(i) $r \cdot \varphi : x \mapsto \varphi(rx)$ *valóban karaktere* $\mathcal{O}/I$*-nek, és ezzel a szorzással* $\widehat{\mathcal{O}/I}$ *egy* $\mathcal{O}$*-modulus.*

(ii) $\widehat{\mathcal{O}/I}$ *egy* $\mathcal{O}/I$*-modulus is a fentinek megfelelő szorzással, azaz ha* r *és* s *ugyanazon mellékosztlyba esnek* I *szerint, akkor* $r \cdot \varphi = s \cdot \varphi$ *minden* $\varphi \in \widehat{\mathcal{O}/I}$*-re.*

Bizonyítás. (i): Ha $x, y \in \mathcal{O}/I : r \cdot \varphi(x+y) = \varphi(r(x+y)) = \varphi(rx) + \varphi(ry) = r \cdot \varphi(x) + r \cdot \varphi(y)$. Az, hogy teljesünek a modulusaxiómák ezzel a szorzással, egyszerű számolással ellenőrizhetőek.

(ii): Elég azt látnunk, hogy $r \in I$ esetén $r \cdot \varphi$ a triviális (azonosan 1) karakter, ez pedig nyilvánvaló, hiszen ekkor minden $x \in \mathcal{O}/I$-re $rx \in I$, és $\varphi(I) = 1$. $\square$

Ha $\lambda \in \widehat{\mathcal{O}/I}$, akkor az $f_\lambda : \mathcal{O}/I \longrightarrow \widehat{\mathcal{O}/I}, r \mapsto r \cdot \lambda$ jóldefiniált a fentiek alapján, és egy $\mathcal{O}/I$-modulusmorfizmus. A következő állításban ennek a felhasználásával többféle karakterizációját is megadjuk $\widehat{\mathcal{O}/I}$ generátorelemeinek.

2.2.2. Állítás. *Ekvivalensek:*

(i) f_λ $\mathcal{O}/I$*-modulusizomorfizmus.*

(ii) λ *generátoreleme* $\widehat{\mathcal{O}/I}$*-nek.*

(iii) $ker\lambda$ *nem tartalmazza* I*-nek egyetlen valódi osztóját sem.*

Bizonyítás. $(i) \Rightarrow (ii)$: Ha f_λ izomorfizmus, akkor speciálisan szürjektív is, így tetszőleges $\varphi \in \widehat{\mathcal{O}/I}$-hez létezik olyan $r \in \mathcal{O}/I$, amelyre $\varphi = r \cdot \lambda$, tehát λ generálja $\widehat{\mathcal{O}/I}$-t.

$(ii) \Rightarrow (iii)$: Ha λ generálja $\widehat{\mathcal{O}/I}$-t, akkor f_λ szürjektív, de így injektív is, hiszen két véges modulus közötti homomorfizmus, amiknek az elemszáma ugyanakkora. Tegyük fel, hogy $J \subseteq ker\lambda$, és J valódi osztója I-nek, azaz $I \subsetneqq J$. De ekkor, ha $s \in J$, $s \notin I$, akkor $J \subseteq ker\lambda$ miatt $s \cdot \lambda = 1$ (ahol 1 a triviális araktert jelöli), ami ellentmond f_λ injektivitásának, hiszen $0 \cdot \lambda$ szintén a triviális karakterrel egyezik meg.

$(iii) \Rightarrow (i)$: Mivel a két véges modulus elemszáma megegyezik, ezért elég f_λ injektivitását belátnunk. Tegyük fel, hogy $r \cdot \lambda = 1$, azaz bármely $x \in \mathcal{O}$-ra $\lambda(rx) = 1$ (természetesen itt is a megfelelő elemek szerinti mellékosztályokra kell gondolni), ezért $(r) \subseteq ker\lambda$. De így $ker\lambda$ tartalmazza az $(r) + I$ ideált, aminek része I, ezért $(r) + I = I$, és így $r \in I$, tehát f_λ tényleg szürjektív. $\square$

$\widehat{\mathcal{O}/I}$ ciklikusságának bizonyításához fő segédeszközünk az ideálokra vonatkozó prímfaktorizációs tétel lesz, vagyis hogy ha I nemnulla ideál, akkor egyértelműen felírható prímideálok szorzataként: $I = P_1^{n_1}P_2^{n_2}...P_k^{n_k}$, és így az első fejezetben látottak szerint $\mathcal{O}/I \cong \mathcal{O}/P_1^{n_1} \times \mathcal{O}/P_2^{n_2} \times ... \times \mathcal{O}/P_k^{n_k}$

Ez a faktorizáció esetünkben azért lesz nagyon hasznos, mert a karakterek is szorzatra bomlanak ezen izomorfizmus mentén, ugyanis bármely $\varphi \in \widehat{\mathcal{O}/I}$ karakter felírható $\varphi = \varphi_1 \times \varphi_2 \times ... \times \varphi_k$ alakban, ahol $\varphi_j \in \widehat{\mathcal{O}/P_j^{n_j}}$, és ezt a szorzatra bontást úgy értjük, hogyha $x = (x_1, x_2, ..., x_k) \in \mathcal{O}/I \cong \mathcal{O}/P_1^{n_1} \times \mathcal{O}/P_2^{n_2} \times ... \times \mathcal{O}/P_k^{n_k}$, akkor $\varphi(x) = \varphi_1(x_1)\varphi_2(x_2)...\varphi_k(x_k)$. Ezt könnyű belátni: ha van egy φ karakterünk, akkor tekinthetjük ennek rendre $\mathcal{O}/P_1^{n_1}$-re, $\mathcal{O}/P_2^{n_2}$-re,..., $\mathcal{O}/P_k^{n_k}$-ra való megszorításait, így kapjuk φ_1, φ_2, ..., φ_k-t, ezek nyilván karakterei lesznek a megfelelő részgyűrűknek, és a karakter művelettartó tulajdonsága miatt ezek szorzatának muszáj φ-nek lennie. Ennek alapján az is könnyen meggondolható, hogy $\varphi = \varphi_1 \times \varphi_2 \times ... \times \varphi_k$ esetén $r \cdot \varphi = r \cdot \varphi_1 \times r \cdot \varphi_2 \times ... \times r \cdot \varphi_k$, valamint, hogy φ pontosan akkor triviális, ha mindegyik φ_j triviális.

Ezek után a következő lemma segítségével kiderül, hogy ez előző állításban kapott (*iii*) karakterizáció és ezen szorzatra bontás segítségével a $\widehat{\mathcal{O}/I}$ ciklikusságának vizsgálatát vissza lehet vezetni arra az esetre, amikor I egy prímideál hatványa.

2.2.3. Lemma. *Legyen $I = P_1^{n_1}P_2^{n_2}...P_k^{n_k}$, $\varphi = \varphi_1 \times \varphi_2 \times ... \times \varphi_k \in \widehat{\mathcal{O}/I}$.*
Legyen $J = P_1^{s_1}P_2^{s_2}...P_k^{s_k}$, ahol $s_i \leq n_i$ nemnegatív egész számok.
Ekkor $J \subseteq ker\varphi$ pontosan akkor, ha $P_i^{s_i} \subseteq ker\varphi_i$ mindegyik i-re.

Bizonyítás. Először tegyük fel, hogy $J \subseteq ker\varphi$ és rögzítsük i-t. Ha $x_i \in P_i^{n_i}$, akkor a kínai maradéktétel szerint létezik olyan $x \in \mathcal{O}$, hogy $x \equiv x_i \pmod{P_i^{n_i}}$, és $x \in P_j^{n_j}$, ha $j \neq i$. Ekkor, ha $x \in P_1^{s_1} \cap P_2^{s_2} \cap ... \cap P_k^{s_k} = P_1^{s_1}P_2^{s_2}...P_k^{s_k} = J$, akkor

$$\varphi_i(x_i) = \varphi_i(x) \cdot \prod_{j \neq i} \varphi_j(x) = \varphi(x) = 1$$

vagyis $x_i \in ker\varphi_i$.

Megfordítva, tegyük fel, hogy $P_i^{s_i} \subseteq ker\varphi_i$ mindegyik i-re. Ha $x \in J$, akkor $x \in P_i^{s_i}$ mindegyik i-re, ezért $\varphi(x) = \varphi_1(x)\varphi_2(x)...\varphi_k(x) = 1 \cdot 1 \cdot ... \cdot 1 = 1$. $\square$

Ezek után rátérhetünk ezen szakasz fő eredményének a bizonyítására.

