Probleme actuale în studiul funcţiei zeta Igusa

Denis Ibadula[1]

[1]This paper is supported by the Sectorial Operational Programme Human Resources Development (SOP HRD), financed from the European Social Fund and by the Romanian Government under the contract number SOP HRD/89/1.5/S/62988. 2010 *Mathematics Subject Classification.* 11D79 11S80 14B05 14E15

Key words. Funcţia zeta Igusa p-adică; designuri eşalon

Cuprins

Capitolul 1

Rezumatul lucrării în limba română

1.1 Prezentare generală a rezultatelor obţinute în cadrul proiectului

Funcţiile zeta locale sunt obiecte matematice relativ noi. Primele teoreme cu caracter general au fost demonstrate între anii 1968-1973. De atunci, şi în special în ultimii 20 ani, au fost obţinute rezultate remarcabile pe această temă.

Pentru un număr prim p, notăm cu $\mathbb{Q}_p$ corpul numerelor p-adice şi cu $\mathbb{Z}_p$ inelul întregilor p-adici.

Funcţia zeta Igusa locală asociată unui polinom $F(x) = F(x_1, \cdots, x_n) \in \mathbb{Z}p[x_1, \cdots, x_n]$ se defineşte ca fiind $Z_F(s) = \int |F(x)|^s |dx|$, integrala dupa x în $(\mathbb{Z}_p)^n$, pentru s număr complex, cu $\Re(s) > 0$, unde cu $|dx|$ am notat măsura Haar pe $(\mathbb{Q}_p)^n$ normalizată astfel încât $(\mathbb{Z}_p)^n$ are masura 1, iar $|x| = p^{-v(x)}$, unde $v(x)$ a p-adică a lui x.

Proprietăţi profunde ale unor obiecte matematice (corpuri de numere algebrice, varietăţi algebrice, algebre, grupuri, etc) sunt codificate de anumite funcţii analitice şi serii formale specifice (funcţii zeta, serii Hilbert, serii Poincaré). Studiul unor astfel de funcţii constituie o temă de mare actualitate a Matematicii contemporane şi datorită aplicaţiilor acestora în studiul diverselor modele din economie. Menţionăm că în ultimii ani problematica legată de funcţia zeta Igusa şi seriile Poincaré asociate unei varietăţi algebrice (analitice) definite peste un corp de numere p-adice a cunoscut o puternică dezvoltare (Igusa, Denef, Veys, Zuniga-Galindo, Segers). Aflat la graniţa dintre teoria numerelor şi geometria algebrică, cu aplicaţii în studiul diverselor probleme din economie, studiul funcţiei zeta Igusa are un caracter interdisciplinar.

In anii '80 fizicienii au propus folosirea numerelor p-adice în anumite modelări ale unor fenomene fizice, iar recent la acestea s-au adaugat modele economice, financiare si cele din data-mining care utilizeaza intens numerele p-adice. Mai mult, funcţiile zeta locale sunt folosite în studiul ecuaţiilor pseudo-diferenţiale de tip parabolic care au aplicaţii în economie şi finante. Wilson Zuniga-Galindo ([Zuniga-Galindo W.A., "Parabolic Equations and Markov Processes over p-adic Fields", Potential Anal.28, (2008), p.185-200]) a demonstrat că soluţia fundamentală (the heat kernel) a unei anumite probleme Cauchy este o densitate de tranziţie a unui proces Markov având spaţiul stărilor $\mathbb{Q}_p^n$(Teorema 4 din articolul mentionat).

Obiectivul general al prezentului proiect de cercetare îl constituie studiul funcţiei zeta Igusa. Având în vedere importanţa funcţiei zeta Igusa în teoria numerelor, aritmetică, geometria algebrică, algebra combinatorială, teoria aranjamentelor de hiperplane, aplicaţiile acesteia în studiul diverselor probleme din aceste domenii, strânsa legatură dintre calculul funcţiei zeta Igusa şi

criprografie la care se adaugă conexiunea între seria Poincaré (şi deci implicit funcţia zeta Igusa) şi cifrurile pe flux, ne-am propus şi am reuşit să extindem rezultatele cunoscute pentru funcţia zeta Igusa locala asociată unei curbe şi să determinăm polii funţiei zeta Igusa pentru curbe. Rezultatele obţinute **au fost *publicate* în două lucrari la reviste din străinătate, *dintre care una ISI*, cu factor de impact mare**:

- Denis Ibadula, Dirk Segers, *"Determination of the real poles of the Igusa zeta functions for curves"*, Revista Matemtica Complutense, vol. 25, no. 2, July 2012, pages 581-597; Impact factor - 0.739;

precum şi în lucrarea

- Denis Ibadula, Dirk Segers, *Convex proofs of some inequalities*, The Mathematical Gazette, November 2012, pages 15-17;

O altă parte importantă a rezultatelor obţinute în această direcţie de cercetare fac parte din lucrarea următoare, **trimisă spre publicare in noiembrie 2011 la o revista ISI foarte bună, în proces de recenzie în momentul actual**:

- Denis Ibadula, Dirk Segers, Edwin Leon Cardenal, *Poles of the Igusa local zeta function of some hybrid polynomials*, Finite Fields and Applications, submitted; Impact factor - 0.674; Scor relativ de influenta - 1,16634

Mai mult, în cadrul acestui proiect am abordat şi o altă direcţie de cercetare în care am studiat designurile eşalon, subiect care aparţine Statisticii matematice. Designul experimentelor este o ramură împortantă a Statisticii care are ca subiect important de studiu designurile full-factorial. În cadrul

acestui proiect ne-am propus şi am reuşit să folosim metode ale Algebrei Comutative pentru a explora probleme relevante (cum ar fi bazele Gröbner, fracţiile, polinomul Hilbert) ale designurilor eşalon, o mulţime $\mathcal{E}$ de puncte experimentale având anumite proprietăţi speciale.

Designurile eşalon generalizează designurile full factorial inverstigate în [CPRW], [CR], [R], [RR]. Pe scurt, contibuţia noastră în acest domeniu constă într-o demonstraţie originală a existenţei unei baze Gröbner pentru un ideal design $\mathcal{I}(\mathcal{E})$. Mai mult, rezultatul nostru generalizează Teorema 2.18 a lui Robbiano [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204]. În plus, am obţinut caracterizarea polinomului Hilbert polynomial asociat unui design eşalon şi am introdus şi studiat fracţii ale designurilor eşalon. Rezultatele din teoremele pe care le-am obţinut extind Teoremele 4.5 şi 5.6 din [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204] de la cazul designurilor full factorial la cazul designurilor eşalon. Rezultatele obţinute au fost **trimise spre publicate la o revistă din străinătate cotată ISI**:

- Denis Ibadula, Corina Birghila, *Echelon Designs and Groebner Bases*, Acta Mathematicae Applicatae Sinica, English Series; Impact factor -0.289 ; Scor relativ de influenta - 0.21795

Vom prezenta în continuare pe scurt **rezumatul rezultatelor obţinute în cele două mari direcţii de cercetare abordate**.

1.2 Prima direcţie de cercetare: Studiul funcţiei zeta Igusa locale si aplicaţii

Funcţiile zeta locale au aparut în matematica ca un instrument de a calcula soluţiile fundamentale ale unor ecuaţii cu derivate partiale cu coeficienţi reali sau complecşi. Mai mult, în studiul acestui tip de ecuaţii anumite integrale oscilatorii joacă un rol central (Teorema 1, [Zuniga-Galindo W.A., "Parabolic Euations and Markov Processes over p-adic Fields", Potential Anal.28, (2008), p.185-200]). Igusa fost cel care a dezvoltat o metoda de estimare a unei largi clase de integrale oscilatorii ([J.-I. Igusa, "Lectures on forms of higher degree", Lectures on mathematics and physics, Tata Institute of Fundamental Research, vol.59, Springer-Verlag, 1978], [J. Igusa, An introduction to the Theory of Local Zeta Functions, AMS, 2002]), iar medodele de lucru recente în domeniu sunt cele folosite de Zuniga-Galindo în lucrarea mai sus mentionată şi au la bază studiul funcţiilor zeta locale pentru polinoame semi-cvasiomogene ([Zuniga-Galindo W.A., "Igusa's Local Zeta Function of semiquasihomogeneous polynomials", Trans.Amer.Math.Soc.353 (2001), p.3193-3207]).

Faptul remarcabil este ca ecuaţiile pseudo-diferentiale p-adice de tip parabolic descriu drumuri aleatoare (random walks) in fractali ($\mathbb{Q}_p$ este un fractal) şi acest tip de ecuaţii stau la baza unor modele matematice noi din finanţe. Studiul acestui tip de ecuaţii foloseşte intens idei şi metode din teoria funcţiilor zeta locale.

Aşa cum am menţionat, există modele în economie, finante şi în data mining care folosesc numerele p-adice. De asemenea, pentru a răspunde la diverse întrebari legate de starea şi dinamica unui ecosistem de afaceri, este important de analizat care este cantitatea de bani pe care o anumită societate

economică o va avea la un moment de timp dat. Dependenţa de momentul de timp ales (sau în general dependenta de viitor) pune în evidenta faptul că este necesara utilizarea unei parametrizari p-adice a timpului. Aceasta abordare este propusă prima data în lucarea [V.S.Vladimirov, I.V.Volovich, E.I.Zelenov, p-Adic Analysis and Mathematical Physics, World Scientific, 2002], unde autorii definesc notiunea de stare a societăţii economice într-un moment de timp dat şi propun folosirea corpurilor de numere p-adice într-o astfel de abordare.

Pentru a modela dinamica ecosistemului de afaceri, este studiată starea unei organizaţii într-un moment dat. Pentru a descrierea acesteia, este necesar sa fie cunoscută probabilitatea plătilor care se fac în cadrul diverselor contracte, lucru care de fapt depinde de comportamentul viitor al agenţilor economici parteneri în aceste contracte pe piaţa. Intervin în acest context metodele de analiza p-adică care se folosesc pentru a studia aceste fenomene.

Pe de alta parte, se asociază ecuaţii diferenţiale p-adice pentru a descrie evoluţia unei societăţi economice. Există o teorie a proceselor stochastice în timp p-adic ([V.S.Vladimirov, I.V.Volovich, E.I.Zelenov, p-Adic Analysis and Mathematical Physics, World Scientific, 2002]) care se folosesc pentru a dezvolta modele Black-Scholes p-adice ([F.Black, M.Scholes, the Pricing of Options and Corporate Liabilities, Journal of Political Economy, 81, 1973, p. 637-654] şi [Jennifer Trelewicz, Igor Volovich, Analysis of Business Connections Utilizing Theory of Topology of Random Graphs, p-adic Mathematical Physiscs, Eds. A.Yu. Khrennikov, Z.Rakic and I.V. Volovich, AIP Conf.Proc.826, pp.330-344, (Melville, New York, 2006)]) care se folosesc pentru a formula din punct de vedere matematic ideea dependenţei de timp a evoluţiei unei societăţi economice folosind corpuri de numere p-adice.

Aşadar, funcţiile zeta locale, în particular funcţia zeta Igusa locală, au

aplicaţii în studiul ecuaţiilor pseudo-diferentiale p-adice, iar astfel de ecuaţii apar în modele fizice, ecomonice şi financiare noi.

Un alt domeniu în care funcţia zeta Igusa are aplicaţii este criptografia, unde una dintre problemele fundamentale este stabilirea existenţei funcţiilor one-way. O functie one-way este o functie F pentru care pentru fiecare x din domeniul de definiţie al lui F, calculul lui $F(x)$ se face în timp polinomial, dar pentru un y dat din codomeniul lui F găsirea unui x astfel incat $y = F(x)$ este, în general, o problema intractabilă. La sfarsitul anilor 90, Anshel şi Goldfeld au propus o nouă clasă de candidaţi pentru funcţii one-way având la bază funcţii zeta ([Anshel, M., and Goldfeld, D., Zeta functions, one-way functions and pseudorandom number generators, Duke Math. J., 88, 2 (1997), 371-390]). De asemenea, seria Poincaré (şi deci implicit funcţia zeta Igusa) are aplicaţii în studiul cifrurilor pe flux bazate pe LFSR-uri, care stau la baza criptografiei cu chei simetrice.

O problemă extrem de actuală de studiu unde am obţinut rezultate în cadrul acestui proiect publicate într-o revista ISI o reprezintă polii funcţiei zeta Igusa. Studiul acestora prezintă un interes special atât pentru faptul că influentează în mod direct numărul de soluţii al congruenţelor polinomiale modulo o putere a unui număr prim p (polii cu partea reală cea mai mare au contribuţia cea mai mare la coeficienţii N_i ai seriei Poincaré) cât şi pentru că sunt subiectul unei importante conjecturi din matematică cunoscută sub numele de Conjectura Monodromiei.

O serie de matematicieni au obţinut rezultate parţiale legate de determinarea polilor reali ai funcţiei zeta Igusa pentru curbe. În acestă cercetare am determinat polii reali pentru un polinom arbirar f în două variabile care este definit peste un corp p-adic. Interesul pentru polii funcţiei zeta Igusa $Z_f(s)$ este justificat pe de o parte de faptul că aceştia determină compor-

tamentul asimptotic al numărului de soluţii al congruenţelor polinomiale, iar pe de alta parte deoarece aceştia sunt subiectul unei renumite conjecturi matematice: conjectura momodromiei (vezi de exemplu [Den91]).

Cronologic, au fost considerate la început curbe absolut analitic ireductibile. Rezultate parţiale au fost obţinute de Igusa [Ig1] şi Strauss [St]. Meuser [Me] a determinat polii reali, dar nu a considerat polul candidat -1. În 1985 Igusa [Ig2] a rezolvat problema complet. El a demonstrat polii candidadti asociaţi unei transformări stricte ale lui f sunt poli cand domeniul de integrare este suficient de mic. Mai mult, un alt pol candidat al unei rezolţii minimale scufundate ale lui f este pol dacă si numai dacă este asociat unei curbe excepţionale care este intersectată de alte trei componente ireductibile ale pull back-ului lui f. Am incorporat o generalizare a acestui rezultat in Propoziţia 5.7.

În cazul general, Loeser [Lo] a demonstrat că o curbă excepţională E_i nu contribuie la polii lui $Z_f(s)$ dacă E_i este intersectat o dată sau de două ori de alte componente ale pull back-ului lui f şi dacă nu sunt alte puncte de intersecţie peste o închidere algebrică. Acest lucru a fost demonstrat pentru prima dată de Strauss in cazul absolut analitic ireductibil, caz în care ultima condiţie este automat satisfăcută.

Următoarea lucrare pe care vrem sa o menţionăm este [Ve1] a lui Veys. El a considerat polinoame f în două variabile peste un corp de numere F si a luat o rezoluţie minimală scufundată a lui f peste o închidere algebrică a lui F. Acest context i-a permis să folosească formula [De1] lui Denef pentru $Z_f(s)$, valabilă pentru aproape toţi completaţii p-adici ai lui F. Veys a presupus de asemenea ca toate punctele de intersecţie ale componentelor ireductibile ale pull-back-ului lui f sunt definite peste F. În aceste condiţii, el a demonstrat reciproca rezultatului lui Loeser pentru poli candidadti reali

şi pentru aproape toţi completaţii p-adici ai lui F. Mai mult, el a considerat si problema unei posibile simplificări ale mai multor contribuţii la acelaşi pol candidat real.

În demonstraţiile rezultatelor menţionate mai sus este nevoie de anumite relaţii dintre invarianţii numerici asaciaţi unei rezoluţii scufundate. Aceste relaţii au fost obţinute în [St], [Me] şi [Ig2] pentru curbe absolut analitic ireductibile. De asemenea, Loeser [Lo] a demonstart relaţia necesară în cazul general. Igusa [Ig2] şi Loeser [Lo] au folosit formula lui Langlands [La] pentru a calcula contribuţia unei curbe excepţionale la reziduul lui $Z_f(s)$ în cazul unui pol candidat de ordin unu.

Pe scurt, **ideea noastra de lucru** este următoarea. Fie K un corp p-adic, adică o extendere finită a lui $\mathbb{Q}_p$. Fie R inelul de valuare al lui K, P idealul maximal al lui R si q cardinalul corpului rezidual R/P. Pentru $z \in K$, notăm cu $\operatorname{ord} z \in \mathbb{Z} \cup \{+\infty\}$ valuarea lui z şi cu $|z| = q^{-\operatorname{ord} z}$ valoarea absolută (p-adică) a lui z.

Fie $f(x_1, x_2) \in K[x_1, x_2]$ un polinom în două variabile peste K. Fie $x = (x_1, x_2)$. Fie X o submulţime deschisa şi compactă a lui K^2. În acest context, **funcţia zeta Igusa p-adică a lui** f este definită de

$$Z_f(s) = \int_X |f(x)|^s \, |dx|$$

pentru $s \in \mathbb{C}$, $\operatorname{Re}(s) > 0$, unde $|dx|$ este măsura Haar K^2, normalizată astfel încât R^2 are măsura 1. Igusa a demonstrat că $Z_f(s)$ este o funcţie raţională în q^{-s} folosind o rezoluţie scufundată a lui f. Aceasta se extinde prin urmare la o funcţie meromorfică $Z_f(s)$ pe $\mathbb{C}$ care se numeşte tot funcţia zeta Igusa p-adică asociată lui f.

Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Aici, Y este o K-varietate analitică. Despre rezoluţia scufundată a lui f mai multe detalii sunt prezentate în [Ig3, Section 3.2]. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ o compunere

de blowing-up-uri $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$. Curba excepţională lui g_i şi transformarea strictă a acestei curbe sunt notate cu E_i. Subvarietăţile lui Y de codimensiune unu reprezentate de zerourile transformării stricte ale unui factor ireductibil f din $K[x, y]$ sunt notate cu E_j, $j \in T_s$. Transformările corespunzătoare în Y_i, $i \in \{0, \ldots, t-1\}$ sunt notate analog. Atenţie aici şi la noţiunea de ireductibil, deoarece X este total disconex ca spaţiu topologic. Fie $T = T_e \cup T_s$. Pentru $i \in T$, fie N_i şi respectiv $\nu_i - 1$ multiplicităţile lui $f \circ g$ şi respectiv g^*dx în E_i. Perechea (N_i, ν_i) reprezintă **invarianţii numerici** ai lui E_i.

Dacă calculăm integrala de definiţie a lui $Z_f(s)$ pe Y cu formula de definiţie

$$Z_f(s) = \int_X |f(x)|^s \, |dx| = \int_Y |f \circ g|^s \, |g^*dx|,$$

şi considerăm b un punct arbitrar al lui Y, sunt posibile următoarele **trei situaţii**.

Primul caz este cel în care sunt două varietăţi E_i şi E_j, cu $i, j \in T$, care trec prin b. Considerăm o vecinătate V a lui b şi coordonatele analitice (y_1, y_2) în V astfel încât y_1 reprezintă ecuaţia lui E_i, y_2 este ecuaţia lui E_j,

$$f \circ g = \varepsilon y_1^{N_i} y_2^{N_j} \qquad \text{şi} \qquad g^*dx = \eta y_1^{\nu_i - 1} y_2^{\nu_j - 1} dy$$

pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\begin{aligned} \int_V |f \circ g|^s \, |g^*dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} |y_2|^{N_j s + \nu_j - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| \left(\frac{q-1}{q} \right)^2 \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}} \frac{q^{-k_2(N_j s + \nu_j)}}{1 - q^{-(N_j s + \nu_j)}}. \end{aligned}$$

Să observăm că am obţinut o funcţie raţională în q^{-s}.

În cel de-al doilea caz, să considerăm situaţia în care există o varietate E_i, $i \in T$, care trece prin b. Considerăm o varietate V a lui b şi coordonatele

analitice (y_1, y_2) pe V astfel încât y_1 este ecuaţia lui E_i,

$$f \circ g = \varepsilon y_1^{N_i} \qquad \text{şi} \qquad g^* dx = \eta y_1^{\nu_i - 1} dy$$

pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\begin{aligned} \int_V |f \circ g|^s \, |g^* dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| q^{-k_2} \frac{q-1}{q} \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}}. \end{aligned}$$

În cea de-a treia situaţie, nu există nici o varietate E_i, $i \in T$, care tece prin b. Fie V o vecinătate a lui b şi fie (y_1, y_2) coordonate analitice pe V astfel încât $f \circ g = \varepsilon$ şi $g^* dx = \eta dy$ pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\int_V |f \circ g|^s \, |g^* dx| = |\varepsilon|^s |\eta| q^{-k_1 - k_2}.$$

Rezultă atunci că $Z_f(s)$ este o funcţie raţională în q^{-s} deoarece putem partiţiona mulţimea Y în submulţimi V de forma de mai sus.

Din cele de mai sus rezultă şi că orice pol al lui $Z_f(s)$ este de forma

$$-\frac{\nu_i}{N_i} + \frac{2k\pi\sqrt{-1}}{N_i \log q},$$

cu $k \in \mathbb{Z}$ şi $i \in T$. Aceste valori se numesc poli candidaţi ai lui $Z_f(s)$. Pentru un $i \in T$ fixat, valorile $-\nu_i/N_i + (2k\pi\sqrt{-1})/(N_i \log q)$, $k \in \mathbb{Z}$, se numesc **polii candidaţi** ai lui $Z_f(s)$ asociaţi lui E_i. Deoarece polii proveniţi din $1/(1 - q^{-N_i s - \nu_i})$ au ordinul unu, definim **ordinul posibil** (ordinul candidat) al unui pol candidat s_0 ca fiind cel mai mare număr de curbe excepţionale E_i care au drept pol candidat pe s_0. Evident, **ordinul (efectiv)** lui s_0 este întotdeauna mai mic sau cel mult egal cu ordinul candidat al lui s_0. De

asemenea, este clar şi faptul că un pol candidat de ordin candidat unu este pol dacă şi numai dacă reziduul lui $Z_f(s)$ calculat în s_0 este diferit de 0.

Obiectivul fundamental al cercetării a fost să determinam când un pol candidat este pol (efectiv) şi când nu. Pentru aceasta am folosit o varianta îmbunătăţită a rezultatului demonstrat în [Se1]. Pe scurt, dată o rezoluţie minimală scufundată scisă ca o compunere de blow-ing-up-uri, Segers a obţinut modalitatea în care se poate calcula aceasta contribuţie la reziduu exact in momentul în care curba exceptională este creată.

Un prim rezultat important obţinut de noi în această direcţie de cercetare este Propoziţia 5.1 de mai jos în care analizăm când această contribuţie este zero şi când nu.

Ipotezele de lucru sunt următoarele: fie $f \in K[x_1, x_2]$ şi fie X o submulţime deschisă şi compactă a lui K^2. Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ compunerea blowing-up-urilor $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$. Curba excepţională a lui g_i şi transformarea strictă a lui sunt notate cu E_i. Fie $r \in T_e$. Curba excepţională E_r este obţinută prin blowing-up în punctul $P \in Y_{r-1}$. Fie (y_1, y_2) coordonatele locale ale lui Y_{r-1} centrate în P. Putem atunci scrie aceste coordonate locale sub forma

$$\begin{aligned} f \circ g_1 \circ \cdots \circ g_{r-1} &= d\left(\prod_{i\in S}(a_{i2}y_1 - a_{i1}y_2)^{M_i}\right)\left(\prod_{i\in S'} h_i^{M_i}(y_1, y_2)\right) + \\ &\quad + \text{termeni de grad mai mare,} \end{aligned}$$

unde factorii $a_{i2}y_1 - a_{i1}y_2$ şi h_i sunt polinoame esenţialmente diferite peste K (în sensul definit mai sus), şi în plus polinoamele h_i sunt polinoame omogene ireductibile de grad mai mare sau egal cu doi, iar $M_i \geq 1$ pentru orice

$i \in S \cup S'$, iar $d \in K^\times$. Fie de asemenea

$$(g_1 \circ \cdots \circ g_{r-1})^* dx = \left(e \prod_{i \in S} (a_{i2}y_1 - a_{i1}y_2)^{\mu_i - 1} + \right. \\ \left. + \text{termeni de grad mai mare} \right) dy,$$

cu $\mu_i \geq 1$ pentru toţi $i \in S$ şi $e \in K^\times$.

Putem acum să enunţăm primul rezultat din această direcţie:

Propoziţia 1.1. *Fie $s_0 := -\nu_r/N_r$ polul real candidat al lui $Z_f(s)$ asociat curbei E_r. Scriem α_i sub forma $\alpha_i := \mu_i + s_0 M_i \neq 0$ pentru orice $i \in S$.*

Fie $\mathcal{R}$ contribuţia curbei excepţionale E_r la reziduul lui $Z_f(s)$ în punctul s_0. Atunci, $\mathcal{R} \neq 0$ dacă şi numai dacă $|S| \geq 3$ sau $|S'| \geq 1$.

Mai mult, dacă $\mathcal{R} \neq 0$, atunci

1. *$\mathcal{R} > 0$ dacă şi numai dacă $\alpha_i > 0$ pentru toţi $i \in S$ şi*
2. *$\mathcal{R} < 0$ daca si numai daca exista $i \in S$ (şi acesta este unic) astfel încât $\alpha_i < 0$.*

Pentru demonstraţia rezultatului de mai sus, a fost nevoie de idei noi. Ceea ce am facut în lucrarea ISI publicată nu a fost doar o generalizare directă a unor rezultate cunoscute deja, ci am analizat cazurile în care contribuţiile la acelaşi pol candidat se anulează sau nu una pe alta. Pentru aceasta, am construit graful dual al rezoluţiei scufundate şi am arătat ɥ a este un arbore ordonat.

Să prezentăm în continuare notaţiile şi ipozele principale de demonstaţie din **rezultatul fundamental din această direcţie de cercetare**, Teorema 5.11.

Fie $f \in K[x_1, x_2]$ şi fie X o submulţime deschisă şi compactă a lui K^2. Să presupunem că f_{red} are doar un punct singular P_0 în X. Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ o

compunere de blowing-up-uri $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$, centrată în $P_{i-1} \in Y_{i-1}$. Curba excepţională a lui g_i şi transformarea strictă a acestei curbe sunt notate cu E_i. Subvarietăţile închise ale lui Y de codimensiune unu care reprezintă zerourile transformării sticte ale unui factor ireductibil al lui f în $K[x, y]$ le notăm cu E_j, $j \in T_s$.

Transformările corespunzătoare în Y_i, $i \in \{0, \ldots, t-1\}$, le notăm similar. Fie $T = T_e \cup T_s$.

În graful (dual) al rezoluţiei scufundate al lui f în P_0, se asociază fiecărei curbe excepţionale un vârf (reprezentat printr-un punct) şi fiecărei intersecţii dintre curbe excepţionale din Y o muchie, care leagă vârfurile corespunzătoare.

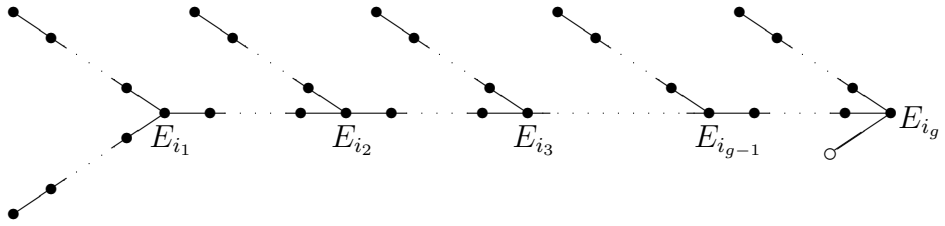
Asociem de asemenea fiecărei componente analitic ireductibile a transformării stricte a lui f în P_0 un vârf (reprezentat de un cerc), şi unicului său punct de intersecţie cu o curbă excepţională în Y muchia corespunzătoare. Este clar din construcţie că acest graf este un arbore finit, conex.

În continuare, fiecărui vârf al grafului rezoluţiei scufundate îi asociem raportul corespunzător ν_i/N_i. Acest fapt transformă graful rezoluţiei scufundate într-un arbore ordonat. Mai precis, vârfurile pentru care numărul asociat este egal cu $\min_{i \in T} \nu_i/N_i$, împreună cu muchiile corespunzătoare, formează o componentă conexă $\mathcal{M}$ a grafului rezoluţiei scufundate. Dacă începem cu un vârf terminal a părţii minimale $\mathcal{M}$, numerele ν_i/N_i sunt strict crescătoare de-a lungul oricărui drum din arbore, exceptând $\mathcal{M}$.

Acest fapt rezultă din relaţia (5.2) şi din marginea pentru α-uri, lucru care implică de exemplu că există cel mult un E_j care intersectează un E_r dat, cu $r \in T_e$, în Y cu $\nu_j/N_j < \nu_r/N_r$. Construţia de mai sus este una nouă, originală. În Teorema 3.3 [Ve2], Veys a făcut o construţie analoagă, dar el a lucrat peste $\mathbb{C}$, iar noi am genelizat construcţia peste un corp arbitrar K. **Această construţie este un alt rezultat original din această direcţie**

de cercetare.

Exemplul 1.2. *Dacă f este absolut analitic ireductibilă în P_0 cu g exponenţi Puiseux diferiţi, atunci graful rezoluţiei este de forma*



Aici, partea minimală $\mathcal{M}$ constă doar din E_{i_1} (vezi [St, Corolarul 2.1] sau [Ve2, Propozitia 3.6]).

Rezultatul de bază din această direcţie de cercetare este calculul polilor reali ai funcţiei zeta Igusa locale pentru curbe din teorema următoare. Noutatatea rezultatului constă în faptul că am reuşit să determinăm polii reali ai funcţiei zeta Igusa locale pentru curbe pentru un număr prim p arbitrar fixat. Rezultatul lui Veys din lucrarea menţionată [Ve1] este valabil doar pentru un număr prim p suficient de mare. Mai mult, ideea de demonstracţie nu este o simpla generalizare a rezultatului lui Veys: fixând un număr prim $p >> 0$ (i.e. suficient de mare), Veys a putut folosi formula lui Denef din [De1]. Fixând un numâr prim p arbitrar, acest rezultat nu mai poate fi folosit şi a fost nevoie de idei noi de demonstraţie.

Teorema 5.11[Calculul polilor reali ai funcţiei zeta Igusa locale] În ipotezele din primul paragraf al acestei seţiuni, avem:

1. un număr real s_0 este pol de ordin doi daca si numai daca exista $i, j \in T$ cu $s_0 = -\nu_i/N_i = -\nu_j/N_j$ astfel încât E_i şi E_j se intersectează în Y. Mai mult, $Z_f(s)$ are cel mult un pol real de ordin doi, iar dacă există un pol de ordin doi, acesta este polul cel mai apropiat de origine.

2. un număr real $s_0 \in \{-\nu_i/N_i \mid i \in T_e\} \setminus \{-\nu_i/N_i \mid i \in T_s\}$ care nu este pol de ordin doi este pol de orin întâi dacă şi numai dacă există cel puţin un $i \in T_e$ cu $s_0 = -\nu_i/N_i$ astfel încât $f \circ g_1 \circ \cdots \circ g_{i-1}$ este dat în coordonate locale centrate în P_{i-1} de o serie de puteri a cărei componentă de grad cel mai mic este un polinom omogen care nu este o putere a unui polinom liniar (de grad unu) sau un produs de două astfel de puteri

3. un număr real $s_0 \in \{-\nu_i/N_i \mid i \in T_s\}$ care nu este pol de ordin doi este pol de ordin unu pentru o vecinătate deschisă şi compactă X a lui P_0 suficient de mică.

1.3 A doua direcţie de cercetare: Studiul designurilor eşalon

Designul experimentelor este o ramură împortantă a Statisticii care are ca subiect important de studiu designurile full-factorial. În cadrul acestui proiect ne-am propus şi am reuşit să folosim metode ale Algebrei Comutative pentru a explora probleme relevante (cum ar fi bazele Gröbner, fracţiile, polinomul Hilbert) ale designurilor eşalon, adică ale unei mulţimi $\mathcal{E}$ de puncte experimentale având anumite proprietăţi speciale.

Designurile eşalon generalizează designurile full factorial inverstigate în [CPRW], [CR], [R], [RR]. Pe scurt, contibuţia noastră în acest domeniu constă într-o demonstraţie originală a existenţei unei baze Gröbner pentru un ideal design $\mathcal{I}(\mathcal{E})$. Mai mult, rezultatul nostru generalizează Teorema 2.18 a lui Robbiano [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251,

Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204]. În plus, am obţinut caracterizarea polinomului Hilbert asociat unui design eşalon şi am introdus şi studiat fracţii ale designurilor eşalon. Rezultatele din teoremele pe care le-am obţinut extind Teoremele 4.5 şi 5.6 din [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204] de la cazul designurilor full factorial la cazul designurilor eşalon.

În ultimii ani, "Statistica Algebrică" s-a dezvoltat la graniţa dintre Algebra Comutativă şi Statistică. Teoria şi rezultatele din Algebra Comutativă au ajutat în procesul de înţelegere a unor diverse ramuri din statistică, cum ar fi Designul Experimentelor (DoE-Design of Experiments). Această interacţiune este ilustrată în direcţia de cercetare pe care am abordat-o, în care demonstrăm proprietăţi importante pentru designurile eşalon.

Mai precis, folosim metode de Algebra Comutativă pentru a studia probleme referitoare la designurile eşalon care provin din DoE. Pentru a înţelege mai bine eficienţa şi importanţa studiului designurilor eşalon în studiul şi analiza unor modele economice cu aplicaţii practice, vom prezenta un exemplu.

Un magazin care comercializează echipamente de calcul are o anumită stategie de aprovizionare, bazată pe diverse considerente economice, cu laptouri de-a lungul unui an. Astfel, în prima perioada (lunile ianuarie-aprilie) magazinul are în stoc următoarele modele de laptopuri: Allview, Acer, HP, Asus, Lenovo, Samsung, Toschiba şi Dell. În următoarea perioada (lunile mai-august), magazinul are în stoc mărcile Allview, Acer, HP, Asus şi Lenovo, iar în ultima perioadă (lunile septembrie-decembrie), din anumite motive, are în stoc doar Allview, Acer şi HP.

Această strategie poate fi văzută ca o mulţime de puncte din $\mathbb{Z}_+^2$, notate (L, M), unde M reprezintă marca (brand-ul) laptopului, iar L reprezintă luna. Variabila M poate lua una dintre valorile 0,1,2,3,4,5,6 sau 7, care au seminicaţia: 0=Allview, 1=Acer, 2=HP, 3=Asus, 4=Lenovo, 5=Samsung, 6=Toschiba şi 7=Dell. Valoarea pentru variabila L poate fi una din mulţimea $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, unde 0=ianuarie, 1=februarie,. . ., 11=decembrie.

Prin urmare, această mulţime de puncte împreună cu resticţiile date de disponibiliatea brand-ului într-o anumită lună, formează un design eşalon. Se poate observa că vectorii dominanţi, adică vectorii care mărginesc designul eşalon, sunt $(0, 8)$, $(4, 5)$, $(8, 3)$ şi $(12, 0)$. Astfel, de exemplu punctul $(3, 3)$ care se găseşte în design arată că în luna aprilie brand-ul Asus este disponibil în magazin.

Departamentul de marketing al magazinului din acest exemplu doreşte să analizeze profitul obţinut din acestă strategie de aprovizionare. În acest scop, işi formează un grup de potenţiali cumpărători cărora le cere să facă un rating, adică să noteze pe o scară de la 0 la 10 diversele posibilităţi, i.e. diversele puncte ale designului eşalon. În acest rating, cumpărătorii trebuie să ia în consideraţie bugetul lor într-o anume perioadă de timp şi preferinţa lor pentru un anumit brand. În acest fel, fiecărui punct al designului îi putem asocia o anumită valoare, de exemplu media notelor acordate de subiecţii chestionarului. Obţinem astfel o funcţie care are ca domeniu de definiţie punctele designului. Din Cororalul 2.14 din lucrarea lui Robiano [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204], rezultă că orice funcţie definită pe o mulţime finită cu valori într-un corp arbitrar este o funcţie polinomială şi se numeşte în Statistica Algebrică modelul polinomial al de-

signului. Această funcţie polinomială furnizează multe informaţii care pot fi folosite pentru a îmbunătăţii stategia de marketing a magazinului.

