ACADEMIA ROMÂNĂ
SCOSAAR

Anexa nr.6

REZUMATUL TEZEI DE ABILITARE*

TITLUL: Metode Algebrice in Teoria Numerelor

Domeniul de abilitare: *Matematica*

Autor: Pasol Vicentiu

În această teză de abilitare am colectat câteva rezultate din teoria numerelor folosind instrumente algebrice, obţinute împreună cu colaboratorii mei în ultimii zece ani.

Una din caracteristicile aritmetice fundamentale pe care le posedă spaţiul formelor (cvasi) -modulare este aceea că au o bază ai căror coeficienţi Fourier sunt întregi. Cu mult inainte de studiul lor sistematic iniţiat de Hecke, Ramanujan a studiat în detaliu relaţiile dintre aceşti coeficienţi Fourier, în special folosind cei trei generatori (serii Eisenstein), în notaţia sa $P(q), Q(q)$, respectiv $R(q)$. Una din observaţiile sale fundamentale este aceea că algebra generată de aceste serii este de fapt o algebră diferenţială. Dacă o forma cvasi-modulară este în imaginea operatorului de diferenţiere coeficienţii săi Fourier vor satisface în mod trivial o relaţie de divizibilitate şi anume $n \mid a_n$. Împreuna cu W. Zudilin am studiat sistematic spaţiul acelor forme cvasi-modulare care satisfac această proprietate de divizibilitate (numită generic magnetică), demonstrând printre altele proprietatea magnetică a anumitor forme cvasi-modulare deja conjecturate anterior de Li-Neururer.

Încă din lucrările semnificative ale lui Eichler şi Shimura din anii 1970, este recunoscut faptul că spaţiul formelor modulare de pondere k pentru un subgrup de congruenţă Γ este asociat cu coomologia parabolică a lui Γ, având coeficienţi în modulul polinoamelor omogene în două variabile de grad $k-2$. Spaţiul polinoamelor de perioade constituie o manifestare concretă a primului grup de coomologie parabolică, fiind extrem de adecvat pentru analiza modului în care operatorii Hecke acţionează pe formele modulare.

Una dintre cele mai semnificative manifestări ale structurilor algebrice în Teoria Numerelor, sau mai exact, structurile aritmetice, sunt cele care se desfăşoară peste corpuri finite. În mod particular, algebrele finite sunt esenţiale pentru înţelegerea structurilor aritmetice de diverse origini. Aceste obiecte, algebrele finite, pot avea reprezentări care complică înţelegerea completă a structurilor lor. Un exemplu esenţial în acest sens este factorizarea polinoamelor peste corpuri finite.

În **Capitolul 1**, trec în revistă rezultatele obţinute împreună cu W. Zudilin în [Nagoya Math. J., 2019]. În acest articol am demonstrat anumite proprietăţi aritmetice ale coefficienţilor unor forme semi-modulare folosind teorema de ridicare a lui Shimura-Borcherds de la forme modulare de ponderi semi-integrale la cele de ponderi pare (clasice) cu nivel. O analiză a acţiunilor Hecke pe aceste spaţii precum şi transferul acestora prin izomorfismul S-B fac posibilă demonstrarea proprietăţilor "magnetice" pentru forme semi-modulare (conjectural, aceste proprietăţi nu există pentru forme modulare)

În **Capitolul 2**, revizuiesc rezultatele obţinute împreună cu A. Popa, publicate în [Proc. London Math. Soc., 2013]. Explorăm spaţiul polinoamelor de perioadă asociate formelor modulare de pondere integrală pentru subgrupuri de indice finit ale grupului modular. În cadrul acestui grup, acest spaţiu include un produs scalar care extinde produsul scalar Petersson pe forme modulare, aşa cum este demonstrat prin formula lui Haberland. Include de asemenea o acţiune algebraică a operatorilor Hecke definită de Zagier. Extindem formula lui Haberland pentru a include forme modulare (nu numai cuspidale) pentru subgrupuri de indice finit şi dezvăluim că încorporează două formule mai puternice. De asemenea, extindem acţiunea operatorilor Hecke la polinoamele de perioadă ale formelor modulare, verificăm nedegenerarea produsului scalar în formula lui Haberland şi identificăm adjuncţii operatorilor Hecke în raport cu aceast produs scalar. Pentru $\Gamma_1(N)$, oferim mai multe aplicaţii: o extindere a izomorfismului Eichler–Shimura pentru a acoperi întregul spectru al formelor

modulare; identificarea relaţiilor satisfăcute de parţile pare şi impare ale polinoamelor de perioadă asociate cu formele cuspidale, care se disting de relaţiile de perioadă; şi o formulă detaliată pentru coeficienţii Fourier ai formelor proprii Hecke derivată din polinoamele lor de perioadă, extinzând teorema coeficientului a lui Manin.

În **Capitolul 3**, explorăm extinderea produsului scalar Petersson la întregul spaţiu al formelor modulare de pondere integrală $k \geqslant 2$ pentru un subgrup de indice finit al grupului modular. Demonstrăm că operatorii Hecke au aceiaşi adjuncţi în raport cu acest produs interior ca şi pentru formele cuspidale. În plus, stabilim că produsul Petersson este nedegenerat pentru $\Gamma_1(N)$

În **Capitolul 4**, calculăm o descompunere algebrică a inelelor black-box în modelul inelului generic. Mai precis, descompunem explicit un inel black-box ca un produs direct între un inel black-box nilpotent şi inele black-box locale şi unitale, prin calculul tuturor idempotenţilor primitivi ai săi. Algoritmul prezentat utilizează subrutine cuantice pentru calculul părţilor de putere p ale unui inel black-box şi apoi algoritmi clasici pentru calculul idempotenţilor primitivi corespunzători. Ca produs secundar, obţinem că reducerea unui inel black-box este, de asemenea, un inel black-box. Prima aplicare a acestei descompuneri este o extensie a lucrării lui Maurer şi Raub (2007) privind problema reprezentării în câmpurile finite black-box pentru cazul inelelor black-box reduse de putere p. O altă aplicare importantă este un atac $IND-CCA^1$ pentru orice schemă de criptare homomorfică pe inele în modelul inelului generic. Mai mult, atunci când spaţiul textului în clar este un inel black-box finit şi redus, prezentăm un atac de recuperare a textului în clar bazat pe problema reprezentării în corpurile prime black-box. Din perspectiva matematică, algoritmii noştri pot deschide unele căi pentru calculul invarianţilor geometrici şi algebrici, cum ar fi componentele conexe ale unei varietăţi algebrice, etc. Aceste rezultate au fost publicate împreuna cu M. Barcau în [Journal of Symb. Comp., 2024].

În **Capitolul 5**, detaliez trei direcţii de cercetare pe care intenţionez să le explorez în viitor, subliniind dezvoltările actuale şi importanţa problemelor discutate.