2.2.4. Tétel. *$\widehat{\mathcal{O}/I}$ ciklikus $\mathcal{O}/I$-modulus.*

Bizonyítás. A 2.2.2 állítás (*iii*) pontja miatt elég azt belátnunk, hogy létezik olyan $\lambda \in \widehat{\mathcal{O}/I}$ elem, hogy I-nek egyetlen valódi osztóját sem tartalmazza $ker\lambda$.

Lássuk be az állítást akkor, amikor $I = P^n$, ahol P egy prímideál, n pedig pozitív egész. (Ha $n = 0$, akkor $I = \mathcal{O}$, és így ekkor $\widehat{\mathcal{O}/I}$ egyelemű, vagyis ciklikus.) Ekkor P^n ideálja P^{n-1}-nek, $\widehat{P^{n-1}/P^n}$ nem egyelemű, hiszen P^{n-1}/P^n sem egyelemű (mert nyilvánvalóan $P^{n-1} \neq P^n$), ezért létezik P^{n-1}/P^n-nek egy λ_0 nemtriviális karaktere. Továbbá P^{n-1}/P^n részcsoportja $\mathcal{O}/P^n$-nek (hiszen P^{n-1} részcsoportja $\mathcal{O}$-nak), így az 1.1.3 állítás miatt λ_0 kiterjed $\mathcal{O}/P^n$ egy λ karakterévé (ami nyilvánvalóan szintén nemtriviális). Erre a λ-ra $P^{n-1} \nsubseteq ker\lambda$, hiszen egyébként minden $x \in P^{n-1}$-re $1 = \lambda(x) = \lambda_0(x)$ teljesülne, ami ellentmondana λ_0 nemtrivialitásának. Ezzel készen is vagyunk ezzel az esettel, hiszen P^n minden valódi osztója osztója P^{n-1}-nek.

Most jöjjön az általános eset: legyen $I = P_1^{n_1}P_2^{n_2}...P_k^{n_k}$. Minden $i = 1, 2, .., k$-ra válasszuk ki $\mathcal{O}/P_i^{n_i}$-nek egy karakterét úgy, mint fent, tehát $P_i^{n_i-1} \nsubseteq ker\lambda_i$. Belátjuk, hogy ekkor $\lambda = \lambda_1 \times \lambda_2 \times ... \times \lambda_k$ generátorelem lesz.

Legyen ugyanis J egy I-t osztó ideál, vagyis $J = P_1^{s_1}P_2^{s_2}...P_k^{s_k}$, ahol $s_j \leq n_j$ nemnegatív egészek, és tegyük fel, hogy $J \subseteq ker\lambda$. Ekkor az előző lemma szerint $P_i^{s_i} \subseteq ker\lambda_i$ minden i-re, de ez a λ_i-k választása miatt minden i-re $s_i = n_i$-t vonja maga után, vagyis $J = I$, tehát λ generálja $\widehat{\mathcal{O}/I}$-t. $\square$

A fenti gondolatokat követve egy kicsit többet is tudunk mondani a generátorokról a prímfelbontáson keresztül:

2.2.5. Állítás. *Legyen $I = P_1^{n_1}P_2^{n_2}...P_k^{n_k}$, $\varphi = \varphi_1 \times \varphi_2 \times ... \times \varphi_k \in \widehat{\mathcal{O}/I}$. Ekkor φ pontosan akkor generálja $\widehat{\mathcal{O}/I}$-t, ha minden i-re φ_i generálja $\widehat{\mathcal{O}/P_i^{n_i}}$-t.*

Bizonyítás. Ha valamelyik i-re φ_i nem generálja $\widehat{\mathcal{O}/P_i^{n_i}}$-t, akkor létezik $s_i < n_i$, amire $P_i^{s_i} \subseteq ker\varphi_i$. Legyen ekkor továbbá $s_j = n_j$ minden $j \neq i$-re. Ekkor $J = P_1^{s_1}P_2^{s_2}...P_k^{s_k}$ valódi osztója I-nek, és $J \subseteq ker\varphi$ a lemma alapján, de ekkor φ nem generálhatja $\widehat{\mathcal{O}/I}$-t.

A megfordításhoz tegyük fel, hogy φ_i generálja $\widehat{\mathcal{O}/P_i^{n_i}}$-t minden i-re, és legyen $I \subseteq j \subseteq ker\varphi$, $J = P_1^{s_1}P_2^{s_2}...P_k^{s_k}$, $s_i \leq n_i$. A lemma miatt ekor $P_j^{s_j} \subseteq ker\varphi_j$ mindegyik j-re. De mivel minden j-re φ_j generálja $\widehat{\mathcal{O}/P_j^{n_j}}$-t, ezért az előző tétel bizonyításában látottak szerint $s_j = n_j$-nek kell teljesülnie mindegyik j-re, vagyis $J = I$, és így φ generállja $\widehat{\mathcal{O}/I}$-t. $\square$

2.3. Számtestek feletti Kloosterman-összegek tulajdonságai

Ebben a részben főként a Selberg-féle azonosság bizonyításához szükséges segédállításokat fogunk belátni, valamint meggyőződünk arról is, hogy $\widehat{\mathcal{O}/I}$ gyűrűvé tételénél a generátorelem választása nem változtatja meg a szóban forgó Kloosterman-összegeket.

2.3.1. Lemma. *Ha $\varphi, \psi \in \widehat{\mathcal{O}/I}$, valamint $r \in \mathcal{O}$ olyan, hogy $(r, I) = 1$, (vagyis $r + I$ egység $\mathcal{O}/I$-ben), akkor $S(r \cdot \varphi, \psi, I) = S(\varphi, r^{-1} \cdot \psi, I)$ (ahol r^{-1} alatt mod I értjük r inverzét).*

Bizonyítás. Ha r relatív prím I-hez, akkor az r-rel való szorzás egy bijekciót ad meg $(\mathcal{O}/I)^\times$-on, hiszen az egy test és r (vagyis r mellékosztálya) egy numnulla eleme. Így tehát

$$S(r \cdot \varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^\times} \varphi(rx)\psi(x^{-1}) = \sum_{y \in (\mathcal{O}/I)^\times} \varphi(y)\psi((r^{-1}y)^{-1}) = S(\varphi, r^{-1} \cdot \psi, I)$$

az $y = r^{-1}x$ helyettesítéssel. $\square$

Ennek alapján már be tudjuk bizonyítani, hogy a megfelelő Kloosterman-összegek függetlenek a generátorelem választásától.

2.3.2. Következmény. Ha λ_I, λ_I' generátorai $\widehat{\mathcal{O}/I}$-nek, és $*$, illetve $*'$ jelöli az általuk indukált szorzásokat $\widehat{\mathcal{O}/I}$-n, akkor bármely φ, $\psi \in \widehat{\mathcal{O}/I}$ esetén

$$S(\lambda_I, \varphi * \psi, I) = S(\lambda_I', \varphi *' \psi, I)$$

Bizonyítás. Mivel λ_I és λ_I' mindketten generátorai $\widehat{\mathcal{O}/I}$-nek, ezért $\lambda_I' = s \cdot \lambda_I$, ahol s egy invártalható elem $\mathcal{O}/I$-ben. Ugyanis, ha mindkettő generátorelem, akkor $\lambda_I' = s \cdot \lambda_I$ és $\lambda_I = s' \cdot \lambda_I'$ valamilyen $s, s' \in \mathcal{O}/I$-re, vagyis $\lambda_I = s's\lambda_I$, de a 2.2.2 állítás szerint $f_{\lambda_I} : \mathcal{O}/I \longrightarrow \widehat{\mathcal{O}/I}, s \mapsto s \cdot \lambda_I$ modulusizomorfizmus, így $ss' = 1$, tehát s valóban invertálható modulo I.