În afară de exemplul prezentat mai sus, există în mod evident numeroase alte exemple din domeniul economic care pot fi modelate folosind designurile experimentale.

Revenind la exemplul prezentat mai sus, este clar că nici un potenţial client nu va dori să noteze toate punctele din design, fiind, în general, mult prea multe posibilităţi. Din acest motiv, se folosesc modele care vin din fracţii (anumite submulţimi) ale designului. Aceste modele pot fi apoi folosite pentru a obţine o reconstruc tie cât mai fidelă a modelului din problema de marketing prezentată.

Dat un design eşalon $\mathcal{E}$, o fracţie $\mathcal{F}$ a desinului este o submulţime a acestei mulţimi de puncte, dar din punct de vedere algebric, descrierea fracţiei nu este deloc una canonică. Este clar că idealul de definiţie $\mathcal{I}(\mathcal{F})$, care defineşte fracţia dată $\mathcal{F}$, conţine $\mathcal{I}(\mathcal{E})$ care reprezintă idealul de definiţie al eşalonului $\mathcal{E}$. Acest lucru are o explicaţie algebrică simplă: orice polinom care se anulează pe toate punctele din $\mathcal{E}$ automat se anulează pe toate punctele din $\mathcal{F}$. Mai multe detalii despre aceste fracţii, pentru a vedea cum pot fi convenabil alese aceste fracţii şi cum pot fi ele folosite în teoria generaă a DoE, recomandăm lucrarea lui Robiano, [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204].

Pentru a putea face un rezumat al principalelor rezultate obţinute în acestă direţie de cercetare, începem prin a reaminti definiţia unui design eşalon.

Definiţia 1.3. *Fie k un corp şi fie $m \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Un **design** $\mathcal{D}$ este o*

mulţime finită de puncte distincte din k^m.

Se numeşte ***idealul designului*** $\mathcal{D}$ *idealul* $I(\mathcal{D})$ *care conţine toate polinoamele din* $k[x_1, \ldots, x_m]$ *care se anulează în toate punctele lui* $\mathcal{D}$.

Pe scurt, rezultatele obţinute în această direcţie de cercetare sunt următoarele.

Un prim rezultat fundamental al cercetării în acestă direcţie îl constituie teorema în care am obţinut o bază Gröbner pentru idealul $\mathcal{I}(\mathcal{E})$, unde $\mathcal{E}$ este un design eşalon, teoremă pe care o vom enunţa mai jos după ce vom defini designul eşalon. Rezultatul obţinut de noi generalizează Teorema 2.18 din lucrarea amintită a lui Robiano.

Am considerat apoi polinomul asociat unui design $\mathcal{D} \subset \mathbb{Z}_+^m$ definit de

$$H_{\mathcal{D}}(t) = \sum_{i \geq 0} a_i t^i,$$

unde $a_i = \#\{a = (a_1, \ldots, a_m) \in \mathcal{D} | a_1 + \ldots + a_m = i\}$. Polinomul $H_{\mathcal{D}}(t)$ se numeşte polinomul Hilbert al designului $\mathcal{D}$.

Al doilea rezultat principal al acestei cercetări în reprezintă caracterizarea polinoamelor cu coeficienţi întregi care pot fi polinoame Hilbert ale unui design eşalon.

De asemenea, am studiat si fracţiile unui design eşalon si am obţinut aici **alte două rezultate principale** pe care le vom detalia mai jos. Cele două teoremele referitoare la fracţiile unui design eşalon extind Teoremele 4.5 şi Teorema 5.6 din lucrarea lui Robiano la cazul designurilor eşalon.

Prezentăm în rezumat rezultatele enunţate mai sus.

Să definim pentru început designurie eşalon in dimensiune m.

Pentru $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, fie $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_m^{\alpha_m} \in k[x_1, \ldots, x_m]$.

Definiţia 1.4. *Fie* $a = (a_1, \ldots, a_m)$ *şi* $b = (b_1, \ldots, b_m)$ *două puncte din* $\mathbb{Z}_+^m$. *Spunem că* a ***domină pe*** b *dacă* $a_i \leq b_i$, *pentru orice* $i = 1, \ldots, m$.

În termeni de monoame, a **domină pe** b dacă $\mathbf{x}^a|\mathbf{x}^b$. Evident, dacă a domină pe b, atunci $\mathbf{x}^a$ domină orice multiplu al lui $\mathbf{x}^b$.

Definiţia 1.5. *Fie $K \in \mathbb{N}^*$ şi fie $\alpha^{(1)}, \ldots, \alpha^{(K)}$ vectori cu componente întregi din $\mathbb{Z}_+^m$ astfel încât nici un $\boldsymbol{x}^{\alpha^{(i)}}$ nu domină nici un $\boldsymbol{x}^{\alpha^{(j)}}$ pentru toţi $1 \leq i \neq j \leq K$. **Designul eşalon** $\mathcal{E} \in \mathbb{Z}_+^m$ determinat de vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ este mulţimea tuturor punctelor $b \in \mathbb{Z}_+^m$ cu proprietatea că $\boldsymbol{x}^b$ nu este divizibil cu $\boldsymbol{x}^{\alpha^{(i)}}$, pentru orice $1 \leq i \leq K$. Cu alte cuvinte, design-ul eşalon definit de vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ este mulţimea de puncte din $\mathbb{Z}_+^m$ care nu sunt dominate de $\alpha^{(1)}, \ldots, \alpha^{(K)}$.*

*Vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ se numesc **vectori dominanţi (sau de definiţie)** ai eşalonului $\mathcal{E}$. Monomul $\boldsymbol{x}^{\alpha^{(i)}}$, pentru $1 \leq i \neq j \leq K$, se numeşte **monomul dominanţ (sau de definiţie)** al lui $\mathcal{E}$.*

Exemplul 1.6. *Fie $m = 2$ şi $\alpha^{(1)} = (0,4)$, $\alpha^{(2)} = (1,3)$, $\alpha^{(3)} = (3,1)$, $\alpha^{(4)} = (5,0)$ vectorii dominanţi care definesc eşalonul $\mathcal{E} \subset \mathbb{Z}_+^2$. Să observăm că nici un $\boldsymbol{x}^{\alpha^{(i)}}$ nu divide nici un $\boldsymbol{x}^{\alpha^{(j)}}$ pentru orice $1 \leq i \neq j \leq 4$.*

Monoamele de definiţie sunt prin urmare x_2^4, $x_1x_2^3$, $x_1^3x_2$ şi x_1^5. Conform Definiţiei 6.3, designul $\mathcal{E} \subset \mathbb{Z}_+^2$ este format din toate punctele din $\mathbb{Z}_+^2$ care nu sunt dominate de $\alpha^{(1)}, \ldots, \alpha^{(4)}$, şi anume din punctele $(0,0)$, $(0,1)$, $(0,2)$, $(0,3)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,0)$, $(2,1)$, $(2,2)$, $(3,0)$ şi $(4,0)$; vezi Figura 1.1.

Este nu foarte dificil de văzut că un design eşalon de dimensiune m poate fi definit şi astfel:

Definiţia 1.7. *Un design $\mathcal{E} \subset \mathbb{Z}_+^m$ este design eşalon dacă şi numai dacă fiecare punct $(d_1, \ldots, d_m)$ din eşalon are proprietatea că toate punctele de forma $(y_1, \ldots, y_m)$ cu $0 \leq y_j \leq d_j$, pentru orice $j = 1, \ldots, m$ se găsesc în designul $\mathcal{E}$.*

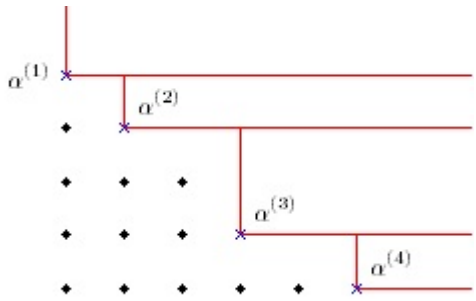


Figura 1.1: Un desig eşalon definit prin vectorii dominanţi

Exemplul 1.8. *În designul eçalon $\mathcal{E}$ din Examplul 6.4, cum punctele* $(0,3)$, $(1,2)$, $(2,0)$, $(3,0)$ *şi* $(4,0)$ *se găsesc în designul $\mathcal{E}$, toate aceste puncte împreună cu cele care se află "mai jos" de ele, adică* $(0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(2,1)$, $(2,0)$ *sunt toate puncte ale designului.*

Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii dominanţi $\alpha^{(1)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^m$.

Fiecărui vector $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_+^m$ îi asociem un polinom $f_\alpha \in k[x_1, \ldots, x_m]$ definit astfel:

$$f_\alpha = \prod_{i=1}^{m} x_i(x_i - 1)\ldots(x_i - \alpha_i + 1).$$

În raport cu orice ordonare monomială $<$ pe $k[x_1, \ldots, x_m]$, avem

$$\mathrm{in}_<(f_\alpha) = x_1^{\alpha_1} \ldots x_m^{\alpha_m},$$

unde cu $\mathrm{in}_<(f)$ am notat monomul iniţial al lui f relativ la $<$. Fie $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ polinoamele asociate vectorilor $\alpha^{(1)}, \ldots, \alpha^{(K)}$ ale lui $\mathcal{E} \subset \mathbb{Z}_+^m$. Rezultă atunci că $f_{\alpha^{(i)}} \in I(\mathcal{E})$, pentru orice $1 \leq i \leq K$, şi deci pentru orice ordonare monomială $<$ pe $k[x_1, \ldots, x_m]$ avem

$$(\mathrm{in}(f_{\alpha^{(1)}}), \ldots, \mathrm{in}(f_{\alpha^{(K)}})) \subset \mathrm{in}(I(\mathcal{E})),$$

unde cu $\text{in}(\mathcal{I}(\mathcal{E}))$ am notat idealul iniţial al lui $\mathcal{I}(\mathcal{E})$ relativ la ordonarea monomială $<$.

Primul nostru rezultat din această cercetare este următoarea teoremă care stabileşte o bază Gröbner a lui $I(\mathcal{E})$ relativ la orice ordonare monomială pe $k[x_1, \ldots, x_m]$.

Teorema 1.9. *Teorema Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^m$. Atunci mulţimea $G = \{f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}\}$ este o bază Gröbner a lui $I(\mathcal{E})$ relativ la orice ordonare monomială pe $k[x_1, \ldots, x_m]$.*

Definiţia 1.10. *Dat un design arbitrar $\mathcal{D} \subset \mathbb{Z}_+^m$, definim **polinomul Hilbert asociat designului** $\mathcal{D}$ ca fiind:*

$$H_{\mathcal{D}}(t) = \sum_{i \geq 0} a_i t^i,$$

unde $a_i = \#\{a = (a_1, \ldots, a_m) \in \mathcal{D} | a_1 + \ldots + a_m = i\}$.

Vom nota $H_{\mathcal{D}}$ polinomul Hilbert asociat designului $\mathcal{D}$.

Al doilea rezultat din această direcţie de cercetare îl reprezintă teorema următoare care caracterizează polinomul Hilbert al unui design eşalon în dimensiune 2.

Teorema 1.11. *Fie $H \in \mathbb{Z}[t]$ un polinom cu coeficienţi întregi ne-negativi. Atunci H este polinomul Hilbert al unui design eşalon în dimensiune doi dacă şi numai dacă există un întreg $i \geq 0$ astfel încât*

$$H(t) = 1 + 2t + 3t^2 + \ldots + (i+1)t^i + a_{i+1}t^{i+1} + \ldots + a_d t^d,$$

cu $d \geq 0$ şi $i + 1 \geq a_{i+1} \geq \ldots \geq a_d$.

Dat un design eşalon $\mathcal{E}$, o **fracţie a eşalonului** este o submulţime proprie $\mathcal{F} \subset \mathcal{E}$. În mod clar, idealul său de definiţie $I(\mathcal{F})$ conţine idealul $I(\mathcal{E})$.

Definiţia 1.12. *Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii dominanţi $\alpha^{(1)}$, ..., $\alpha^{(K)} \in \mathbb{Z}_+^m$. Fiecărui astfel de vector $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_+^m$ îi asociem un polinom $f_\alpha \in k[x_1, \ldots, x_m]$ definit astfel:*

$$f_\alpha = \prod_{i=1}^{m} x_i(x_i - 1)\ldots(x_i - \alpha_i + 1).$$

Polinoamele $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ le-am numit ***polinoamele canonice*** *ale designului eşalon $\mathcal{E}$.*

Definiţia 1.13. *Orice submulţime de polinoame care, adăugate polinoamelor canonice ale unui design eşalon $\mathcal{E}$, generează idealul unei fracţii $\mathcal{F}$, se numesc* ***polinoame confounding*** *ale lui $\mathcal{F}$ în $\mathcal{E}$.*

Definiţia 1.14. *Fie $\mathcal{E}$ un design eşalon şi fie $\mathcal{F}$ o fracţie a acestuia. Se numeşte* ***polinomul caracteristic al lui*** *$\mathcal{F} \subset \mathcal{E}$ polinomul f cu proprietatea că $f(P) = 0$ pentru orice $P \in \mathcal{F}$ şi $f(P) = 1$ pentru orice $P \in \mathcal{E} \setminus \mathcal{F}$.*

Dacă aplicăm Teorema 6.9 şi Proposition 4.4 din lucrarea menţinată a lui Robiano, obţinem:

Propoziţia 1.15. *Fie $\mathcal{E}$ un design eşalon şi fie $\mathcal{F} \subset \mathcal{E}$ o fracţie a acestuia. Fie f polinomul caracteristic al lui $\mathcal{F}$. Atunci*

$$I(\mathcal{F}) = \left(f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}, f\right).$$

Al treilea rezultat din acestă direcţie de cercetare este dat în următoarea teoremă:

Teorema 1.16. *Fie $<$ o ordonare monomială pe $k[x_1, \ldots, x_m]$, $\mathcal{E} \in \mathbb{Z}_+^m$ un design eşalon, $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ polinoamele canonice ale lui $\mathcal{E}$ şi fie $\mathcal{F} \subset \mathcal{E}$ o fracţie a designului $\mathcal{E}$.*

Există atunci un unic polinom caracteristic f al lui $\mathcal{F}$ în $\mathcal{E}$ astfel încat $in(f)$ nu este dominat de nici un $\mathrm{in}_<(f_{\alpha^{(i)}})$, $1 \leq i \leq n$.

Definiţia 1.17. *Fie $\mathcal{E} \subset k^m$ un design eşalon. Notăm cu $\mathcal{O}(\mathcal{E})$ mulţimea de monoame $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m} | (\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathcal{E}\}$.*

Definiţia 1.18. *Fie $\mathcal{O} \subseteq \mathrm{Mon}(\mathcal{S})$. Spunem că $\mathcal{O}$ este o **mulţime standard de monoame** dacă $T \in \mathcal{O}$ şi T' divide T implică $T' \in \mathcal{O}$, i.e. toţi divizorii unui element din $\mathcal{O}$ sunt de asemenea în $\mathcal{O}$.*

Definiţia 1.19. *Date n variabile $x_1, x_2, \dots, x_m$, fie $\mathcal{E} \subset \mathbb{Z}_+^2$ un design eşalon şi fie $\mathcal{O} \subset \mathcal{O}(\mathcal{E})$ o mulţime standard de monoame. Atunci, din Lema lui Dickson, vezi [HH] rezultă că există o unică mulţime minimală, $\mathrm{Min}(\mathcal{O})$, de monoame care generează $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$. Adică, fiecare element din $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$ este un multiplu al unui element din $\mathrm{Min}(\mathcal{O})$. Mulţimea de monoame din $\mathrm{Min}(\mathcal{O})$, care nu se găsesc printre termenii dominanţi ai polinoamelor canonice ale lui $\mathcal{E}$, se notează cu $\mathrm{CutOut}(\mathcal{O})$.*

Definiţia 1.20. *Date n variabile $x_1, x_2, \dots, x_m$, fie $\mathcal{E} \subset \mathbb{Z}_+^2$ un design eşalon şi fie $\mathcal{O} \subset \mathcal{O}(\mathcal{E})$ o mulţime standard de monoame. Atunci, din Lema lui Dickson, vezi [HH] rezultă că există o unică mulţime minimală, $\mathrm{Min}(\mathcal{O})$, de monoame care generează $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$. Adică, fiecare element din $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$ este un multiplu al unui element din $\mathrm{Min}(\mathcal{O})$. Mulţimea de monoame din $\mathrm{Min}(\mathcal{O})$, care nu se găsesc printre termenii dominanţi ai polinoamelor canonice ale lui $\mathcal{E}$, se notează cu $\mathrm{CutOut}(\mathcal{O})$.*

Înainte de a da **cel de-al patrulea rezultat din această direcţie de cercetare**, să reamintim o definiţie introdusă de L. Robbiano, în [R].

Definiţia 1.21. *Fie K un corp infinit, $T := x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ şi fie $\alpha_1, \alpha_2, \dots, \alpha_n$ n şiruri de elemente din corpul de bază K, unde $\alpha_r = (\alpha_{r,i})_{i \in \mathbb{N}}$, pentru $r := 1, 2, \dots, n$ şi $\alpha_{r,i} \neq \alpha_{r,j}$, dacă $i \neq j$. Polinomul*

$$D(T) := \prod_{i=1}^{a_1} (x_1 - \alpha_{1,i}) \prod_{i=1}^{a_2} (x_2 - \alpha_{2,i}) \cdots \prod_{i=1}^{a_n} (x_n - \alpha_{n,i})$$

se numeşte ***distragerea (the disytraction)*** *lui* T *relativ la* $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Cel de-al patrulea rezulat din acestă direcţie de cercetare este următorul rezultat:

Teorema 1.22. *Fie* $\mathcal{E}$ *un design eşalon definit de vectorii dominanţi* $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^m$. *Fie* $\mathcal{I}(\mathcal{E}) := (f_{\alpha^{(1)}}, f_{\alpha^{(2)}}, \ldots, f_{\alpha^{(K)}})$ *idealul său de definiţie, unde* $f_{\alpha^{(j)}}$ *sunt polinoamele canonice, pentru* $j = 1, \ldots, K$. *Fie* $\mathcal{O}(\mathcal{E})$ *mulţimea standard de monoame corespunzătoare şi fie* $\mathcal{O} \subset \mathcal{O}(\mathcal{E})$ *o mulţime standard de monoame. Să presupunem că* $\{T_1, T_2, \ldots, T_h\} = \mathrm{CutOut}(\mathcal{O})$ *şi fie* $D(T_1), D(T_2), \ldots, D(T_h)$ *distragea lui* $T_1, T_2, \ldots, T_h$.
Atunci, pentru orice ordonare monomială pe $k[x_1, x_2, \ldots, x_n]$, *mulţimea*

$$\{f_{\alpha^{(1)}}, f_{\alpha^{(2)}}, \ldots, f_{\alpha^{(K)}}, D(T_1), D(T_2), \ldots, D(T_h)\}$$

este o bază Gröbner neredusă pentru idealul $\mathcal{I}(\mathcal{F})$, *unde* $\mathcal{F} \subset \mathcal{E}$ *este o fracţie a eşalonului* $\mathcal{E}$ *astfel încât* $\mathcal{O}(\mathcal{F}) = \mathcal{O}$.

Capitolul 2

Rezumatul lucrării în limba engleză

Several mathematicians have already obtained partial results about the determination of the poles of Igusa's p-adic zeta function for curves. In this paper, we will determine the real poles for an arbitrary polynomial f in two variables which is defined over a p-adic field. People are interested in the poles of Igusa's p-adic zeta function $Z_f(s)$ because they determine the asymptotic behaviour of the number of solutions of polynomial congruences and because they are the subject of the monodromy conjecture (see for example [Den91]).

Historically, one considered first only curves which are absolutely analytically irreducible. Partial results were obtained by Igusa [Ig1] and Strauss [St]. Meuser [Me] determined the real poles, but she did not consider the candidate pole -1. In 1985 Igusa [Ig2] solved that problem completely. He proved that the candidate poles associated to the strict transform of f are poles when the domain of integration is small enough. Moreover, another candidate pole of the minimal embedded resolution of f is a pole if and only if it is associated to an exceptional curve which is intersected by three

other irreducible components of the pull-back of f. We have incorporated a generalization of this result (Proposition 2).

In the general case, Loeser [Lo] obtained that an exceptional curve E_i does not contribute to the poles of $Z_f(s)$ if E_i is intersected one or two times by other components of the pull-back of f and if there are no other intersection points over an algebraic closure. This was first proved by Strauss in the absolutely analytically irreducible case, where the last condition is automatically satisfied.

The next paper we want to mention is [Ve1] of Veys. He considers a polynomial f in two variables over a number field F and takes the minimal embedded resolution of f over an algebraic closure of F. This setup allowed him to use a formula [De1] of Denef for $Z_f(s)$, which is valid for almost all p-adic completions of F. He supposes that all intersection points of irreducible components of the pull-back of f are defined over F. Under this condition, he proves the converse of the result of Loeser for real candidate poles and for almost all p-adic completions of F. Moreover, he deals with the problem of a possible cancellation of several contributions to the same real candidate pole.

In the proofs of the mentioned vanishing and non-vanishing results, one needed certain relations between the various numerical data of the embedded resolution. They were systematically derived in [St], [Me] and [Ig2] for absolutely analytically irreducible curves and finally, Loeser [Lo] obtained the necessary relations in the general case. Igusa [Ig2] and Loeser [Lo] used a formula of Langlands [La] to calculate the contribution of an exceptional curve to the residue of $Z_f(s)$ at a candidate pole of candidate order one. We will use a slight variant of this formula which was obtained in [Se1]. Given an embedded resolution written as a composition of blowing-ups, the second

author explained there how to calculate this contribution to the residue at the stage where the exceptional curve is created. In Proposition 1, we determine when this contribution is zero and when not. For this, we need new ideas. It is not at all a straightforward generalization of what was already known. Finally in Section 4, we will prove that contributions to the same candidate pole will not cancel out. For this, we use that the dual embedded resolution graph is an ordered tree. This was obtained in [Ve2] when the base field is algebraically closed.

Let K be a p-adic field, i.e., an extension of $\mathbb{Q}_p$ of finite degree. Let R be the valuation ring of K, P the maximal ideal of R and q the cardinality of the residue field R/P. For $z \in K$, let $\operatorname{ord} z \in \mathbb{Z} \cup \{+\infty\}$ denote the valuation of z and $|z| = q^{-\operatorname{ord} z}$ the absolute value of z.

Let $f(x_1, x_2) \in K[x_1, x_2]$ be a polynomial in two variables over K and put $x = (x_1, x_2)$. Let X be an open and compact subset of K^2. Igusa's p-adic zeta function of f is defined by

$$Z_f(s) = \int_X |f(x)|^s \, |dx|$$

for $s \in \mathbb{C}$, $\operatorname{Re}(s) > 0$, where $|dx|$ denotes the Haar measure on K^2, normalised so that R^2 has measure 1. Igusa proved that $Z_f(s)$ is a rational function of q^{-s} by calculating the integral on an embedded resolution of f. Therefore, it extends to a meromorphic function $Z_f(s)$ on $\mathbb{C}$ which is also called Igusa's p-adic zeta function of f.

Let $g : Y \to X$ be an embedded resolution of f. Here, Y is a K-analytic manifold. The meaning of embedded resolution in our context is explained in [Ig3, Section 3.2]. Write $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ as a composition of blowing-ups $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$. The exceptional curve of g_i and also the strict transforms of this curve are denoted by E_i. The closed submanifolds of Y of codimension one which are the zero locus of the strict

transform of an irreducible factor of f in $K[x,y]$ are denoted by E_j, $j \in T_s$. The corresponding transforms in Y_i, $i \in \{0,\dots,t-1\}$, are denoted in the same way. Note that we had to be careful with the notion of irreducible, because X is totally disconnected as a topological space. Put $T = T_e \cup T_s$. For $i \in T$, let N_i and $\nu_i - 1$ be the multiplicities of respectively $f \circ g$ and g^*dx along E_i. The (N_i, ν_i) are called the numerical data of E_i.

Let us recall Igusa's proof of the rationality of $Z_f(s)$. As we already said, we calculate the defining integral on Y:

$$Z_f(s) = \int_X |f(x)|^s \, |dx| = \int_Y |f \circ g|^s \, |g^*dx|.$$

Let b be an arbitrary point of Y. There are three cases. In the first case, there are two varieties E_i and E_j, with $i,j \in T$, that pass through b. We take a neighborhood V of b and analytic coordinates (y_1, y_2) on V such that y_1 is an equation of E_i, y_2 is an equation of E_j,

$$f \circ g = \varepsilon y_1^{N_i} y_2^{N_j} \qquad \text{and} \qquad g^*dx = \eta y_1^{\nu_i - 1} y_2^{\nu_j - 1} dy$$

on V for non-vanishing K-analytic functions ε and η on V. We may suppose that $y(V) = P^{k_1} \times P^{k_2}$, with $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, and that $|\varepsilon|$ and $|\eta|$ are constant on V. We get

$$\begin{aligned} \int_V |f \circ g|^s \, |g^*dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} |y_2|^{N_j s + \nu_j - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| \left(\frac{q-1}{q} \right)^2 \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}} \frac{q^{-k_2(N_j s + \nu_j)}}{1 - q^{-(N_j s + \nu_j)}}. \end{aligned}$$

Note that this is a rational function of q^{-s}. In the second case, there is one variety E_i, $i \in T$, that passes through b. We take a neighborhood V of b and analytic coordinates (y_1, y_2) on V such that y_1 is an equation of E_i,

$$f \circ g = \varepsilon y_1^{N_i} \qquad \text{and} \qquad g^*dx = \eta y_1^{\nu_i - 1} dy$$

on V for non-vanishing K-analytic functions ε and η on V. We may suppose that $y(V) = P^{k_1} \times P^{k_2}$, with $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, and that $|\varepsilon|$ and $|\eta|$ are constant on V. We get

$$\begin{aligned}\int_V |f \circ g|^s \, |g^* dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| q^{-k_2} \frac{q-1}{q} \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}}.\end{aligned}$$

In the third case, there is no variety E_i, $i \in T$, that passes through b. We take a neighborhood V of b and analytic coordinates (y_1, y_2) on V such that $f \circ g = \varepsilon$ and $g^* dx = \eta dy$ on V for non-vanishing K-analytic functions ε and η on V. We may suppose that $y(V) = P^{k_1} \times P^{k_2}$, with $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, and that $|\varepsilon|$ and $|\eta|$ are constant on V. We get

$$\int_V |f \circ g|^s \, |g^* dx| = |\varepsilon|^s |\eta| q^{-k_1 - k_2}.$$

It follows now that $Z_f(s)$ is a rational function of q^{-s} because we can partition Y into sets V of the above form.

We obtain also from this calculation that every pole of $Z_f(s)$ is of the form

$$-\frac{\nu_i}{N_i} + \frac{2k\pi\sqrt{-1}}{N_i \log q},$$

with $k \in \mathbb{Z}$ and $i \in T$. These values are called the candidate poles of $Z_f(s)$. If $i \in T$ is fixed, the values $-\nu_i/N_i + (2k\pi\sqrt{-1})/(N_i \log q)$, $k \in \mathbb{Z}$, are called the candidate poles of $Z_f(s)$ associated to E_i. Because the poles of $1/(1 - q^{-N_i s - \nu_i})$ have order one, we define the expected order of a candidate pole s_0 as the highest number of E_i's with candidate pole s_0 and with non-empty intersection. The order of s_0 is of course less than or equal to its expected order and a candidate pole s_0 of expected order one is a pole if and only if the residue of $Z_f(s)$ at s_0 is different from 0.

Let us explain the formula for the residue that we will use. Let s_0 be a candidate pole of E_i, $i \in T$, and suppose that s_0 is not a candidate pole of any E_j, with $j \in T$ and $j \neq i$, which intersects E_i in Y. Let U be an open and compact subset of E_i. The contribution of U to the residue of $Z_f(s)$ at s_0 is by definition the contribution to the residue of $Z_f(s)$ at s_0 of an open and compact subset V of Y which satisfies $V \cap E_i = U$ and which is disjoint from every other E_j with candidate pole s_0. Suppose that U already exists in Y_r and if $i \in T_s$ we also suppose that it is non-singular in Y_r. Suppose that W is an open and compact subset of Y_r for which $W \cap E_i = U$ and that (z_1, z_2) are analytic coordinates on W such that $z_1 = 0$ is an equation of U on W. Write

$$f \circ g_1 \circ \cdots \circ g_r = \gamma z_1^{N_i} \qquad \text{and} \qquad (g_1 \circ \cdots \circ g_r)^* dx = \delta z_1^{\nu_i - 1} dy$$

on W, for K-analytic functions γ and δ on W. Then, the contribution of U to the residue of $Z_f(s)$ at s_0 is equal to

$$\frac{q-1}{qN_i \log q} \left[\int_U |\gamma|^s |\delta| |dz_2| \right]_{s=s_0}^{\mathrm{mc}}, \tag{2.1}$$

where $[\cdot]_{s=s_0}^{\mathrm{mc}}$ denotes the evaluation in $s = s_0$ of the meromorphic continuation of the function between the brackets. This formula was obtained by Langlands [La] in the case $r = t$ and in general by the second author in [Se1, Section 2.6].

We explain now the relations that we will need. Fix $r \in T_e$. The exceptional curve E_r is obtained by blowing-up at a point $P \in Y_{r-1}$. Let $y = (y_1, y_2)$ be local coordinates on Y_{r-1} centered at P. Write in these local coordinates

$$f \circ g_1 \circ \cdots \circ g_{r-1} = d \left(\prod_{i \in S} (a_{i2} y_1 - a_{i1} y_2)^{M_i} \right) \left(\prod_{i \in S'} h_i^{M_i}(y_1, y_2) \right) + \text{terms of higher degree},$$

where all factors $a_{i2}y_1 - a_{i1}y_2$ and h_i are essentially different (i.e. no factor is equal to another multiplied by an element of $K^\times$) polynomials over K, where the h_i are irreducible homogeneous polynomials of degree at least two, where $M_i \geq 1$ for every $i \in S \cup S'$ and where $d \in K^\times$. Write also

$$(g_1 \circ \cdots \circ g_{r-1})^* dx = \left(e \prod_{i \in S} (a_{i2}y_1 - a_{i1}y_2)^{\mu_i - 1} + \text{terms of higher degree} \right) dy,$$

where $\mu_i \geq 1$ for every $i \in S$ and $e \in K^\times$. Let $s_0 = -\nu_r/N_r + (2k\pi\sqrt{-1})/(N_r \log q)$ be an arbitrary candidate pole of $Z_f(s)$ associated to E_r. We advise the reader to specialize everything what follows in this section to the case $k = 0$. Put $\alpha_i := \mu_i + s_0 M_i$ for every $i \in S$. Because

$$N_r = \sum_{i \in S} M_i + \sum_{i \in S'} (\deg h_i) M_i \qquad \text{and} \qquad \nu_r = \sum_{i \in S} (\mu_i - 1) + 2,$$

it is straightforward to check that

$$\sum_{i \in S} (\alpha_i - 1) + \sum_{i \in S'} s_0 (\deg h_i) M_i = -2 + \frac{2k\pi\sqrt{-1}}{\log q}. \tag{2.2}$$

We now give another description of the α_i. Let F_i be the point on E_r which has coordinates $(a_{i1} : a_{i2})$ with respect to the homogenous coordinates $(y_1 : y_2)$ on $E_r \subset Y_r$. Let j be the unique element of $T \setminus \{r\}$ such that E_j passes through F_i in Y. Let ρ be the number of blowing-ups among $g_r, \ldots, g_t$ which are centered at F_i. Then, the announced description is $\alpha_i = \nu_j + s_0 N_j - (2\rho k\pi\sqrt{-1})/(\log q)$. The second author proved this in [Se1, Section 2.7] in the case $k = 0$, and the general case is treated in a similar way. It follows that $\mathrm{Re}(\alpha_i) < 0$ if and only if $-\nu_r/N_r < -\nu_j/N_j$. One checks also easily that

$$\begin{aligned} s_0 \text{ is a candidate pole of } E_j &\iff \nu_j + s_0 N_j \text{ is a multiple of } 2\pi\sqrt{-1}/(\log q) \\ &\iff \alpha_i \text{ is a multiple of } 2\pi\sqrt{-1}/(\log q). \end{aligned}$$

It is proved in [Lo, Proposition II.3.1] that $\mathrm{Re}(\alpha_i) < 1$. Together with (5.2), this implies that $\mathrm{Re}(\alpha_i) \geq -1$ and that there is at most one $i \in S$ with $\mathrm{Re}(\alpha_i) < 0$.

The numerical data of an embedded resolution determine the candidate poles of Igusa's p-adic zeta function. We have determined in complete generality which real candidate poles are actual poles in the curve case.

Capitolul 3

Stadiul actual al cercetării în domeniu

3.1 Introducere

Proprietăţi profunde ale unor obiecte matematice (corpuri de numere algebrice, varietăţi algebrice, algebre, grupuri, etc) sunt codificate de anumite funcţii analitice şi serii formale specifice (funcţii zeta, serii Hilbert, serii Poincaré). Studiul unor astfel de funcţii constituie o temă de mare actualitate a Matematicii contemporane.

Funcţiile zeta locale sunt obiecte matematice relativ noi. Primele teoreme cu caracter general au fost demonstrate între anii 1968-1973. De atunci, şi în special în ultimii 20 ani, au fost obţinute rezultate remarcabile pe aceasta temă. Menţionăm că în ultimii ani problematica legată de funcţia zeta Igusa şi seriile Poincaré asociate unei varietăţi algebrice (analitice) definite peste un corp de numere p-adice a cunoscut o puternică dezvoltare (Igusa, Denef, Veys, Zuniga-Galindo, Segers). Aflat la graniţa dintre teoria numerelor şi geometria algebrică, studiul funcţiei zeta Igusa are un caracter interdisci-

plinar, un rol important în aceste cercetări revenind şi logicii matematice şi teoriei modelelor (în special tehnicilor de eliminare a cuantificatorilor) dar şi aritmeticii.

Obiectivul general al prezentului proiectului de cercetare îl constituie studiul functiei zeta Igusa. Având în vedere importanţa funcţiei zeta Igusa în teoria numerelor, aritmetică, geometria algebrică, algebra combinatorială, teoria aranjamentelor de hiperplane, aplicaţiile acesteia în studiul diverselor probleme din aceste domenii, strânsa legatură dintre calculul funcţiei zeta Igusa şi criprografie la care se adaugă conexiunea între seria Poincaré (şi deci implicit funcţia zeta Igusa) şi cifrurile pe flux, ne-am propus să extindem rezulatele cunoscute pentru funcţia zeta Igusa locala asociată unei curbe şi să determinăm polii funţiei zeta Igusa pentru curbe.

Ţinând cont de relevanţa studiului polilor funcţiei zeta Igusa în comportarea numarului de soluţii al unor congruenţe polinomiale şi de faptul că partea reală a polilor este subiectul Conjecturii monodromiei care a preocupat şi preocupă matematicieni de marca, intenţionăm să determinăm polinoamele omogene pentru care funcţia zeta Igusa acociată are un pol cu partea reală $-2/n$ şi, mai mult, să determinăm polii reali ai funcţiei zeta Igusa locale ataşată curbelor definite peste un corp p-adic.

Pentru un număr prim p, notăm cu $\mathbb{Q}_p$ corpul numerelor p-adice şi cu $\mathbb{Z}_p$ inelul întregilor p-adici.

Funcţia zeta Igusa locală asociată unui polinom $F(x) = F(x_1, \cdots, x_n) \in \mathbb{Z}p[x_1, \cdots, x_n]$ se defineşte ca fiind $Z_F(s) = \int |F(x)|^s |dx|$, integrala dupa x în $(\mathbb{Z}_p)^n$, pentru s număr complex, cu $\Re(s) > 0$, unde cu $|dx|$ am notat măsura Haar pe $(\mathbb{Q}_p)^n$ normalizată astfel încât $(\mathbb{Z}_p)^n$ are masura 1, iar $|x| = p - v(x)$, cu $v(x)$ valuarea p-adică a lui x.