Legyen $\varphi = r \cdot \lambda_I$, $\psi = r' \cdot \lambda_I$, ekkor $\varphi = rs^{-1} \cdot \lambda_I'$, $\psi = r's^{-1} \cdot \lambda_I'$. Így a szorzatok: $\varphi * \psi = rr'\lambda_I$ és $\varphi *' \psi = rs^{-1}r's^{-1}\lambda_I' = rr's^{-1}\lambda_I$. De ekkor

$$S(\lambda_I', \varphi *' \psi, I) = S(s \cdot \lambda_I, rr's^{-1} \cdot \lambda_I, I)$$

$$S(\lambda_I, \varphi * \psi, I) = S(\lambda_I, rr' \cdot \lambda_I, I)$$

A jobboldalok az előző lemma miatt megegyeznek, így készen vagyunk. □

A Selberg-azonosság bizonyításánál hasonló stratégiát szeretnénk követni, mint $\widehat{\mathcal{O}/I}$ ciklikusságának bizonyításánál: először prímideálok hatványaira látjuk be az állítást, aztán a prímfaktorizációs tétel és megfelelő multiplikatív tulajdonságok alapján ezt kiterjesztjük tetszőleges ideálokra. Ahhoz, hogy ez működőképes legyen, a Kloosterman-összegeknek is teljesíteniük kell valamilyen multiplikatív tulajdonságot, ezt a következő lemmában fogjuk megvizsgálni.

Legyenek A, B ideálok $\mathcal{O}$-ban, amik relatív prímek egymáshoz, és $I = AB$. Ekkor, ahogy már korábban használtuk is, $\mathcal{O}/I \cong \mathcal{O}/A \times \mathcal{O}/B$ (kínai maradéktétel), és azt is láttuk, hogy minden $\varphi \in \widehat{\mathcal{O}/I}$ felírható $\varphi = \varphi_1 \times \varphi_2$ alakban, ahol $\varphi_1 \in \widehat{\mathcal{O}/A}$, $\varphi_2 \in \widehat{\mathcal{O}/B}$.

2.3.3. Lemma. *Ha $\varphi = \varphi_1 \times \varphi_2$, $\psi = \psi_1 \times \psi_2$, akkor*

$$S(\varphi, \psi, I) = S(\varphi_1, \psi_1, A)S(\varphi_2, \psi_2, B)$$

.

Bizonyítás. Legyen $x_1 \in (\mathcal{O}/A)^\times$, $x_2 \in (\mathcal{O}/B)^\times$. Ekkor, ha $(x_1, x_2) \in \mathcal{O}/A \times \mathcal{O}/B$ az $x \in \mathcal{O}/I$-nek felel meg, akkor x invertálható és az inverzének (x_1^{-1}, x_2^{-1}) felel meg, és fordítva is igaz ez, tehát $(\mathcal{O}/A)^\times \times (\mathcal{O}/B)^\times \cong (\mathcal{O}/I)^\times$ az előző izomorfizmus megszorításával. Így

$$S(\varphi_1, \psi_1, A)S(\varphi_2, \psi_2, B) = \sum_{x_1 \in (\mathcal{O}/A)^\times} \varphi_1(x_1)\psi_1(x_1^{-1}) \sum_{x_2 \in (\mathcal{O}/B)^\times} \varphi_2(x_2)\psi_2(x_2^{-1}) =$$

$$= \sum_{x \in (\mathcal{O}/I)^\times} \varphi(x)\psi(x^{-1}) = S(\varphi, \psi, I)$$

és éppen ezt akartuk belátni. □

2.3.4. Következmény. Ha $I = P_1^{n_1} P_2^{n_2} ... P_k^{n_k}$ az I ideál prímfelbontása, a φ, $\psi \in \widehat{\mathcal{O}/I}$ karaktereknek pedig az ehhez tartozó felbontása rendre $\varphi = \varphi_1 \times \varphi_2 \times ... \times \varphi_k$,
$\psi = \psi_1 \times \psi_2 \times ... \times \psi_k$, akkor

$$S(\varphi, \psi, I) = \prod_{i=1}^{k} S(\varphi_i, \psi_i, P^{n_i})$$

A fentiek szellemében most rátérünk a $\mathcal{O}/P^m$ gyűrűk feletti Kloosterman-összegek részletesebb tanulmányozására, ahol P prímideál. A továbbiákban λ_m-fel fogjuk jelölni a $\widehat{\mathcal{O}/P^m}$ modulus egy előre rögzített generátorelemét. Azt már láttuk korábban, hogy ha

$\varphi \in \mathcal{O}/P^m$, akkor φ tekinthető úgy, mint egy $\mathcal{O} \to S^1$ leképezésre, aminek a magjának része P^m. Ha valamelyik $j < m$-re még $P^j \subsetneqq ker\varphi$ is teljesül akkor tekinthetjók φ-t $\widehat{\mathcal{O}/P^j}$-beli elemként is. A $P^j \subsetneqq ker\varphi$ feltétel egy karakterizációját adja meg a következő lemma a generátorelem ismeretében:

2.3.5. Lemma. *Legyen $j < m$ és $r \in \mathcal{O}$. Ekkor $P^j \subsetneqq ker\ r \cdot \lambda_m \Leftrightarrow P^{m-j}|(r)$.*

Bizonyítás. Először tegyük fel, hogy $P^{m-j}|(r)$, vagyis $(r) = P^{m-j}K$ valamilyen K ideálra. Ekkor $r = a \cdot k$, ahol $a \in P^{m-j},\ k \in K$. Ha $p \in P^j$, akkor ezek alapján

$$(r \cdot \lambda_m)(p) = \lambda_m(rp) = \lambda_m(kap) = 1$$

hiszen $ap \in P^m$, és így $kap \in P^m$, ami benne van λ_m magjában. Tehát $P^j \subsetneqq ker\ r \cdot \lambda_m$.

A másik irányhoz tegyük fel, hogy $P^j \subsetneqq ker\ r \cdot \lambda_m$, ekkor $r \cdot P^j$-n és P^m-n is, ezért eltűnik $rP^j + P^m = (rP^j, P^m)$-en. Másrészt létezik egy $q \leq s \leq m$ egész szám, amire $(r, P^m) = P^s$, hiszen P^m osztói mind ilyen alakúak. Ebből adódóan $(rP^j, P^m) = P^{min(s+j,m)}$. De $P^{m-1} \nsubseteq ker\ \lambda_m$ a 2.2.2 állítás (iii) pontja szerint, ezért (rP^j, P^m) -ben P hatványának legalább m-nek kell lennie, tehát $m \leq s + j$, vagyis $m - j \leq s$, és $(r, P^m) = P^s$, mindebből adódóan $P^{m-j}|(r)$, és ezt akartuk belátni. $\square$

2.3.6. Lemma. *Legyen $0 < n \leq m$ és $\varphi,\ \psi \in \widehat{\mathcal{O}/P^m}$. Ekkor*

$$S(\varphi, \psi, P^m) = \sum_{s \in (\mathcal{O}/P^n)^\times} \varphi(s)\psi(s^{-1}) \sum_{t \in P^n/P^m} \varphi(t)\psi(\sum_{j=1}^{m}(-1)^{j+1}s^{-j}t^{j-1})$$

Bizonyítás. Ha s $\mathcal{O}/P^n$, t pedig P^n/P^m egy teljes reprezentánsrendszerén fut végig, akkor $s + t$ $\mathcal{O}/P^m$ egy teljes reprezentánsrendszerén fut végig.Továbbá az is igaz, hogy $s + t \in (\mathcal{O}/P^m)^\times$ pontosan akkor, ha $s \in (\mathcal{O}/P^n)^\times$. Hiszen, ha $s + t$ invertálható $\mathcal{O}/P^m$-ben, akkor az inverz egy reprezentánselemét választva, az ahhoz az elemhez tartozó mellékosztály $\mathcal{O}/P^n$-ben megfelel majd s inverzének. Megfordítva, ha s invertálható $\mathcal{O}/P^n$-ben, akkor jelölje itt s^{-1} az inverzét. Ekkor $s + t$ inverzének modulo P^m megfelelő lesz

$$\sum_{j=1}^{m}(-1)^{j+1}s^{-j}t^{j-1}$$

A fentieket összrakva adódik a lemma állítása. $\square$

$\varphi \in \widehat{\mathcal{O}/P^m}$ esetén legyen $N_\varphi = min\{n \geq 0 : P^n \subsetneqq ker\varphi\}$. Tehát P^{N_φ} a legbővebb olyan P-hatvány, amin φ eltűnik.

2.3.7. Lemma. *Legyenek* $\varphi,\ \psi \in \widehat{\mathcal{O}/P^m}$.

(i) Ha $N_\varphi,\ N_\psi \leq N < m$ *és* $N > 0$, *akkor* $S(\varphi,\psi,P^m) = S(\varphi,\psi,P^N)N(P)^{m-N}$.