În legatură directă cu numărul de soluţii ale congruenţei $F(x) \equiv 0 \mod p^m$,

$m = 1, 2, 3 \cdots$ apare seria Poincaré (se mai numeşte şi seria Poincaré-Igusa) asociată polinomului $F(x)$ definită ca $P(t) = \sum N_e(p^{-nT})e$, suma dupa $e = 0, 1, .., \infty$, unde $N_0 := 1$, iar pentru e?1, am notat cu N_e cardinalul multimii $\{(x_1, \cdots, x_n) \in (\mathbb{Z}/p^e\mathbb{Z})n | F(x) = 0 \mod p^e\}$. Calcularea seriei Poincaré este echivalentă cu calcularea funcţiei zeta Igusa locale, relaţia de legatură dintre cele două fiind $P(t) = (1 - tZF(s))/(1 - t)$, unde $t = p^s$.

Borevici şi Safarevici au conjecturat raţionalitatea seriei Poincaré P(t) în cartea lor Number Theory publicată în limba rusă ţn 1964 şi apoi în 1966 în limba engleză. Raţionalitatea acesteia a fost demonstrată în 1974, când Igusa a introdus funcţia zeta Igusa locală şi a arătat că aceasta este raţională. Demonstraţia acestui fapt a fost făcută folosind analiză p-adica şi rezoluţia singularităţilor a lui Hironaka în caracteristică 0. O demonstraţie complet diferită a fost dată de contemporanul nostru Jan Denef folosind descompunerea celulară p-adica şi teorema lui Angus Macintyre de eliminare a cuantificatorilor. Pentru a calcula explicit, pentru un polinom dat F, ZF(s) şi a determina polii acestuia este, în cea mai mare parte a cazurilor, o problemă dificilă. O serie de rezultate (le vom menţiona doar pe cele mai importante publicate după anul 2000) au fost obţinute de Igusa în cazul în care F este un invariant al unui spaţiu vectorial preomogen (vezi [J. Igusa, An introduction to the Theory of Local Zeta Functions, AMS, 2002, Teorema 6.3.1, p.91]), la care se adaugă rezultatele lui Jan Denef, Kathleen Hoornaert, Wilson Zuniga-Galingo şi Marcelo Jos Saia în cazul în care F este polinom nedegenerat relativ la poliedrul Newton asociat ([J. Denef, K.Hoornaert, Newton polyhedra and Igusa's local zeta function, J.Number Theory, 89: 31-64, 2001], [Zuniga-Galindo W.A., Local Zeta Functions and Newton Polyhedra, Nagoya Math. J., Vol 172 (2003), 31-58], [Saia M. J., Zuniga-Galindo, W.A., Local Zeta Functions for Curves, Non-degeneracy Conditions and Newton Polygons,

Trans. Amer. Math. Soc. 357 (2005), no. 1, 59-88]), ale lui Margaret Robinson şi Diane Meuser privind calculul funcţiei zeta Igusa pentru curbe eliptice ([D. Meuser, M.Robinson, Igusa Local Zeta Functions of Elliptic Curves, Mathematics of Computation, 71 (2001), no. 238, 815-823]), ale lui Wilson Zuniga-Galingo privind forma explicită a funcţiei zeta Igusa locale pentru aşa-numitele polinoame semi-cvasiomogene ([W.A.Zuniga-Galindo, Igusa's Local Zeta Function of semiquasihomogeneous polynomials, Trans. Amer. Math. Soc. 353 (2001), pp. 3193-3207]), ale lui Dirk Segers referitoare la polii funcţiei zeta Igusa asociata curbelor ([D. Segers, On the smallest poles of Igusa's p-adic zeta functions, Mathematische Zeitschrift 252 (2006), 429-455], [D. Segers, Lower bound for the poles of Igusa's p-adic zeta functions, Mathematische Annalen 336 (2006), 659-669]), la care se adaugă [Denis Ibadula, The Classification of the Non-Degenerated Plane Cubics over Qp From the Point of View of the Associated Igusa Local Zeta Function, Bulletin Mathematique Soc. Sci. Math. Roumanie, Tome 49(97), No.3, 2006, pg 253-277], [Denis Ibadula, The Igusa Zeta Functions of the GL2(Qp)-orbit of Fermat's Binary Form, Contemporary Mathematics, vol. 502, American Mathematical Society, Providence, RI, 2009, 59-72] precum şi rezultatele lui Mircea Mustaţă referitoare la polii funcţiei zeta Igusa asociată unui ideal monomial ([Jason Howald; Mircea Mustata; Cornelia Yuen, On Igusa zeta functions of monomial ideal, Amer. Math. Soc. 135 (2007), 3425-3433]) şi preprintul foarte recent al lui Nero Budur, Morihiko Saito, Sergey Yuzvinsky, On the local zeta functions and the b-functions of certain hyperplane arrangements. Să mai adăugăm aici că unul dintre cele mai importante rezultate în domeniu este formula lui Jan Denef de calcul a funcţiei zeta Igusa locale ZF(s) când F satisface aşa-numitele de "bună-reducere mod p" ("good reduction mod p"), pentru un prim p suficient de mare ([J. Denef, On the degree of Igusa's local

zeta function , Amer.J.Math., 109: 991-1008, 1987]). Metodele de studiu a funcţiei zeta Igusa locală au un caracter interdisciplinar şi se situează la confluenţa dintre teoria numerelor, geometria algebrică, la care se adaugă mai nou şi teoria grupurilor (cele mai importante rezultate în această direcţie sunt cele referitoare la studiului funcţiilor tip zeta Igusa pentru grupuri şi inele infinite - Christopher Voll, Marcus du Sautoy şi studenţii acestora), algebră comutativă (vezi rezultatele lui Mircea Mustata si a colaboratorilor lui) şi aranjamentele de hiperplane (Marcelo Saito, Nero Budur, Morihiko Saito, Sergey Yuzvinsky). Funcţiile zeta Igusa sunt interesante nu numai pentru a lucra cu ele, dar şi pentru că au şi numeroase aplicaţii în teoria numerelor şi, mai mult, din perspectiva soluţiilor pe care le pot oferi în criptografie, una dintre principalele direcţii ale cercetării ştiinţifice economice actuale. Mai mult, polii funcţiei zeta Igusa sunt unei conjecturi foarte interesante (conjectura monodromiei) care a preocupat şi preocupa pe multi matematicieni. Voi prezenta în continuare pe scurt câteva informaţii care să releve caracterul multidisciplinar al abordărilor, dar şi importanţa subiectului propus. Aşa cum am menţionat mai sus, cea mai importantă aplicaţie în teoria numerelor este calculul numărului de soluţii al unor congruenţe polinomiale (codificate de seria Poincaré) care se reduce la calculul funcţiei zeta Igusa locale. La sfârşitul anilor 90, Anshel şi Goldfeld au arătat că există o foarte strânsă legătură între calculul funcţiilor zeta şi criptografie [Anshel, M., and Goldfeld, D., Zeta functions, one-way functions and pseudorandom number generators, Duke Math. J., 88, 2 (1997), 371-390.]. Într-adevăr, cei doi au propus o nouă clasă de candidaţi pentru funcţii one-way având la bază funcţii zeta globale. O funcţie one-way este o funcţie F pentru care pentru fiecare x din domeniul de definiţie al lui F, este usor de calculat F(x), dar pentru aproape toţi y din domeniul lui F, este o problemă intractabilă găsirea unui x

astfel încât y=F(x). Funcţiile one-way au un rol foarte important, atât practic cât şi teoretic, în criptografia modernă. Există o strânsă legatură între seria Poincaré (şi deci implicit funcţia zeta Igusa) şi cifrurile pe flux pe care o vom explica pe scurt în continuare. Pentru orice număr întreg r¿0 şi r elemente fixate qi, i=1,..r, din corpul finit cu pn elemente $\mathbb{F}_p^n$, un LFSR (Linear Feedback Shift Register) de lungime r constă din r celule al căror conţinut iniţial este ai2 $\mathbb{F}_p^n$ — i=1,..r; pentru orice n?r, dacă conţinutul curent al celulelor este (an-1,,an-r), atunci an este determinat prin relaţia de recurenţă an=-? an-i qi, suma făcându-se după i de la 1 la r. Sistemul are drept output elementul cel mai din dreapta al sirului an-r şi shift-eaza toate celule cu o unitate la dreapta, reiniţializând apoi cu an cea mai din stânga celulă. Se ştie de exemplu că seria Poincaré g(x)= ? ai xi, cu suma dupa i?0 asociată unui şir obţinut după procedeul descris mai sus (numită şi funcţia generatoare a şirului) este o funcţie raţională peste $\mathbb{F}_p^n$ de forma g(x)=L(x)/R(x), unde $L(x), R(x) \in \mathbb{F}_p[x]$, deg(R(x))¡r şi că există o corespondenţă bijectivă între LFSR-urile de lungime r cu qr ?0 si funcţiile raţionale de forma L(x)/R(x), cu deg(R(x))=r si deg(L(x))¡r. Legătura dintre seria Poincaré-Igusa şi LSFR este acum evidentă: pentru un număr prim p fixat şi pentru orice număr natural u, aplicaţia Fu,p care asociază fiecarei serii Poincaré-Igusa şirul finit de numere întregi N0, N1,,Nu (cu Ni coeficienţii seriei Poincaré-Igusa) sunt LSFR-uri (sau cifrurilor pe flux) peste Z. Criptografia cu chei simetrice se referă la metode de criptare în care atât trimitorul cât şi receptorul folosesc aceeaşi cheie (sau, mai rar, în care cheile sunt diferite, dar într-o relaţie ce la face uşor calculabile una din cealaltă). Acest tip de criptare a fost singurul cunoscut publicului larg până în 1976 [Whitfield Diffie şi Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644-654.]. Studiul modern al cifrurilor cu

chei simetrice se leagă mai ales de studiul cifrurilor pe blocuri şi al cifrurilor pe flux si al aplicaţiilor acestora. Cifrurile pe flux de date, în contrast cu cele pe blocuri, creează un flux arbitrar de material-cheie, care este combinat cu textul clar, bit cu bit sau caracter cu caracter. Aşa cum am explicat mai sus, într-un cifru pe flux de date, fluxul de ieşire este creat pe baza unei stări interne care se modifică pe parcursul operării cifrului. O serie de matematicieni au obţinut rezultate parţiale în problema determinarii polilor funcţiei zeta Igusa locale ataşată curbelor. Studiul polilor funcţiei zeta Igusa locale prezintă un interes special de studiu atât pentru faptul că influenţează în mod direct numărul de soluţii al congruenţelor polinomiale modulo o putere a unui nŭmar prim p (polii cu partea reală cea mai mare au contribuţtia cea mai mare la coeficienţii Ni ai seriei Poincaré P(t)) cât şi pentru că sunt subiectul unei importante conjecturi din matematica cunoscută sub numele de Conjectura Monodromiei. Această conjectură, formulată pentru prima dată de J.Igusa pentru funcţia zeta Igusa locală şi apoi extinsă de Denef şi Loeser pentru funcţia zeta topologică asocită unei hipersuprafeţe şi, mai recent, pentru aranjamente de hiperplane, afirmă o remarcabilă legătură între proprietăţi din sfera teoriei numerelor şi proprietăţi geometrice/topologice asociate unui polinom. Pe scurt, Conjectura Monodromiei afirmă că dacă s0 este pol al funcţiei zeta locale topologice asociată unei hipersuprafeţe (se include aici şi cazul funcţiei zeta Igusa locale), atunci exp(2?is0) este o valuare proprie a monodromiei coomologiei fibrei Milnor. Forma tare a conjecturii spune că partea reală a oricarui pol al funcţiei zeta Igusa locală asociată unui polinom F este rădăcină a polinomului Bernstein-Sato (b-polinomului) b_F asociat polinomului F Această conjectură a suscitat de-a lungul timpului interesul multor matematicieni, dintre care menţionăm doar rezultatele cele mai recente: demonstrarea conjecturii în cazul funcţiei zeta Igusa asociată

unui ideal monomial (Jason Howald; Mircea Mustata; Cornelia Yuen, On Igusa zeta functions of monomial ideal, Amer. Math. Soc. 135 (2007), 3425-3433), demonstrarea conjecturii în forma ei slabă pentru cazul funcţiei zeta locale topologice asociată aranjamentelor de hiperplane (Nero Budur, Mircea Mustaţă Zach Teitler, The Monodromy Conjecture for Hyperplane Arrangements, preprint 2010) la care se adaugă un al preprint extrem de recent Nero Budur, Morihiko Saito, Sergey Yuzvinsky, On the local zeta functions and the b-functions of certain hyperplane arrangements, în care autorii demonstrează conjectura în forma ei tare pentru anumite aranjamente de hiperplane, inclusiv pentru cazul aranjamentelor reduse de hiperplane în spaţiul afin 3-dimensional. Iniţial, în studiul polilor funcţiei zeta Igusa locale, au fost considerate curbe absolut analitic ireductibile (adică curbe ireductibile în Qpalgcl[[x1,x2]]). Rezultate parţiale au fost obţinute de Igusa ([J. Igusa, On the first terms of certain asymptotic expansions, Complex Analysis and Algebraic Geometry, Iwanami Shoten (1977), 357-368]) si Strauss ([L. Strauss, Poles of a two-variable p-adic complex power, Trans. Amer. Math. Soc. 278, 1983, 481-493]). Diane Meuser ([D. Meuser, On the Poles of a Local Zeta Function for Curves, Invent. Math. 73 (1983), 445-465]). În 1985 Igusa ([J. Igusa, Complex powers of irreducible algebroid curves, Geometry today, Roma 1984, Progress in Math. 60, Birkhauser, 1985, pp. 207-230]) a rezolvat complet problema pentru o curbă F absolut analitic ireductibilă. El a demonstrat că potenţialii poli asociaţi unei transformări stricte ale lui F sunt poli atunci când domeniul de integrare este suficient de mic. De asemenea, un alt posibil pol asociat unei rezoluţii minimale scufundate (minimal embedded resolution) asociate lui F este pol dacă şi numai dacă polul este asociat unei curbe exceptionale (exceptional curve) care se intersectează cu alte trei componente ireductibile ale pull-back-ului lui F. Pentru cazul gen-

eral al unui polinom arbitrar F în două nedeterminate, Loeser (F. Loeser, Fonctions d'Igusa p-adiques et polynomes de Bernstein, Amer. J. Math. 110, (1988), 1-21) a demonstrat că o curbă excepţională Ei nu contribuie la polii funcţiei zeta Igusa locale ZF(s) dacă Ei se intersectează o dată sau de două ori cu alte componente ale pull-back-ului lui F şi dacă nu există alte puncte de intersecţie într-o închidere algebrică arbitrară. Acest rezultat a fost demonstrat şi de Strauss în cazul absolut analitic ireductibil, caz în care ultima condiţie este automat satisfăcută. Un alt rezultat remarcabil în acestă direcţie este datorat lui Wim Veys (W. Veys, On the poles of Igusa's local zeta function for curves, J. London Math. Soc. 41 (1990), 27-32). Acesta a considerat un polinom F în două variabile peste un corp de numere (number field??) K şi o rezoluţie minimală a lui F peste o închidere algebrică a lui K. Situarea în acest context i-a permis să folosească o formulă a lui Denef (J. Denef, On the degree of Igusa's local zeta function, Amer. J. Math. 109 (1987), 991-1008.) care se poate aplica pentru aproape toţi completaţii p-adici ai corpului K şi pentru polinoame F cu "bună reducere mod p". În aceste ipoteze, Veys a determinat polii funcţiei zeta Igusa pentru orice număr prim p suficient de mare folosind urmatoarea construcţie. Fie K o extindere de grad finit a lui Qp, F(x)=F(x1,,xn) un polinom în n variabile din K[x], fie : $X \to K^n$ o rezoluţie scufundată (embedded resolution) pentru F=0 astfel încat ? este proiectivă şi ?-1(F-1(0)) are numai intersecţii normale (normal crossing) în X (existenţa (X, ?) este asigurată de teorema lui Hironaka referitoare la existenţa unei rezoluţii a singularităţilor ??). Fie (Nj,?j), cu j2T caracteristicile numerice asociate resolutiei (X, ?) a lui F. Cu aceste notaţii, un rezultat cunoscut în domeniul următor: din demonstraţia dată de Igusa raţionalităţii funcţiei zeta Igusa locale folosind teorema lui Hironaka de existenţă a unei rezoluţii a singularităţilor că o compunere de blowing-up-

uri, rezultă ca orice posibil pol real al lui $Z_F(s)$ poate fi exprimat sub forma s0=-?j/Nj, cu j2T. Vom numi această listă drept lista posibililor poli reali ai funcţiei zeta Igusa locale. Pentru determinarea polilor lui ZF(s) Veys a eliminat din acestă listă falşii posibili poli folosind pentru calculul funcţiei zeta Igusa locale formula lui Jan Denef de calcul a funcţiei zeta Igusa pentru polinoame cu o "bună reducere mod p" ("good reduction mod p") şi pentru un prim p suficient de mare.

3.2 Inelul $\mathbb{Z}_p$ si corpul $\mathbb{Q}_p$

3.2.1 Definiţii generale

Fie p un număr prim fixat. Pentru orice n număr natural $n \geq 1$ fie $A_n := \mathbb{Z}/p^n\mathbb{Z}$ inelul claselor de resturi $\mod p^n$. Unui element din A_n ii asociem un element din A_{n-1} prin aplicaţia

$$\begin{aligned} \phi_n : A_n &\to A_{n-1} \\ \phi_n(x \mod p^n) &= x \mod p^{n-1}, \end{aligned}$$

care este un morfism surjectiv de inele având nucleul $p^{n-1}A_n$.

Şirul

$$... \to A_n \to A_{n-1} \to ... \to A_2 \to A_1$$

formează un sistem proiectiv de inele comutative unitare indexat de întregi ≥ 1.

Definiţia 3.1. ***Inelul intregilor*** p***-adici*** $\mathbb{Z}_p$ *este limita proiectivă a sistemului proiectiv* $(A_n, \phi_n)_{n\geq 1}$ *definit mai sus.*

Prin definiţie, un element din $\mathbb{Z}_p = \varprojlim_{n\geq 1}(A_n, \phi_n)$ este un şir $x = (x_n)_{n\geq 1}$, cu $x_n \in A_n$ si $\phi_n(x_n) = x_{n-1}$, pentru $n \geq 2$. Adunarea şi înmulţirea în $\mathbb{Z}_p$ se definesc pe componente: dacă $x, y \in \mathbb{Z}_p$, cu $x = (x_n)_{n\geq 1}$ si $y = (y_n)_{n\geq 1}$, atunci

$$\begin{aligned} x + y : &= (x_n + y_n)_{n\geq 1} \in \mathbb{Z}_p \\ x \cdot y : &= (x_n \cdot y_n)_{n\geq 1} \in \mathbb{Z}_p. \end{aligned}$$

Prin urmare, $\mathbb{Z}_p$ este un subinel al inelului produs $\prod_{n\geq 1} A_n$.

3.2.2 Proprietăţile inelului $\mathbb{Z}_p$

Fie $\epsilon_n : \mathbb{Z}_p \to A_n$ proiecţia canonică: ϵ_n asociază unui întreg p-adic $x = (x_n)_{n\geq 1}$ componenta sa de pe poziţia n, x_n.

Propoziţia 3.2. *Pentru orice $n \geq 1$, sirul*

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} A_n \to 0,$$

este un şir exact de grupuri abeliene, unde aplicaţia $\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p$ este multiplicarea cu p^n. În particular,

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Demonstraţie: Înmulţirea cu p (prin urmare şi înmulţirea cu p^n) este o aplicaţie injectivă în $\mathbb{Z}_p$. Într-adevăr, dacă $x = (x_n)_{n\geq 1}$ este un întreg p-adic astfel încât $px = 0$, rezulta ca $px_{n+1} = 0$ pentru orice n din $\mathbb{N}$ si x_{n+1} este de forma $p^n y_{n+1}$, cu $y_{n+1} \in A_{n+1}$. Din $x_n = \phi_{n+1}(x_{n+1})$ rezulta ca x_n este divizibil cu p^n si, prin urmare, este zero.

Morfismul ϵ_n este, în mod evident, surjectiv. Să mai verificăm că nucleul lui ϵ_n coincide cu imaginea lui $\mathbb{Z}_p$ prin prima aplicaţie, adică cu $p^n\mathbb{Z}_p$. Este clar că nucleul lui ϵ_n conţine $p^n\mathbb{Z}_p$; reciproc, dacă $x = (x_n)_{n\geq 1}$ este un element din $ker(\epsilon_m)$, rezultă că $x_m \equiv 0 \mod p^n$, pentru orice $m \geq n$, ceea ce înseamnă că există un element y_{m-n} in A_{m-n} astfel încât imaginea sa prin izomorfismul $A_{m-n} \to p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ satisface $x_m \equiv p^n \mod y_{m-n}$. y_i defineşte astfel un element y din $\mathbb{Z}_p = \varprojlim A_i$ şi se verifică imediat ca $p^n y = x$, ceea ce incheie demonstraţia propoziţiei. □

Propoziţia 3.3. ***a)*** *Un element din $\mathbb{Z}_p$ (respectiv A_n) este inversabil daca si numai daca nu este divizibil cu p.*
b) *Dacă notăm cu U grupul elementelor inversabile din $\mathbb{Z}_p$ (i.e. $U = \mathbb{Z}_p^\times$) atunci orice element nenul din $\mathbb{Z}_p$ poate fi scris în mod unic sub forma $p^n u$, cu $u \in U$ si $n \geq 0$. (Un element din U se numeşte* ***unitate p-adica****).*

Demonstraţie: **a)** Este suficient să verificăm a) pentru A_n, afirmaţia pentru $\mathbb{Z}_p$ rezultând imediat din acesta. Fie $x \in A_n$ un element care nu se gaseşte în pA_n. Atunci imaginea sa în $A_1 = \mathbb{F}_p$ este un element inversabil (fiind diferit de zero): exista $y, z \in A_n$ astfel încât $xy = 1 - pz$, de unde

$$xy(1 + pz + ... + p^{n-1}z^{n-1}) = 1,$$

ceea ce arată că x este inversabil.

b) Pe de altă parte, dacă $x \in \mathbb{Z}_p$ este diferit de zero, există un cel mai mare numar natural n astfel încât $x_n = \epsilon_n(x)$ este zero. Atunci $x = p^n u$ si u nu este divizibil cu p, adica $u \in U$, conform cu a). Unicitatea scrierii este clară. □

Notaţie: Fie x un element din $\mathbb{Z}_p$ diferit de zero care se scrie sub forma $x = p^n u$, cu $u \in U$. Numărul natural n se numeşte **valuarea p-adică a lui**

x şi se notează $v_p(x)$.

Prin convenţie, $v_p(0) = +\infty$. Sunt adevarate relaţiile:

$$\begin{aligned} v_p(xy) &= v_p(x) + v_p(y), \\ v_p(x+y) &\geq min\left\{v_p(x), v_p(y)\right\}. \end{aligned}$$

Din aceste formule rezultă imediat că $\mathbb{Z}_p$ este un domeniu de integritate.

Propoziţia 3.4. *Idealele proprii ale inelului $\mathbb{Z}_p$ sunt idealele de forma $p^n\mathbb{Z}_p$, cu $n \in \mathbb{N}_{\geq 1}$.*

Demonstraţie: Fie $\underline{a}$ un ideal propriu al lui $\mathbb{Z}_p$ si x un element nenul din $\underline{a}$ de forma $p^n u$, cu $u \in U$ astfel încât $v_p(x) = n$ este minimă. Vom arăta că $\underline{a} = p^n\mathbb{Z}_p$.

Incluziunea $p^n\mathbb{Z}_p \subseteq \underline{a}$ este clară. Reciproc, fie y un element din idealul $\underline{a}$ de forma $p^m z$, cu $z \in U$. Atunci, deoarece $m \geq n$, y se poate scrie sub forma $y = p^n(p^{m-n}z) \in p^n\mathbb{Z}_p$, ceea ce încheie demonstraţia propoziţiei.

□

Propoziţia 3.5. *Topologia pe $\mathbb{Z}_p$ se defineşte prin distanţa*

$$d(x,y) := p^{-v_p(x-y)}.$$

Inelul $\mathbb{Z}_p$ este un spaţiu metric complet în care $\mathbb{Z}$ este dens.

Demonstraţie: Idealele $p^n\mathbb{Z}_p$ formează o bază de vecinătăţi a lui 0. Deoarece $x \in p^n\mathbb{Z}_p$ este echivalent cu faptul că $v_p(x) \geq n$, topologia pe $\mathbb{Z}_p$ este definită prin distanţa $d(x,y) := p^{-v_p(x-y)}$. Deoarece $\mathbb{Z}_p$ este compact, este complet. De asemenea, dacă $x = (x_n)_{n\geq 1}$ este un element din $\mathbb{Z}_p$, şi dacă $y_n \in \mathbb{Z}$ astfel încât $y_n \equiv x_n \mod p^n$, atunci $lim\ y_n = x$, ceea ce arată că $\mathbb{Z}$ este dens în $\mathbb{Z}_p$. □

3.2.3 Corpul $\mathbb{Q}_p$

Definiţia 3.6. ***Corpul numerelor p-adice****, notat cu $\mathbb{Q}_p$, este corpul de fracţii al lui inelului $\mathbb{Z}_p$.*

Se observă că $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$. Orice element x din $\mathbb{Q}_p^\times$ poate fi scris în mod unic sub forma $p^n u$, cu $n \in \mathbb{Z}$, $u \in U$. Aici n se numeşte **valuarea p-adica** a lui x şi se notează $v_p(x)$. Dacă $v_p(x) \geq 0$, atunci x se gaseşte în $\mathbb{Z}_p$. Altfel, dacă $v_p(x)$ este număr negativ,

$$v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0,$$

ceea ce arată că $p^{-v_p(x)}x \in \mathbb{Z}_p$.

Propoziţia 3.7. *Corpul $\mathbb{Q}_p$, cu topologia definită de $d(x,y) := p^{-v_p(x-y)}$, este local compact şi $\mathbb{Z}_p$ este un subinel al său. Corpul $\mathbb{Q}$ este dens în $\mathbb{Q}_p$.*

Demonstraţie: Evident. □

Observaţia 3.8. *Se mai poate defini $\mathbb{Q}_p$ (respectiv $\mathbb{Z}_p$) ca fiind completatul lui $\mathbb{Q}$ (respectiv $\mathbb{Z}$) în raport cu distanţa p-adică d.*

3.3 Grupul multiplicativ al corpului $\mathbb{Q}_p$

Pentru a descrie tipurile de izomorfism peste $\mathbb{Q}_p$ ale formelor cubice binare peste $\mathbb{Q}_p$ avem nevoie, pentru început, de structura grupului multiplicativ $\mathbb{Q}_p^*$.

3.3.1 Filtrarea grupului unitaţilor

Fie $U := \mathbb{Z}_p^*$ grupul unitaţilor p-adice. Pentru $n \geq 1$, notăm cu U_n următorul subgrup al lui U:

$$U_n := 1 + p^n\mathbb{Z}_p := \{1 + p^n x | x \in \mathbb{Z}_p\}.$$

Sa remarcăm faptul că U_n este nucleul morfismului de grupuri

$$\begin{aligned} \epsilon_n : U &\to (\mathbb{Z}/p^n\mathbb{Z})^* \\ \epsilon_n(u) &\equiv u \mod p^n\mathbb{Z}_p, \text{ pentru orice } u \in U. \end{aligned}$$

În particular, pentru $n = 1$, obţinem şirul exact:

$$1 \to U_1 \to U \xrightarrow{\epsilon_1} (\mathbb{Z}/p\mathbb{Z})^* \to 1;$$

prin urmare, $U/U_1 \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ este un grup ciclic de ordin $p-1$.

Subgrupurile U_n, pentru $n \geq 1$, formează un şir descrescător de subgrupuri deschise ale lui U:

$$U := U_0 \geq U_1 \geq U_2 \geq ... \geq U_n \geq ...,$$

iar $U = \varprojlim_{n\geq 1} U/U_n$, întrucât

$$U = \mathbb{Z}_p^* = \left(\varprojlim_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}\right)^* \cong \varprojlim_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^* \cong \varprojlim_{n\geq 1} U/U_n.$$

Propoziţia 3.9. *Cu notaţiile de mai sus, pentru orice $n \geq 1$, aplicaţia:*

$$\begin{aligned} U_n &\to \mathbb{Z}/p\mathbb{Z} \\ 1 + p^n x &\mapsto x \mod p, \quad \forall x \in \mathbb{Z}_p, \end{aligned}$$

induce izomorfismul

$$U_n/U_{n+1} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}.$$

Demonstraţie: Pentru x si x_2 in $\mathbb{Z}_p$,

$$(1+p^n x)(1+p^n x_2) = 1 + p^n(x+x_2) + p^{2n} x x_2 \equiv 1 + p^n(x+x_2) \mod p^{n+1},$$

întrucât $2n \geq n+1$.

Morfismul este surjectiv, iar nucleul său este, în mod evident, U_{n+1}. □

Corolar 3.10. *Pentru orice $n \geq 1$, grupul factor U_1/U_n are ordinul p^{n-1}.*

Demonstraţie: Inducţie după n.Pentru $n = 1$ afirmaţia este verificată. Să presupunem că $(U_1 : U_n) = p^{n-1}$. Cum

$$U_{n+1} \leq U_n \leq U_1,$$

rezultă, ţinând cont şi de propoziţia precedentă, că

$$(U_1 : U_{n+1}) = (U_1 : U_n) \cdot (U_n : U_{n+1}) = p^{n-1} \cdot p = p^n$$

□

Lema 3.11. *Fie*

$$0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0$$

un şir exact de grupuri abeliene finite (notate aditiv), cu $(A : 0) = a$, $(B : 0) = b$ si $(a, b) = 1$.

Fie B' mulţimea acelor $x \in E$ pentru care $bx = 0$.

Atunci grupul E este suma directă a grupurilor A si B'. Mai mult, B' este unicul subgrup al lui E izomorf cu B.

Demonstraţie: Deoarece a si b sunt prime între ele, exista $r, s \in \mathbb{Z}$ astfel incat $ar + bs = 1$. Fie acum $x \in A \cap B'$; rezulta ca $ax = bx = 0$. Atunci

$$x = 1 \cdot x = (ar + bs)x = arx + bsx = 0,$$

deci $A \cap B^{'} = 0$. De asemenea,

$$x = 1 \cdot x = \underbrace{bsx}_{\in A} + \underbrace{arx}_{\in B'} :$$

din $bB^{'} = 0$, rezulta $bE \subset A$, deci $bsx \in A$; pe de altă parte, din $barx = 0$, obţinem $arx \in B^{'}$. Am demonstrat astfel că $E = A \oplus B^{'}$.

Este clar faptul că $B^{'}$ este un subgrup al lui E izomorf cu B. Să arătăm că este singurul. Fie $B^{''}$ un alt subgrup al lui E izomorf cu B. Atunci $bB^{''} = 0$ şi deci $B^{''} \subset B^{'}$. Dar $B^{'}$ si $B^{''}$, fiind ambele izomorfe cu B, au acelaşi cardinal. Rezulta $B^{''} = B^{'}$. □

Propoziţia 3.12. *Pentru $U := \mathbb{Z}_p^*$ si $U_1 = 1 + p\mathbb{Z}_p$, avem:*

$$U = V \times U_1,$$

unde $V = \{x \in U | x^{p-1} = 1\}$ este unicul subgrup al lui U izomorf cu $\mathbb{F}_p^*$.

Demonstratie: Pentru a demonstra acestă propoziţie, vom aplica lema precedentă şirului exact:

$$0 \longrightarrow U_1/U_n \longrightarrow U/U_n \longrightarrow \mathbb{F}_p^* \longrightarrow 0,$$

lucru care este posibil datorită faptului că ordinul lui U_1/U_n este p^{n-1}, ordinul lui $\mathbb{F}_p^*$ este $p-1$ si $(p^{n-1}, p-1) = 1$. Conform lemei, $V_n = \{x \in U/U_n | x^{p-1} = 1\}$ este unicul subgrup al lui U/U_n izomorf cu $\mathbb{F}_p^*$. Proiecţia $U/U_{n+1} \twoheadrightarrow U/U_n$ duce V_{n+1} în V_n. Fie $V := \varprojlim_{n \geq 1} V_{n+1} = \{x \in U | x^{p-1} = 1\}$. Cum $U = \varprojlim_{n \geq 1} U/U_n$ obţinem, prin trecere la limită, că V este unicul subgrup al lui U izomorf cu $\mathbb{F}_p^*$. Rezultă că $U = V \times U_1$, iar unicitatea lui V rezultă din unicitatea lui V_n. □

Din teorema precedentă rezultă imediat următorul corolar:

Corolar 3.13. *Corpul $\mathbb{Q}_p$ conţine rădăcinile unităţii de ordin $p-1$.*□

Definiţia 3.14. *Grupul* $V = \{x \in U | x^{p-1} = 1\}$ *se numeşte* ***grupul reprezentanţilor lui*** $\mathbb{F}_p^*$ ***in*** $\mathbb{Q}_p^*$.

3.3.2 Structura grupului $U_1 := 1 + p\mathbb{Z}_p$

Lema 3.15. *Fie* $x \in U_n - U_{n+1}$ *cu* $n \geq 1$, *dacă* $p \neq 2$ *şi* $n \geq 2$, *dacă* $p = 2$. *Atunci* $x^p \in U_{n+1} - U_{n+2}$.

Demonstraţie: Deoarece $x \in U_n - U_{n+1}$, rezulta ca $x = 1 + p^n x_2$, cu $x_2 \in \mathbb{Z}_p - p\mathbb{Z}_p$. Să calculăm x^p:

$$x^p = (1 + p^n x_2)^p = 1 + \begin{pmatrix} p \\ 1 \end{pmatrix} p^n y + \sum_{i=2}^{p-1} \begin{pmatrix} p \\ i \end{pmatrix} p^{ni} y^i + p^{np} y^p.$$

Exponentul lui p din fiecare termen al sumei $\sum_{i=2}^{p-1} \begin{pmatrix} p \\ i \end{pmatrix} p^{ni} y^i$ este $\geq 2n+1$, deci $\geq n+2$. Dar şi $np \geq n+2$ (datorită faptului că $n \geq 2$ pentru $p = 2$); rezultă atunci că

$$x^p \equiv 1 + p^{n+1} y (mod\ p^{n+2}),$$

deci $x^p \in U_{n+1} - U_{n+2}$. □

Propoziţia 3.16. ***1)*** *Dacă* $p \neq 2$, *atunci* U_1 *este izomorf cu* $\mathbb{Z}_p$.

2) *Dacă* $p = 2$, *atunci* $U_1 = \{\pm 1\} \times U_2$ *şi* U_2 *este izomorf cu* $\mathbb{Z}_2$.

Demonstraţie: **1)** Fie pentru început p un număr prim, $p \neq 2$ şi α un element din $U_1 - U_2$, de exemplu $\alpha = 1 + p$.

Din lema precedentă, avem $\alpha^p \in U_2 - U_3$ şi, inductiv, obţinem $\alpha^{p^n} \in U_{n+1} - U_{n+2}$, pentru orice $n \geq 1$.

Notând cu $\alpha_n := \alpha \mod U_n$, $\alpha_n \in U_1/U_n$ pentru $n \geq 1$, observăm că $\alpha^{p^{n-1}} = 1$ şi $\alpha^{p^{n-2}} \neq 1$. Dar ştim că $(U_1 : U_n) = p^{n-1}$; rezultă că U_1/U_n este

un grup ciclic generat de α_n. Morfismul surjectiv

$$\begin{aligned} \mathbb{Z} &\twoheadrightarrow U_1/U_n \\ i &\mapsto \alpha_n^i \end{aligned}$$

are nucleul $p^{n-1}\mathbb{Z}$; să notăm cu $\varphi_{n,\alpha} : \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$ izomorfismul indus de acesta.