(ii) Ha $N_\varphi \neq N_\psi$ *és* $max(N_\varphi, N_\psi) \geq 2$, *akkor* $S(\varphi,\psi,P^m) = 0$.

Bizonyítás.

(i) Az előző lemmát használjuk $n = N$ esetén. Felhasználva, hogy P^N benne van φ és ψ magjában, a következőt kapjuk:

$$S(\varphi,\psi,P^m) = \sum_{s\in(\mathcal{O}/P^N)^\times} \varphi(s)\psi(s^{-1}) \sum_{t\in P^N/P^m} 1 = S(\varphi,\psi,P^m) = S(\varphi,\psi,P^N)N(P)^{m-N}$$

(ii) $S(\varphi,\psi,P^m) = S(\psi,\varphi,P^m)$ miatt szimmetriaokokból feltehetjük, hogy $N_\varphi > N_\psi$. Válaszuk $n = N_\varphi - 1 \geq 1$-et az előző lemmában. Ekkor ψ magjában benne van P^n, de φ nem azonosan 1 P^n-en, ezért ψ eltűnik a belső szummából és

$$\sum_{t\in P^n/P^m} \varphi(t) = 0$$

ami igazolja az állításunkat.

□

2.4. A Selberg-azonosság általánosításának bizonyítása

A korábban vázolt gondolatmenet szerint, először abban az esetben látjuk be az azonosságot, amikor I egy prímideál hatványa, majd a 2.3.3 lemma segítségével ezt átvisszük az általános esetre.

2.4.1. Állítás. *Legyen* P *prímideál* $\mathcal{O}$*-ban,* $m \in \mathbb{N}$ *és* $\varphi,\ \psi \in \widehat{\mathcal{O}/P^m}$. *Ekkor*

$$S(\varphi,\psi,P^m) = \sum_{\substack{0\leq j\leq m \\ P^j \subseteqq ker\varphi\cap ker\psi}} N(P)^{m-j} S(\lambda_{P^j}, \varphi * \psi, P^j)$$

Bizonyítás. A bizonyítás során a $\widehat{\mathcal{O}/P^n}$ modulus generátorát továbbra is λ_n-nel fogjuk jelölni, a jelölés egyszerűsítése végett. Legyen $N_\varphi = min\{n \geq 0 : P^n \subseteqq ker\varphi\}$,
$N_\psi = min\{n \geq 0 : P^n \subseteqq ker\psi\},\ n = min\{j \geq 0 : P^j \subseteqq ker\varphi \cap ker\psi\}$. Világos, hogy ekkor $N = max\{N_\varphi, N_\psi\}$.

Legyen $\varphi = r \cdot \lambda_m$ és $\psi = r' \cdot \lambda_m$. Ekkor a 2.3.5 lemma szerint $P^j \subsetneqq ker\varphi \cap ker\psi$ pontosan akkor, ha $(r, r', P^m) = P^{m-n}$.

Három különböző esetet kell megvizsgálnunk.

(i) Ha $n = 0$, akkor φ és ψ is azonosan 1-et vesznek fel, így $S(\varphi, \psi, P^m) = N(P)^m - N(P)^{m-1}$, hiszen éppen ennyi az invertálható elemek száma $\mathcal{O}/P^m$-ben. $\varphi * \psi$ is az azonosan 1 karakter, így $N_{\varphi*\psi} = 0$, és az is világos, hogy $N_{\lambda_j} = j$. Így a 2.3.7 lemma miatt $S(\lambda_j, \varphi * \psi, P^j) = 0$, ha $j \geq 2$. Így az állítás jobb oldala:
$N(P)^m S(\lambda_0, 1, \mathcal{O}) + N(P)^{m-1} S(\lambda_1, 1, P) = N(P)^m - N(P)^{m-1}$.

(ii) Ha $n = m$, akkor a jobboldali összegben egyedül csak $j = m$-es tag szerepel, tehát azt kell belátnunk, hogy $S(\varphi, \psi, P^m) = S(\lambda_m, \varphi * \psi, P^m)$. Az $n = m$ feltétel miatt vagy $P^{m-1} \nsubseteqq ker\varphi$, vagy $P^{m-1} \nsubseteqq ker\psi$, szimmetria miatt feltehetjük, hogy az előbbi áll fenn. Ekkor a 2.3.5 lemma miatt $(r, P^m) = 1$. Így, a 2.3.1 lemmát felhasználva:

$$S(\varphi, \psi, P^m) = S(r \cdot \lambda_m, r' \cdot \lambda_m, P^m) = S(\lambda_m, rr' \cdot \lambda_m, P^m) = S(\lambda_m, \varphi * \psi, P^m)$$

(iii) Ha $1 \leq n < m$, akkor a 2.3.7 lemma (i) pontja miatt $S(\varphi, \psi, P^m) = N(P)^{m-n} S(\varphi, \psi P^n)$. Belátjuk, hogy ebben az esetben a jobb oldali összeg egy tagból áll, és az éppen a baloldali mennyiséggel egyezik meg; a fentiek alapján ehhez azt kell ltánunk, hogy $S(\lambda_j, \varphi * \psi, P^j) = 0$, ha $j > n$, valamint, hogy $S(\lambda_n, \varphi * \psi, P^n) = S(\varphi, \psi, P^n)$.
Az utóbbi bizonyításához legyen $\varphi_n = r_1 \cdot \lambda_n$, $\psi = r_2 \cdot \lambda_n$. Szimmetria miatt feltehetjük, hogy $N_\varphi = n$, ekkor $(r_1, P) = 1$ a 2.3.5 lemma miatt és így a 2.3.1 lemmát felhasználva: $S(r_1 \cdot \lambda_n, r_2 \cdot \lambda_n, P^n) = S(\lambda_n, r_1 r_2 \cdot \lambda_n, P^n) = S(\lambda_n, \varphi * \psi, P^n)$.
A másik állítás igazolásához legyen j olyan, amire $n < j < m$. $P^j \subsetneqq P^n \subsetneqq ker\varphi \cap ker\psi$, legyenek r_1, r_1' olyan $\mathcal{O}/P^j$-beli elemek, amikre $\varphi = r_1 \cdot \lambda_n$ és $\psi = r_1' \cdot \lambda_n$. Így n definíciója miatt $P^{j-1} \subsetneqq ker r_1 \cdot \lambda_j$. A 2.3.5 lemma miatt így ezek alapján P osztja az (r_1) ideált, és így $P^{j-1} | ker(r_1 r_1' \lambda_j)$. Tehát $N_{\varphi*\psi} < j$, és azt tudjuk, hogy $N_{\lambda_j} = j$, és mivel $j \geq 2$, így a 2.3.7 lemma (ii) pontját felhasználva kapjuk, hogy $S(\lambda_j, \varphi * \psi, P^j) = 0$.

□

Ennek ismeretében már rátérhetünk a fő tétel bizonyítására.

2.4.2. Tétel. *Legyen I nemnulla ideál $\mathcal{O}$-ban és $\varphi, \psi \in \widehat{\mathcal{O}/I}$. Ekkor*

$$S(\varphi, \psi, I) = N(I) \sum_{\substack{J|I \\ J \subsetneqq ker\varphi \cap ker\psi}} N(J)^{-1} S(\lambda_J, \varphi * \psi, J)$$

Bizonyítás. Ha I egy prímideál hatványa, akkor az előző állítás értelmében készen vagyunk. Az I prímfelbontásában szereplő különböző prímfaktorok szerinti teljes indukcióval bizonyítunk, így elég azt belátnunk, hogy ha A, B relatív prím ideálok, amikre teljesül a tétel állítása, akkor $I = AB$-re is teljesül.

A már többször használt kínai maradéktételes állítás értelmében ekkor $\mathcal{O}/I \cong \mathcal{O}/A \times \mathcal{O}/B$, és φ, ψ-t felírhatjuk $\varphi = \varphi_1 \times \varphi_2$, $\psi = \psi_1 \times \psi_2$ alakban, ahol φ_1, $\psi_1 \in \widehat{\mathcal{O}/A}$ és φ_2, $\psi_2 \in \widehat{\mathcal{O}/B}$.