Deoarece diagrama:

$$\begin{array}{ccccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\varphi_{n+1,\alpha}} & U_1/U_{n+1} & \longleftarrow & U_1 \\ & \searrow & \downarrow & & \downarrow & \swarrow & \\ & & \mathbb{Z}/p^{n-1}\mathbb{Z} & \xrightarrow{\varphi_{n,\alpha}} & U_1/U_n & & \end{array}$$

este comutativă, rezultă că familia de izomorfisme $(\varphi_{n,\alpha})_{n\geq 1}$ este coerentă. Prin urmare, $\varphi_n := \varprojlim_{n\geq 1} \varphi_{n,\alpha}$ defineşte un izomorfism

$$\varphi_\alpha : \varprojlim_{n\geq 1} \mathbb{Z}/p^{n-1}\mathbb{Z} \to \varprojlim_{n\geq 1} U_1/U_n,$$

adică de la $\mathbb{Z}_p = \varprojlim_{n\geq 1} \mathbb{Z}/p^{n-1}\mathbb{Z}$ in $U_1 = \varprojlim_{n\geq 1} U_1/U_n$.

2) Fie un $\alpha \in U_2 - U_3 := (1+4\mathbb{Z}_2) - (1+8\mathbb{Z}_2)$, de forma $\alpha = 1+4x$, unde x nu este multiplu de 2 in $\mathbb{Z}_2$; rezulta $x \equiv 1 \mod 2$ şi deci $\alpha \equiv 5 \mod 8$.

Folosind Lema 3.15, obţinem inductiv $\alpha^{2^n} \in U_{n+2} - U_{n+3}$, pentru $n \geq 1$. Ca şi în cazul precedent, notând $\alpha_n := \alpha(mod\ U_n) \in U_2/U_n$, pentru $n \geq 2$, obţinem că U_2/U_n este un grup ciclic de ordin 2^{n-2} generat de α_n.

Fie $\varphi_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to U_2/U_n$ izomorfismul indus de $\mathbb{Z} \to U_2/U_n$, $i \in \mathbb{Z} \mapsto \alpha_n^i$; familia de morfisme $(\varphi_{n,\alpha})_{n\geq 2}$ este coerenta, i.e. diagrama

$$\begin{array}{ccccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/2^{n-1}\mathbb{Z} & \xrightarrow{\varphi_{n+1,\alpha}} & U_2/U_{n+1} & \longleftarrow & U_2 \\ & \searrow & \downarrow & & \downarrow & \swarrow & \\ & & \mathbb{Z}/2^{n-2}\mathbb{Z} & \xrightarrow{\varphi_{n,\alpha}} & U_2/U_n & & \end{array}$$

este comutativă, pentru $n \geq 2$. Rezultă că $\varphi_n := \varprojlim_{n\geq 1} \varphi_{n,\alpha}$ defineste un izomorfism de la $\mathbb{Z}_p$ in U_2:

$$\varphi_\alpha : \underbrace{\varprojlim_{n\geq 2} \mathbb{Z}/2^{n-2}\mathbb{Z}}_{\cong \mathbb{Z}_p} \to \underbrace{\varprojlim_{n\geq 2} U_2/U_n}_{\cong U_2}.$$

Pe de altă parte, morfismul surjectiv

$$\begin{aligned} U_1 := 1 + 2\mathbb{Z}_2 &\to (\mathbb{Z}/2\mathbb{Z}, +) \to 0 \\ 1 + 2x &\mapsto x \mod 2\mathbb{Z}_2 \end{aligned}$$

are nucleul U_2. Deci, avem şirul exact:

$$1 \to U_2 \to U_1 \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

de unde obţinem:

$$U_1 = U_2 \times \{1, -1\} \cong U_2 \times \mathbb{Z}/2\mathbb{Z}.$$

□

3.3.3 Structura grupului multiplicativ $\mathbb{Q}_p^*$

Vom formula şi demonstra urmatoarea teoremă de structură a grupului multiplicativ al corpului $\mathbb{Q}_p$, $\mathbb{Q}_p^*$.

Teorema 3.17 (Teorema de structura a lui $\mathbb{Q}_p^*$)**.** *Grupul multiplicativ $\mathbb{Q}_p^*$ este izomorf cu $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, dacă $p \neq 2$ şi cu $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, dacă $p = 2$.*

Demonstraţie: Orice element $x \in \mathbb{Q}_p^*$ se poate scrie, în mod unic, sub forma $x = p^n u$, unde $n = v_p(x) \in \mathbb{Z}$ si $u \in U$. Prin urmare,

$$\mathbb{Q}_p^* \cong < p > \times U \cong (\mathbb{Z}, +) \times U.$$

Dar din Propoziţia 3.12, $U \cong V \times U_1$, unde V este ciclic de ordin $p-1$, deci izomorf cu $\mathbb{Z}/(p-1)\mathbb{Z}$. Prin urmare,

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times V \times U_1,$$

şi teorema rezultă acum din Propoziţia 3.16. □

3.3.4 Patrate în $\mathbb{Q}_p^*$

Teorema 3.18. *Fie p un număr prim, $p \neq 2$ şi fie $x = p^n u$ un element din $\mathbb{Q}_p^*$, cu $n \in \mathbb{Z}$ şi $u \in U$.*

Atunci $x \in \mathbb{Q}_p^{*2}$, i.e. elementul x este pătrat, dacă şi numai dacă n este par şi $\bar{u} := u \mod U_1$ este patrat, i.e. $\left(\begin{array}{c} \bar{u} \\ p \end{array}\right) = 1$ (simbolul Legendre al lui $\bar{u}$ este 1).

Demonstraţie: Fie $u = v \cdot u_1$, cu $v \in V$ si $u_1 \in U_1$. Deoarece

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times V \times U_1,$$

rezulta ca x este patrat daca si numai daca n este par si v si u_1 sunt patrate. Numărul prim p fiind diferit de 2, U_1 este izomorf cu $\mathbb{Z}_p$ si 2 este inversabil în $\mathbb{Z}_p$; prin urmare, toate elementele lui U_1 sunt pătrate, i.e. $U_1 = U_1^2$. Pe de altă parte, conform Propoziţiei 3.12, V este izomorf cu $\mathbb{F}_p^*$ şi teorema este acum demonstrată. □

Corolar 3.19. *Dacă p este un număr prim diferit de 2, atunci*

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

iar un sistem de reprezentanţi este $\{1, p, u, up\}$, cu $u \in U$ astfel incat $u \mod U_1 \notin \mathbb{F}_p^{*2}$.

Demonstraţie: Din Teorema 3.17 de structura a lui $\mathbb{Q}_p^*$ şi teorema precedentă, obţinem:

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \frac{\mathbb{Z}\times V\times U_1}{2\mathbb{Z}\times V^2\times U_1^2} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}\times\frac{\mathbb{F}_p^*}{\mathbb{F}_p^{*2}}\times\frac{U_1}{U_1} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

deoarece $(p,2)=1$. Cum ultima parte a enunţului este evidentă, corolarul este demonstrat. □

Teorema 3.20. *Un element $x=p^nu$ din $\mathbb{Q}_2^*$ este pătrat daca si numai daca n este par şi $u\equiv 1 \mod 8$.*

Demonstraţie: Deoarece $U=U_1\cong\{\pm1\}\times U_2$, $u\in U$ este pătrat daca si numai daca $u\in U_2$ şi este pătrat in U_2. Ţinând cont acum de faptul că $U_2^2=U_3$, obţinem că $u\in U$ este patrat daca si numai daca $u\equiv 1 \mod 8$, ceea ce incheie demonstraţia teoremei. □

Corolar 3.21. $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, *iar un sistem de reprezentanţi este* $\{\pm1,\pm5,\pm2,\pm10\}$.

Demonstraţie: Din teorema precedentă, obţinem:

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}\cong\frac{\mathbb{Z}\times U}{2\mathbb{Z}\times U_3}\cong\mathbb{Z}/2\mathbb{Z}\times U/U_3.$$

Din $U\cong\{\pm1\}\times U_2$ rezulta ca

$$U/U_3\cong\frac{\{\pm1\}\times U_2}{U_3}\cong\{\pm1\}\times U_2/U_3\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

de unde

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

Un sistem de reprezentanţi în $\mathbb{Q}_2^*$ pentru clasele modulo $\mathbb{Q}_2^{*2}$ este constituit deci din $\{\pm1,\pm5,\pm2,\pm10\}$ ($\{\pm1,\pm5\}$ este un sistem de reprezentanţi pentru U/U_3). □

3.4 Lema lui Hensel şi aplicaţii

Teorema cunoscută drept "*Lema lui Hensel*" este una dintre cele mai importante proprietăţi algebrice ale numerelor p-adice.

Teorema 3.22. ***("Lema lui Hensel")*** *Fie $f(x)$ un polinom într-o variabilă x cu coeficienţi în $\mathbb{Z}_p$ şi $k \in \mathbb{N}\setminus\{0\}$. Fie $a \in \mathbb{Z}_p$ astfel incat $f(a) \equiv 0 \mod p^k$ şi $f^{'}(a) \not\equiv 0 \mod p$, unde $f^{'}(x)$ este derivata lui $f(x)$.*

Atunci exista un unic $\xi \in \mathbb{Z}_p$ astfel incat

$$f(\xi) = 0 \text{ şi } \xi \equiv a \mod p^k.$$

Demonstraţie: Vom demonstra teorema pentru $k = 1$. Cazul $k > 1$ rezultă din cazul $k = 1$ aplicat polinomului $g(y) = p^{-(k-1)} f(a + p^{k-1}y)$, care are coeficienţii în $\mathbb{Z}_p$ deoarece $f(a) \equiv 0 \mod p^k$.

Pentru $k = 1$, vom demonstra existenţa rădăcinii ξ construind un şir Cauchy care converge către ξ (idee cunoscută sub numele de "*metoda lui Newton*"). Şirul $\alpha_1 = a$, α_2,...,α_n,... pe care îl vom construi va avea, pentru orice $n \geq 1$, urmatoarele proprietăţi: *i)*$f(\alpha_n) \equiv 0 \mod p^n$;

ii)$\alpha_n \equiv \alpha_{n+1} \mod p^n$.

Este clar că un astfel de şir este Cauchy şi limita sa satisface $f(\xi) = 0$ (din continuitate) şi $\xi \equiv a \mod p$ (din construcţie). Prin urmare, dacă construim un şir $(\alpha_n)_{n\geq 1}$ cu cele două proprietăţi de mai sus, teorema este demonstrată.

Fie acum $\alpha_1 = a$. Pentru a determina α_2, din condiţia *ii)*, rezulta ca trebuie să avem $\alpha_2 = \alpha_1 + b_1 p$, cu $b_1 \in \mathbb{Z}_p$. Înlocuind în $f(x)$ şi dezvoltând în serie Taylor, obţinem:

$$\begin{aligned} f(\alpha_2) &= f(\alpha_1 + b_1 p) = \\ &= f(\alpha_1) + f^{'}(\alpha_1) b_1 p + \text{termeni in } p^n,\ n \geq 2 \\ &\equiv f(\alpha_1) + f^{'}(\alpha_1) b_1 p \mod p^2. \end{aligned}$$

Aşadar, pentru a arata că exista un α_2 cu proprietăţile cerute, trebuie să demonstrăm că exista un b_1 astfel incat $f(\alpha_1) + f'(\alpha_1)b_1 p \equiv 0 \mod p^2$. Deoarece $f(\alpha_1) \equiv 0 \mod p$, $f(\alpha_1) = px$, cu $x \in \mathbb{Z}_p$ şi ecuaţia precedentă devine $px + f'(\alpha_1)b_1 p \equiv 0 \mod p^2$, adică $x + f'(\alpha_1)b_1 \equiv 0 \mod p$. Nefiind divizibil cu p, $f'(\alpha_1)$ este element inversabil în $\mathbb{Z}_p$ şi deci putem lua $b_1 \equiv -x(f'(\alpha_1))^{-1} \mod p$. (De fapt, putem alege $b_1 \in \mathbb{Z}$, cu $0 \leq b_1 \leq p-1$). Obţinem astfel $\alpha_2 = \alpha_1 + b_1 p$ care are proprietăţile cerute.

Am demonstrat în acest fel primul pas: dat α_1, am determinat α_2. Analog, construim înterg şirul $(\alpha_n)_{n \geq 1}$ care indeplineşte proprietăţile cerute. □

Una dintre aplicaţiile lemei lui Hensel este **determinarea rădăcinilor unităţii care se gasesc în $\mathbb{Q}_p$.**

Să ne reamintim că un element ξ dintr-un corp arbitrar se numeşte *rădăcină de ordin m a unităţii* dacă $\xi^m = 1$ şi se numeşte *rădăcină primitivă de ordin m a unităţii* dacă, în plus, $\xi^n \neq 1$, pentru orice $0 < n < m$. De exemplu, corpul numerelor reale $\mathbb{R}$ conţine doar două rădăcini ale unităţii: 1 si -1. Pe de altă parte, de exemplu, ecuaţia $x^2 + 1 = 0$ are o rădăcină în $\mathbb{Q}_5$ care, în mod evident, este rădăcină de ordin 4 a unităţii.

Pentru a aplica lema lui Hensel, avem nevoie de un polinom. Deoarece căutăm rădăcini de ordin m ale unităţii, vom folosi polinomul $f(x) = x^m - 1$. Din $f'(x) = mx^{m-1}$ obţinem că $f'(\lambda) = m\lambda^{m-1}$ va fi congruent cu 0 modulo p dacă sau p divide λ (caz in care λ nu mai poate fi soluţie a lui $f(x)$ mod p), fie p divide m. Prin urmare, cea de-a doua condiţie din teorema va fi satisfăcută dacă m este divizibil cu p. Pentru prima condiţie, trebuie să gasim o rădăcină a lui $f(x)$ modulo p.

Propoziţia 3.23. *Fie p un număr prim fixat şi m un întreg care nu este divizibil cu p. Atunci există un întreg $\alpha_1 \in \mathbb{Z}$ astfel incat $\alpha_1^m \equiv 1 \mod p$ si $\alpha_1 \not\equiv 1 \mod p$ daca si numai daca $(m, p-1) \neq 1$.*

În plus, dacă există un astfel de α_1 in $\mathbb{Z}$, cel mai mic întreg pozitiv m cu proprietatea de mai sus trebuie să fie divizor al lui $p-1$.

Demonstraţie: Dacă există un întreg $\alpha_1 \in \mathbb{Z}$ astfel incat $\alpha_1^m \equiv 1 \mod p$ şi $\alpha_1 \not\equiv 1 \mod p$, atunci $\bar{\alpha_1} \equiv \alpha_1 \mod p$ este un element din grupul ciclic cu $p-1$ elemente $(\mathbb{Z}/p\mathbb{Z})^\times$ care are ordinul un divizor al lui m. Rezulta ca $(m, p-1) \neq 1$, pentru ca $\alpha_1 \not\equiv 1 \mod p$.

Mai mult, cel mai mic exponent m cu acesta proprietate este un divizor al $(m, p-1)$, deci al lui $p-1$.

Reciproc, într-un grup ciclic de ordin $p-1$ există elemente de orice ordin d, cu d divizor al lui $p-1$ (daca x este un generator, $x^{\frac{p-1}{d}}$ este un element de ordin d). □

Astfel, din lema lui Hensel, rezultă imediat urmatoarea

Propoziţia 3.24. *Pentru orice număr prim p şi orice număr întreg pozitiv m care nu este divizibil cu p, există o rădăcină primitivă de ordin m a unităţii în $\mathbb{Q}_p$ daca si numai daca m divide $p-1$.*

Demonstraţie: Rezultă folosind lema lui Hensel şi propoziţia anterioara. □

Dacă m divide $p-1$, atunci orice radacină de ordin m a unitaţii este şi rădăcină de ordin $p-1$ a unităţii. Prin urmare, rădăcinile unităţii de ordin prim cu p care se gasesc în $\mathbb{Q}_p$ sunt cele de ordin $p-1$.

În acest mod am determinat toate rădăcinile unităţii din $\mathbb{Q}_p$, cu excepţia celor de ordin o putere a lui p. Se poate arăta că acestea nu sunt în $\mathbb{Q}_p$, excepţie făcând cazul $p=2$, când ± 1 apartin lui $\mathbb{Q}_p$.

Propoziţia 3.25. ***1.****Multimea rădăcinilor unităţii din $\mathbb{Q}_p$ formează un subgrup al lui $\mathbb{Z}_p^\times$.*

2.*Multimea rădăcinilor unităţii de ordin* $p-1$ *din* $\mathbb{Q}_p$ *este un grup ciclic de ordin* $p-1$.

Demonstraţie: Cum orice rădăcină de ordin m a unităţii se gaseşte în $\mathbb{Z}_p^\times$ (valoarea sa absolută trebuie să fie 1), rădăcinile unităţii de un ordin m sunt exact acele elemente din $\mathbb{Z}_p^\times$ care satisfac $x^m = 1$. Se arată uşor că mulţimea tuturor rădăcinilor de un ordin m ale unităţii din orice grup formează întotdeauna un subgrup.

Pentru a vedea ca sunt exact $p-1$ rădăcini de ordin $p-1$ ale unităţii, se observă că $1,\ 2,\ ,3,...,p-1$ sunt soluţii ale congruenţei $x^{p-1} \equiv 1 \mod p$, şi nu sunt congruenţe între ele modulo p. Aplicând lema lui Hensel polinomului $x^{p-1}-1$, "ridicăm" aceste soluţii în $\mathbb{Z}_p$ şi obţinem astfel toate cele $p-1$ rădăcini ale acestuia care, nefiind congruente modulo p, sunt toate diferite între ele. Cum, din propoziţia precedentă, orice rădăcină a unităţii trebuie să fie rădăcină a polinomului precedent, rezultă că acestea sunt toate redacinile unităţii din $\mathbb{Q}_p$. În plus, orice subgrup finit al unui corp este ciclic. □

3.5 Măsura Haar pe $\mathbb{Q}_p$

Mulţimea mulţimilor măsurabile din $\mathbb{Q}_p$ este cea mai mică submulţime a mulţimii parţilor lui $\mathbb{Q}_p$ care conţine mulţimile deschise din $\mathbb{Q}_p$ şi satisface urmatoarele proprietăţi:

(M1) dacă o mulţime E este măsurabiu a, atunci şi complementara sa $\mathbb{Q}_p \backslash E$ este măsurabilă;

(M2) dacă $(E_n)_{n\geq 1}$ este o familie de mulţimi măsurabile, atunci şi reuniunea

$\bigcup_{n\geq 1} E_n$ este măsurabilă.

De aici rezultă şi că intersecţie finită de mulţimi măsurabile, mulţimile închise din $\mathbb{Q}_p$ şi mulţimile compacte din $\mathbb{Q}_p$ sunt măsurabile.

Definiţia 3.26. *O **măsura Haar** meas pe $\mathbb{Q}_p$ este funcţie (nenula) definită pe mulţimea mulţimilor măsurabile ale lui $\mathbb{Q}_p$ cu valori în $[0,\infty]$ care satisface urmatoarele proprietăţi:*

(H1) meas(∅)=0;

(H2) dacă $(E_n)_{n\geq 1}$ este o familie de mulţimi măsurabile disjuncte, atunci

$$meas\left(\bigcup_{n\geq 1} E_n\right) = \sum_{n\geq 1} meas(E_n);$$

(H3) pentru orice mulţime compactă C din $\mathbb{Q}_p$ are loc $meas(C) < \infty$;

(H4) funcţia meas este invariantă la translaţii, adică, pentru orice mulţime măsurabilă E din $\mathbb{Q}_p$ şi pentru orice $x \in \mathbb{Q}_p$ are loc $meas(x+E) = meas(E)$;

(H5) pentru orice mulţime măsurabilă E are loc

$$meas(E) = inf\left\{meas(O)|\ O \text{ mulţime deschisă în } \mathbb{Q}_p, O \supseteq E\right\};$$

(H6) pentru orice mulţime deschisă O din $\mathbb{Q}_p$ are loc

$$meas(O) = sup\left\{meas(C)|C \text{ mulţime deschisă în } \mathbb{Q}_p, C \subset O\right\}.$$

Măsura Haar *meas* pe $\mathbb{Q}_p$ este complet determinată dacă presupunem că măsura Haar pe mulţimea compactă $\mathbb{Z}_p$ este egală cu 1, deoarece toate măsurile Haar pe $\mathbb{Q}_p$ sunt egale până la un factor normalizator.

În continuare, vom arăta că $meas(\mathbb{Z}_p) = 1$ implica $meas(x+p^k\mathbb{Z}_p) = p^{-k}$, pentru orice $x \in \mathbb{Q}_p$ şi orice $k \in \mathbb{N}$. Deoarece mulţimea $\mathbb{Z}_p$ este egală cu reuniunea disjunctă $\bigcup_{a\in\{0,\ldots,p^k-1\}} a + p^k\mathbb{Z}_p$, obţinem:

$$\begin{aligned} 1 = meas(\mathbb{Z}_p) &= \sum_{a\in\{0,\ldots,p^k-1\}} meas(a + p^k\mathbb{Z}_p) && \text{cf.(H2)} \\ &= \sum_{a\in\{0,\ldots,p^k-1\}} meas(p^k\mathbb{Z}_p) && \text{cf.(H4)} \\ &= p^k meas(p^k\mathbb{Z}_p) \\ &= p^k meas(x + p^k\mathbb{Z}_p), && \text{cf.(H4)} \end{aligned}$$

de unde rezultă că $meas\left(x + p^k\mathbb{Z}_p\right) = p^{-k}$.

Din proprietăţile valuarii pe $\mathbb{Q}_p$, rezultă că orice mulţime deschisă din $\mathbb{Q}_p$ este o reuniune disjunctă de mulţimi de forma $x + p^k\mathbb{Z}_p$ cu $x \in \mathbb{Q}_p$ si $k \in \mathbb{N}$; măsura oricărei mulţimi măsurabile este determinată de (H2) si de (H5), iar măsura Haar pe $\mathbb{Q}_p^n$ este produsul a n mulţimi măsurabile din $\mathbb{Q}_p$.

Capitolul 4

Funcţia zeta a lui Igusa şi seria Poincaré

4.1 Funcţia zeta a lui Igusa şi seria Poincaré - definiţii generale

Definiţia 4.1. *Fie* $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. *Pentru* $z \in \mathbb{Q}_p$, *notăm cu* $v_p(z) \in \mathbb{Z} \cup \{\infty\}$ *valuarea sa p-adică şi cu* $|z|_p := p^{-v_p(z)}$ *valoarea sa absolută.*

Funcţia zeta a lui Igusa asociată lui f *se defineşte ca fiind*

$$Z_f(s) = \int_{x \in \mathbb{Z}_p^n} |f(x)|^s |dx|,$$

unde $s \in \mathbb{C}$, *cu* $Re(s) > 0$, *iar* $|dx|$ *reprezintă măsura Haar pe* $\mathbb{Q}_p^n$ *normată astfel încat* $\mathbb{Z}_p^n$ *are masura* 1.

Funcţia zeta a lui Igusa $Z_f(s)$ conţine toate informaţiile referitoare la numărul de soluţii modulo p^e ale congruenţei $f(x) \equiv 0 \mod p^e$, $e = 1, 2, 3, ...$, fiind strâns legată de seria Poincaré asociată lui f, pe care o definim în con-

tinuare.

Definiţia 4.2. *Fie* $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. ***Seria Poincaré asociată lui*** f *este seria formală*

$$P(t) = \sum_{e=0}^{\infty} N_e p^{-ne} t^e,$$

unde N_e *reprezintă cardinalul mulţimii*

$$\left\{ x + p^e \mathbb{Z}_p^n |\, x \in \mathbb{Z}_p^n \text{ si } f(x) \equiv 0 \mod p^e \right\},$$

pentru $e \geq 1$ *si* $N_0 = 1$.

Relaţia dintre seria Poincaré asociată lui f şi funcţia zeta a lui Igusa $Z_f(s)$ este dată în urmatoarea propoziţie:

Propoziţia 4.3. *Fie* $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$, $t := p^{-s}$, *cu* $s \in \mathbb{C}$ *si* $Re(s) > 0$.

Atunci

$$Z_f(s) = P(t) - \frac{P(t) - 1}{t} \quad si \quad P(t) = \frac{1 - tZ_f(s)}{1 - t}.$$

Demonstraţie: Vom rescrie funcţia zeta a lui Igusa asociată lui F astfel:

$$\begin{aligned} Z_f(s) &= \int_{x \in \mathbb{Z}_p^n} |f(x)|^s |dx| = \\ &= \sum_{e=0}^{\infty} \int_{\left\{x \in \mathbb{Z}_p^n | v_p(f(x)) = e\right\}} |f(x)|^s |dx| = \\ &= \sum_{e=0}^{\infty} p^{-es} \cdot meas \left\{ x \in \mathbb{Z}_p^n | v_p(f(x)) = e \right\}, \end{aligned}$$

unde cu $meas \left\{ x \in \mathbb{Z}_p^n | v_p(f(x)) = e \right\}$ am notat măsura Haar a mulţimii.

Ţinând cont de definiţia valuarii şi de proprietăţile măsurii Haar, obţinem:

$$
\begin{aligned}
&meas\left\{x \in \mathbb{Z}_p^n | v_p(f(x)) = e\right\} = \\
&= meas\left(\left\{x \in \mathbb{Z}_p^n | f(x) \equiv 0 \mod p^e\right\} \setminus \left\{x \in \mathbb{Z}_p^n | f(x) \equiv 0 \mod p^{e+1}\right\}\right) = \\
&= meas\left(\left\{x \in \mathbb{Z}_p^n | f(x) \equiv 0 \mod p^e\right\}\right) - meas\left(\left\{x \in \mathbb{Z}_p^n | f(x) \equiv 0 \mod p^{e+1}\right\}\right) = \\
&= meas \bigcup_{\substack{a \in \{0,1,\ldots,p^e-1\}^n, \\ f(a) \equiv 0 \mod p^e}} a + p^e \mathbb{Z}_p^n - \\
&\quad - meas \bigcup_{\substack{a \in \left\{0,1,\ldots,p^{e+1}-1\right\}^n, \\ f(a) \equiv 0 \mod p^{e+1}}} a + p^{e+1} \mathbb{Z}_p^n = \\
&= N_e p^{-en} - N_{e+1} p^{-(e+1)n}.
\end{aligned}
$$

Prin urmare, am obţinut:

$$
\begin{aligned}
Z_f(s) &= \sum_{e=0}^{\infty} p^{-es}\left(N_e p^{-en} - N_{e+1} p^{-(e+1)n}\right) = \\
&= \sum_{e=0}^{\infty} N_e p^{-en} (p^{-s})^e - \sum_{e=0}^{\infty} N_{e+1} p^{-n(e+1)} (p^{-s})^e = \\
&= P(t) - \frac{P(t)-1}{t}
\end{aligned}
$$

□

Folosind rezoluţia singularităţilor, Igusa [Igu74] a arătat că $Z_f(s)$ este o funcţie raţională în p^{-s} (vezi şi [Igu78]). O demostraţie complet diferită a raţionalitatii seriei Poincaré a fost dată, zece ani mai tarziu, de Jan Denef în [Den84] care a folosit descompunerea celulară p-adica în locul rezoluţiei singularităţilor a lui Hironaka.

Să facem urmatoarea observaţie: faptul că $Z_f(s)$ este o funcţie raţională în p^{-s} arată că infinitate de informaţii, şi anume numerele N_e, pentru orice $e \in \mathbb{N}$, este conţinută într-un număr finit de coeficienţi ai numărătorului şi numitorului funcţiei raţionale zeta. Polii lui $Z_f(s)$ şi ordinul acestora

determină comportamentul numărului de soluţii ale congruenţei $f(x) \equiv 0 \mod p^e$, pentru e suficient de mare. Mai mult, polii care au partea reală cea mai mare au cea mai mare contribuţie la aceste numere (pentru e suficient de mare). Dacă $f(0) = 0$, toţi N_e din Definiţia 4.2 sunt > 0. Deci, în acest caz, Definiţia 4.2, legătura dintre $Z_f(s)$ si $P(t)$ din Propoziţia 4.3 şi raţionalitatea acestora implică faptul că seria $Z_f(s)$ are cel putin un pol.

4.2 Formula fazei staţionare

În [Igu94], Igusa a introdus o formula pe care a numit-o "*formula fazei staţionare*", care permite calcularea efectivă a multor funcţii zeta Igusa. Demonstraţia pe care a dat-o Igusa în articolul menţionat foloseşte aşa-numitele "restricted power series". Demonstraţia pe care o vom face în acestă secţiune este una elementară, dată de Denef şi Hoornaert în [DH01] şi are la bază lema lui Hensel.

4.2.1 Calculul unei integrale bine-cunoscute folosind Lema lui Hensel

Propoziţia 4.4. *Fie* $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ *si* $a \in \mathbb{Z}_p^n$ *astfel incat sistemul de congruenţe:*

$$\begin{cases} f(x) & \equiv & 0 \ mod \ p \ , \\ \frac{\partial f}{\partial x_i}(x) & \equiv & 0 \ mod \ p \ , \ i = 1, ..., n, \end{cases}$$

nu are solutii in $a + (p\mathbb{Z}_p)^n$.

Pentru o variabilă complexă s *cu* $Re(s) > 0$, *avem:*

$$\int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s \, |dx| = \begin{cases} p^{-n} & , \ daca \quad f(a) \not\equiv 0 \ mod \ p \ , \\ p^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}} & , \ daca \quad f(a) \equiv 0 \ mod \ p \ , \end{cases}$$

unde $|dx|$ reprezintă măsura Haar pe $\mathbb{Q}_p^n$ normată astfel incat $\mathbb{Z}_p^n$ are măsura 1.

Observaţia 4.5. *Propoziţia de mai sus reprezintă, de fapt, un caz special al unui rezultat mai general (vezi [Den87]), dar aici vom da o demonstraţie bazată pe Lema lui Hensel. Din propoziţia de mai sus rezultă imediat următorul corolar care ne va fi foarte util în calculul funcţiilor zeta Igusa asociate diferitelor polinoame.*

Corolar 4.6. *Fie p un număr prim şi $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. Fie $\bar{f}$ polinomul cu coeficienţi în $\mathbb{F}_p$ obţinut din f prin reducerea modulo $p\mathbb{Z}_p$ a coeficienţilor lui f. Să notăm cu N numărul de elemente al mulţimii $\left\{a \in \mathbb{F}_p^{\times} | \bar{f}(a) = 0\right\}$. Să presupunem că sistemul de congruenţe*

$$\begin{cases} f(x) & \equiv & 0 \ mod \ p \ , \\ \frac{\partial f}{\partial x_i}(x) & \equiv & 0 \ mod \ p \ , \ i = 1, ..., n, \end{cases}$$

nu are soluţii în $\left(\mathbb{Z}_p^{\times}\right)^n$. Atunci, pentru o variabilă complexă s cu $Re(s) > 0$, avem:

$$\int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s \, |dx| = p^{-n} \left((p-1)^n - pN \frac{(p^s - 1)}{p^{s+1} - 1} \right),$$

unde $|dx|$ reprezintă măsura Haar pe $\mathbb{Q}_p^n$ normată astfel incat $\mathbb{Z}_p^n$ are măsura 1.

Demonstraţie: Deoarece $\bigcup\limits_{a \in \{1,...,p\}^n} a + (p\mathbb{Z}_p)^n$ reprezintă o partiţie a lui $\left(\mathbb{Z}_p^{\times}\right)^n$, obţinem:

$$\begin{aligned} \int\limits_{\left(\mathbb{Z}_p^{\times}\right)^n} |f(x)|^s \, |dx| = & \sum_{\substack{a \in \{0,1,...,p-1\}^n \\ f(a) \not\equiv 0 mod p}} \int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s \, |dx| + \\ & + \sum_{\substack{a \in \{0,1,...,p-1\}^n \\ f(a) \equiv 0 mod p}} \int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s \, |dx| \, . \end{aligned}$$

Din condiţia pusă în enunţul Corolarului 4.6 şi din Propoziţia 4.4 rezultă că:

$$\int\limits_{\left(\mathbb{Z}_p^{\times}\right)^n} |f(x)|^s \, |dx| = \left((p-1)^n - N\right) p^{-n} + Np^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}} =$$

$$= p^{-n}\left((p-1)^n - N\frac{1-p^{-s}}{1-p^{-(s+1)}}\right).$$

□

Din Teorema 3.22 lui Hensel, rezultă uşor următorul corolar:

Corolar 4.7. *Fie $f(x) \in \mathbb{Z}_p[x]$, $k \in \mathbb{N}\setminus\{0\}$. Fie $a \in \mathbb{Z}_p$ astfel incat $f(a) \equiv 0 \mod p^k$ si $f'(a) \not\equiv 0 \mod p$. Atunci exista un $\xi \in \mathbb{Z}_p$ astfel incat*

$$\xi + p^k\mathbb{Z}_p = \left\{x \in a + p\mathbb{Z}_p | f(x) \equiv 0 \mod p^k\right\}.$$

Demonstraţie: Din Teorema 3.22, rezulta ca exista un unic $\xi \in \mathbb{Z}_p$ astfel incat $f(\xi) = 0$ si $\xi \equiv a \mod p^k$. Vrem să arătăm că

$$\xi + p^k\mathbb{Z}_p = \left\{x \in a + p\mathbb{Z}_p | f(x) \equiv 0 \mod p^k\right\}.$$

Pentru incluziunea $\subseteq$, fie $x \in \mathbb{Z}_p$ astfel incat $x \equiv \xi \mod p^k$. Atunci $x \equiv \xi \equiv a \mod p$ şi $f(x) \equiv f(\xi) \equiv 0 \mod p^k$.

Reciproc, pentru incluziunea $\supseteq$, fie $x \in a + p\mathbb{Z}_p$ astfel incat $f(x) \equiv 0 \mod p^k$. Deoarece $x \equiv a \mod p$, rezulta $f'(x) \equiv f'(a) \not\equiv 0 \mod p$. Din Teorema 3.22, rezultă atunci că exista un unic $\eta \in \mathbb{Z}_p$ astfel incat $f(\eta) = 0$ şi $\eta \equiv x \mod p^k$. Mai mult, $\eta \equiv x \equiv a \mod p$ şi, din unicitatea lui ξ, obţinem $\eta = \xi$ şi deci $x \equiv \xi \mod p^k$. □

Corolarul precedent se poate generaliza pentru polinoame în mai multe variabile:

Lema 4.8. *Fie $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ si $k \in \mathbb{N}\setminus\{0\}$. Fie $a = (a_1, ..., a_n) \in \mathbb{Z}_p^n$ astfel incat $f(a) \equiv 0 \mod p$ si $(\frac{\partial f}{\partial x_1})(a) \not\equiv 0 \mod p$. Fie $\xi_2, ..., \xi_n \in \mathbb{Z}_p$ cu $\xi_i \equiv a_i \mod p$, pentru $i = 2, ..., n$.*

Atunci exista un $\xi_1 = \xi_1(\xi_2, ..., \xi_n) \in \mathbb{Z}_p$ *astfel incat, pentru orice* $x_2, ..., x_n \in \mathbb{Z}_p$ *cu proprietatea că* $x_i \equiv \xi_i \mod p^k$, *cu* $i = 2, ..., n$, *avem:*

$$\xi_1 + p^k\mathbb{Z}_p = \left\{x_1 \in a_1 + p\mathbb{Z}_p | f(x_1, ..., x_n) \equiv 0 \mod p^k\right\}.$$

De aici rezulta ca mulţimea $\left\{(x_1, ..., x_n) \in a + (p\mathbb{Z}_p)^n | f(x_1, ..., x_n) \equiv 0 \mod p^k\right\}$ *este egală cu*

$$\bigcup (\xi_1(\xi_2, ..., \xi_n), \xi_2, ..., \xi_n) + (p^k\mathbb{Z}_p)^n,$$

reuniunea de mai sus făcându-se după toate acele $(n-1)$*-upluri* $\left(\xi_2 + p^k\mathbb{Z}_p, ..., \xi_n + p^k\mathbb{Z}_p\right)$, *cu* $\xi_i \equiv a_i \mod p$, *cu* $i = 2, ..., n$.