A 2.2.5 állítás miatt, ha λ_A generátora $\widehat{\mathcal{O}/A}$-nak, λ_B generátora $\widehat{\mathcal{O}/B}$-nek, akkor $\lambda_I = \lambda_A \times \lambda_B$ generátora $\widehat{\mathcal{O}/I}$-nek.Továbbá, az ezek által generált gyűrűstruktúrákra teljesül, hogy $\varphi * \psi = (\varphi_1 * \psi_1) \times (\varphi_2 * \psi_2)$, hiszen $\varphi = r \cdot \lambda_I = r \cdot \lambda_A \times r \cdot \lambda_B$ és $\psi = r' \cdot \lambda_I = r' \cdot \lambda_A \times r' \cdot \lambda_B$. Mivel feltettük ,hogy a tétel igaz A-ra és B-re, így teljesül a következő két egyenlőség:

$$S(\varphi_1, \psi_1, A) = N(A) \sum_{\substack{J_1 | A \\ J_1 \subseteqq ker\varphi_1 \cap \psi_1}} N(J_1)^{-1} S(\lambda_{J_1}, \varphi_1 * \psi_1, J_1)$$

$$S(\varphi_2, \psi_2, B) = N(B) \sum_{\substack{J_2 | B \\ J_2 \subseteqq ker\varphi_2 \cap \psi_2}} N(J_2)^{-1} S(\lambda_{J_2}, \varphi_2 * \psi_2, J_2)$$

A 2.3.3 lemmát és a norma multiplikativitását felhasználva, ezeket összeszorozva:

$$S(\varphi, \psi, I) = N(I) \sum_{\substack{J_1 | A \\ J_1 \subseteqq ker\varphi_1 \cap \psi_1}} \sum_{\substack{J_2 | B \\ J_2 \subseteqq ker\varphi_2 \cap \psi_2}} N(J_1 J_2)^{-1} S(\lambda_{J_1}, \varphi_1 * \psi_1, J_1) S(\lambda_{J_2}, \varphi_2 * \psi_2, J_2)$$

Ismét felhasználva a 2.3.3 lemmát, valamint a generátorokra vonatkozó fenti megjegyzéseinket:

$$S(\varphi, \psi, I) = N(I) \sum_{\substack{J_1 | A \\ J_1 \subseteqq ker\varphi_1 \cap \psi_1}} \sum_{\substack{J_2 | B \\ J_2 \subseteqq ker\varphi_2 \cap \psi_2}} N(J_1 J_2)^{-1} S(\lambda_{J_1 J_2}, \varphi * \psi, J_1 J_2)$$

I-nek minden J osztója $J = J_1 J_2$ alakú, ahol J_1 osztója A-nak és J_2 osztója B-nek, és minden ilyen alakú J osztója is I-nek, ez könnyen következik a prímfaktorizáció tulajdonságaiból. Emellett még az is igaz, hogy $J \subseteqq ker\varphi$ akkor és csak akkor, ha $J_1 \subseteqq ker\varphi_1$ és $J_2 \subseteqq ker\varphi_2$.

Valóban, ha $J \subseteqq ker\varphi$ és $x_1 \in J_1$, akkor a kínai maradéktétel miatt létezik olyan $x \in \mathcal{O}$, amire $x \equiv x_1 \pmod{A}$ és $x \equiv 0 \pmod{B}$. Ekkor $\varphi(x) = \varphi_1(x_1)$ és $\varphi_2(x) = 1$. Mivel $x \in J_1 \cap B = J_1 B \subseteqq J$, ezért $1 = \varphi(x) = \varphi_1(x_1)$, tehát $x_1 \in ker\varphi_1$, és ugyanígy kijön $x_2 \in ker\varphi_2$.

Megfordítva, ha $J_1 \subseteqq ker\varphi_1$ és $J_2 \subseteqq ker\varphi_2$, akkor bármely $x \in J$-re $\varphi(x) = \varphi_1(x_1)\varphi_2(x_2) = 1$, hiszen $J \subseteqq J_1 \cap J_2$.

Ezt felhasználva, a fenti egyenlőséget a következő alakra írhatjuk:

$$S(\varphi, \psi, I) = N(I) \sum_{\substack{J|I \\ J \subseteqq ker\varphi \cap ker\psi}} N(J)^{-1} S(\lambda_J, \varphi * \psi, J)$$

és éppen ezt a formulát akartuk belátni. $\square$

3. fejezet

Kapcsolat a moduláris formákkal

A Kloosterman-összegeknek a moduláris formák elméletében van jelentőségük, ezt fogjuk az elkövetkező fejezetben részletesebben megvizsgálni. Ehhez bevezetjük a moduláris formákat, majd rátérünk a Poincaré-sorokra.

3.1. Moduláris formák

Az ebben a részben levő állítások megtalálhatóak például a [3] könyvben. Jelölje $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$ a komplex felső félsíkot,

$$SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, ad-bc = 1 \right\}$$

pedig a 2×2-es, egész elemű, 1 determinánsú mátrixok csoportját a szorzásra nézve. $SL(2,\mathbb{Z})$ hat $\mathbb{H}$-n a következő módon (ezután élünk azzal a jelöléssel, hogy $\gamma \in SL(2,\mathbb{Z})$ esetén γ elemei rendre a,b,c,d):

$$\gamma z = \frac{az+b}{cz+d}$$

Ez $\mathbb{H}$-t valóban önmagára képezi, hiszen $z = x + iy$-t írva

$$\gamma z = \frac{az+b}{cz+d} = \frac{(az+b)\left(\overline{cz+d}\right)}{|cz+d|^2} = \frac{(ax+b+ayi)(cx+d-cyi)}{|cz+d|^2}$$

és ezért

$$Im(\gamma z) = \frac{-acxy - bcy + acxy + ady}{|cz+d|^2} = \frac{(ad-bc)y}{|cz+d|^2} = \frac{y}{|cz+d|^2} = \frac{Im(z)}{|cz+d|^2}$$

tehát ha $Im(z) > 0$, akkor $Im(\gamma z) > 0$.

Azt is gyorsan kiszámolhatjuk, hogy ez valóban csoporthatás. Az egységelem triviálisan hat, hiszen $Iz = \frac{1\cdot z+0}{0\cdot z+1} = z$ minden $z \in \mathbb{H}$-ra. Ha pedig $\gamma_1, \gamma_2 \in \Gamma$, és γ_1, γ_2 elemeit értelemszerűen indexeljük, akkor

$$\gamma_1(\gamma_2 z) = \frac{a_1 \frac{a_2 z+b_2}{c_2 z+d_2} + b_1}{c_1 \frac{a_2 z+b_2}{c_2 z+d_2} + d_1} = \frac{a_1 a_2 z + a_1 b_2 + c_2 b_1 z + d_2 b_1}{c_1 a_2 z + c_1 b_2 + d_1 c_2 z + d_1 d_2} =$$

$$= \frac{(a_1 a_2 + b_1 c_2)\, z + a_1 b_2 + b_1 d_2}{(a_2 c_1 + c_2 d_1)\, z + b_2 c_1 + d_1 d_2} = \gamma_1 \gamma_2(z)$$

Nézzük meg, hogy ennek a hatásnak mi a magja! Ha $\gamma z = z$ minden $z \in \mathbb{H}$-ra, akkor az azt jelenti, hogy $\frac{az+b}{cz+d} = z$, vagyis átszorozva és 0-ra rendezve $cz^2 + (d-a)z - b = 0$ minden $z \in \mathbb{H}$-ra. Mivel $\mathbb{H}$-nak végtelen sok eleme van, egy numnulla polinomnak pedig csak véges sok gyöke, így ennek a polinomnak az azonosan nulla polinamnak kell lennie, tehát az együtthatói nullák, vagyis $c = b = 0$ és $a = d$, de akkor, mivel a determináns 1, $a = d = \pm 1$ adódik. Azt kaptuk tehát, hogy a hatás magja I-ből és $-I$-ből áll. Kifaktorizálva ezzel, a hatás hű lesz.

3.1.1. Definíció. $\Gamma = PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\{I, -I\}$ *a moduláris csoport.*

Ennek ismeretében már definiálhatjuk a moduláris formákat:

3.1.2. Definíció. *Legyen k pozitív egész. Az $f : \mathbb{H} \to \mathbb{C}$ függvényt k súlyú moduláris formának nevezzük, ha*

(i) f *holomorf*

(ii) $f(\gamma z) = (cz+d)^k f(z)\ \forall\ \gamma \in \Gamma$

(iii) f *holomorf* $i\infty$*-ben*

Legyen $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ és $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Ezek könnyen láthatóan Γ-beli elemek, és ezekre felírva a (ii) feltételt a moduláris formákra, a következők adódnak:
$f(z+1) = f(z)$ és $f\left(-\frac{1}{z}\right) = z^k f(z)$.

Valójában az előbbi két egyenlet teljesülése már garantálja a (ii) tulajdonságot, mert most belátjuk, hogy S és T generálják Γ-t. Mátrixszorzással adódnak, hogy

$$T^k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+kc & b+kc \\ c & d \end{pmatrix}$$

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

Ezek alapján látható, hogy ha adott $\gamma \in \Gamma$, akkor S-sel és T-vel való balszorzásokkal tudjuk futtatni az euklideszi algoritmust a-n és c-n, amik relatív prímek (hiszen a determináns 1), így az euklideszi algoritmus végessége miatt véges sok szorzás után elérünk egy olyan mátrixhoz, ahol a bal felső sarokban 1, bal alsó sarokban 0 áll, és mivel a determináns 1, így a jobb alsó sarokban is 1 áll. De ez ekkor egy T^n alakú mátrix lesz éppen, és mivel Γ-ban minden mátrix invertálható, a megfelelő inverzekkel beszorozva kapjuk a γ előállítását T-k és S-ek szorzataként.

Vizsgáljuk még meg azt, hogy mit jelent a (iii) feltétel. Az előbbiek szerint $f(z+1) = f(z)$, ezért f Fourier-sorba-fejthető: léteznek c_n komplex együtthatók, $n \in \mathbb{Z}$, hogy

$$f(z) = \sum_{n=-\infty}^{\infty} c_n e(nz)$$

A (iii)-ban levő holomorfitási feltétel azt követeli meg, hogy $c_n = 0$ legyen, ha $n < 0$.

3.1.3. Példa. Legyen $k \geq 4$ pozitív egész. Az

$$E_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m+nz)^k}$$

alakú sorokat Eisenstein-soroknak nevezzük.

Belátható, hogy ha $k \geq 4$, akkor $E_k(z)$ minden $z \in \mathbb{H}$ esetén konvergálni fog, és holomorf lesz $\mathbb{H}$-n és $i\infty$-ben is. A (ii) moduláris forma-tulajdonság is teljesülni fog rá ekkor, mert

$$E_k\left(\frac{az+b}{cz+d}\right) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\frac{az+b}{cz+d})^k} = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{(cz+d)^k}{(m(cz+d)+n(az+b))^k} =$$

$$= (cz+d)^k \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{((mc+na)z+(md+nb))^k} =$$

$$= (cz+d)^k \sum_{\substack{(m',n')\in\mathbb{Z}^2 \\ (m',n')\neq(0,0)}} \frac{1}{(m'+n'z)^k} = (cz+d)^k E_k(z)$$

Az utolsó egyenlőség abból ered, hogy könnyen ellenőrizhetően minden $(m', n') \neq (0, 0)$ számpárt megkaphatunk egyértelműen $(mc+na, md+nb)$ alakban. Így tehát $E_k(z)$ egy k súlyú moduláris forma lesz, ha $k \geq 4$.

Vegyük észre, hogy páratlan k esetén E_k azonosan 0. Ez egy általánosabb tétel következménye: páratlan k esetén az azonosan 0 függvény az egyetlen k súlyú moduláris forma. Páros k esetén viszont nem triviális moduláris formát ad a konstrukció.

3.2. Poincaré-sorok

Az Eisentein-sorok után most egy másik konstrukciót adunk moduláris formákra, aminél természetes módon megjelennek majd a Kloosterman-összegek. A [6] jegyzetben levő gondolatmenetet fogjuk követni. A konstrukció során először az $f(\gamma z) = (cz+d)^k f(z) \forall \gamma \in \Gamma$ feltételt szeretnénk biztosítani. Ehhez először általánosabb formában fogalmazzuk meg ezt a feltételt.

3.2.1. Definíció. *Egy $j : \Gamma \times \mathbb{H} \to \mathbb{C}^\times$ függvényt automorfitási tényezőnek hívunk, ha minden $\alpha, \beta, \gamma \in \Gamma$ esetén j_γ holomorf $\mathbb{H}$-n és $j_{\alpha\beta}(z) = j_\alpha(\beta z) j_\beta(z)$.*

Így a fenti feltételt úgy általánosíthatjuk, hogy $f(\gamma z) = j_\gamma(z) f(z)$ $\forall \gamma \in \Gamma$ valamilyen j automorfitási tényezőre. Az ötlet a konstrukcióhoz az, hogy ezt a tulajdonságot úgy biztosítjuk, hogy egy megfelelő függvényt átlagolunk Γ elemein. Például, ha $j \equiv 1$, akkor

$$f(z) = \sum_{\alpha \in \Gamma} h(\alpha z)$$

alakú függvény teljesítené a feltételt (hiszen Γ csoport), ha h olyan függvény, amire megfelelő konvergenciafeltételek teljesülnek. Ennek nyomán az általános esetben is hasonló alakban keressük, csak a h-t is $\Gamma \times \mathbb{H} \to \mathbb{C}^\times$ függvényként képzeljük el. Így tehát f-et most formálisan

$$f(z) = \sum_{\alpha \in \Gamma} h_\alpha(z)$$

alakban keressük. Erre az $f(\gamma z) = j_\gamma(z) f(z)$ feltételt így írhatjuk át:

$$\sum_{\alpha \in \Gamma} h_\alpha(\gamma z) = \sum_{\alpha \in \Gamma} j_\gamma(z) h_\alpha(z) = \sum_{\alpha \in \Gamma} j_\gamma(z) h_{\alpha\gamma}(z)$$

minden $\gamma \in \Gamma$ esetén. h-t úgy fogjuk keresni, hogy fent a két oldalon álló összeg tagonként is egyenlő legyen, vagyis $h_\alpha(\gamma z) = j_\gamma(z) h_{\alpha\gamma}(z)$ teljesüljön minden $\alpha, \gamma \in \Gamma$ esetén.

Ha itt $\alpha = 1$-et helyettesítünk, akkor rendezés után azt kapjuk, hogy $h_\gamma(z) = \frac{h_1(\gamma z)}{j_\gamma(z)}$. Az is kiderül, hogy ha h ezt teljesíti, akkor már minden más α-ra is megfelelő lesz, hiszen használva j tulajdonságát:

$$h_\alpha(\gamma z) = \frac{h_1(\alpha\gamma z)}{j_\alpha(\gamma z)} = j_\gamma(z)\frac{h_1(\alpha\gamma z)}{j_{\alpha\gamma}(z)} = j_\gamma(z) h_{\alpha\gamma}(z)$$

Így tehát, a $h = h_1$ egyszerűsítő jelöléssel élve, a következő konstrukcióhoz jutottunk:

$$f(z) = \sum_{\gamma\in\Gamma} \frac{h(\gamma z)}{j_\gamma(z)}$$

Ha h holomorf függvény, és a fenti sor egyenletesen konvergál, akkor ez az f holomorf lesz és teljesülni fog rá $f(\gamma z) = j_\gamma(z) f(z)\ \forall \gamma \in \Gamma$.

Sajnos kiderül, hogy ilyen h keresése nem megvalósítható a számunkra érdekes esetekben. A fő problémát az okozza, hogy végtelen sok olyan γ van, amire $j_\gamma \equiv 1$. Szerencsére azonban ezen tudunk segíteni, ugyanis nyilvánvalóan a kérdéses γ-k egy részcsoportját alkotják Γ-nak:

$$\Gamma_\infty = \{\gamma \in \Gamma | j_\gamma \equiv 1\}$$

Innen a következő lépésünk az, hogy a konstrukciónál nem egész Γ-n összegzünk, hanem a Γ_∞ szerinti mellékosztályain. Ehhez feltesszük, hogy h olyan függvény, ami Γ_∞-invariáns (vagyis $\gamma \in \Gamma_\infty$ esetén $h(\gamma z) = h(z)$). Ahhoz, hogy Γ_∞ szerinti mellékosztályokon összegezhessünk, azt kell megmutatnunk, hogy $\frac{h(\gamma z)}{j_\gamma(z)}$ csak a γ Γ_∞ szerinti mellékosztályától függ.Ez viszont adódik abból, hogy külön-külön a nevező és a számláló is csak a mellékosztálytól függ, hiszen ha $\gamma = \beta\gamma'$ valamilyen $\beta \in \Gamma_\infty$-re, akkor $h(\gamma z) = h(\beta\gamma' z) = h(\gamma' z)$, valamint $j_\gamma(z) = j_{\beta\gamma'}(z) = j_\beta(\gamma' z) j_{\gamma'}(z) = j_{\gamma'}(z)$.