Observaţia 4.9. *Este clar faptul că avem un rezultat similar pentru orice altă variabilă* x_i *care satisface* $(\frac{\partial f}{\partial x_i})(a) \not\equiv 0 \mod p$.

Demonstraţie: Lema de mai sus rezultă din Corolarul 4.7 deoarece $f(x_1, x_2..., x_n) \equiv f(x_1, \xi_2..., \xi_n) \mod p^k$ pentru orice $x_2, ..., x_n \in \mathbb{Z}_p$ cu $x_i \equiv \xi_i \mod p^k$; $f(a_1, \xi_2..., \xi_n) \equiv f(a_1, a_2..., a_n) \equiv 0 \mod p$ si $(\frac{\partial f}{\partial x_1})(a_1, \xi_2..., \xi_n) \equiv \frac{\partial f}{\partial x_1})(a_1, a_2..., a_n) \not\equiv 0 \mod p$. □

4.10 (Demonstraţia Propoziţiei 4.4).

Cazul 1: $f(a) \not\equiv 0 \mod p$. Pentru orice $x \in a + (p\mathbb{Z}_p)^n$, avem: $f(x) \equiv f(a) \not\equiv 0 \mod p$. Prin urmare, $v_p(f(x)) = 0$ si $|f(x)|^s = 1$, pentru orice $x \in a + (p\mathbb{Z}_p)^n$. Rezultă că:

$$\int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s \, |dx| = \int\limits_{a+(p\mathbb{Z}_p)^n} 1 \, |dx| = p^{-n}.$$

Cazul 2: $f(a) \equiv 0 \mod p$. Pentru orice $x \in a + (p\mathbb{Z}_p)^n$, avem: $f(x) \equiv f(a) \equiv 0 \mod p$. Prin urmare, $v_p(f(x)) \geq 1$, pentru orice $x \in a + (p\mathbb{Z}_p)^n$.

Rezultă că:

$$\begin{aligned}\int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| &= \sum_{k=1}^{\infty} \int\limits_{\substack{x\in a+(p\mathbb{Z}_p)^n \\ v_p(f(a))=k}} |f(x)|^s |dx| = \\ &= \sum_{k=1}^{\infty} p^{-ks} \cdot meas\left\{x \in a+(p\mathbb{Z}_p)^n \,|v_p(f(x))=k\right\}.\end{aligned}$$

Vom arăta că măsura mulţimii $\{x \in a+(p\mathbb{Z}_p)^n \,|v_p(f(x))=k\}$ este $p^{-k-n+1}-p^{-k-n}$. Dacă arătăm acest lucru, obţinem:

$$\begin{aligned}\int\limits_{a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| &= \sum_{k=1}^{\infty} p^{-ks}\left(p^{-k-n+1}-p^{-k-n}\right) = \\ &= p^{-n}(p-1)\sum_{k=1}^{\infty}\left(p^{-(s+1)}\right)^k = \\ &= p^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}},\end{aligned}$$

deoarece $Re(s)>0$ implică faptul că modulul lui $p^{-(s+1)}$ este <1.

Să demonstrăm acum afirmaţia de mai sus, şi anume faptul că măsura mulţimii $\{x \in a+(p\mathbb{Z}_p)^n \,|v_p(f(x))=k\}$ este $p^{-k-n+1}-p^{-k-n}$. Cum mulţimea de mai sus este complementul mulţimii $\left\{x \in a+(p\mathbb{Z}_p)^n \,|f(x) \equiv 0 \mod p^{k+1}\right\}$ in

$\left\{x \in a+(p\mathbb{Z}_p)^n \,|f(x) \equiv 0 \mod p^{k}\right\}$, din aditivitatea măsurii Haar, rezultă că este suficient să arătăm că mulţimea $\left\{x \in a+(p\mathbb{Z}_p)^n \,|f(x) \equiv 0 \mod p^{k}\right\}$ are măsura p^{-k-n+1}, pentru $k \in \mathbb{N}\setminus\{0\}$.

Din ipoteza Propoziţiei 4.4 şi din faptul că $f(a) \equiv 0 \mod p$, rezulta ca exista un $i \in \{1,...,n\}$ astfel incat $(\frac{\partial f}{\partial x_i})(a) \not\equiv 0 \mod p$. Putem presupune acum, fără pierderea generalităţii, că $(\frac{\partial f}{\partial x_1})(a) \not\equiv 0 \mod p$. Din Lema 4.8 rezultă atunci că mulţimea $\left\{x \in a+(p\mathbb{Z}_p)^n \,|f(x) \equiv 0 \mod p^{k}\right\}$ este egala cu reuniunea

$$\bigcup \left(\xi_1\left(\xi_2,...,\xi_n\right),\xi_2,...,\xi_n\right)+(p^k\mathbb{Z}_p)^n,$$

unde $\xi_1\,(\xi_2,...,\xi_n)$ este ca în Lema 4.8 şi reuniunea se face după toate acele $(n-1)$-upluri $\left(\xi_2+p^k\mathbb{Z}_p,...,\xi_n+p^k\mathbb{Z}_p\right)$, cu $\xi_i \equiv a_i \mod p$, pentru $i=2,...,n$. Aceasta reuniune este în mod evident disjunctă şi măsura lui $\xi+\left(p^k\mathbb{Z}_p\right)^n$ este p^{-kn}. Obţinem astfel că mulţimea $\left\{x\in a+(p\mathbb{Z}_p)^n\,|f(x)\equiv 0 \mod p^k\right\}$ are măsura egală cu $p^{(k-1)(n-1)}p^{-kn}=p^{-k-n+1}$. □

4.2.2 Formula Fazei staţionare

Teorema 4.11 (Formula Fazei staţionare; SPF-stationary phase formula)**.** *Fie p un număr prim şi $f(x)=f(x_1,x_2...,x_n)\in\mathbb{Z}_p[x]$. Fie $\bar{f}\in\mathbb{F}_p[x]$ polinomul obţinut din f prin reducerea modulo $p\mathbb{Z}_p$ a coeficienţilor. Fie $\bar{E}$ o submulţime a lui $\mathbb{F}_p^n$ si fie $\bar{S}$ submulţimea sa formată din toţi acei $\bar{a}\in\bar{E}$ soluţii ale sistemului*

$$\begin{cases} \bar{f}(\bar{a}) &= 0 \\ \frac{\partial\bar{f}}{\partial x_i}(\bar{a}) &= 0,\ i=1,...,n. \end{cases}$$

Să notăm cu E, S preimaginile lui $\bar{E}$, $\bar{S}$ prin proiecţia canonică $\mathbb{Z}_p^n\to\mathbb{Z}_p^n/p\mathbb{Z}_p^n$ şi cu N numărul de elemente al mulţimii $\left\{\bar{a}\in\bar{E}|\bar{f}(\bar{a})=0\right\}$. Atunci

$$\begin{aligned}\int\limits_E |f(x)|^s\,|dx| &= p^{-n}\left(card(\bar{E})-N\right)+p^{-n}\left(N-card(\bar{S})\right)\frac{(1-p^{-1})t}{1-p^{-1}t}+ \\ &+ \int\limits_S |f(x)|^s\,|dx|\,,\end{aligned}$$

unde $t:=p^{-s}$, iar cu $card(\bar{E})$, $card(\bar{S})$ am notat cardinalul mulţimilor $\bar{E}$, respectiv $\bar{S}$ şi cu $|dx|$ măsura Haar pe $\mathbb{Q}_p^n$, normată astfel încât $\mathbb{Z}_p^n$ are măsura 1.

Observaţia 4.12. *Aceasta teoremă este demonstrată în [Igu00], folosind SRP-uri ("special restricted power series"). Aici vom prefera să dăm o demonstraţie elementară, folosind rezultatele precedente.*

Demonstraţie: Evident,

$$\int_E |f(x)|^s |dx| = \int_S |f(x)|^s |dx| + \int_{E\setminus S} |f(x)|^s |dx| .$$

Să calculăm cea de-a doua integrală. Pentru toţi $a \in \mathbb{Z}_p^n$, notăm cu $\bar{a} = a \mod p$; obţinem:

$$\int_{E\setminus S} |f(x)|^s |dx| = \sum_{\bar{a}\in\bar{E}\setminus\bar{S}} \int_{x\in a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| .$$

Desfacem suma de mai sus în două parţi:

i) $\bar{a} \in \bar{E}\setminus\bar{S}$, cu $\bar{f}(\bar{a}) \neq 0$;

ii) $\bar{a} \in \bar{E}\setminus\bar{S}$, astfel incat $\bar{f}(\bar{a}) = 0$ şi exista $1 \leq i \leq n$ cu $\frac{\partial \bar{f}}{\partial x_i}(\bar{a}) \neq 0$.

În cazul i), conform Propoziţiei 4.4 (condiţia din ipoteza propoziţiei este satisfăcută deoarece $\bar{a} \in \bar{E}\setminus\bar{S}$), $\int_{x\in a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| = p^{-n}$. Deoarece numărul acelor $\bar{a}$ care satisfac i) este $card(\bar{E} - N)$, am obţinut că:

$$\sum_{\left\{\bar{a}\in\bar{E}\setminus\bar{S} | \bar{f}(\bar{a})\neq 0\right\}} \int_{x\in a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| = p^{-n}(card(\bar{E} - N)).$$

În cazul ii), conform Propoziţiei 4.4, deoarece numărul acelor $\bar{a}$ care satisfac ii) este $N - card(\bar{S})$, am obţinut că

$$\sum_{\substack{\left\{a\in\bar{E}\setminus\bar{S} | \bar{f}(\bar{a})=0,\right. \\ \left.\exists 1\leq i\leq n \text{ a.i. } \frac{\partial \bar{f}}{\partial x_i}(\bar{a})\neq 0\right\}}} \int_{x\in a+(p\mathbb{Z}_p)^n} |f(x)|^s |dx| = (N - card(\bar{S}))p^{-n} t \frac{1-p^{-1}}{1-p^{-1}t},$$

ceea ce încheie demonstraţia teoremei. □

Propoziţia 4.13 (Igusa)**.** *Fie p un număr prim şi $f(x) = f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$ un polinom omogen de grad d astfel încât singura soluţie a sistemului*

$$\begin{cases} \bar{f}(\bar{a}) &= 0 \\ \frac{\partial \bar{f}}{\partial x_i}(\bar{a}) &= 0 \ i\text{=}1,\ldots,n, \end{cases}$$

este $\bar{a} = 0$. *Dacă notăm cu* N *numărul de elemente al mulţimii* $\left\{\bar{a} \in \mathbb{F}_p^n | \bar{f}(\bar{a}) = 0\right\}$, *atunci:*

$$Z_f(s) = \frac{(1-p^{-1})(1-p^{-n})t + (1-p^{-n})N(1-t)}{(1-p^{-1}t)(1-p^{-n}t^d)},$$

unde $t := p^{-s}$, *cu* $s \in \mathbb{C}$ *astfel incat* $Re(s) > 0$.

Demonstraţie: În teorema precedentă, luând $\bar{E} = \mathbb{F}_p^n$, din ipoteza propoziţiei rezultă că $\bar{S} = 0$, adica $E = \mathbb{Z}_p^n$ şi $S = (p\mathbb{Z}_p)^n$. Aplicând formula fazei staţionare, obţinem:

$$\begin{aligned} Z_f(s) = \int\limits_{x \in \mathbb{Z}_p^n} |f(x)|^s |dx| &= p^{-n}(p^n - N) + p^{-n}(N-1)\frac{(1-p^{-1})t}{1-p^{-1}t} + \\ &+ \int\limits_{x \in \left(p\mathbb{Z}_p^n\right)^n} |f(x)|^s |dx| . \end{aligned}$$

În integrala de mai sus, dacă facem schimbarea de variabilă $y = px$, obţinem $|dy| = p^{-n}|dx|$. Pe de altă parte, deoarece f este un polinom omogen de grad d, $f(px) = p^d f(x)$ şi avem:

$$\int\limits_{x \in \left(p\mathbb{Z}_p^n\right)^n} |f(x)|^s |dx| = p^{-n}t^d \int\limits_{x \in \mathbb{Z}_p^n} |f(x)|^s |dx| = p^{-n}t^d Z_f(s).$$

Înlocuind în formula de mai sus, obţinem $Z_f(s)$ ca în enunţul propoziţiei. □

4.2.3 Exemple

1) Fie p un număr prim diferit de 2 si 3, $f(x_1, x_2) = x_1^3 + x_2^3 \in \mathbb{Z}_p[x_1, x_2]$ forma cubică binară Fermat şi $Z_f(s)$ funcţia zeta Igusa asociată. Dacă notăm cu $\bar{f}$ polinomul obţinut din f prin reducerea modulo $p\mathbb{Z}_p$ a coeficienţilor, avem $\bar{f}(x_1, x_2) = x_1^3 + x_2^3 \in \mathbb{F}_p[x_1, x_2]$, $\frac{\partial \bar{f}}{\partial x_1}(x_1, x_2) = 3x_1^2$, $\frac{\partial \bar{f}}{\partial x_2}(x_1, x_2) = 3x_2^2$.

Cu notaţiile din SPF, fie $\bar{E} = \mathbb{F}_p^2$. Cum p este un numar prim diferit de 3, soluţia în $\mathbb{F}_p^2$ a sistemului

$$\begin{cases} x_1^3 + x_2^3 = 0 \\ 3x_1^2 = 0 \\ 3x_2^2 = 0 \end{cases}$$

este $\bar{S} = (0,0)$. Prin urmare, $E = \mathbb{Z}_p^2$ şi $S = p\mathbb{Z}_p \times p\mathbb{Z}_p$.

Dacă calculăm numărul N de elemente ale mulţimii $\left\{\bar{x} \in \mathbb{F}_p^2 | \bar{f}(\bar{x}) = 0\right\}$, obţinem:

$$N = \begin{cases} 3(p-1)+1 = 3p-2, & \text{daca } p \equiv 1 \mod 3, \\ p, & \text{daca } p \equiv 2 \mod 3. \end{cases}$$

Aplicând formula fazei staţionare, obţinem:

$$\begin{aligned} Z_f(s) &= \int\limits_{\mathbb{Z}_p^2} |f(x)|^s |dx| = p^{-2}\left[(p^2 - N) + p^{-2}(N-1)\right] \frac{(1-p^{-1})t}{1-p^{-1}t} + \\ &+ \int\limits_{(p\mathbb{Z}_p)^2} \left|x_1^3 + x_2^3\right|^s |dx_1|\,|dx_2|\,. \end{aligned}$$

Să calculăm acum integrala de mai sus. Cu schimbarea de variabilă $(x_1, x_2) := (py_1, py_2)$, rezulta $|dx_1| = p^{-1}|dy_1|$, $|dx_2| = p^{-1}|dy_2|$ şi integrala devine:

$$\begin{aligned} \int\limits_{(p\mathbb{Z}_p)^2} \left|x_1^3 + x_2^3\right|^s |dx_1|\,|dx_2| &= p^{-2}t^3 \int\limits_{\mathbb{Z}_p^2} \left|x_1^3 + x_2^3\right|^s |dx_1|\,|dx_2| = \\ &= p^{-2}t^3 Z_f(s). \end{aligned}$$

Prin urmare, făcând calculele, obţinem că:

$$Z_f(s) = \begin{cases} \frac{(1-p^{-1})(1-2p^{-1}+2p^{-1}t-p^{-2}t)}{(1-p^{-1}t)(1-p^{-2}t^3)} = \frac{(p-1)(p^2-2p+2tp-t)}{(p-t)(p^2-t^3)}, & \text{daca } p \equiv 1 \mod 3 \\ \frac{(1-p^{-1})(1-p^{-2}t)}{(1-p^{-1}t)(1-p^{-2}t^3)} = \frac{(p-1)(p^2-t)}{(p-t)(p^2-t^3)}. & \text{daca } p \equiv 2 mod 3 \end{cases}$$

Să mai remarcăm aici faptul că funcţia zeta Igusa asociată formei cubice binare Fermat $x_1^3 + x_2^3$ se mai putea calcula folosind Propoziţia lui Igusa 4.13:

deoarece $\bar{f}(x_1,x_2)=x_1^3+x_2^3$, $\frac{\partial \bar{f}}{\partial x_1}(x_1,x_2)=3x_1^2$, iar $\frac{\partial \bar{f}}{\partial x_2}(x_1,x_2)=3x_2^2$, rezultă că singura soluţie a sistemului $\bar{f}(x_1,x_2)=\frac{\partial \bar{f}}{\partial x_1}(x_1,x_2)=\frac{\partial \bar{f}}{\partial x_2}(x_1,x_2)=0$ este $(0,0)$ şi, astfel, ipoteza de nedegenerare din propoziţia lui Igusa este safistacută.

2) Fie p un număr prim diferit de 2 si 3 si $f(x_1,x_2)=px_1^3+x_2^3\in\mathbb{Z}_p[x_1,x_2]$. Să calculăm funcţia zeta Igusa asociată lui f.

Deoarece $\bar{f}(x_1,x_2)=x_2^3$, $\frac{\partial \bar{f}}{\partial x_1}(x_1,x_2)=0$, $\frac{\partial \bar{f}}{\partial x_2}(x_1,x_2)=3x_2^2$, cum $p\neq 3$, rezultă că soluţiile sistemului:

$$\begin{cases} \bar{f}(x_1,x_2)=0 \\ \frac{\partial \bar{f}}{\partial x_1}(x_1,x_2)=0 \\ \frac{\partial \bar{f}}{\partial x_2}(x_1,x_2)=0, \end{cases}$$

echivalent cu

$$\begin{cases} x_2^3=0 \\ 3x_2^3=0 \end{cases}$$

sunt de forma $\bar{S}=\{(x_1,0)|x_1\in\mathbb{F}_p\}$ si, prin urmare, $S=\mathbb{Z}_p\times p\mathbb{Z}_p$. Pe de altă parte, numărul de elemente al mulţimii $\left\{\bar{x}\in\mathbb{F}_p^2|\bar{f}(\bar{x})=0\right\}$ este $N=p$.

Cu formula fazei staţionare, obţinem:

$$\begin{aligned} Z_f(s) &= p^{-2}(p^2-p)+p^{-2}(p-p)\frac{(1-p^{-1})t}{1-p^{-1}t}+\int\limits_{\mathbb{Z}_p\times(p\mathbb{Z}_p)}\left|px_1^3+x_2^3\right|^s|dx_1|\,|dx_2|= \\ &= (1-p^{-1})+p^{-1}t\int\limits_{\mathbb{Z}_p^2}\left|x_1^3+p^2x_2^3\right|^s|dx_1|\,|dx_2| \end{aligned}$$

Pentru calculul integralei din relaţia de mai sus, mai aplicam o dată SPF. Avem:

$$\begin{aligned} Z_f(s) &= 1-p^{-1}+p^{-1}t\left(1-p^{-1}+p^{-1}t^2\int\limits_{\mathbb{Z}_p^2}\left|px_1^3+x_2^3\right|^s|dx_1|\,|dx_2|\right)= \\ &= (1-p^{-1})+p^{-1}t\left(1-p^{-1}+p^{-1}t^2Z_f(s)\right). \end{aligned}$$

Am obţinut astfel că:

$$Z_f(s) = \frac{(p-1)(p+t)}{p^2 - t^3}.$$

4.3 Corpuri locale. Structura grupului multiplicativ al unui corp local.

Definiţia 4.14. *Să ne reamintim că un corp valuat $(K, |.|)$ se numeşte **complet** dacă orice şir Cauchy $(a_n)_{n\in\mathbb{N}}$ din K converge catre un element $a \in K$ i.e.*

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

Definiţia 4.15. *Prin **sir Cauchy** întelegem un şir $(a_n)_{n\in\mathbb{N}}$ cu proprietatea că pentru orice $\epsilon > 0$ exista $N \in \mathbb{N}$ astfel incat*

$$|a_n - a_m| < \epsilon, \text{ pentru orice } n, m \geq N.$$

Din orice corp valuat $(K, |.|)$ putem obţine un corp valuat complet $(\hat{K}, |.|)$ prin procesul de *completare* în acelaşi mod în care este construit corpul numerelor reale pornind de la corpul numerelor raţionale. Pentru un corp valuat complet $(K, |.|)$ şi L o extindere algebrică a lui K, valuarea de pe K se extinde în mod unic la o valuare pe L. Mai precis are loc:

Teorema 4.16. *Fie $(K, |.|)$ un corp valuat complet şi L/K o extindere algebrică a lui K de grad finit $[L : K] = n$. Atunci $|.|$ se extinde în mod unic la o valuare pe L dată prin formula*

$$|\alpha| = \sqrt[n]{N_{L/K}(\alpha)}, \text{ pentru orice } \alpha \in L,$$

unde $N_{L/K}(\alpha)$ reprezintă norma lui α în extinderea L/K. În acest caz, L este de asemenea complet.

Demonstraţie: Vezi [Neu99], pagina 131. □

Dintre toate corpurile valuate complete (nearhimedeene) cele care apar drept completatul unui *corp global* i.e. o extindere finită a lui $\mathbb{Q}$ sau $\mathbb{F}_p(t)$ au cea mai mare importanţa în teoria numerelor. Valuarea unui astfel de corp complet este *discretă* (i.e. grupul sau de valuare este izomorf cu $\mathbb{Z}$), iar corpul rezidual este finit.

Definiţia 4.17. *Toate corpurile care sunt complete în raport cu o valuare discretă şi au corpul rezidual finit se numesc* ***corpuri locale.***

Propoziţia 4.18. *Un corp K este local dacă şi numai dacă este o extindere finită a lui $\mathbb{Q}_p$ sau $\mathbb{F}_p((t))$.*

Demonstraţie: Vezi [Neu99], pagina 135. □

De fapt, se arată că corpurile locale de caracteristică p sunt seriile de puteri $\mathbb{F}_q((t))$, unde q este o putere a lui p, iar corpurile locale de caracteristic a 0 sunt extinderi finite ale lui $\mathbb{Q}_p$ şi se numesc *corpuri de numere p-adice.*

Structura grupului multiplicativ K^* a unui corp local K este urmatoarea:

Teorema 4.19 (Structura grupului multiplicativ local compact K^* al unui corp local K)**.** *Fie K un corp local şi $q = p^f$ numărul de elemente din corpul său rezidual. Au loc atunci urmatoarele afirmaţii:*

1) *Dacă K este un corp de caracteristică 0,*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

unde $a \geq 0$ si $d = [K : \mathbb{Q}_p]$ (algebric şi topologic).

2) *Dacă K este un corp de caracteristică p,*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}} \text{(algebric şi topologic).}$$

Demonstraţie: Vezi [Neu99]. □

Capitolul 5

Rezultate fundamentale privind funţia zeta Igusa

5.1 Prezentarea rezultatelor fundamentale urmărite

Invarianţii numerici asociaţi unei rezoluţii scufundate determină polii candidaţi ai funcţiei zeta Igusa. În această lucrare determinăm, în completă generalitate, care poli reali candidaţi sunt poli în cazul curbelor. O serie de matematicieni au obţinut rezultate parţiale legate de determinarea polilor reali ai funcţiei zeta Igusa pentru curbe. În acestă lucrare am determinat polii reali pentru un polinom arbirar f în două variabile care este definit peste un corp p-adic. Interesul pentru polii funcţiei zeta Igusa $Z_f(s)$ este justificat pe de o parte de faptul că aceştia determină comportamentul asimptotic al numărului de soluţii al congruenţelor polinomiale, iar pe de alta parte deoarece aceştia sunt subiectul unei renumite conjecturi matematice: conjectura momodromiei (vezi de exemplu [Den91]).

Cronologic, au fost considerate la început curbe absolut analitic ireductibile. Rezultate parţiale au fost obţinute de Igusa [Ig1] şi Strauss [St]. Meuser [Me]

a determinat polii reali, dar nu a considerat polul candidat -1. În 1985 Igusa [Ig2] a rezolvat problema complet. El a demonstrat polii candidadti asociaţi unei transformări stricte ale lui f sunt poli cand domeniul de integrare este suficient de mic. Mai mult, un alt pol candidat al unei rezolţii minimale scufundate ale lui f este pol dacă si numai dacă este asociat unei curbe excepţionale care este intersectată de alte trei componente ireductibile ale pull back-ului lui f. Am incorporat o generalizare a acestui rezultat in Propoziţia 5.7.

În cazul general, Loeser [Lo] a demonstrat că o curbă excepţională E_i nu contribuie la polii lui $Z_f(s)$ dacă E_i este intersectat o dată sau de două ori de alte componente ale pull back-ului lui f şi dacă nu sunt alte puncte de intersecţie peste o închidere algebrică. Acest lucru a fost demonstrat pentru prima dată de Strauss in cazul absolut analitic ireductibil, caz în care ultima condiţie este automat satisfăcută.

Următoarea lucrare pe care vrem sa o menţionăm este [Ve1] a lui Veys. El a considerat polinoame f în două variabile peste un corp de numere F si a luat o rezoluţie minimală scufundată a lui f peste o închidere algebrică a lui F. Acest context i-a permis să folosească formula [De1] lui Denef pentru $Z_f(s)$, valabilă pentru aproape toţi completaţii p-adici ai lui F. Veys a presupus de asemenea ca toate punctele de intersecţie ale componentelor ireductibile ale pull-back-ului lui f sunt definite peste F. În aceste condiţii, el a demonstrat reciproca rezultatului lui Loeser pentru poli candidadti reali şi pentru aproape toţi completaţii p-adici ai lui F. Mai mult, el a considerat si problema unei posibile simplificări ale mai multor contribuţii la acelaşi pol candidat real.

În demonstraţiile rezultatelor menţionate mai sus este nevoie de anumite relaţii dintre invarianţii numerici asaciaţi unei rezoluţii scufundate. Aceste

relaţii au fost obţinute în [St], [Me] şi [Ig2] pentru curbe absolut analitic ireductibile. De asemenea, Loeser [Lo] a demonstart relaţia necesară în cazul general. Igusa [Ig2] şi Loeser [Lo] au folosit formula lui Langlands [La] pentru a calcula contribuţia unei curbe excepţionale la reziduul lui $Z_f(s)$ în cazul unui pol candidat de ordin unu. În continuare vom folosi o varianta îmbunătăţită a acestui rezultat demonstrată în [Se1]. Pe scurt, dată o rezoluţie minimală scufundată scisă ca o compunere de blow-ing-up-uri, Segers a obţinut modalitatea în care se poate calcula aceasta contribuţie la reziduu exact in momentul în care curba exceptională este creată. În Propoziţia 5.1 demonstrăm când această contribuţie este zero şi când nu. Pentru acest lucru, este nevoie de idei noi. Ceea ce vom face nu este o generalizare directă a unor rezultate cunoscute deja. De asemenea, în finalul acestui capitol, vom demonstra faptul că contribuţiile la acelaşi pol candidat nu se simplifica. Pentru aceasta, am folosit faptul ca graful dual al rezoluţiei scufundate este un arbore ordonat. Acest lucru a fost demonstrat în [Ve2] În cazul în care corpul de bază eset algebric în chis.

5.2 Rezultate cheie obţinute şi contribuţii personale

5.2.1 Evidenţirea contribuţiilor proprii la determinarea polilor funcţiei zeta Igusa pentru curbe

Fie K un corp p-adic, adică o extendere finită a lui $\mathbb{Q}_p$. Fie R inelul de valuare al lui K, P idealul maximal al lui R si q cardinalul corpului rezidual R/P. Pentru $z \in K$, notăm cu $\operatorname{ord} z \in \mathbb{Z} \cup \{+\infty\}$ valuarea lui z şi cu $|z| = q^{-\operatorname{ord} z}$ valoarea absolută (p-adică) a lui z.

Fie $f(x_1, x_2) \in K[x_1, x_2]$ un polinom în două variabile peste K. Fie $x = (x_1, x_2)$. Fie X o submulţime deschisa şi compactă a lui K^2. În acest context, funcţia zeta Igusa p-adică a lui f este definită de

$$Z_f(s) = \int_X |f(x)|^s \, |dx|$$

pentru $s \in \mathbb{C}$, $\mathrm{Re}(s) > 0$, unde $|dx|$ este măsura Haar K^2, normalizată astfel încât R^2 are măsura 1. Igusa a demonstrat că $Z_f(s)$ este o funcţie raţională în q^{-s} folosind o rezoluţie scufundată a lui f. Aceasta se extinde prin urmare la o funţie meromorfică $Z_f(s)$ pe $\mathbb{C}$ care se numeşte tot funcţia zeta Igusa p-adică asociată lui f.

Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Aici, Y este o K-varietate analitică. Despre rezoluţia scufundată lui f mai multe detalii sunt prezentate în [Ig3, Section 3.2]. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ o compunere de blowing-up-uri $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$. Curba excepţională lui g_i şi transformarea strictă a acestei curbe sunt notate cu E_i. Subvarietăţile lui Y de codimensiune unu reprezentate de zerourile transformării stricte ale unui factor ireductibil f din $K[x, y]$ sunt notate cu E_j, $j \in T_s$. Transformările corespunzătoare în Y_i, $i \in \{0, \ldots, t-1\}$ sunt notate analog. Atenţie aici şi la noţiunea de ireductibil, deoarece X este total disconex ca spaţiu topologic. Fie $T = T_e \cup T_s$. Pentru $i \in T$, fie N_i şi respectiv $\nu_i - 1$ multipliciţăţile lui $f \circ g$ şi respectiv g^*dx în E_i. Perechea (N_i, ν_i) reprezintă invarianţii numerici ai lui E_i.

Vom reaminti în continuare pe scurt demonstraţia dată de Igusa raţionalităţii lui $Z_f(s)$. Aşa cum am menţionat mai sus, calculăm integrala de definiţie pe Y:

$$Z_f(s) = \int_X |f(x)|^s \, |dx| = \int_Y |f \circ g|^s \, |g^*dx|.$$

Fie b un punct arbitrar al lui Y. Sunt posibile următoarele trei situaţii.

Primul caz este cel în care sunt două varietăţi E_i şi E_j, cu $i, j \in T$, care trec prin b. Considerăm o vecinătate V a lui b şi coordonatele analitice (y_1, y_2) în V astfel încât y_1 reprezintă ecuaţia lui E_i, y_2 este ecuaţia lui E_j,

$$f \circ g = \varepsilon y_1^{N_i} y_2^{N_j} \qquad \text{şi} \qquad g^* dx = \eta y_1^{\nu_i - 1} y_2^{\nu_j - 1} dy$$

pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\begin{aligned} \int_V |f \circ g|^s \, |g^* dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} |y_2|^{N_j s + \nu_j - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| \left(\frac{q-1}{q} \right)^2 \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}} \frac{q^{-k_2(N_j s + \nu_j)}}{1 - q^{-(N_j s + \nu_j)}}. \end{aligned}$$

Să observăm că am obţinut o funcţie raţională în q^{-s}.

În cel de-al doilea caz, să considerăm situaţia în care există o varietate E_i, $i \in T$, care trece prin b. Considerăm o varietate V a lui b şi coordonatele analitice (y_1, y_2) pe V astfel încât y_1 este ecuaţia lui E_i,

$$f \circ g = \varepsilon y_1^{N_i} \qquad \text{şi} \qquad g^* dx = \eta y_1^{\nu_i - 1} dy$$

pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\begin{aligned} \int_V |f \circ g|^s \, |g^* dx| &= \int_{P^{k_1} \times P^{k_2}} |\varepsilon|^s |\eta| |y_1|^{N_i s + \nu_i - 1} \, |dy| \\ &= |\varepsilon|^s |\eta| q^{-k_2} \frac{q-1}{q} \frac{q^{-k_1(N_i s + \nu_i)}}{1 - q^{-(N_i s + \nu_i)}}. \end{aligned}$$

În cea de-a treia situaţie, nu există nici o varietate E_i, $i \in T$, care tece prin b. Fie V o vecinătate a lui b şi fie (y_1, y_2) coordonate analitice pe V astfel încât $f \circ g = \varepsilon$ şi $g^* dx = \eta dy$ pe V, unde ε şi η sunt funcţii K-analitice pe V. Putem presupune că $y(V) = P^{k_1} \times P^{k_2}$, cu $k_1, k_2 \in \mathbb{Z}_{\geq 0}$, şi că $|\varepsilon|$ şi $|\eta|$ sunt constante pe V. Obţinem

$$\int_V |f \circ g|^s \, |g^* dx| = |\varepsilon|^s |\eta| q^{-k_1 - k_2}.$$

Rezultă atunci că $Z_f(s)$ este o funcţie raţională în q^{-s} deoarece putem partiţiona mulţimea Y în submulţimi V de forma de mai sus.

Din cele de mai sus rezultă şi că orice pol al lui $Z_f(s)$ este de forma

$$-\frac{\nu_i}{N_i} + \frac{2k\pi\sqrt{-1}}{N_i \log q},$$

cu $k \in \mathbb{Z}$ şi $i \in T$. Aceste valori se numesc poli candidaţi ai lui $Z_f(s)$. Pentru un $i \in T$ fixat, valorile $-\nu_i/N_i + (2k\pi\sqrt{-1})/(N_i \log q)$, $k \in \mathbb{Z}$, se numesc polii candidaţi ai lui $Z_f(s)$ asociaţi lui E_i. Deoarece polii proveniţi din $1/(1-q^{-N_i s-\nu_i})$ au ordinul unu, definim ordinul posibil (ordinul candidat) al unui pol candidat s_0 ca fiind cel mai mare număr de curbe excepţionale E_i care au drept pol candidat pe s_0. Evident, ordinul (efectiv) lui s_0 este întotdeauna mai mic sau cel mult egal cu ordinul candidat al lui s_0. De asemenea, este clar şi faptul că un pol candidat de ordin candidat unu este pol dacă şi numai dacă reziduul lui $Z_f(s)$ calculat în s_0 este diferit de 0.

În continuare vom explica formula de calcul a reziduului pe care o vom folosi. Fie s_0 un pol candidat asociat unei curbe excepţionale E_i, $i \in T$ astfel încât s_0 nu este pol candidat pentru nici o altă curbă excepţională E_j, cu $j \in T$ şi $j \neq i$, care intersectează E_i în Y. Fie U o submulţine compactă deschisă a lui E_i. Contribuţia lui U la reziduul lui $Z_f(s)$ calculat în s_0 este prin definiţie contribuţia la reziduul lui $Z_f(s)$ calculat în s_0 a unei submulţimi compacte, deschise V a lui Y care satisface condiţia $V \cap E_i = U$ şi care în plus este disjunctă de toate celelalte E_j care au polul candidat s_0.

Să presupunem că W este o submulţime deschisă şi compactă a lui Y_r cu proprietatea că $W \cap E_i = U$. Fie (z_1, z_2) coordonatele analitice pe W astfel încât $z_1 = 0$ este ecuaţia lui U pe W. Fie

$$f \circ g_1 \circ \cdots \circ g_r = \gamma z_1^{N_i} \qquad \text{şi} \qquad (g_1 \circ \cdots \circ g_r)^* dx = \delta z_1^{\nu_i - 1} dy$$

pe W, unde γ şi δ sunt funţii K-analitice pe W. Cu aceste notaţii, contribuţia

lui U la reziduul lui $Z_f(s)$ calculat în s_0 este egal cu

$$\frac{q-1}{qN_i \log q} \left[\int_U |\gamma|^s |\delta| |dz_2| \right]_{s=s_0}^{\mathrm{mc}}, \tag{5.1}$$

unde cu $[\cdot]_{s=s_0}^{\mathrm{mc}}$ am notat prelungirea meromorfică a funţiei dintre paranteze calculată în $s = s_0$. Această formula a fost obţinută prima dată de Langlands [La] în the cazul $r = t$ şi apoi în cazul general de Dirk Segers în [Se1, Section 2.6].

Vom explica în continuare relaţiile de care vom avea nevoie în cele ce urmează. Fie $r \in T_e$ fixat. Curba excepţională E_r este obţinută prin procesul de eclatare (blowing-up) în punctul $P \in Y_{r-1}$. Fie $y = (y_1, y_2)$ coordonatele locale ale lui Y_{r-1} centrate în P. Scriind acum relaţiile în coordonate locale, obţinem

$$\begin{aligned} f \circ g_1 \circ \cdots \circ g_{r-1} &= d \left(\prod_{i \in S} (a_{i2} y_1 - a_{i1} y_2)^{M_i} \right) \left(\prod_{i \in S'} h_i^{M_i}(y_1, y_2) \right) + \\ &\quad + \text{termeni de grad mai mare,} \end{aligned}$$

unde toţi factorii $a_{i2} y_1 - a_{i1} y_2$ şi h_i sunt polinoame esenţialmente diferite peste K, adică nici un factor nu este egal cu un altul înmulţit eventual cu o constantă din $K^\times$, şi unde polinoamele h_i sunt polinoame omogene, ireductibile de grad cel puţin doi, cu $M_i \geq 1$ pentru toţi $i \in S \cup S'$ şi unde $d \in K^\times$.

Fie

$$(g_1 \circ \cdots \circ g_{r-1})^* dx = \left(e \prod_{i \in S} (a_{i2} y_1 - a_{i1} y_2)^{\mu_i - 1} + \text{termeni de grad mai mare} dy, \right)$$

unde $\mu_i \geq 1$ pentru orice $i \in S$ şi unde $e \in K^\times$. Fie $s_0 = -\nu_r / N_r + (2k\pi\sqrt{-1})/(N_r \log q)$ un pol candidat al funcţiei zeta Igusa $Z_f(s)$ asociat curbei excepţionale E_r. Fie $\alpha_i := \mu_i + s_0 M_i$ pentru toţi $i \in S$. Deoarece

$$N_r = \sum_{i \in S} M_i + \sum_{i \in S'} (\deg h_i) M_i \qquad \text{şi} \qquad \nu_r = \sum_{i \in S} (\mu_i - 1) + 2,$$

se verifică printr-un calcul direct că

$$\sum_{i\in S}(\alpha_i - 1) + \sum_{i\in S'} s_0(\deg h_i)M_i = -2 + \frac{2k\pi\sqrt{-1}}{\log q}. \tag{5.2}$$

În continuare, vom da o altă descriere pentru α_i. Fie F_i punctul de pe E_r care are coordonatele $(a_{i1} : a_{i2})$ relativ la coordonatele omogene $(y_1 : y_2)$ pe $E_r \subset Y_r$. Fie j unicul element din $T \setminus \{r\}$ cu proprietatea că E_j trece prin F_i în Y. Fie ρ numărul de blowing-up-uri de-a lungul lui $g_r, \ldots, g_t$ care sunt centrate în F_i. Obţinem atunci descrierea lui α_i ca fiind $\alpha_i = \nu_j + s_0N_j - (2\rho k\pi\sqrt{-1})/(\log q)$. Aceast rezultat este demonstrat în [Se1, Secţiunea 2.7] în cazul $k = 0$, iar cazul general poate fi tratat în mod similar. Obţinem astfel că $\mathrm{Re}(\alpha_i) < 0$ dacă şi numai dacă $-\nu_r/N_r < -\nu_j/N_j$. Se poate de asemenea verifica fară mare dificultate că

$$\begin{aligned} s_0 \text{ este pol candidat al lui } E_j &\iff \nu_j + s_0N_j \text{ este multiplu de } 2\pi\sqrt{-1}/(\log q) \\ &\iff \alpha_i \text{ este multiplu de } 2\pi\sqrt{-1}/(\log q). \end{aligned}$$

Se ştie (a fost demonstrat în [Lo, Proposition II.3.1]) că $\mathrm{Re}(\alpha_i) < 1$. Împreună cu relaţia (5.2), aceasta arată că $\mathrm{Re}(\alpha_i) \geq -1$ şi că există cel mult un $i \in S$ cu $\mathrm{Re}(\alpha_i) < 0$.

5.2.2 Contribuţia unei curbe excepţionale

Condiţiile (ipotezele) de lucru pentru Propoziţiile 5.1 şi 5.7 Fie $f \in K[x_1, x_2]$ şi fie X o submulţime deschisă şi compactă a lui K^2. Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ compunerea blowing-up-urilor $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$. Curba excepţională a lui g_i şi transformarea strictă a lui sunt notate cu E_i. Fie $r \in T_e$. Curba excepţională E_r este obţinută prin blowing-up în punctul

$P \in Y_{r-1}$. Fie (y_1, y_2) coordonatele locale ale lui Y_{r-1} centrate în P. Putem atunci scrie aceste coordonate locale sub forma

$$\begin{aligned} f \circ g_1 \circ \cdots \circ g_{r-1} &= d\left(\prod_{i\in S}(a_{i2}y_1 - a_{i1}y_2)^{M_i}\right)\left(\prod_{i\in S'} h_i^{M_i}(y_1, y_2)\right) + \\ &\quad + \text{termeni de grad mai mare,} \end{aligned}$$

unde factorii $a_{i2}y_1 - a_{i1}y_2$ şi h_i sunt polinoame esenţialmente diferite peste K (în sensul definit mai sus), şi în plus polinoamele h_i sunt polinoame omogene ireductibile de grad mai mare sau egal cu doi, iar $M_i \geq 1$ pentru orice $i \in S \cup S'$, iar $d \in K^\times$. Fie de asemenea

$$\begin{aligned} (g_1 \circ \cdots \circ g_{r-1})^* dx &= \left(e\prod_{i\in S}(a_{i2}y_1 - a_{i1}y_2)^{\mu_i - 1} + \right. \\ &\quad \left. + \text{termeni de grad mai mare}\right) dy, \end{aligned}$$

cu $\mu_i \geq 1$ pentru toţi $i \in S$ şi $e \in K^\times$.

Propoziţia 5.1. *Fie $s_0 := -\nu_r/N_r$ polul real candidat al lui $Z_f(s)$ asociat curbei E_r. Scriem α_i sub forma $\alpha_i := \mu_i + s_0 M_i \neq 0$ pentru orice $i \in S$.*

Fie $\mathcal{R}$ contribuţia curbei excepţionale E_r la reziduul lui $Z_f(s)$ în punctul s_0. Atunci, $\mathcal{R} \neq 0$ dacă şi numai dacă $|S| \geq 3$ sau $|S'| \geq 1$.

Mai mult, dacă $\mathcal{R} \neq 0$, atunci

1. *$\mathcal{R} > 0$ dacă şi numai dacă $\alpha_i > 0$ pentru toţi $i \in S$ şi*
2. *$\mathcal{R} < 0$ daca si numai daca exista $i \in S$ (şi acesta este unic) astfel încât $\alpha_i < 0$.*

Demonstraţie. Dacă mulţimea S are una sau două elemente şi S' este mulţime vidă, este atunci bine-cunoscut faptul că $\mathcal{R} = 0$. Am menţionat deja în introducere că Loeser [Lo] a demonstrat aceast rezultat folosind formula lui Langlands, iar Dirk Segers a redemonstrat acest rezultat în [Se1, Secţiunea 3.1] ca un caz particular al formulei obţinute de el.

Putem atunci presupune în continuare că $|S| \geq 3$ sau $|S'| \geq 1$.

Să considerăm pentru început cazul în care exista un element $l \in S$ astfel incat $\alpha_l < 0$. Fie $Q := S \setminus \{l\}$ şi $Q' = S'$. Aplicând, eventual, o transformare afină de coordonate, putem presupune că

$$f \circ g_1 \circ \cdots \circ g_{r-1} = d\left(y_2^{M_l} \prod_{i \in Q} (y_1 - a_i y_2)^{M_i}\right)\left(\prod_{i \in Q'} h_i^{M_i}(y_1, y_2)\right) +$$

$+$ termeni de grad mai mare,

şi

$$(g_1 \circ \cdots \circ g_{r-1})^* dx = \left(e y_2^{\mu_l - 1} \prod_{i \in Q} (y_1 - a_i y_2)^{\mu_i - 1} + \right.$$
$$\left. + \text{termeni de grad mai mare}\right) dy,$$

de grad $d_i \geq 2$ având coeficientul lui $y_1^{d_i}$ egal cu 1, $M_i \geq 1$ pentru orice $i \in Q \cup Q'$ iar $d, e \in K^\times$.

Ştim că $\mathcal{R}$ este sumă a dou u a contribuţii, contibuţii pe care le calculăm în două chart-uri diferite folosind formula (5.1). Pentru a calcula prima contribuţie, considerăm coordonatele (z_1, z_2) ale lui Y_r pentru care $g_r(z_1, z_2) = (z_1, z_1 z_2)$, şi obţinem $\kappa := (q-1)/(qN_r \log q)$ înmulţit cu

$$\left[|d|^s |e| \int_P |z_2|^{M_l s + \mu_l - 1} \prod_{i \in Q} \left(|1 - a_i z_2|^{M_i s + \mu_i - 1}\right) \left(\prod_{i \in Q'} |h_i(1, z_2)|^{M_i s}\right) |dz_2|\right]_{s=s_0}^{\text{mc}}$$
$$= |d|^{s_0} |e| \left[\int_P |z_2|^{M_l s + \mu_l - 1} |dz_2|\right]_{s=s_0}^{\text{mc}}$$
$$= |d|^{s_0} |e| \frac{q-1}{q} \frac{1}{q^{\alpha_l} - 1}.$$

Pentru a calcula a doua contribuţie, considerăm coordonatele (z_1', z_2') ale lui Y_r pentru care $g_r(z_1', z_2') = (z_1' z_2', z_2')$, şi obţinem faptul că această contribuţie este κ înmulţit cu

$$\left[|d|^s |e| \int_R \prod_{i \in Q} \left(|z_1' - a_i|^{M_i s + \mu_i - 1}\right) \left(\prod_{i \in Q'} |h_i(z_1', 1)|^{M_i s}\right) |dz_1'|\right]_{s=s_0}^{\text{mc}},$$

care corespunză tor Lemei 5.6 este mai mic decât κ înmulţit cu

$$|d|^{s_0}|e|\left[\int_R |z_1'-a|^{Ms+\mu-1}\,|dz_1'|\right]_{s=s_0}^{\mathrm{mc}} = |d|^{s_0}|e|\frac{q-1}{q}\frac{1}{1-q^{-(Ms_0+\mu)}},$$

unde $a \in R$, $M := \left(\sum_{i\in Q} M_i\right) + \left(\sum_{i\in Q'} d_i M_i\right)$ şi $\mu := \left(\sum_{i\in Q}(\mu_i - 1)\right) + 1$. Folosind faptul că $\alpha_l + (Ms_0 + \mu) = 0$, rezultă că

$$\frac{1}{q^{\alpha_l}-1} + \frac{1}{1-q^{-(Ms_0+\mu)}} = 0,$$

deci $\mathcal{R} < 0$.

Să considerăm acum cazul în care $\alpha_i > 0$ pentru toţi $i \in S$. Acest caz este mai simplu decât celelalte. După ce se calculează $\mathcal{R}$ procedând exact ca în cazul precedent şi folosind formula (5.1), se obţine faptul că $\mathcal{R}$ este o sumă de numere pozitive şi prin urmare este pozitiv. De asemenea, se mai foloseşte şi faptul că $|h|$ este o funţie local constantă dacă h este un polinom ireductibil peste K într-o variabilă de grad cel puţin doi. □

Ne-a mai rămas de demonstrat Lema 5.6. Vom demonstra pentru început Lema 5.3, care este un caz special al Lemei 5.6. În demonstraţia Lemei 5.3, avem nevoie de Lema 5.2.

Lema 5.2. *Fie $h \in R[x]$ un polinom monic, ireductibil, de grad $d \geq 2$ într-o singura variabilă. Există atunci un unic $r \in \mathbb{N}$ şi un element b în R astfel încât*

$$|h(x)| = |(x-b)^d| \qquad \textit{dacă } x \in R \textit{ şi } x \not\equiv b \bmod P^r$$

şi

$$q^{-dr} \leq |h(x)| < q^{-d(r-1)} \qquad \textit{dacă } x \in R \textit{şi } x \equiv b \bmod P^r.$$

Mai mult, b este unic determinat modulo P^r şi $|h(x)|$ este constant pe $b + P^r$.

Demonstraţie. Fie $\beta_1, \ldots, \beta_d$ rădăcinile polinomului h într-o închidere algebrică a lui K. Fie $L := K(\beta_1, \ldots, \beta_d)$ şi fie R_L inelul de valuare al lui L. Notăm extinderea normei de pe K pe L tot cu $|\cdot|$. Să orservăm că $\beta_1, \ldots, \beta_d$ sunt diferiţi deoarece lucrăm în caracteristică zero. De asemenea, $\beta_1, \ldots, \beta_d$ se găsesc în R_L deoarece h este monic iar R_L este închiderea lui R în L. Deoarece

$$\begin{aligned} |h(x)| &= |(x-\beta_1)(x-\beta_2)\cdots(x-\beta_d)| \\ &= |x-\beta_1|\,|x-\beta_2|\cdots|x-\beta_d|, \end{aligned}$$

trebuie să evaluăm $|x-\beta_i|$.

Fie $i \in \{1, \ldots, d\}$. Fie r_i cel mai mare număr natural pentru care există un element $b_i \in R$ care satisface $|b_i - \beta_i| < q^{-(r_i-1)}$. Să remarcăm că exista un cel mai mare astfel de număr deoarece $\beta_i \notin R$. Să remarcăm de asemenea că b_i este demetrminat doar modulo P^{r_i}. Se verifică în continuare că

$$|x-\beta_i| = |x-b_i| \qquad \text{dacă } x \in R \text{ şi } x \not\equiv b_i \bmod P^{r_i}$$

şi

$$q^{-r_i} \le |x-\beta_i| < q^{-(r_i-1)} \qquad \text{dacă } x \in R \text{ şi } x \equiv b_i \bmod P^{r_i}.$$

mai mult, $|x-\beta_i|$ este constant pe $b_i + P^{r_i}$.

În final, vom demonstra că $r_1 = r_2 = \cdots = r_d$ şi vom nota valoarea lor comună cu r. Vom demonstra de asemenea că toate elementele b_i, $i \in \{1, \ldots, d\}$, coincid modulo P^r. Dacă demonstrăm aceste lucruri, cum elementele b_i sunt unic determinate modulo P^r, putem considera $b_1 = b_2 = \cdots = b_d$ şi vom nota valoarea lor comună cu b. Lema atunci rezultă imediat.

Fie $i, j \in \{1, \ldots, d\}$ şi să presupunem că $r_i \ge r_j$. Deoarece β_i şi β_j sunt conjugate şi deoarece $b_i \in R$, obţinem că $b_i - \beta_i$ şi $b_i - \beta_j$ sunt de asemenea conjugate. Cum elementele conjugate au aceeaşi normă, rezultă că

$|b_i - \beta_j| = |b_i - \beta_i| < q^{-(r_i-1)}$. Acest fapt implică $r_i \leq r_j$ şi astfel $r_i = r_j$ şi deci $b_i \equiv b_j \mathrm{mod}\ P^{r_i}$. □

Lema 5.3. *Fie s_0 un număr raţional negativ. Fie $a_1, \ldots, a_k$ elemente diferite din R. Să presupunem că pentru fiecare $i \in \{1, \ldots, k\}$ numerele întregi $M_i \geq 1$ şi $\mu_i \geq 1$ satisfac $\alpha_i := \mu_i + s_0 M_i < 1$. Fie $h_{k+1}, \ldots, h_l \in R[x]$ polinoame monice ireductibile într-o variabilă de grad cel puţin doi. Să notăm cu d_i gradul polinomului h_i şi să presupunem că pentru fiecare $i \in \{k+1, \ldots, l\}$ avem un întreg $M_i \geq 1$. Fie r_i numărul natural pe care l-am asociat lui h_i în lema precedentă, şi fie b_i elementul corespunzător din R care este determinat modulo P^{r_i}.*

Să presupunem că $r_{k+1} = \cdots = r_l$ şi să notăm acest număr cu r. Să presupunem că $a_1 \equiv \cdots \equiv a_k \equiv b_{k+1} \equiv \cdots \equiv b_l \ mod\ P^r$ şi că $a_i \not\equiv a_j \ mod\ P^{r+1}$ pentru $i \neq j$. Fie acum $a \in R$ astfel încât $a \equiv a_1 \ mod\ P^r$. Să notăm $M := M_1 + \cdots + M_k + d_{k+1}M_{k+1} + \cdots + d_l M_l$, $\mu := (\mu_1 - 1) + \cdots + (\mu_k - 1) + 1$ şi $\alpha := \mu + s_0 M$. Să presupunem că $0 < \alpha$ şi că $k \geq 2$ sau $l \geq k+1$. Atunci

$$\left[\int_{a+P^r} |x-a_1|^{M_1 s+\mu_1-1} \cdots |x-a_k|^{M_k s+\mu_k-1} |h_{k+1}(x)|^{M_{k+1}s} \ldots |h_l(x)|^{M_l s} |dx|\right]_{s=s_0}^{\mathrm{mc}}$$
$$< \left[\int_{a+P^r} |x-a|^{Ms+\mu-1} |dx|\right]_{s=s_0}^{\mathrm{mc}}.$$

Mai mult, integranţii sunt aceiaşi pentr fiecare $x \in R \setminus (a + P^r)$.

Observaţia 5.4. *Condiţiile $a_i \equiv a_j \ mod\ P^r$ şi $a_i \not\equiv a_j \ mod\ P^{r+1}$ pentru $i, j \in \{1, \ldots, k\}$ cu $i \neq j$ implică faptul că $k \leq q$.*

Observaţia 5.5. *Ştim că*

$$\alpha - 1 = \sum_{i=1}^{k} (\alpha_i - 1) + \sum_{i=k+1}^{l} s_0 d_i M_i.$$

Prin urmare, condiţia $\alpha_i < 1$ pentru fiecare $i \in \{1, \ldots, k\}$ implică faptul că $\alpha < \alpha_i$.

Demonstraţie. Într-o primă etapă, ne reducem la cazul în care polinoamele h_i nu apar. Obţinem succesiv că

$$\begin{aligned}
&\left[\int_{a+P^r} |x-a|^{Ms+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}} \\
&\quad= \frac{q-1}{q}\frac{q^{-r\alpha}}{1-q^{-\alpha}} \\
&\quad= \frac{q-1}{q}\frac{q^{-r((M_1+\cdots+M_k)s_0+\mu)}}{1-q^{-\alpha}} q^{-r(d_{k+1}M_{k+1}+\cdots+d_lM_l)s_0} \\
&\quad\geq \frac{q-1}{q}\frac{q^{-r((M_1+\cdots+M_k)s_0+\mu)}}{1-q^{-((M_1+\cdots+M_k)s_0+\mu)}} q^{-r(d_{k+1}M_{k+1}+\cdots+d_lM_l)s_0} \\
&\quad= q^{-r(d_{k+1}M_{k+1}+\cdots+d_lM_l)s_0}\left[\int_{a+P^r} |x-a|^{(M_1+\cdots+M_k)s+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}},
\end{aligned}$$

cu inegalitate strictă dacă $l \geq k+1$. Deoarece $|h_i|$ este constant pe $a+P^r$ cu $q^{-d_ir} \leq |h_i(a)|$, $s_0 < 0$ şi cel de-al doilea factor din membrul drept al următoarei inegalităţi este pozitiv (acest fapt rezultă din calculul acestui factor în partea a doua a demonstraţiei), obţinem:

$$\begin{aligned}
&\left[\int_{a+P^r} |x-a_1|^{M_1s+\mu_1-1}\cdots|x-a_k|^{M_ks+\mu_k-1}|h_{k+1}(x)|^{M_{k+1}s}\ldots|h_l(x)|^{M_ls}\,|dx|\right]_{s=s_0}^{\mathrm{mc}} \\
&\leq\ q^{-r(d_{k+1}M_{k+1}+\cdots+d_lM_l)s_0}\left[\int_{a+P^r} |x-a_1|^{M_1s+\mu_1-1}\cdots|x-a_k|^{M_ks+\mu_k-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}.
\end{aligned}$$

Aceste două inegalităţi implică faptul că este suficient să considerăm cazul în care polinoamele h_i nu apar.

În cea de-a doua etapă, vom demonstra faptul că

$$\begin{aligned}
&\left[\int_{a+P^r} |x-a|^{Ms+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}} > \\
&> \left[\int_{a+P^r} |x-a_1|^{M_1s+\mu_1-1}\cdots|x-a_k|^{M_ks+\mu_k-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}
\end{aligned}$$

dacă $k \geq 2$, unde $M = M_1 + \cdots + M_k$.

Să calculăm cei doi membrii. Pentru început, să partiţionăm domeniul de integrare al integralei din membrul drept în următoarele $k+1$ mulţimi:

$a_1 + P^{r+1}, \ldots, a_k + P^{r+1}$ şi în mulţimea constând din toate celelalte puncte ale mulţimii $a + P^r$. În acest fel, inegalitatea de mai sus devine.

$$\begin{aligned}\frac{q-1}{q}\frac{q^{-(r-1)\alpha}}{q^\alpha - 1} &> \frac{q-1}{q}\frac{q^{-r\alpha_1}}{q^{\alpha_1}-1}q^{-r(\alpha_2-1)-r(\alpha_3-1)-\ldots-r(\alpha_k-1)} + \cdots \\ &+\frac{q-1}{q}\frac{q^{-r\alpha_k}}{q^{\alpha_k}-1}q^{-r(\alpha_1-1)-r(\alpha_2-1)-\ldots-r(\alpha_{k-1}-1)} \\ &+\frac{q-k}{q^{r+1}}q^{-r(\alpha_1-1)-r(\alpha_2-1)-\ldots-r(\alpha_k-1)}.\end{aligned}$$

Dacă folosim faptul că $\alpha - 1 = \sum_{i=1}^{k}(\alpha_i - 1)$, acest inegalitatea devine echivalentă cu

$$(q-1)\frac{q^\alpha}{q^\alpha - 1} > \frac{q-1}{q^{\alpha_1}-1} + \cdots + \frac{q-1}{q^{\alpha_k}-1} + q - k$$

şi deci şi cu

$$\frac{1}{q^\alpha - 1} + \frac{k-1}{q-1} > \frac{1}{q^{\alpha_1}-1} + \cdots + \frac{1}{q^{\alpha_k}-1}.$$

Să considerăm funcţia

$$h :]0,1] \to \mathbb{R} : x \mapsto \frac{1}{q^x - 1}.$$

Se arată fără mare dificultate că funcţia h este convexă, adică că, i.e. $h''(x) > 0$ ppentru orice $x \in]0,1[$. Fie funţia liniară g, i.e. funcţia polinomială de grad unu, determinată unic de relaţiile $g(\alpha) = h(\alpha) = 1/(q^\alpha - 1)$ şi $g(1) = h(1) = 1/(q-1)$. Atunci

$$\begin{aligned}\frac{1}{q^\alpha - 1} + \frac{k-1}{q-1} &= g(\alpha) + (k-1)g(1) \\ &= g(\alpha_1) + \cdots + g(\alpha_k) \\ &> h(\alpha_1) + \cdots + h(\alpha_k) \\ &= \frac{1}{q^{\alpha_1}-1} + \cdots + \frac{1}{q^{\alpha_k}-1}.\end{aligned}$$

în relaţiile de mai sus, am folosit în linia a doua faptul că funcţia g este liniară şi că $\alpha + k - 1 = \alpha_1 + \cdots + \alpha_k$. În linia a treia a inegalităţilor de mai

sus am folosit faptul că funţia g este liniară şi funţia h este convexă, adică $g(\alpha) = h(\alpha)$ şi $g(1) = h(1)$ şi de asemenea faptul că $0 < \alpha < \alpha_i < 1$ pentr orice $i \in \{1, \ldots, k\}$.

Ultima afirmaţie din lema este uşor de verificat. □

Lema 5.6. *Fie s_0 un număr raţional negativ. Fie $\gamma, \delta \in R[x]$ polinoame monice într-o variabilă. Să presupunem că δ se descompune în factori (polinoame) liniari peste R şi că toate rădăcinile lui δ sunt de asemenea rădăcini ale lui γ.*

Scriem polinomul γ sub forma

$$\gamma(x) = \left(\prod_{i\in Q}(x - a_i)^{M_i}\right)\left(\prod_{i\in Q'} h_i^{M_i}(x)\right)$$

unde a_i, pentru $i \in Q$, sunt elemente diferite ale lui R, unde h_i, $i \in Q'$, polinoame monice ireductibile peste R, diferite, de grad cel puţin doi, şi unde $M_i \geq 1$ pentru orice $i \in Q \cup Q'$.

Să notăm cu d_i gradul polinomului h_i. Scriem polinomul $\delta(x)$ sub forma

$$\delta(x) = \prod_{i\in Q}(x - a_i)^{\mu_i - 1},$$

unde $\mu_i \geq 1$ pentru orice $i \in Q$. Fie un $a \in R$ arbitrar. Notăm cu $M := \left(\sum_{i\in Q} M_i\right) + \left(\sum_{i\in Q'} d_i M_i\right)$ şi $\mu := \left(\sum_{i\in Q}(\mu_i - 1)\right) + 1$. Să presupunem că $0 < \alpha := \mu + s_0 M$ şi $1 > \alpha_i := \mu_i + s_0 M_i$ pentru orice $i \in Q$. Fie $|Q| \geq 2$ sau $|Q'| \geq 1$.

Atunci

$$\left[\int_R |\gamma(x)|^s |\delta(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}} < \left[\int_R |x - a|^{Ms+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}.$$

Demonstraţie. Pentru a demonstra această lemă, vom asocia un arbore polinomului monic $g \in R[x]$ într-o singură variabilă. Construcţia arborelui o

vom face astfe: dacă $a_1, a_2 \in R$ sunt rădăcini ale lui g şi dacă $a_1 \equiv a_2 \bmod P^r$ astfel încât $a_1 \not\equiv a_2 \bmod P^{r+1}$, atunci asociem un vârf în arbore lui $a_1 + P^r$.

Dacă polinomul g are un factor ireductibil de grad cel puţin doi, acestui factor i-am asociat mai sus un număr natural $r \in \mathbb{N}$ precum şi $b + P^r$; în arbore îi asociem lui $b + P^r$ un vârf. Dacă de exemplu $a + P^r$ apare de mai multe ori în ca în procedeul descris mai sus, îi asociem în arbore un singur vârf.

Muchiile din graf sunt definite astfel: dacă avem două vârfuri în graf asociate lui $a + P^r$ şi lui $b + P^t$, cu $r > t$, atunci unim cele două vârfuri dacă $a + P^r \subset b + P^t$ şi în plus dacă pentru orice $c + P^u$ corespunzător unui alt vârf, avem $a + P^r \subset c + P^u \subset b + P^t$.

Să observăm că acest arbore este finit şi are o rădăcină.

Să pornim din membrul stâng al inegalităţii pe care vrem să o demonstrăm şi să considerăm arborele asociat lui γ. Vom construi pas cu pas alţi integranţi cărora le asociem arbori construiţi ca mai devreme, exceptând un vârf de la capătul arborelui. Prin urmare, arborele se reduce la fiecare pas şi devine astfel din ce în ce mai simplu. Continuăm procedeul descris mai sus până când arborele dispare complet. La finalul acestui procedeu, integrandul care se va obţine va fi cel din membrul drept al inegalităţii pe care vrem să o demonstrăm.

Pentru început, să explicăm în detaliu prima etapă. Alegem un vârf de la capătul (sfârşitul) arborelui lui γ. Acest vârf este asociat unui anume element, deci exista un r astfel încât elementul ales este de forma $a_0 + P^r$ şi aparţine lui R/P^r. Fie $a_1, \ldots, a_k$ toate rădăcinile lui γ pentru care $a_i \equiv a_0 \bmod P^r$. Să remarcăm faptul că $a_i \not\equiv a_j \bmod P^{r+1}$ pentru $i, j \in \{1, \ldots, k\}$ cu $i \neq j$, deoarece am ales un vârf de la sfârşitul arborelui.

Să notăm cu $h_{k+1}, \ldots, h_l$ toţi factorii ireductibili ai lui γ cărora li se

asociază $a_0 + P^r$. Fie

$$\gamma(x) = \widetilde{\gamma}(x)(x-a_1)^{M_1}\cdots(x-a_k)^{M_k}h_{k+1}^{M_{k+1}}\cdots h_l^{M_l}$$

şi

$$\delta(x) = \widetilde{\delta}(x)(x-a_1)^{\mu_1-1}\cdots(x-a_k)^{\mu_k-1}.$$

Notăm cu $M_0 := M_1+\cdots+M_k+d_{k+1}M_{k+1}+\cdots+d_lM_l$ şi cu $\mu_0 := (\mu_1-1)+\cdots+(\mu_k-1)+1$. Fie $\gamma_1(x) = \widetilde{\gamma}(x)(x-a_0)^{M_0}$ şi $\delta_1(x) = \widetilde{\delta}(x)(x-a_0)^{\mu_0-1}$.

Rezultă atunci că

$$\begin{aligned}
&\left[\int_{a_0+P^r}|\gamma(x)|^s|\delta(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&= \left[|\widetilde{\gamma}(a_0)|^s|\widetilde{\delta}(a_0)|\int_{a_0+P^r}\prod_{i=1}^{k}|x-a_i|^{M_is+\mu_i-1}\prod_{j=k+1}^{l}|h_j(x)|^{M_js}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&= |\widetilde{\gamma}(a_0)|^{s_0}|\widetilde{\delta}(a_0)|\left[\int_{a_0+P^r}\prod_{i=1}^{k}|x-a_i|^{M_is+\mu_i-1}\prod_{j=k+1}^{l}|h_j(x)|^{M_js}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&< |\widetilde{\gamma}(a_0)|^{s_0}|\widetilde{\delta}(a_0)|\left[\int_{a_0+P^r}|x-a_0|^{M_0s+\mu_0-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&= \left[|\widetilde{\gamma}(a_0)|^s|\widetilde{\delta}(a_0)|\int_{a_0+P^r}|x-a_0|^{M_0s+\mu_0-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&= \left[\int_{a_0+P^r}|\widetilde{\gamma}(x)|^s|\widetilde{\delta}(x)||x-a_0|^{M_0s+\mu_0-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\
&= \left[\int_{a_0+P^r}|\gamma_1(x)|^s|\delta_1(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}.
\end{aligned}$$

Am folosit aici lema precedentă şi de două ori faptul că $|\widetilde{\gamma}|$ şi $|\widetilde{\delta}|$ sunt constante pe $a_0 + P^r$.

Rezultă mai departe că

$$\begin{aligned}
&\left[\int_{R\setminus(a_0+P^r)} |\gamma(x)|^s|\delta(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}} \\
&= \left[\int_{R\setminus(a_0+P^r)} |\widetilde{\gamma}(x)|^s|\widetilde{\delta}(x)| \prod_{i=1}^{k} |x-a_i|^{M_i s+\mu_i-1} \prod_{j=k+1}^{l} |h_j(x)|^{M_j s}\,|dx|\right]_{s=s_0}^{\mathrm{mc}} \\
&= \left[\int_{R\setminus(a_0+P^r)} |\widetilde{\gamma}(x)|^s|\widetilde{\delta}(x)||x-a_0|^{M_0 s+\mu_0-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}} \\
&= \left[\int_{R\setminus(a_0+P^r)} |\gamma_1(x)|^s|\delta_1(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}},
\end{aligned}$$

unde am folosit ultima afirmaţie din lema precedentă, şi am obţinut că

$$\left[\int_{R} |\gamma(x)|^s|\delta(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}} < \left[\int_{R} |\gamma_1(x)|^s|\delta_1(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}.$$

În cea de-a doua etapă procedăm analog cu ceea ce am făcut în prima fază, dar folosim acum $\gamma_1(x)$ în loc de $\gamma(x)$ şi $\delta_1(x)$ în loc de $\delta(x)$. Să observăm că M şi μ determinaţi de γ şi δ sunt identice cu cele analoage determinate de γ_1 şi δ_1. Să mai observăm aici că arborele asociat lui γ_1 coincide cu arborele asociat lui γ, cu excepţia faptului că lipseşte un vârf.

Să notăm cu w numărul de vârfuri din arborele asociat lui γ. Atunci, după w paşi, arborele dispare complet. Dacă rădăcina arborelui este asociată lui $a_0' + P^{r'}$, atunci $\gamma_w(x) = (x-a_0')^M$ şi $\delta_w(x) = (x-a_0')^{\mu-1}$.

Prin urmare,

$$\begin{aligned}\left[\int_R |\gamma(x)|^s|\delta(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}} &< \left[\int_R |\gamma_1(x)|^s|\delta_1(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\ &< \left[\int_R |\gamma_2(x)|^s|\delta_2(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\ &< \dots\\ &< \left[\int_R |\gamma_w(x)|^s|\delta_w(x)|\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\ &= \left[\int_R |x-a_0'|^{Ms+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}\\ &= \left[\int_R |x-a|^{Ms+\mu-1}\,|dx|\right]_{s=s_0}^{\mathrm{mc}}.\end{aligned}$$

□

Ipotezele de lucru ale propoziţiei care urmează sunt ipotezele de la începutul acestei secţiuni.

Propoziţia 5.7. *Fie* $s_0 := -\nu_r/N_r + (2k\pi\sqrt{-1})/(N_r \log q)$ *un pol arbitrar candidat al funcţiei* $Z_f(s)$ *asociat lui* E_r.

Să presupunem că $\alpha_i := \mu_i + s_0 M_i$ *nu este un multiplu al lui* $2\pi\sqrt{-1}/(\log q)$ *pentru toţi* $i \in S$.

Să presupunem că $|S| = 3$ *şi* $|S'| = 0$. *Fie* $\mathcal{R}$ *contribuţia lui* E_r *la reziduul lui* $Z_f(s)$ *în* s_0. *Atunci,* $\mathcal{R} \neq 0$.

Demonstraţie. Notăm elementele mulţimii S cu 1, 2 şi 3. Cu aceste notaţii, din egalitatea (5.2) rezultă că $\alpha_1 + \alpha_2 + \alpha_3 = 1 + (2k\pi\sqrt{-1})/(\log q)$.

Făcând eventual o transformare afină de coordonate, putem presupune că

$$f \circ g_1 \circ \cdots \circ g_{r-1} = dy_2^{M_1} y_1^{M_2} (y_1 - a y_2)^{M_3} + \text{ termeni de grad mai mare,}$$

şi

$$(g_1 \circ \cdots \circ g_{r-1})^* dx = \left(e y_2^{\mu_1 - 1} y_1^{\mu_2 - 1} (y_1 - a y_2)^{\mu_3 - 1} + \text{ termeni de grad mai mare}\right) dy$$

cu $a \in R \setminus P$ şi $d, e \in K^\times$.