Mindezek alapján a következő lett tehát a konstrukciónk (itt és a továbbiakban Γ_∞/Γ a Γ_∞ szerinti bal mellékosztályokat jelöli Γ-ban, ha ennek elemeire összegzünk, azt úgy értjük, hogy mindegyik mellékosztályból egy reprezentánselemet választunk):

$$f(z) = \sum_{\gamma\in\Gamma_\infty/\Gamma} \frac{h(\gamma z)}{j_\gamma(z)}$$

Most ezt ültessük át a moduláris formák esetére, tehát $j_\gamma(z) = (cz + d)^k$. Γ_∞ éppen ezekből a mátrixokból fog állni, aminek az alsó sorában 0 és 1 áll. (vagy 0 és -1, de mivel

$PSL(2,\mathbb{Z})$-ben vagyunk, ezért feltehetjük, hogy 0 és 1). Így, mivel a mátrixok determinánsainak 1-nek kell lennie, azt kapjuk, hogy $\Gamma_\infty = \{T^n | n \in \mathbb{Z}\}$. Ezért a Γ_∞-invariáns függvények éppen az 1-periodikus függvények. Ilyenekre kézenfekvő példa $h(z) = e(mz)$, és ez lesz a mi választásunk h-ra.

A konstrukcióbeli összeg jobb megértéséhez karakterizáljuk a Γ_∞ szerinti mellékosztályokat. Ha $\alpha, \beta \in \Gamma$, akkor $\alpha = T^n\beta$ valamilyen $n \in \mathbb{Z}$-re pontosan akkor, ha az alsó soraik megegyeznek, ezt láttuk akkor, amikor kiszámoltuk $T^k\gamma$ pontos alakját. Viszont ha adott egy Γ-beli elem alsó sora, ami álljon c-ből és d-ből, akkor c-nek és d-nek relatív prímnek kell lennie, hiszen a determináns 1. Másrészt, ha c és d relatív prím egészek, akkor létezik olyan Γ-beli elem, aminek az alsó sora éppen (c,d). Így mindezt összerakva, a következőt kaptuk:

$$\Gamma_\infty/\Gamma \cong \{(c,d) | c \geq 0, gcd(c,d) = 1\}$$

(A $c \geq 0$ feltétel azért kell, hogy ne válasszuk ki egy elem két reprezentánsát is). Mindezek után mostmár definiálhatjuk a Poincaré-sorokat:

3.2.2. Definíció.

$$P_m^k(z) = \sum_{\gamma \in \Gamma_\infty/\Gamma} \frac{e(m\gamma z)}{j_\gamma(z)} = \sum_{c \geq 0, (c,d)=1} \frac{e(m\gamma z)}{(cz+d)^k}$$

az m-edik k súlyú Poincaré-sor.

Itt a c-hez és d-hez egy olyan γ tartozik, hogy $ad - bc = 1$ legyen. Ha $(c,d) = 1$, akkor $e(m\gamma z)$ nem függ a és b választásától (azaz a Poincaré-sorok jóldefiniáltak). Ezt úgy láthatjuk be, hogy ha $c = 0$, akor $d = 1$ és az állításunk adódik az $e(\cdot)$ függvény 1-periodicitásából (hasonlóan kijön $d = 0$ eset is). Ha $c, d \neq 0$, és $a, a', b, b' \in \mathbb{Z}$ úgy, hogy $ad - bc = 1$ és $a'd - b'c = 1$ akkor kivonva egymásból a két egyenletet és rendezve $(a - a')d = (b - b')c$ adódik. Innen $(c,d) = 1$ miatt $c|a - a'$ és $d|b - b'$, leosztva c-vel és d-vel: $\frac{a-a'}{c} = \frac{b-b'}{d} = k$ valamilyen k egész számra. Így tehát

$$\frac{az+b}{cz+d} - \frac{a'z+b'z}{cz+d} = \frac{(a-a')\,z + b - b'}{cz+d} = \frac{kcz+kd}{cz+d} = k$$

és az állításunk ismét adódik az $e(\cdot)$ függvény 1-periodicitásából.

3.2.3. Tétel. *Ha $k, m \in \mathbb{N}$, $m \geq 0$ és $k > 2$, akkor P_m^k egy k súlyú moduláris forma.*

A tételt most nem bizonyítjuk, csak megjegyezzük, hogy a feltételek egyenletes és abszolút konvergenciát biztosítanak $\mathbb{H}$ kompakt részhalmazain, mert a P_m^k majorálható

E_k-val, és ennek alapján belátható mindhárom szükséges tulajdonság. A bizonyítás megtalálható például a [9] könyvben.

Ahogyan korábban is említettük, a moduláris formák 1-periodikusak, így Fourier-sorba fejthetők. P_m^k Fourier-sorfejtésénél pedig megjelennek a Kloosterman-összegek, így ezen a ponton kapcsolódik össze az exponenciális összegek és a moduláris formák elmélete. A következőekben ezt fogjuk kiszámolni.

3.2.4. Állítás. *Legyen $k, m \in \mathbb{N}$, $n \in \mathbb{Z}$, $n \neq 0$, $m > 0$, $k > 2$, és jelölje a_n P_m^k n-edik Fourier-együtthatóját. Ekkor*

$$a_n = \delta_{mn} + \sum_{c>0} c^{-k} S(m,n,c) \int_{-\infty+iy}^{\infty+iy} z^{-k} e\left(-\frac{m}{c^2 z} - nz\right) dz$$

ahol δ_{mn} a Kronecker-deltát jelöli.

Bizonyítás. Definíció szerint az a_n Fourier-együttható:

$$a_n = \int_{0+iy}^{1+iy} P_m^k(z) e(-nz) dz = \sum_{c\geq 0,(c,d)=1} \int_{0+iy}^{1+iy} \frac{e(m\gamma z)}{j_\gamma(z)} e(-nz) dz$$

Vegyük észre, hogy ha $c > 0$ és $(c,d) = 1$, akkor létezik $l \in \mathbb{Z}$ és $0 \leq d' < c$, amire $(c,d') = 1$, amire $d = lc + d'$. Ezzel a formulával meg is kapunk minden c-hez relatív prím d-t. Így a $c = 0$-s tagot leválasztva az összegről, a maradékot pedig az előbbiek szerint továbbfejtve:

$$a_n = \int_{0+iy}^{1+iy} e((m-n)z) dz + \sum_{\substack{c>0 \\ 0\leq d'<c \\ (c,d')=1}} \sum_{\substack{l\in\mathbb{Z} \\ d=lc'+d}} \int_{0+iy}^{1+iy} \frac{e(m\gamma z)}{j_\gamma(z)} e(-nz) dz$$

Az első tagból kapjuk δ_{nm}-et, a második tagnál pedig vegyük észre, hogy $j_{\gamma_d}(z) = (cz+d)^k = (c(z+l)+d')^k = j_{\gamma'_d}(z+l)$, ahol γ_d-vel olyan Γ-beli mátrixot jelölünk, aminek jobb alsó eleme d. Továbbá $\gamma z = \frac{az+b}{cz+d} = \frac{a}{c} - \frac{1}{c(cz+d)}$. így $\gamma_d z = \gamma_{d'}(z+l)$
Ezeket beírva és a $z + l \mapsto z$ változócserét alkalmazva:

$$a_n = \delta_{mn} + \sum_{\substack{c>0 \\ 0\leq d<c \\ (c,d)=1}} \sum_{l\in\mathbb{Z}} \int_{l+iy}^{l+1+iy} \frac{e(m\gamma z)}{j_\gamma(z)} e(-nz) dz = \delta_{mn} + \sum_{\substack{c>0 \\ 0\leq d<c \\ (c,d)=1}} \int_{-\infty+iy}^{\infty+iy} \frac{e(m\gamma z)}{j_\gamma(z)} e(-nz) dz$$