Prin urmare, am obţinut

$$\begin{aligned}\mathcal{R} &= |d|^{s_0}|e|\left(\frac{q-1}{q}\frac{1}{q^{\alpha_1}-1}+\frac{q-1}{q}\frac{1}{q^{\alpha_2}-1}+\frac{q-1}{q}\frac{1}{q^{\alpha_3}-1}+\frac{q-2}{q}\right)\\ &= |d|^{s_0}|e|\left(\frac{1-q^{\alpha_1-1}}{1-q^{-\alpha_1}}\cdot\frac{1-q^{\alpha_2-1}}{1-q^{-\alpha_2}}\cdot\frac{1-q^{\alpha_3-1}}{1-q^{-\alpha_3}}\right)\\ &\neq 0.\end{aligned}$$

În calculele de mai sus, a doua egalitate poate fi verificată prin calcul direct şi se datorează lui Sally and Taibleson[ST]. □

Observaţia 5.8. *Determinarea tuturor polilor (reali şi complecşi) ai unei curbe absolut analitic ireductibile este acum imediată. Acesta a fost unul dintre rezultatele fundamentale ale lucrării [Ig2] a lui Igusa. Igusa a mai folosit în demonstraţia acestui rezultat şi formula lui Sally-Taibleson.*

Observaţia 5.9. *Să subliniem aici faptul că dacă $|S| \neq 3$ sau $|S'| \neq 0$, nu se ştie care poli candidaţi non-reali sunt poli şi care nu. Este posibil ca un pol candidat real să fie pol, iar alţi poli candidat având aceeaşi parte reală să nu fie poli. Acest lucru se întâmplă de exemplu în cazul curbei $f = x_1^2 + x_2^2$ şi $p = 2$ (vezi [Se1, Exemplul 2.8]).*

5.2.3 Concluzii finale: Polii funcţiei zeta Igusa p-adice

Fie $f \in K[x_1, x_2]$ şi fie X o submulţime deschisă şi compactă a lui K^2. Să presupunem că f_{red} are doar un punct singular P_0 în X. Fie $g : Y \to X$ o rezoluţie scufundată a lui f. Fie $g = g_1 \circ \cdots \circ g_t : Y = Y_t \to X = Y_0$ o compunere de blowing-up-uri $g_i : Y_i \to Y_{i-1}$, $i \in T_e := \{1, \ldots, t\}$, centrată în $P_{i-1} \in Y_{i-1}$. Curba excepţională a lui g_i şi transformarea strictă a acestei curbe sunt notate cu E_i. Subvarietăţile închise ale lui Y de codimensiune

unu care reprezintă zerourile transformării sticte ale unui factor ireductibil al lui f în $K[x,y]$ le notăm cu E_j, $j \in T_s$.

Transformările corespunzătoare în Y_i, $i \in \{0,\dots,t-1\}$, le notăm similar. Fie $T = T_e \cup T_s$.

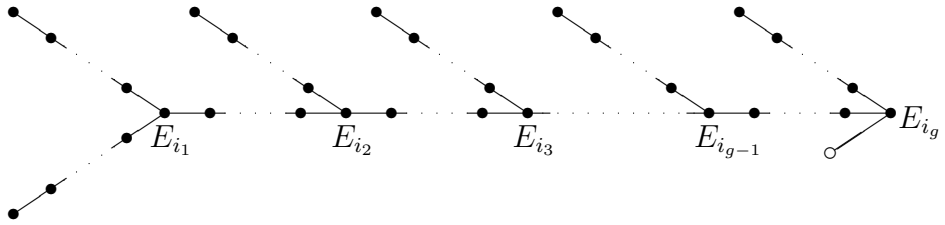
În graful (dual) al rezoluţiei scufundate al lui f în P_0, se asociază fiecărei curbe excepţionale un vârf (reprezentat printr-un punct) şi fiecărei intersecţii dintre curbe excepţionale din Y o muchie, care leagă vârfurile corespunzătoare.

Asociem de asemenea fiecărei componente analitic ireductibile a transformării stricte a lui f în P_0 un vârf (reprezentat de un cerc), şi unicului său punct de intersecţie cu o curbă excepţională în Y muchia corespunzătoare. Este clar din construcţie că acest graf este un arbore finit, conex.

În continuare, fiecărui vârf al grafului rezoluţiei scufundate îi asociem raportul corespunzător ν_i/N_i. Acest fapt transformă graful rezoluţiei scufundate într-un arbore ordonat. Mai precis, vârfurile pentru care numărul asociat este egal cu $\min_{i\in T} \nu_i/N_i$, împreună cu muchiile corespunzătoare, formează o componentă conexă $\mathcal{M}$ a grafului rezoluţiei scufundate. Dacă începem cu un vârf terminal a părţii minimale $\mathcal{M}$, numerele ν_i/N_i sunt strict crescătoare de-a lungul oricărui drum din arbore, exceptând $\mathcal{M}$.

Acest fapt rezultă din relaţia (5.2) şi din marginea pentru α-uri, lucru care implică de exemplu că există cel mult un E_j care intersectează un E_r dat, cu $r \in T_e$, în Y cu $\nu_j/N_j < \nu_r/N_r$ (vezi secţiunea precedentă). Pentru mai multe detalii, referinţa bibliografică este [Ve2, Teorema 3.3], unde corpul de bază peste care se lucrează este $\mathbb{C}$ în loc de K, dar demonstraţia este absolut similară.

Exemplul 5.10. *Dacă f este absolut analitic ireductibilă în P_0 cu g exponenţi Puiseux diferiţi, atunci graful rezoluţiei este de forma*



Aici, partea minimală $\mathcal{M}$ constă doar din E_{i_1} (vezi [St, Corolarul 2.1] sau [Ve2, Propozitia 3.6]).

Teorema 5.11. *Să presupunem că suntem în ipotezele din primul paragraf al acestei seţiuni.*

Atunci:

1. *un număr real s_0 este pol de ordin doi daca si numai daca exista $i, j \in T$ cu $s_0 = -\nu_i/N_i = -\nu_j/N_j$ astfel încât E_i şi E_j se intersectează în Y. Mai mult, $Z_f(s)$ are cel mult un pol real de ordin doi, iar dacă există un pol de ordin doi, acesta este polul cel mai apropiat de origine.*

2. *un număr real $s_0 \in \{-\nu_i/N_i \mid i \in T_e\} \setminus \{-\nu_i/N_i \mid i \in T_s\}$ care nu este pol de ordin doi este pol de orin întâi dacă şi numai dacă există cel puţin un $i \in T_e$ cu $s_0 = -\nu_i/N_i$ astfel încât $f \circ g_1 \circ \cdots \circ g_{i-1}$ este dat în coordonate locale centrate în P_{i-1} de o serie de puteri a cărei componentă de grad cel mai mic este un polinom omogen care nu este o putere a unui polinom liniar (de grad unu) sau un produs de două astfel de puteri*

3. *un număr real $s_0 \in \{-\nu_i/N_i \mid i \in T_s\}$ care nu este pol de ordin doi este pol de ordin unu pentru o vecinătate deschisă şi compactă X a lui P_0 suficient de mică.*

Demonstraţie. (1) Este clar că există $i, j \in T$ cu $s_0 = -\nu_i/N_i = -\nu_j/N_j$ astfel încât E_i şi E_j se intersectează în Y dacă s_0 este un pol real de ordin 2. Dacă E_i şi E_j se intersectează în Y cu $s_0 = -\nu_i/N_i = -\nu_j/N_j$, atunci contribuţia lui $P := E_i \cap E_j$ la coeficientul b_{-2} în seria Laurent

$$\frac{b_{-2}}{(s-s_0)^2} + \frac{b_{-1}}{s-s_0} + b_0 + b_1(s-s_0) + \cdots$$

a lui $Z_f(s)$ în s_0 este egal cu

$$|\varepsilon(P)|^{s_0}|\eta(P)|\frac{(q-1)^2}{q^2 N_i N_j (\log q)^2} > 0.$$

Prin urmare, contribuţia a două perechi diferite care se intersectează ambele în Y nu se pot anula una pe cealaltă. Cealaltă afirmaţie din acest punct al teoremei rezultă din structura de arbore ordonat al grafului rezoluţiei scufundate.

(2) Partea cu 'şi numai dacă' a afirmaţiei din teoremă este partea cunoscută din Propoziţia 5.1 şi care se datorează lui Loeser.

Pentru implicaţia reciprocă, vom folosi Propoziţia 5.1 şi structura de arbore ordonat al grafului rezoluţiei scufundate. Există două posibilităţi.

Să considerăm primul caz în care E_i este partea minimală a grafului rezoluţiei scufundate. În acest caz, există o singură contribuţie la reziduu, care este pozitivă. În celălat caz, există cel puţin o contribuţie la reziduu care nu este zero, iar toate contribuţiile de acest fel sunt negative.

(3) Există şi în acest caz două posibilităţi. Primul caz este acela în care $s_0 = -\nu_i/N_i$, cu $i \in T_s$ şi E_i este partea minimală a grafului rezoluţiei scufundate. În această situaţie există o singură contribuţie la reziduu, care este pozitivă.

în cel de-al doilea caz, considerăm o vecinătate suficient de mică deschisă şi compactă V a lui $\cup_{i\in T_e} E_i \subset Y$ pe care toţi E_i cu $i \in T_s$ astfel încât $s_0 = -\nu_i/N_i$, au o contribuţie negativă la reziduul lui $Z_f(s)$ în s_0. E_i-urile,

cu $i \in T_e$ şi $s_0 = -\nu_i/N_i$, au o contribuţie negativă la reziduul lui $Z_f(s)$ în s_0. Dacă înlocuim X cu $g(V)$ sau cu o vecinătate deschisă şi compactă a lui P conţinută în $g(V)$, obţinem ceea ce aveam de demonstrat. □

Observaţia 5.12. *Din teorema precedentă şi din rezultatul lui Loeser menţionat în introducere, rezultă că t $Re(s_0)$ este pol al lui $Z_f(s)$ dacă s_0 este pol al lui $Z_f(s)$. Prin urmare, mulţimea părţilor reale ale polilor lui $Z_f(s)$ este cunoscută. Acest lucru este important deoarece aceştia determină comportamentul asimptotic al numărului de soluţii al congruenţelor polinomiale corespunzătoare (vezi [Se2] pentru mai multe detalii).*

Capitolul 6

Rezultate fundamentale privind designurile eşalon şi baze Gröbner asociate

Designul experimentelor este o ramură importantă a Statisticii care are ca subiect important de studiu designurile full-factorial. În cadrul acestui proiect ne-am propus şi am reuşit să folosim metode ale Algebrei Comutative pentru a explora probleme relevante (cum ar fi bazele Gröbner, fracţiile, polinomul Hilbert) ale designurilor eşalon, o mulţime $\mathcal{E}$ de puncte experimentale având anumite proprietăţi speciale.

Designurile eşalon generalizează designurile full factorial inverstigate în [CPRW], [CR], [R], [RR]. Pe scurt, contibuţia noastră în acest domeniu constă într-o demonstraţie originală a existenţei unei baze Gröbner pentru un ideal design $\mathcal{I}(\mathcal{E})$. Mai mult, rezultatul nostru generalizează Teorema 2.18 a lui Robbiano [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001,

pp.179-204]. În plus, am obţinut caracterizarea polinomului Hilbert polynomial asociat unui design eşalon şi am introdus şi studiat fracţii ale designurilor eşalon. Rezultatele din teoremele pe care le-am obţinut extind Teoremele 4.5 şi 5.6 din [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204] de la cazul designurilor full factorial la cazul designurilor eşalon.

În ultimii ani, "Statistica Algebrică" s-a dezvoltat la graniţa dintre Algebra Comutativă şi Statistică. Intr-adevăr, teoria si rezultatele din Algebra Comutativă au ajutat în procesul de înţelegere a unor diverse ramuri din statistică, cum ar fi Designul Experimentelor (DoE-Design of Experiments). Această interacţiune este ilustrată în lucrarea noastră, în care demonstrăm proprietăţi importante pentru designurile eşalon.

Mai precis, folosim metode de Algebra Comutativă pentru a studia probleme referitoare la designurile eşalon care provin din DoE. Pentru a înţelege mai bine eficienţa şi importanţa studiului designurilor eşalon în studiul şi analiza unor modele economice cu aplicaţii practice, vom prezenta un exemplu. Un magazin care comercializează echipamente de calcul are o anumită stategie de aprovizionare, bazată pe diverse considerente economice, cu laptouri de-a lungul unui an. Astfel, în prima perioada (lunile ianuarie-aprilie) magazinul are în stoc următoarele modele de laptopuri: Allview, Acer, HP, Asus, Lenovo, Samsung, Toschiba şi Dell. În următoarea perioada (lunile mai-august), magazinul are în stoc mărcile Allview, Acer, HP, Asus şi Lenovo, iar în ultima perioadă (lunile septembrie-decembrie), din anumite motive, poate are în stoc doar Allview, Acer şi HP.

Această strategie poate fi văzută ca o mulţime de puncte din $\mathbb{Z}_+^2$, notate (L, M), unde M reprezintă marca (brand-ul) laptopului, iar L reprezintă

luna. Variabila M poate lua una dintre valorile 0,1,2,3,4,5,6 sau 7, care au seminicaţia: 0=Allview, 1=Acer, 2=HP, 3=Asus, 4=Lenovo, 5=Samsung, 6=Toschiba şi 7=Dell. Valoarea pentru variabila L poate fi una din mulţimea $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, unde 0=ianuarie, 1=februarie,. . ., 11=decembrie.

Prin urmare, această mulţime de puncte împreună cu resticţiile date de disponibiliatea brand-ului într-o anumită lună, formează un design eşalon. Se poate observa că vectorii dominanţi, adică vectorii care mărginesc designul eşalon, sunt $(0, 8)$, $(4, 5)$, $(8, 3)$ şi $(12, 0)$. Astfel, de exemplu punctul $(3, 3)$ care se găseşte în design arată că în luna aprilie brand-ul Asus este disponibil în magazin.

Departamentul de marketing al magazinului din acest exemplu doreţe să anaizeze profitul obţinut din acestă strategie. În acest scop, işi formează un grup de potenţiali cumpărători cărora le cere să facă un rating, adică să noteze pe o scară de la 0 la 10 diverse posibilităţi, i.e. diverse puncte ale designului eşalon. În acest rating, cumpărătorii trebuie să ia în consideraţie bugetul lor într-o anume perioadă de timp şi preferinţa lor pentru un anumit brand. În acest fel, fiecărui punct al desginului îi putem asocia o anumită valoare, de exemplu media notelor acordate de subiecţii chestionarului. Obţinem astfel o funţie care are ca domeniu de definiţie punctele designului. Din Cororalul 2.14 din lucrarea lui Robiano [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204], rezultă că orice funţie definită pe o mulţime finită cu valori într-un corp arbitrar este o funcţie polinomială şi se numeşte în Statistica Algebrică modelul polinomial al designului. Această funţie polinomială furnizează multe informaţii care pot fi folosite pentru a îmbunătăţii stategia de marketing a magazinului.

În afară de exemplului prezentat mai sus, există în mod evident numeroase alte exemple din domeniul economic care pot fi modelate folosind designurile experimentale.

Revenind la exemplul prezentat mai sus, este clar că nici un potenţial client nu va dori să noteze toate punctele din design, fiind În general mult prea multe posibilităţi. Din acest motiv, se folosesc modele care vin din fraţii (anumite submulţimi) ale designului. Aceste modele pot fi apoi folosite pentru a obţine o reconstru]c tie cât mai fidelă a modelului din problema de marketing prezentată.

Dat un design eşalon $\mathcal{E}$, o fracţie $\mathcal{F}$ a desinului este o submulţime a acestei mulţimi de puncte, dar din punct de vedere algebric, descrierea fraţiei nu este deloc una canonică. Este clar că idealul de definiţie $\mathcal{I}(\mathcal{F})$, care defineşte fraţia dată $\mathcal{F}$, conţine $\mathcal{I}(\mathcal{E})$ care reprezintă idealul de definiţie al eşalonului $\mathcal{E}$. Acest lucru are o explicaţie algebrică simplă: orice polinom care se anulează pe toate punctele din $\mathcal{E}$ automat se anulează pe toate punctele din $\mathcal{F}$. Pentru mai multe detalii despre aceste fraţii, pentru a vedea cum pot fi convenabil alese aceste fracţii şi cum pot fi ele folosite în teoria generaă a DoE, recomandăm lucrarea lui Robiano, [L.Robiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 2001, pp.179-204].

Pentru a enunţa principalele rezultate obţinute în acestă direcţie de cercetare, începem prin a reaminti definiţia unui design eşalon.

Definiţia 6.1. *Fie k un corp şi fie $m \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Un **design** $\mathcal{D}$ este o mulţine finită de puncte distincte din k^m.*

*Se numeşte **idealul designului** $\mathcal{D}$ idealul $I(\mathcal{D})$ care conţine toate polinoamele din $k[x_1, \ldots, x_m]$ care se anulează în toate punctele lui $\mathcal{D}$.*

Un prim rezultat fundamental al acestei cercetări îl constituie teorema în care am obţinut o bază Gröbner pentru idealul $\mathcal{I}(\mathcal{E})$, unde $\mathcal{E}$ este un design eşalon, teoremă pe care o vom enunţa mai jos după ce vom defini designul eşalon. Rezultatul obţinut de noi generalizează Teorema 2.18 din lucrarea amintită a lui Robiano.

Am considerat apoi polinomul asociat unui design $\mathcal{D} \subset \mathbb{Z}_+^m$ definit de

$$H_{\mathcal{D}}(t) = \sum_{i \geq 0} a_i t^i,$$

unde $a_i = \#\{a = (a_1, \ldots, a_m) \in \mathcal{D} | a_1 + \ldots + a_m = i\}$. Polinomul $H_{\mathcal{D}}(t)$ se numeşte polinomul Hilbert al designului $\mathcal{D}$.

Al doilea rezultat principal al acestei cercetări în reprezintă caracterizarea polinoamelor cu coeficienţi întregi care pot fi polinoame Hilbert ale unui design eşalon.

De asemenea, am studiat si fracţiile unui design eşalon si am obţinut aici alte două rezultate pe care le vom prezenta mai jos. Cele două teoremele referitoare la fracţiile unui design eşalon extind Teoremele 4.5 and Theorem 5.6 din lucrarea lui Robiano la cazul designurilor eşalon.

Să defini în continuare designurie eşalon in dimensiune m.

Pentru $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, fie $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_m^{\alpha_m} \in k[x_1, \ldots, x_m]$.

Definiţia 6.2. *Fie $a = (a_1, \ldots, a_m)$ şi $b = (b_1, \ldots, b_m)$ două puncte din $\mathbb{Z}_+^m$. Spunem că a **domină pe** b dacă $a_i \leq b_i$, pentru orice $i = 1, \ldots, m$.*

În termeni de monoame, a **domină pe** b dacă $\mathbf{x}^a | \mathbf{x}^b$. Evident, dacă a domină pe b, atunci $\mathbf{x}^a$ domină orice multiplu al lui $\mathbf{x}^b$.

Definiţia 6.3. *Fie $K \in \mathbb{N}^*$ şi fie $\alpha^{(1)}$, ..., $\alpha^{(K)}$ vectori cu componente întregi din $\mathbb{Z}_+^m$ astfel încât nici un $\boldsymbol{x}^{\alpha^{(i)}}$ nu domină nici un $\boldsymbol{x}^{\alpha^{(j)}}$ pentru toţi $1 \leq i \neq j \leq K$. **Designul eşalon** $\mathcal{E} \in \mathbb{Z}_+^m$ determinat de vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ este*

mulţimea tuturor punctelor $b \in \mathbb{Z}_+^m$ *cu proprietatea că* $\boldsymbol{x}^b$ *nu este divizibil cu* $\boldsymbol{x}^{\alpha^{(i)}}$, *pentru orice* $1 \leq i \leq K$. *Cu alte cuvinte, design-ul eşalon definit de vectorii* $\alpha^{(1)}$, ..., $\alpha^{(K)}$ *este mulţimea de puncte din* $\mathbb{Z}_+^m$ *care nu sunt dominate de* $\alpha^{(1)}, \ldots, \alpha^{(K)}$.

Vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ *se numesc* ***vectori dominanţi (sau de definiţie)*** *ai eşalonului* $\mathcal{E}$. *Monomul* $\boldsymbol{x}^{\alpha^{(i)}}$, *pentru* $1 \leq i \neq j \leq K$, *se numeşte* ***monomul dominanţ (sau de definiţie)*** *al lui* $\mathcal{E}$.

Exemplul 6.4. *Fie* $m = 2$ *şi* $\alpha^{(1)} = (0,4)$, $\alpha^{(2)} = (1,3)$, $\alpha^{(3)} = (3,1)$, $\alpha^{(4)} = (5,0)$ *vectorii dominanţi care definesc eşalonul* $\mathcal{E} \subset \mathbb{Z}_+^2$. *Să observăm că nici un* $\boldsymbol{x}^{\alpha^{(i)}}$ *nu divide nici un* $\boldsymbol{x}^{\alpha^{(j)}}$ *pentru orice* $1 \leq i \neq j \leq 4$.

Monoamele de definiţie sunt prin urmare x_2^4, $x_1x_2^3$, $x_1^3x_2$ *şi* x_1^5. *Conform Definiţiei 6.3, designul* $\mathcal{E} \subset \mathbb{Z}_+^2$ *este format din toate punctele din* $\mathbb{Z}_+^2$ *care nu sunt dominate de* $\alpha^{(1)}, \ldots, \alpha^{(4)}$, *şi anume din punctele* $(0,0)$, $(0,1)$, $(0,2)$, $(0,3)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,0)$, $(2,1)$, $(2,2)$, $(3,0)$ *şi* $(4,0)$*; vezi Figura 6.1.*

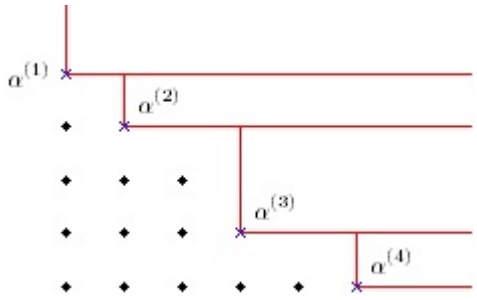


Figura 6.1: Un design eşalon definit prin vectorii dominanti

Este nu foarte dificil de văzut că un design eşalon de dimensiune m poate fi definit şi astfel:

Definiţia 6.5. *Un design* $\mathcal{E} \subset \mathbb{Z}_+^m$ *este design eşalon dacă şi numai dacă fiecare punct* $(d_1, \ldots, d_m)$ *din eşalon are proprietatea că toate punctele de*

forma $(y_1, \ldots, y_m)$ *cu* $0 \leq y_j \leq d_j$, *pentru orice* $j = 1, \ldots, m$ *se găsesc în designul* $\mathcal{E}$.

Exemplul 6.6. *În designul eçalon* $\mathcal{E}$ *din Examplul 6.4, cum punctele* $(0,3)$, $(1,2)$, $(2,0)$, $(3,0)$ *şi* $(4,0)$ *se găsesc în designul* $\mathcal{E}$, *toate aceste puncte împreună cu cele care se află "mai jos" de ele, adică* $(0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(2,1)$, $(2,0)$ *sunt toate puncte ale designului.*

6.1 Designuri eşalon: definiţii, exemple

6.1.1 Definiţii echivalente pentru designurile eşalon în dimensiune m

6.1.2 Designurile eşalon în dimensiune 2

Vom demonstra în continuare că un design eşalon în dimensiune 2 poate fi de asemenea definit ca o reunuine de puncte, vezi şi [CPRW].

Propoziţia 6.7. *Fie* $\mathcal{E} \subset \mathbb{Z}_+^2$ *un design eşalon definit de vectorii dominanţi* $\alpha^{(1)}, \ldots, \alpha^{(K)}$.

Există atunci $l+1$ *întregi pozitivi* $k_0 \geq k_1 \geq \ldots \geq k_l$ *astfel incat designul* $\mathcal{E}$ *este reuniunea coloanelor de puncte*

$$\begin{aligned} &(0,h), && \text{cu } h = 0, \ldots, k_0; \\ &(1,h), && \text{cu } h = 0, \ldots, k_1; \\ &\quad\vdots \\ &(l,h), && \text{cu } h = 0, \ldots, k_l. \end{aligned} \tag{6.1}$$

Reciproc, daca un design $\mathcal{E}$ *este o reuniune de coloane de puncte de forma (6.1), atunci exista niste vectori* $\alpha^{(1)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^2$ *cu proprietatea că nici*

un $\boldsymbol{x}^{\alpha^{(i)}}$ *nu divide nici un* $\boldsymbol{x}^{\alpha^{(j)}}$ *pentru orice* $1 \leq i \neq j \leq K$*, iar designul* $\mathcal{E}$ *este dat de reuniunea tuturor punctelor din* $\mathbb{Z}_+^2$ *care nu sunt dominate de* $\boldsymbol{x}^{\alpha^{(i)}}$*, pentru* $i = 1, \ldots, K$*.*

Demonstraţie: Incepem demonstratia prin a face cateva observatii generale asupra vectorilor $\alpha^{(1)}, \ldots, \alpha^{(K)}$. Deoarece acesti vectori satisfac conditia ca nici un $\mathbf{x}^{\alpha^{(i)}}$ nu divide nici un $\mathbf{x}^{\alpha^{(j)}}$ pentru orice $1 \leq i \neq j \leq K$, rezulta ca acesti vectori nu pot avea doi aceeasi valoare nici pe prima, nici pe a doua coordonata.

De asemenea, printre vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ exista un singur vector care are prima coordonata egala cu 0. Intr-adevar, daca nu ar exista un astfel de vector, atunci designul esalon ar contine o infinitate de puncte cu prima coordonata zero, in contradictie cu definitia designului esalon ca o multime finita de puncte. In mod analog, se poate justifica si faptul ca exista un unic vector dominant care are a doua coordonata zero.

Fie acum $\mathcal{E} \subset \mathbb{Z}_+^2$ un design esalon definit de vectorii dominanti $\alpha^{(1)}, \ldots, \alpha^{(K)}$. Fie $(l+1, 0)$ unicul vector dominant cu a doua coordonata nula. Am definit astfel intregul l.

Definim in continuare intregii $k_0 \geq k_1 \geq \ldots \geq k_l \geq 0$ astfel: $k_0 + 1$ este a doua coordonata a unicului vectorului cu prima coordonata zero. Recursiv, pentru $1 \leq i \leq l$, fie $k_i + 1$ a doua coordonata a unicului vector care are prima coordonata egala cu i. Daca un asemenea vector nu exista, luam $k_i = k_{i-1}$. Deoarece vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ satisfac conditia ca nici un $\mathbf{x}^{\alpha^{(i)}}$ nu divide nici un $\mathbf{x}^{\alpha^{(j)}}$ pentru nici un $1 \leq i \neq j \leq K$, rezulta ca $k_0 \geq k_1 \geq \ldots \geq k_l$. Rezulta atunci ca esalonul dat $\mathcal{E}$ este reuniunea coloanelor de puncte (6.1), asa cum aveam nevoie.

Reciproc, daca designul $\mathcal{E}$ este dat de o reuniune de puncte ca in (6.1), atunci multimea de vectori dominanti se obtine dupa urmatorul algoritm:

pentru fiecare $i = 0, \ldots, l$, fie j_i cel mai mic intreg t cu proprietatea ca $k_{j_i} = k_t$ si fie $\alpha^{(K_i)} = (j_i, k_{j_i} + 1)$. La multimea de vectori astfel obtinuta adaugam vectorul $(l + 1, 0)$ si apoi notam acesti vectorii cu $\alpha^{(1)}, \ldots, \alpha^{(K)}$. Cum $k_0 \geq k_1 \geq \ldots \geq k_l$, vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)}$ sunt chiar vectorii dominanti cautati. □

Exemplul 6.8. *Sa exemplificam procedeul din demonstratia teoremei precedente definind un design esalon in dimensiune* 2 *folosind ambele definitii de mai sus.*

Fie vectorii dominanti $\alpha^{(1)}, \ldots, \alpha^{(4)}$ *definiti prin* $\alpha^{(1)} = (0, 4)$, $\alpha^{(2)} = (1, 3)$, $\alpha^{(3)} = (3, 1)$, $\alpha^{(4)} = (5, 0)$. *Sa observam ca nici un* $\boldsymbol{x}^{\alpha^{(i)}}$ *nu divide* $\boldsymbol{x}^{\alpha^{(j)}}$, *pentru orice* $1 \leq i \neq j \leq 4$. *Monoamele dominante corespunzatoare sunt deci* x_2^4, $x_1x_2^3$, $x_1^3x_2$, x_1^5. *Din Definitia 6.3, designul* $\mathcal{E} \subset \mathbb{Z}_+^2$ *este format din punctele care nu sunt dominate de* $\alpha^{(1)}, \ldots, \alpha^{(4)}$. *Aceste puncte sunt* $(0, 0)$, $(0, 1)$, $(0, 2)$, $(0, 3)$, $(1, 0)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 1)$, $(2, 2)$, $(3, 0)$ *şi* $(4, 0)$*; vezi Figura 6.2.*

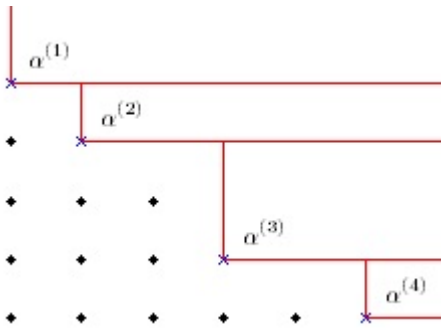


Figura 6.2: Un design eşalon în dimensiune 2

De asemenea, plecand cu vectorii dominanti $\alpha^{(1)} = (0, 4)$, $\alpha^{(2)} = (1, 3)$, $\alpha^{(3)} = (3, 1)$, $\alpha^{(4)} = (5, 0)$ *putem obtine definitia echivalenta a unui esalon, asa cum apare ea in Propozitia 6.7: cum* $\left\{x_2^{k_0+1}, x_1x_2^{k_1+1}, \ldots x_1^l x_2^{k_l+1}, x_1^{l+1}\right\} =$

$\{x_2^4, x_1x_2^3, x_1^3x_2, x_1^5\}$, *rezulta* $l = 4$, $k_0 = 3$, $k_1 = 2$, $k_2 = 2$ *şi* $k_3 = 0$. *Deoarece in multimea data nu exista nici un monom care sa contina* x_1^2, *intregul* k_2 *pe care il cautam este egal cu precedentul, i.e.* $k_2 = k_1 = 2$.

Este acum evident cum se obtine lista de puncte (6.1) din esalon, asa cum apare in demonstratia Propozitiei 6.7.

6.1.3 Baze Gröbner pentru designurile eşalon

Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii dominanţi $\alpha^{(1)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^m$.

Fiecărui vector $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_+^m$ îi asociem un polinom $f_\alpha \in k[x_1, \ldots, x_m]$ definit astfel:

$$f_\alpha = \prod_{i=1}^{m} x_i(x_i - 1)\ldots(x_i - \alpha_i + 1).$$

În raport cu orice ordonare monomială $<$ pe $k[x_1, \ldots, x_m]$, avem

$$\mathrm{in}_<(f_\alpha) = x_1^{\alpha_1} \ldots x_m^{\alpha_m},$$

unde cu $\mathrm{in}_<(f)$ am notat monomul iniţial al lui f relativ la $<$. Fie $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ polinoamele asociate vectorilor $\alpha^{(1)}, \ldots, \alpha^{(K)}$ ale lui $\mathcal{E} \subset \mathbb{Z}_+^m$. Rezultă atunci că $f_{\alpha^{(i)}} \in I(\mathcal{E})$, pentru orice $1 \leq i \leq K$, şi deci pentru orice ordonare monomială $<$ pe $k[x_1, \ldots, x_m]$ avem

$$(\mathrm{in}(f_{\alpha^{(1)}}), \ldots, \mathrm{in}(f_{\alpha^{(K)}})) \subset \mathrm{in}(I(\mathcal{E})),$$

unde cu $\mathrm{in}(\mathcal{I}(\mathcal{E}))$ am notat idealul iniţial al lui $\mathcal{I}(\mathcal{E})$ relativ la ordonarea monomială $<$.

Primul nostru rezultat din această cercetare este următoarea teoremă care stabileşte o bază Gröbner a lui $I(\mathcal{E})$ relativ la orice ordonare monomială pe $k[x_1, \ldots, x_m]$.

Teorema 6.9. *Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii $\alpha^{(1)}, \ldots, \alpha^{(K)} \in \mathbb{Z}_+^m$. Atunci mulţimea $G = \{f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}\}$ este o bază Gröbner a lui $I(\mathcal{E})$ relativ la orice ordonare monomială pe $k[x_1, \ldots, x_m]$.*

Demonstraţie: Fie $J = (\text{in}(f_{\alpha^{(1)}}), \ldots, \text{in}(f_{\alpha^{(K)}}))$ un ideal monomial din $k[x_1, \ldots, x_m]$. Fie $R_1 = k[x_1, \ldots, x_m]/J$ şi $R_2 = k[x_1, \ldots, x_m]/I(\mathcal{E})$ doua k-algebre.

Deoarece $I(\mathcal{E}) = \bigcap_{P \in \mathcal{E}} \mathfrak{m}_P$, unde pentru $P = (a_1, \ldots, a_m)$ am notat cu $\mathfrak{m}_P$ idealul maximal generat de $x_1 - a_1$,$x_2 - a_2, \ldots, x_m - a_m$, rezulta ca $k[x_1, x_2, \ldots, x_m]/I(\mathcal{E}) \cong k^{|\mathcal{E}|}$, izomorfism de k-spatii vectoriale. Sa observam si ca $\dim_k S/J = |\mathcal{E}|$, asa cum rezulta din definitiile lui J si ale lui $\mathcal{E}$.

Asadar, nici un monom care nu se gaseste in $\text{in}_<(I(\mathcal{E}))$ nu se gaseste nici in J. Pe de alta parte,

$$|\mathcal{E}| = \dim_k \frac{S}{J} \geq \dim_k \frac{S}{\text{in}_<(I(\mathcal{E}))} = \dim_k \frac{S}{I(\mathcal{E})} = |\mathcal{E}|,$$

ceea ce incheie domonstratia teoremei. □

Ca un caz spacial al teoremei de mai sus obtinem Teorema 2.18 din [R] si ecuatiile (2) din [CPRW]. Intr-adevar, orice design full factorial de leveluri $(l_1, \ldots, l_n)$ (i.e. produsul cartezian al multimilor finite $\{0, 1, \ldots, l_1 - 1\}, \ldots,$ $\{0, 1, \ldots, l_n - 1\}$) este un design esalon de monoame dominante $\mathbf{x}^{\alpha(i)} = x_i^{l_i}$, pentru $1 \leq i \leq m$.

Inspirati de Definitia 2.19 din [R], numim polinoamele $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ **polinoamele canomice** ale designului esalon $\mathcal{E}$.

6.2 Cocluzii finale

6.2.1 Polinomul Hilbert asociat unui design eşalon în dimensiune doi

Definiţia 6.10. *Dat un design arbitrar $\mathcal{D} \subset \mathbb{Z}_+^m$, definim polinomul Hilbert asociat designului $\mathcal{D}$ ca fiind:*

$$H_{\mathcal{D}}(t) = \sum_{i \geq 0} a_i t^i,$$

unde $a_i = \#\{a = (a_1, \ldots, a_m) \in \mathcal{D} | a_1 + \ldots + a_m = i\}$.

Vom nota $H_{\mathcal{D}}$ polinomul Hilbert asociat designului $\mathcal{D}$.

Al doilea rezultat din această cercetare îl reprezintă teorema următoare care caracterizează polinomul Hilbert al unui design eşalon în dimensiune 2.

Teorema 6.11. *Fie $H \in \mathbb{Z}[t]$ un polinom cu coeficienţi întregi ne-negativi. Atunci H este polinomul Hilbert al unui design eşalon în dimensiune doi dacă şi numai dacă există un întreg $i \geq 0$ astfel încât*

$$H(t) = 1 + 2t + 3t^2 + \ldots + (i+1)t^i + a_{i+1}t^{i+1} + \ldots + a_d t^d,$$

cu $d \geq 0$ şi $i + 1 \geq a_{i+1} \geq \ldots \geq a_d$.

Demonstraţie: Intai, demonstram ca orice design esalon in dimensiune doi are polinomul Hilber ca mai sus. Toate partratele pe care le vom considera vor avea un varf in origine si o latura pe axa Ox.

Dat un design esalon $\mathcal{E}$ in dimensiune doi, exista un cel mai mare intreg $i \geq 0$ astfel incat toate cele $i+1$ puncte de pe diagonala patratului de latura i apartin esalonului. Cum i este ales maxim cu aceasta proprietate, rezulta ca pentru toti $j = 0, .., i$, toti coeficientii lui t^j din polinomul Hilber sunt $a_j = j + 1$; vezi Figura 6.3.

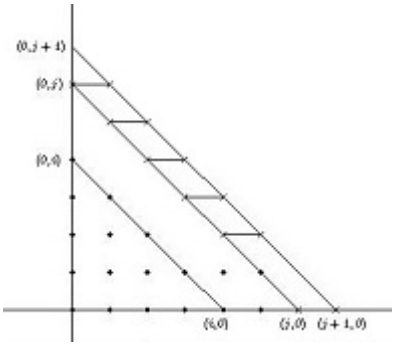


Figura 6.3: Polinomul Hilbert al unui design eşalon

Coeficientul a_{i+1} al lui t^{i+1} in polinomul Hilbert $H_{\mathcal{E}}(t)$ este egal cu numarul de puncte din esalon care se gasesc pe diagonala patratului de latura $i+1$. Deoarece sunt $i+2$ puncte pe diagonala si cel putin un punct nu se gaseste in esalon (din alegerea lui i), rezulta ca $a_{i+1} \leq i+1$.

Pentru $j \geq i+1$, avem $a_j \geq a_{j+1}$: intr-adevar, fiecarui punct de pe diagonala patratului de latura j care nu se gaseste in esalon ii corespunde un punct de pe diagonala patratului de latura $j+1$ care are are coordonata a doua identica cu punctul fixat initial si cea de-a doua coordonata cu o unitate mai mare. Acest punct nu se gaseste in esalon deoarece este dominat de punctul fixat initial. Mai mult, aceasta corespondenta este o bijectie, asa cum ilustreaza liniile orizontale din Figura 6.3. Prin urmare, numarul de puncte de pe diagonala patratului de latura $j+1$ care nu sunt in esalon este mai mare sau egal cu numarul de puncte de pe diagonala patratului de latura j care nu sunt in esalon. Deci, $a_j \geq a_{j+1}$, pentru orice $j \geq i+1$.

Reciproc, fie $H(t) = 1 + 2t + 3t^2 + \ldots + (i+1)t^i + a_{i+1}t^{i+1} + \ldots + a_d t^d$, cu $i+1 \geq a_{i+1} \geq \ldots \geq a_d$ un polinom din $\mathbb{Z}[t]$. Construim un design esalon $\mathcal{E} \subset \mathbb{Z}_+^2$ (care nu este neaparat unic) astfel incat $H_{\mathcal{E}}(t) = H(t)$.

Fie i cel mai mare intreg cu proprietatea ca coeficientul lui t^i este $i+1$.

Rezulta atunci ca toate punctele de pe diagonalele patratelor de latura j, pentru orice $0 \leq j \leq i$ apartin esalonului $\mathcal{E}$.

In continuare, pentru orice j cu $i+1 \leq j \leq d$, gasim a_j puncte din esalon situate pe diagonala corespunzatoare patratului de latura j prin urmatorul procedeu. Din toate cele $j+1$ astfel de puncte, agelem $a_j < j+1$ puncte avand, de exemplu, coordonata a doua cea mai mica. Se pot alege cele a_j din esalon dintre cele $j+1$ puncte de pe diagonala avand coordonata a doua cea mai mare. Acest fapt arata ca designul esalon asociat unui polinom Hilbert dat nu este unic.

Desigul esalon astfel construit are $l = d$ şi $k_0 = a_i - 1 = i$. Fie acum k_1+1 cel mai mare coeficient al lui $H(t)$ diferit de a_{k_0+1}; fie apoi k_2+1 cel mai mare dintre coeficientii lui $H(t)$ diferiti de a_{k_0+1} si a_{k_1+1}; fie k_3+1 cel mai mare coeficient al lui $H(t)$ diferit de a_{k_0+1}, a_{k_1+1} şi a_{k_2+1} şi asa mai departe. Astfel, la fiecare pas alegem cel mai mare dintre coeficientii lui $H(t)$ care nu au fost anterior considerati. Astfel, deoarece $a_i \geq a_{k_1} \geq ... \geq a_{k_d}$, rezulta ca $k_0 \geq k_1 \ldots \geq k_l$. Am obtinut in acest fel un design esalon $\mathcal{E}$ care are drept polinom Hilbert polinomul H dat. □

Exemplul 6.12. *Sa consideram un polinom H care satisface conditiile din Teorema 6.11:*

$$H(t) = 1 + 2t + 3t^2 + 4t^3 + 5t^4 + 6t^5 + 6t^6 + 4t^7 + 2t^8 + 2t^9 + 2t^{10}.$$

Folosind procedeul descris in Teorema 6.11, construin un design esalon $\mathcal{E} \in \mathbb{Z}_+^2$ cu $H_{\mathcal{E}}(t) = H(t)$. Sa observam pentru inceput ca $i = 5$ este cel mai mare intreg cu proprietatea ca coeficientul corespunzator (in cazul nostru coeficientul lui t^5, adica a_5) este egal cu $i+1$. Prin urmare, toate punctele de pe diagonala patratului de latura j, cu $0 \leq j \leq 5$, se gasesc in designul esalon.

In continuare, pe diagonala corespunzatoare lui a_j, cu $j \geq 5$, asezam a_j puncte avand cea mai mica a doua coordonata. De exemplu, dintre punctele de pe diagonala patratului de latura 8 alegem punctele $(8,0)$ şi $(7,1)$.

Procedand in acest fel, am obtinut designul esalon din Figura 6.4. Numerele intregi $k_0, \ldots, k_l$ sunt egale respectiv cu $5,5,4,3,3,2,1,1,1,1,0$, iar vectorii dominanti sunt $\alpha^{(1)} = (0,6)$, $\alpha^{(2)} = (2,5)$, $\alpha^{(3)} = (3,4)$, $\alpha^{(4)} = (5,3)$, $\alpha^{(5)} = (6,2)$, $\alpha^{(6)} = (10,1)$ şi $\alpha^{(7)} = (11,0)$.

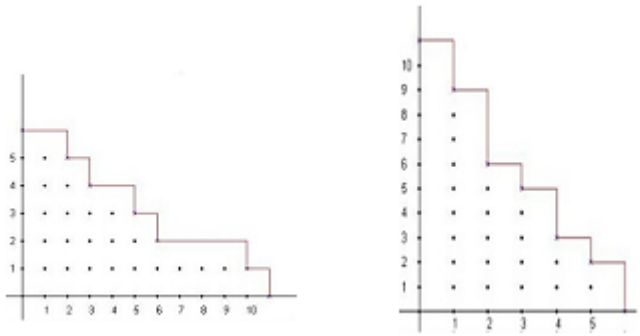


Figura 6.4: Un design eşalon $\mathcal{E}$ asociat unui polinom Hilbert dat

Asa cum am mentionat si in demonstratia teoremei, designul esalon avand drept polinom Hilbert un polinomul dat nu este unic. In exemplul de mai sus, putem alege punctele cu a doua coordonata cea mai mare. Se obtine atunci esalonul din partea dreapta a figurii de mai sus. Ambele designuri esalon din Figura 6.4 au acelasi polinom Hilbert $H(t)$.

6.2.2 Fracţii ale unui design eşalon

Dat un design eşalon $\mathcal{E}$, o **fracţie a eşalonului** este o submulţime proprie $\mathcal{F} \subset \mathcal{E}$. În mod clar, idealul său de definiţie $I(\mathcal{F})$ conţine idealul $I(\mathcal{E})$.

Definiţia 6.13. *Fie $\mathcal{E} \subset \mathbb{Z}_+^m$ un design eşalon definit de vectorii dominanţi*

$\alpha^{(1)}$, ..., $\alpha^{(K)} \in \mathbb{Z}_+^m$. *Fiecărui astfel de vector* $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_+^m$ *îi asociem un polinom* $f_\alpha \in k[x_1, \ldots, x_m]$ *definit astfel:*

$$f_\alpha = \prod_{i=1}^{m} x_i(x_i - 1)\ldots(x_i - \alpha_i + 1).$$

Polinoamele $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ *le-am numit* ***polinoamele canonice*** *ale designului eşalon* $\mathcal{E}$.

Definiţia 6.14. *Orice submulţime de polinoame care, adăugate polinoamelor canonice ale unui design eşalon* $\mathcal{E}$*, generează idealul unei fraţii* $\mathcal{F}$*, se numeşc* ***polinoame confounding*** *ale lui* $\mathcal{F}$ *în* $\mathcal{E}$.

Definiţia 6.15. *Fie* $\mathcal{E}$ *un design eşalon şi fie* $\mathcal{F}$ *o fracţie a acestuia. Se numeşte* ***polinomul caracteristic al lui*** $\mathcal{F} \subset \mathcal{E}$ *polinomul* f *cu proprietatea că* $f(P) = 0$ *pentru orice* $P \in \mathcal{F}$ *şi* $f(P) = 1$ *pentru orice* $P \in \mathcal{E} \setminus \mathcal{F}$.

Dacă aplicăm Teorema 6.9 şi Proposition 4.4 din lucrarea menţinat]u a a lui Robiano, obţinem:

Propoziţia 6.16. *Fie* $\mathcal{E}$ *un design eşalon şi fie* $\mathcal{F} \subset \mathcal{E}$ *o fracţie a acestuia. Fie* f *polinomul caracteristic al lui* $\mathcal{F}$*. Atunci*

$$I(\mathcal{F}) = (f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}, f)\,.$$

Al treilea rezultat din acesta cercetare este dat în următoarea teoremă:

Teorema 6.17. *Fie* $<$ *o ordonare monomială pe* $k[x_1, \ldots, x_m]$, $\mathcal{E} \in \mathbb{Z}_+^m$ *un design eşalon,* $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ *polinoamele canonice ale lui* $\mathcal{E}$ *şi fie* $\mathcal{F} \subset \mathcal{E}$ *o fracţie a designului* $\mathcal{E}$.

Există atunci un unic polinom caracteristic f *al lui* $\mathcal{F}$ *în* $\mathcal{E}$ *astfel încat* $in(f)$ *nu este dominat de nici un* $\mathrm{in}_<(f_{\alpha^{(i)}})$, $1 \leq i \leq n$.

Demonstraţie: Deoarece polinoamele $f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ formeaza o baza Gröbner pentru idealul designului $\mathcal{E}$, rezulta ca $I(\mathcal{E}) = (f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}})$ şi $\text{in}_<(I(\mathcal{E})) = (\text{in}_<(f_{\alpha^{(1)}}), \ldots, \text{in}_<(f_{\alpha^{(K)}}))$.

Fie acum h polinomul caracteristic al fractiei $\mathcal{F}$ in $\mathcal{E}$ şi fie r forma normala a lui h relativ la $\{f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}\}$, i.e. r este restul impartirii lui h la baza Gröbner $\{f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}\}$.Vom arata ca polinomul r este polinomul caracteristic pe care il cautam.

Din Teorema de impartire din $k[x_1, \ldots, x_m]$, (vezi [PRW], Teorema 2) rezulta ca $\text{in}_<(f)$ nu este dominat de nici un $\text{in}_<(f_{\alpha^{(i)}})$, $1 \leq i \leq n$.

In mod evident, r se anuleaza in orice $P \in \mathcal{F}$, deoarece polinoamele $h, f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}}$ se anuleaza toate in P. Mai mult, pentru $P \in \mathcal{E} \setminus \mathcal{F}$, obtinem $h(P) = 1$, $f_{\alpha^{(1)}}(P) = \ldots = f_{\alpha^{(K)}}(P) = 0$ şi deci $r(P) = 1$. Am obtinut astfel că r este un polinom caracteristic al lui $\mathcal{F}$ in $\mathcal{E}$.

Fie h_1, h_2 doua polinoame caracteristice ale lui $\mathcal{F}$ in $\mathcal{E}$. Prin definitie, $h_1 - h_2$ se anuleaza pe $\mathcal{E}$, prin urmare apartine idealului $I(\mathcal{E}) = (f_{\alpha^{(1)}}, \ldots, f_{\alpha^{(K)}})$. Daca am avea $h_1 - h_2 \neq 0$, ar rezulta ca $\text{in}_<(h_1 - h_2) \in (\text{in}_<(f_{\alpha^{(1)}}), \ldots, \text{in}_<(f_{\alpha^{(K)}}))$. Dar $\text{in}_<(h_1 - h_2)$ este unul dintre monoamele din suportul lui h_1 sau h_2, ceea ce contrazice definitia polinomului caracteristic. □

In cazul special al designurilor full factorial, din teorema de mai sus rezulta Teorema 4.5 din [R].

Exemplul 6.18. *Fie* $\mathcal{E} := \{(0,0), (1,0), (0,1)\}$ *un design esalon definit de vectorii dominanti* $\alpha^{(1)} = (2,0)$, $\alpha^{(2)} = (1,1)$ *şi* $\alpha^{(3)} = (0,2)$. *Polinoamele sale canonice confounding sunt*

$$f_{\alpha^{(1)}} := x_2(x_2 - 1); f_{\alpha^{(2)}} := x_1x_2, f_{\alpha^{(3)}} = x_1(x_1 - 1)$$

Fie $\mathcal{F} := \{(0,0), (1,0)\}$ *o fractie a esalonului* $\mathcal{E}$. *Fie* $P := (0,1)$. *Atunci* $\mathcal{E} = \mathcal{F} \cup \{P\}$.

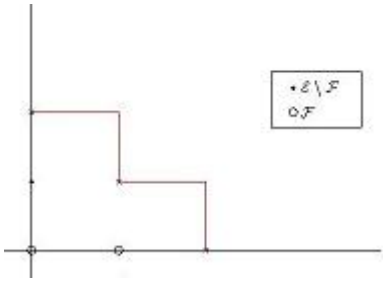


Figura 6.5: Un design eşalon $\mathcal{E}$ şi o fraţie $\mathcal{F}$ a sa

Folosind algoritmul Buchberger-Möller din [R], separatorul $s_P = x_2$ *este polinomul canonic confounding al lui* $\mathcal{F}$ *in* $\mathcal{E}$.
Prin urmare, conform Propozitiei 6.16, $\mathcal{I}(\mathcal{F}) = (x_2(x_2-1), x_1x_2, x_1(x_1-1), x_2)$

Definiţia 6.19. *Fie* $\mathcal{E} \subset k^m$ *un design eşalon. Notăm cu* $\mathcal{O}(\mathcal{E})$ *mulţimea de monoame* $\{x_1^{\alpha_1}x_2^{\alpha_2}\dots x_m^{\alpha_m} | (\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathcal{E}\}$.

Definiţia 6.20. *Fie* $\mathcal{O} \subseteq \mathrm{Mon}(\mathcal{S})$. *Spunem că* $\mathcal{O}$ *este o* ***mulţime standard de monoame*** *dacă* $T \in \mathcal{O}$ *şi* T' *divide* T *implică* $T' \in \mathcal{O}$, *i.e. toţi divizorii unui element din* $\mathcal{O}$ *sunt de asemenea în* $\mathcal{O}$.

Definiţia 6.21. *Date n variabile* $x_1, x_2, \dots, x_m$, *fie* $\mathcal{E} \subset \mathbb{Z}_+^2$ *un design eşalon şi fie* $\mathcal{O} \subset \mathcal{O}(\mathcal{E})$ *o mulţime standard de monoame. Atunci, din Lema lui Dickson, vezi [HH] rezultă că există o unică mulţime minimală,* $\mathrm{Min}(\mathcal{O})$, *de monoame care generează* $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$. *Adică, fiecare element din* $\mathrm{Mon}(\mathcal{S}) \setminus \mathcal{O}$ *este un multiplu al unui element din* $\mathrm{Min}(\mathcal{O})$. *Mulţimea de monoame din* $\mathrm{Min}(\mathcal{O})$, *care nu se găsesc printre termenii dominanţi ai polinoamelor canonice ale lui* $\mathcal{E}$, *se notează cu* $\mathrm{CutOut}(\mathcal{O})$.

Exemplul 6.22. *Fie* $\mathcal{E} := \{(0,0),(0,1),(1,0)\}$ *designul esalon descris in Exemplul 6.18. Polinoamele sala canonice confounding sunt:*

$$f_{\alpha^{(1)}} := x_2(x_2-1); f_{\alpha^{(2)}} := x_1x_2; f_{\alpha^{(3)}} = x_1(x_1-1)$$

Polinoamele dominante ale celor trei generatori ai idealului $\mathcal{I}(\mathcal{E})$ *sunt* x_2^2, x_1x_2 *şi* x_1^2. *Mai mult, stim ca* $\mathcal{O}(\mathcal{E}) = \{1, x_1, x_2\}$.

Daca $\mathcal{O}_1 = \{1, x_1\}$, *atunci* $\mathrm{Min}(\mathcal{O}_1) = \{x_2, x_1^2\}$ *şi astfel* $\mathrm{CutOut}(\mathcal{O}_1) = \{x_2\}$.

Daca $\mathcal{O}_2 = \{1, x_2\}$, *atunci* $\mathrm{Min}(\mathcal{O}_2) = \{x_2^2, x_1\}$ *şi deci* $\mathrm{CutOut}(\mathcal{O}_2) = \{x_1\}$.

Înainte de a da cel de-al patrulea rezultat din această direcţie de cercetare, să reamintim o definiţie introdusă de L. Robbiano, în [R].

Definiţia 6.23. *Fie* K *un corp infinit,* $T := x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ *şi fie* $\alpha_1, \alpha_2, \dots, \alpha_n$ n *şiruri de elemente din corpul de bază* K, *unde* $\alpha_r = (\alpha_{r,i})_{i\in\mathbb{N}}$, *pentru* $r := 1, 2, \dots, n$ *şi* $\alpha_{r,i} \neq \alpha_{r,j}$, *dacă* $i \neq j$. *Polinomul*

$$D(T) := \prod_{i=1}^{a_1}(x_1 - \alpha_{1,i}) \prod_{i=1}^{a_2}(x_2 - \alpha_{2,i}) \cdots \prod_{i=1}^{a_n}(x_n - \alpha_{n,i})$$

se numeşte ***distragerea*** *lui* T *relativ la* $\alpha_1, \alpha_2, \dots, \alpha_n$.

Cel de-al patrulea rezulat din acestă direcţie de cercetare este următorul rezultat:

Teorema 6.24. *Fie* $\mathcal{E}$ *un design eşalon definit de vectorii dominanţi* $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(K)} \in \mathbb{Z}_+^m$. *Fie* $\mathcal{I}(\mathcal{E}) := (f_{\alpha^{(1)}}, f_{\alpha^{(2)}}, \dots, f_{\alpha^{(K)}})$ *idealul său de definiţie, unde* $f_{\alpha^{(j)}}$ *sunt polinoamele canonice, pentru* $j = 1, \dots, K$. *Fie* $\mathcal{O}(\mathcal{E})$ *mulţimea standard de monoame corespunzătoare şi fie* $\mathcal{O} \subset \mathcal{O}(\mathcal{E})$ *o mulţime standard de monoame. Să presupunem că* $\{T_1, T_2, \dots, T_h\} = \mathrm{CutOut}(\mathcal{O})$ *şi fie*

$D(T_1), D(T_2), \ldots, D(T_h)$ *distragea lui* $T_1, T_2, \ldots, T_h$.
Atunci, pentru orice ordonare monomială pe $k[x_1, x_2, \ldots, x_n]$, *mulţimea*

$$\{f_{\alpha^{(1)}}, f_{\alpha^{(2)}}, \ldots, f_{\alpha^{(K)}}, D(T_1), D(T_2), \ldots, D(T_h)\}$$

este o bază Gröbner neredusă pentru idealul $\mathcal{I}(\mathcal{F})$, *unde* $\mathcal{F} \subset \mathcal{E}$ *este o fracţie a eşalonului* $\mathcal{E}$ *astfel încât* $\mathcal{O}(\mathcal{F}) = \mathcal{O}$.

Demonstraţie: În multimea $\{f_{\alpha^{(1)}}, f_{\alpha^{(2)}}, \ldots, f_{\alpha^{(K)}}, D(T_1), D(T_2), \ldots, D(T_h)\}$, putem observa ca daca exista o distragere al carei monom dominant domina monomul dominant al polinoamleor canonice ale designului esalon, atunci polinomul sau canonic va fi eliminat din multime.
Demonstarea faptului ca aceasta multime formeaza o baza Gröbner basis a idealului design al fractiei este analoaga cu demonstratia Proposition 5.6, din [R]. □

Bibliografie selectivă

[AS89] A.Adolphson and S.Sperber, *Exponential sums and Newton polyhedra: Cohomology and estimates*, Ann. of Math., **130(2)(1989)**, 367-406.

[AZ00] V.Albis W.A.Zúñiga-Galindo, *Un introducción elemental a la teoría de las functiones zeta locales de Igusa*, preprint, 2000;

[Bru02] L.Brünjes, *Über die Zetafunktion von Formen von Fermatgleichungen. Dissertattion zur Erlangung des Doktorgrades*, Universitaet Regensburg, 2002, http://www.bibliothek.uni-regensburg.de/opus/volltexte/2002/98/.

[Bru03] L.Brünjes, *On the Zeta Functions of forms of Fermat equations*, preprint, 2003;

[BS66] Z.I.Borevici, I.R.Shafarevici, *Teoria numerelor*, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1985.

[CFR] G.Carra'Ferro, L.Robianno, *On Super G-Bases*, Journal of Pure and Applied Algebra **68(1990)**, 279-292.

[CPRW] M. Caboara, G. Pistone, E.Riccomagno, H.P.Wynn, *The Fan of an Experimental Design*, SCU Research Report **33(1997)**, Department of Statistics, University of Warwich.

[CR] M.Caboara, L.Robbiano, *Families of Ideals in Statistics*, In Küchlin, (ed.) Proceeding ISSAC '97, ACM Press, New York, USA, 1997;

[CDJ02] M.Campbell, E. Dubois, M.Joyce, A.Krishnachander, M.Robinson, K.Schneider, J.Slemons, *On Igusa local zeta function of elliptic curves*, preprint, 2002.

[Den84] J. Denef, *The rationality of Poincaré series associated to the p-adic points on a variety*. Invent.Math., **77(1984)**, 1-23.

[De1] J. Denef, *On the degree of Igusa's local zeta function*, Amer.J.Math. **109(1987)**, 991-1008.

[Den91] J. Denef, *Report on Igusa's local zeta function*, Sém. Bourbaki 741, Astérisque **201/202/203 (1991)**, 359-386.

[Den95] J. Denef, *Poles of p-adic complex powers and Newton polyhedra*. Nieuw Arch.Wisk., **13(3)(1995)**,289-295.

[Den00] J. Denef, *Arithmetic and geometric applications of quantifier elimination for valued fields*, Model Theory, Algebra and Geometry, MSRI Publications, **39(2000)**.

[DH01] J. Denef, K.Hoornaert,*Newton polyhedra and Igusa's local zeta function*, J.Number Theory, **89(2001)**, 31-64.

[DL] J. Denef, F. Loeser, *Caractéristique d'Euler-Poincaré, fonctions zêta locales et modifications analytiques*, J. Amer. Math. Soc. 5, **4(1992)**, 705-720.

[DL98] J. Denef, F.Loeser, *Motivic Igusa zeta functions*. J.Algebraic Geom., **7(1998)**, 505-537.

[DL99] J. Denef, F.Loeser, *Definable sets, motives and p-adic integrals*, 1999, preprint.

[DLS97] J. Denef, A.Laeremans, P.Sargos, *On the largest nontrivial pole of the distribution* $|f|^s$. RIMS Kokyuroku, **999(1997)**, 1-9.

[DM91] J. Denef, D.Meuser, *A functional equation of Igusa's local zeta function*,**113(1991)**, 1135-1152.

[DS89] J. Denef, P.Sargos, *Polydre de Newton et distribution* f_+^s. *I.* J.Anal.Math, 53(1989), 201-218.

[DS92] J. Denef, P.Sargos, *Polydre de Newton et distribution* f_+^s. *II.* J.Anal.Math, 293(1992), 193-211.

[DS99] J. Denef, S.Sperber,*Exponential sums mod* p^n *and Newton polyhedra.*. Bull. Belg.Math. Soc-Simon Stevin, preprint 1999; se gaseste si pe http://www.wis.kuleuven.ac.be/wis/algebra/denef.html;

[DV95] J. Denef, W.Veys, *On the holomorphy conjecture for Igusa's local zeta function*. Proc.Amer.Math.Soc., **123(10)(1995)**,2981-2988.

[EH] V.Ene, J.Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Texts in Mathematics, **130**, Amer.Math.Soc, Providence, RI, 2011.

[FGR94] R.Field, V.Gargeya, M.Robinson, F.Schoenberg, R.Scott, *The Igusa Local zeta function for* $x^m + y^n$. preprint, 1994.

[Ful69] W.Fulton, *Algebraic Curves*, Mathematics Lecture Note Series. Benjamin, New-York-Amsterdam, 1969.

[Gol83] J.R.Goldman, *Numbers of solutions of congruences: Poincarë series for strongly nondegenerate forms*, Proc.Amer.Math.Soc., 87(4)(1983), 586-590.

[Gou97] F.Q.Gouvêa, *p-adic numbers. An introduction*, Springer Verlag, Berlin-Heidelberg-New York, 1997.

[GR97] J.S.Grus, D.C.Reuman, *The Igusa local zeta function for Fermat hypersuprafaces with exponent* p^l, preprint, 1997.

[Gre65] N. Greenleaf, *Irreductible subvarieties and rational points*, Amer.J.Math., **87(1965)**, 25-31.

[HH] J.Herzog, T.Hibi, *Monomial ideals*, Graduate Texts in Mathematics **260**, Springer, 2010;

[Hi] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann.Math. **79 (1964)**, 109-326.

[HL00] K.Hoornaert, D.Loots, *Polygusa: a computer program for Igusa's local zeta function.* http://www.wis.kuleuven.ac.be/wis/algebra/kathleen.html, 2000.

[Hoo01] K.Hoornaert, *Newton Polyhedra and the poles of Igusa's local zeta function.* Bull.Belg.Math.Soc-Simon Stevin, 2001, preprint;

[Hoo02a] K.Hoornaert, *Newton Polyhedra, unstable faces and the poles of Igusa's local zeta function*, Bull.Belg.Math.Soc-Simon Stevin, 2002, preprint;

[Hoo02b] K.Hoornaert, *Newton Polyhedra and Igusa's local zeta function*. Teza de doctorat. http://www.wis.kuleuven.ac.be/wis/algebra/kathleen.html, 2002;

[Iba98] D.Ibadula, *The Nonsingularity of the Gradient System Associated to a Finite Type Lie Algebra*, Analele stiintifice la Universitatii Ovidius Constanta, Seria Matematica VI Volume 6, Fasc.**2, 1998**, 69-87.

[Iba01] D.Ibadula, *Structura extinderilor moderat ramificate şi aplicatii*, Analele stiintifice la Universitatii Ovidius Constanta, Seria Matematica VI Volume 9, Fasc.**2, 2001**, 69-86.

[Iba06] D.Ibadula, *On the Plane Cubics over $\mathbb{Q}_p$ and the Associated Igusa Zeta Function*, Bulletin Mathematique Soc. Sci. Math. Roumanie, **Tome 49(97)**, Number **3/2006**, 253-277.

[Iba] D.Ibadula, *The Arboreal Structure of the Metric Space $X := GL2(\mathbb{Q}_p)/\mathbb{Q}_p^{\times} GL_2(\mathbb{Z}_p)$*, Communications in Algebra,Volume **34**, Number **12/2006**, 4563-4571.

[Iba09] D.Ibadula, *On the rationality of Igusa zeta functions of some classes of polynomials*, Analele Universitatii din Bucuresti, Seria Matematica,Anul LVIII (2009), Number **2/2009**, 199-210.

[Iba9] D.Ibadula, *The Igusa Zeta Functions of the $GL_2(\mathbb{Q}_p)$-orbit of Fermat's Binary Form*, Combinatorial Aspects of Commutative Algebra, Contemporary Mathematics (CONM), AMS, vol **502 (2009)**, 59-72.

[Iba12IS] D.Ibadula, Dirk Segers, *Determination of the real poles of the Igusa zeta functions for curves*, Revista Matemtica Complutense, vol. **25**, no. 2, July 2012, 581-597.

[Iba12] D.Ibadula, *Convex proofs of some inequalities*, The Mathematical Gazette, **11/2012**, 15-17.

[Iba12ISC] D.Ibadula, Dirk Segers, Edwin Leon Cardenal,*Poles of the Igusa local zeta function of some hybrid polynomials*, preprint.

[Iba12IB] D.Ibadula, Corina Birghilă,*Echelon Designs and Gröbner Bases*, preprint.

[Igu74a] J.-I. Igusa, *Complex powers and asymptotic expansions I.* J.Reine Angew.Math.,268/269; 110-130, 1974, II, ibid, 278/279, 307-321, 1975.

[Igu74b] J.-I. Igusa, *On a certain poisson formula*, Nagoya Math. J., **53:1974**, 211-233.

[Ig1] J. Igusa, *On the first terms of certain asymptotic expansions*, Complex Analysis and Algebraic Geometry, Iwanami Shoten **(1977)**, 357-368.

[Igu78] J.-I. Igusa, *Lectures on Forms of Higher Degree*, volume 59 of Tata Institute Fund. Res. Lectures on Math. and Phys. Springer-Verlag, Heidelberg-New York-Berlin, 1978;

[Ig2] J. Igusa, *Complex powers of irreducible algebroid curves*, Geometry today, Roma 1984, Progress in Math. **60**, Birkhäuser, **1985**, 207-230.

[Igu94] J.-I. Igusa, *A stationary phase formula for p-adic integrals and its applications*, în "Algebraic geometry and its applications"', Springer-Verlag, New York, 1994, 175-194.

[Igu96] J.-I. Igusa, *On local zeta functions*, In Amer.Math.Soc.Transl., volume **172(2)(1996)**, 1-20.

[Ig3] J. Igusa, *An Introduction to the Theory of Local Zeta Functions*, Amer. Math. Soc., Studies in Advanced Mathematics **14(2000)**.

[Jol73] J.-R. Joly, *Ëquations et variëtës algëbriques sur un corps fini*, Enseignement Math.,2(1973), 1-117.

[Kob77] N.Koblitz, *p-adic numbers, p-adic Analysis and Zeta-functions*, volumul **58**, Gratuate Texts in Mathematics, 1977.

[La] R.P. Langlands, *Orbital integrals on forms of SL*(3), Amer. J. Math. **105(1983)**, 465-506.

[Lin92] C.Y.Lin, *On the Igusa's Local Zeta Function of* $x^a + y^b$, în Algebraic geometry and algebraic number theory (Tianjin, 1989-1990), Nankai Ser.Pure Appl.Math Theoret. Phys, World Sci.Publishing, River Edge, NJ, **3 (1992)**, 64-70.

[LM85] B.Lichtin, D.Meuser, *Poles of a local zeta function and Newton Polygons*, Compositio Math., **55(1985)**, 313-332.

[Lo] F. Loeser, *Fonctions d'Igusa p-adiques et polynômes de Bernstein*, Amer. J. Math. **110(1988)**, 1-21.

[Loe02] F.Loeser, *Arizona winter school lecture notes on p-adic and motivic integration*, preprint, 1998.

[Mar95] R.Martin, *On simple Igusa local zeta functions*, Electr.Research Announc.of the Amer.Math.Soc., Vol.**1,1995**.

[Me] D. Meuser, *On the Poles of a Local Zeta Function for Curves*, Invent. Math. **73(1983)**, 445-465.

[MR02] D.Meuser, M.Robinson, *The Igusa local zeta function of elliptic curves*. Math.Comp, 2002.

[MW03] B.Marko, A.H.Wiswell, *Igusa Local Zeta function of the cubic polynomial* $f(x) = x_1^3 + ... + x_n^3$, preprint, 2003;

[Neu99] J.Neukirch, *Algebraic Number Theory*. Translated from the German by Norbert Schappacher, Springer Verlag, Berlin-Heidelberg-New York, 1999;

[PRW] G. Pistone, E. Riccomagno, H. Wynn, *Algebraic Statistics*, Computational Commutative Algebra in Statistics, Chapman & Hall, 2001.

[PR84] A.Prestel, P.Roquette, *Formally p-adic Fields*. Springer Verlag, Berlin-Heidelberg-New York-Tokyo, 1984.

[R] L. Robbiano, *Gröbner Bases and Statistics*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series **251(2001)**, Edited by Bruno Buchberger & Franz Winkler, Cambridge University Press, 179-204.

[RR] L. Robbiano, M.P.Rogantin, *Full Factorial Designs and Distracted Fractions*, Gröbner Bases and Applications, London Mathematical Society Lecture Note Series 251(2001), Edited

by Bruno Buchberger & Franz Winkler, Cambridge University Press, 473-482.

[Rup03] Christoper Rupprecht, *Cohomological Invariants for Higher Degree Forms*. Dissertation zur Erlangung des Doktorgrades, Universitaet Regensburg, 2003.

[ST] P.J. Sally, M.H. Taibleson, *Special functions on locally compact fields*, Acta Math.**116(1966)**, 279-309.

[Se1] D. Segers, *On the smallest poles of Igusa's p-adic zeta functions*, Math. Z. **252(2006)**, 429-455.

[Se2] D. Segers, *The asymptotic behaviour of the number of solutions of polynomial congruences*, An. St. Univ. Ovidius Constanta, 2011.

[Ser73] J.-P.Serre, *A course in arithmetic*. Springer Verlag, New York-Heidelberg-Berlin, 1973;

[Ser80] J.-P.Serre, *Trees*. Springer Verlag, Berlin-Heidelberg-New York, 1980;

[SG05] M.J.Saia, W.A.Zúñiga-Galindo, *Local zeta functions for curves, non-degeneracy conditions and Newton polygons*. Trans. Amer. Math. Soc. **357 (2005)**, no. 1, 59-88.

[St] L. Strauss, *Poles of a two-variable p-adic complex power*, Trans. Amer. Math. Soc. **278(1983)**, 481-493.

[Ve1] W. Veys, *On the poles of Igusa's local zeta function for curves*, J. London Math. Soc.**41(1990)**, 27-32.

[Ve2] W. Veys, *Relations between numerical data of an embedded resolution*, Amer. J. Math. **113(1991)**, 573-592.

[Ve3] W. Veys, *Congruences for numerical data of an embedded resolution*, Compositio Math. **80(1991)**, 151-169.

[Ve4] W. Veys, *Poles of Igusa's local zeta function and monodromy*, Bull. Soc. Math. France **121(1993)**, 545-598.

[Ve2] W. Veys, *Determination of the poles of the topological zeta function for curves*, Manuscripta Math. **87(1995)**, 435-448.

[Ve6] W. Veys, *More congruences for numerical data of an embedded resolution*, Compositio Math. **112(1998)**, 313-331.

[We65] A. Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*. Acta Math., **113 (1965)**, 1-87.

[Zie95] G.M.Ziegler, *Lectures on Polytopes*, volume 152 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1995.

[Zn99] W.A.Zúñiga-Galindo, *Igusa's Local Zeta Functions of non-degenerated polynomials*, preprint, 1999.

[Zn01] W.A.Zúñiga-Galindo, *Igusa's Local Zeta Functions of semiquasihomogeneus polynomials*. Trans.Amer.Math.Soc.,**353(8)(2001)**, 3193-3207.

[Zn03a] W.A.Zúñiga-Galindo, *Computing Igusa's Local Zeta Functions of univariate polynomials and linear feedback shift register*. J. Integer Seq. Vol **6(2003)**.

[Zn03b] W.A.Zúñiga-Galindo, *Local Zeta Functions and Newton polyhedra*. Nagoya Math.J.,Vol **172 (2003)**, 31-58.

[Zn04] W.A.Zúñiga-Galindo, *On the poles of Igusa's Local Zeta Function for algebraic sets*. Bull. London Math. Soc. **36 (2004**), 310-320.

[Zn05a] W.A.Zúñiga-Galindo, *Multiparametric exponential sums associated wit semiquasi- homogeneous mappings*, Preprint 2005.

[Zn05b] W.A.Zúñiga-Galindo, *Local Zeta Function for non-degenerate homogeneus mappings*. Pac. J. Math., no. 1(2005), 187-200.