Vegyük észre, hogy $c > 0$-ra $j_\gamma(z) = (cz+d)^k = c^k(z+\frac{d}{c})^k$ és $\gamma z = \frac{a}{c} - \frac{1}{c^2\left(z+\frac{d}{c}\right)}$. Így a $z + \frac{d}{c} \mapsto z$ változócserével:

$$\delta_{mn} + \sum_{\substack{c>0 \\ 0\le d<c \\ (c,d)=1}} \int_{-\infty+iy}^{\infty+iy} c^{-k} z^{-k} e\left(\frac{ma}{c}\right) e\left(-\frac{m}{c^2 z}\right) e\left(-n\left(z-\frac{d}{c}\right)\right) dz =$$

$$= \delta_{mn} + \sum_{c>0} c^{-k} S(m,n,c) \int_{-\infty+iy}^{\infty+iy} z^{-k} e\left(-\frac{m}{c^2 z} - nz\right) dz$$

□

3.2.5. Megjegyzés. Az integrálos tagot Bessel-függvények segítségével jobban kezelhető formában is fel lehet írni. Ehhez alapvető komplex függvénytani eszközöket fogunk használni, amik megtalálhatóak például a [10] könyvben. Írjuk fel ugyanis $e\left(-\frac{m}{c^2 z}\right)$ Laurent-sorfejtését!

$$e\left(-\frac{m}{c^2 z}\right) = \sum_{l=0}^{\infty} (-1)^l \frac{(2\pi i m)^l}{c^{2l} z^l l!}$$

Az integrálban levő többi taggal is beszorozva az integráljel mögött egy konvergens numerikus sorral majorolható sort kapunk, így Weierstrass-kritérium szerint egyenletes konvergencia van, ezért az integrált és a szummát felcserélhetjük. Így tehát

$$\int_{-\infty+iy}^{\infty+iy} z^{-k} e\left(-\frac{m}{c^2 z} - nz\right) dz = \int_{-\infty+iy}^{\infty+iy} \sum_{l=0}^{\infty} (-1)^l \frac{(2\pi i m)^l}{c^{2l} z^{l+k} l!} e\left(-nz\right) dz =$$

$$= \sum_{l=0}^{\infty} \int_{-\infty+iy}^{\infty+iy} (-1)^l \frac{(2\pi i m)^l}{c^{2l} z^{l+k} l!} e\left(-nz\right) dz$$

Ha $z = x + iy$, akkor $|e(-nz)| = |e^{2\pi i(-nz)}| = |e^{2\pi i - nzx + 2\pi ny}| = e^{2\pi ny}$. Most $y > 0$.

Legyen először $n < 0$. Vegyünk egy integrált a szummán belülről! Ha $y_1 > 0$, akkor integrálhatunk y_1 magasságban is y magasság helyett, mert a felső félsíkon holomorf az integrálon belüli függvény, így ha veszünk egy téglalapot, aminek vízszintes oldalai y, illetve y_1 magasságban vannak (rögzítettek), akkor az integrál azon 0 lesz. A függőleges oldalakkal tartunk a végtelenhez, és azokon az integrál nullához fog tartani az $e(-nz)$-s tényező miatt. Vagyis, ha $I(t)$ jelöli t magasságban az integrál értékét, akkor ezzel azt láttuk be, hogy $y_1 > 0$ esetén $I(y) = I(y_1)$. De ha y_1-gyel tartunk végtelenhez, akkor $I(y_1)$ nullához fog tartani, hiszen $e(-nz)$ fog dominálni, és az előbb kiszámolt abszolútérték szerint, mivel n negatív, ez 0-hoz fog tartani. De mivel az integrál értéke konstans, így az eredeti integrálnak is 0-nak kell lennie, tehát $a_n = 0$, ha $n < 0$.

Most legyen $n > 0$. Ekkor nem tudjuk felfelé tolni az integrált, mert így végtelenhez tartana. Ezért negatív irányba fogjuk tolni, hiszen úgy 0-hoz fog tartani az értéke az előbbiekhez hasonlóan. A probléma ezzel az, hogy azon a tartományon, ahol mozgatni akarunk, a függvény nem lesz holomorf: $z = 0$-ban szingularitása van. Ezért a reziduumot hozzá kell adni az alsó félsíkra való lecsúsztatáskor a reziduum-tételt alkalmazva, majd az alsó félsíkon alkalmazhatjuk az előző gondolatmenetet, tehát ott az integrál értéke 0 lesz. Így az eredeti integrálunk értéke éppen a $z = 0$-beli reziduum, amit most kiszámolunk. A reziduum a Laurent-sor -1-es taghoz tartozó együtthatója, így a $(-1)^l \frac{(2\pi im)^l}{c^{2l} z^{l+k} l!} e(-nz)$ függvénynél $e(-nz)$-t kell sorba fejteni, és annak kell nézni az $l+k-1$-edik együtthatóját, és azt beszorozni a megfelelő konstanssal. Így tehát

$$\operatorname*{Res}_{z=0} (-1)^l \frac{(2\pi im)^l}{c^{2l} z^{l+k} l!} e(-nz) = (-1)^l \frac{(2\pi im)^l}{c^{2l} l!} \cdot \frac{(-2\pi in)^{k+l-1}}{(k+l-1)!} =$$

$$= (-1)^{k+l-1} \frac{(2\pi)^{k+2l-1} m^l n^{k+l-1} i^{k-1}}{c^{2l} l! (k+l-1)!}$$

Így ezeket beírva az összegbe, az integrál értékére a következőt kapjuk:

$$\int_{-\infty+iy}^{\infty+iy} z^{-k} e\left(-\frac{m}{c^2 z} - nz\right) dz = \sum_{l=0}^{\infty} (-1)^{k+l-1} \frac{(2\pi)^{k+2l-1} m^l n^{k+l-1} i^{k-1}}{c^{2l} l! (k+l-1)!} =$$

$$= (-1)^{k-1} i^{k-1} \left(\frac{n}{m}\right)^{\frac{k-1}{2}} c^{k-1} \sum_{l=0}^{\infty} \frac{(-1)^l}{l!(l+k-1)!} \left(\frac{2\pi\sqrt{nm}}{c}\right)^{2l+k-1} =$$

$$= (-i)^{k-1} \left(\frac{n}{m}\right)^{\frac{k-1}{2}} c^{k-1} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right)$$

ahol J_{k-1} a $(k-1)$-edik Bessel-függvényt jelöli. (Bessel-függvények: https://dlmf.nist.gov/10.2)

Láttuk tehát, hogy a klasszikus Kloosterman-összegek megjelennek a moduláris formák kapcsán. Hasonló módon jelennek meg az algebrai számtestek feletti Kloosterman-összegek is, csak olyankor nem a szokásos moduláris formákat vizsgáljuk, hanem hasonló tulajdonságú függvényeket, amiknél Γ szerepét $PSL(2, \mathcal{O})$ veszi át, ahol $\mathcal{O}$ az egészek gyűrűje $\mathbb{Q}$ egy véges bővítésében.

Irodalomjegyzék

[1] I. PACHARONI. *Kloosterman sums on number fields.* Communications in Algebra, 26:8, 2653-2667 (1998)

[2] E. KOWALSKI. *Exponential sums over finite fields, I: elementary methods.* https://people.math.ethz.ch/ kowalski/exp-sums.pdf

[3] J.-P. SERRE. *A course in arithmetic.* Springer, 1973.

[4] A. WEIL. *On some exponential sums.* Proceedings of the National Academy of Sciences of the United States of America, Volume 34, Issue 5, pp. 204-207 (1948)

[5] G. ZÁBRÁDI. *Algebrai számelmélet jegyzet.* http://zabradi.web.elte.hu/Jegyzetek/algszamjegyzet.pdf

[6] J. LEIS. *The Poincaré series.* http://www2.math.ethz.ch/education/bachelor/seminars/ws0607/modular-forms/THE_POINCARE_SERIES.pdf

[7] H. D. KLOOSTERMAN. *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. Acta Mathematica 49, 407-464 (1926)

[8] H. POINCARÉ. *Fonctions modulaires et fonctions fuchsiennes.* Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3), 3:125–149 (1911)

[9] H. IWANIEC. *Topics in classical automorphic forms.* Springer, 1997

[10] GY. PETRUSKA. *Komple függvénytan.* Nemzeti Tankönyvkiadó, 1998