INSTITUTUL DE MATEMATICA
"SIMION STOILOW"
AL ACADEMIEI ROMANE

PREPRINT SERIES OF THE INSTITUTE OF MATHEMATICS
OF THE ROMANIAN ACADEMY

ISSN 0250 3638

Teoria numerelor azi. O privire de ansamblu

by

Nicuşor Dan

Preprint nr. 5/2015

BUCURESTI

Teoria numerelor azi. O privire de ansamblu

by

Nicuşor Dan

Preprint nr. 5/2015

November 2015

Simion Stoilow Institute of Matematics of the Romanian Academy
E-mail: nd@nicusordan.ro

TEORIA NUMERELOR AZI. O PRIVIRE DE ANSAMBLU

NICUSOR DAN

1. Precautie si conventie

Privirea de ansamblu prezentata in prezentul text este evident subiectiva si nu isi propune sa fie exhaustiva. Nu contine spre exemplu nicio referinta la teoria analitica a numerelor. Anumite concepte sunt prezentate in mod deliberat intr-un mod simplificat, pentru ca expunerea sa fie accesibila si nespecialistilor (o sa ne referim de exemplu la functii zeta ale varietatilor in loc de functii L, nu o sa indicam produsul riguros al adelelor, nu o sa ne referim la graduarea K-teoriei, etc.).

Referinta la toate numerele prime p (inclusiv ∞) semnifica referinta la toate numerele prime p si la valuarea arhimedeana a corpului numerelor rationale $\mathbb{Q}$. In acest context, $\mathbb{Q}_p$ pentru $p = \infty$ semnifica corpul numerelor reale R, care este completarea corpului $\mathbb{Q}$ pentru valuarea arhimedeana asa cum $\mathbb{Q}_p$ este completarea lui $\mathbb{Q}$ pentru valuarea p-adica] (vezi sectiunea 3.3).

2. Ce este teoria numerelor?

Teoria numerelor (sau arimetica) este studiul sistemelor de ecuatii diofantiene (ecuatii polinomiale cu coeficientii si nedeterminatele in inelul numerelor intregi $\mathbb{Z}$). Dupa un proces de maturizare, matematicienii au inteles ca nu pot sa rezolve toate sistemele de ecuatii diofantiene si si-au propus un obiectiv mai rezonabil: studiul calitativ al sistemelor de ecuatii diofantiene. Un sistem de ecuatii diofantiente defineste o varietate algebrica peste $Spec\mathbb{Z}$ (numita in continuare varietate aritmetica), unde $Spec\mathbb{Z}$ este un obiect geometric atasat inelului numerelor intregi $\mathbb{Z}$. Teoria numerelor este deci studiul calitativ al varietatilor aritmetice. Asa cum geometria algebrica este studiul calitativ al varietatilor peste obiectul geometric $Spec\mathbb{C}$ asociat corpului numerelor complexe $\mathbb{C}$ iar topologia studiul calitativ al varietatilor topologice si diferentiale.

Un studiu calitativ presupune definirea unor invarianti. Ca si in geometria algebrica si in topologie, acestia sunt obtinuti cu tehnici coomologice. Invariantii aritmetici sunt mai multi si mai fini decit cei topologici si cei din geometria algebrica. O parte dintre invariantii unei varietati aritmetice sunt codificati de functia sa zeta, o generalizare a functiei zeta Riemann.

Complexitatea teoriei numerelor fata de geometria algebrica si de topologie poate fi vazuta si prin complexitatea obiectului sau fundamental $Spec\mathbb{Z}$

fata de obiectul fundamental din geometria algebrica, S*pec*$\mathbb{C}$ si fata de obiectul fundamental din topologie, punctul. Astfel, dualitatea Poincare pentru S*pec*$\mathbb{Z}$ se exprima in ecuatia functionala a functiei zeta Riemann, rezultat netrivial (iar "teoria Hodge" pentru S*pec*$\mathbb{Z}$ este ipoteza Riemann).

3. Achizitiile teoriei numerelor la 1950 esentiale in teoria numerelor de azi

3.1. **Teoria corpului de clase.** Istoric, primul rezultat din teoria corpului de clase este ca -1 este rest patratic modulo p, p numar prim impar, daca si numai daca p este de forma $4k+1$. A fost primul pas intr-un set de intrebari si teorii partiale care a culminat cu teoria globala a corpului de clase (adica teoria corpului de clase pentru corpuri de numere), o mare realizare a matematicii anilor 1920, datorata lui Takagi si Artin. Un rezultat partial a fost teorema Kroneker-Weber, care a descris extinderea abeliana maximala a corpului numerelor rationale $\mathbb{Q}$ ca fiind $\mathbb{Q}(\mu_n)_n$ (extinderea minima a lui $\mathbb{Q}$ care contine toate radacinile unitatii). Practic, teoria globala a corpului de clase: a) da o descriere explicita a abelianizatului grupului Galois al oricarui corp de numere (adica extindere finita a lui $\mathbb{Q}$); b) enunta o general reciprocity law care generalizeaza rezultatul cu -1 rest patratic modulo p de mai sus si reciprocitatea patratica.

Hasse a rescris in anii 1930 teoria corpului de clase intr-un principiu local-global. Rezultatul asupra abelianizatului grupului Galois al unui corp de numere a fost conectat cu un rezultat de caracterizare al abelianizatelor grupurilor Galois ale localizatelor corpului de numere (extinderi finite ale lui $\mathbb{Q}_p$ (inclusiv $\mathbb{R}$) numite in continuare corpuri locale): teoria locala a corpului de clase.

Iin anii 1950 Hochild, Nakayama si Tate au rescris teoria (locala si globala) a corpului de clase intr-un limbaj coomologic.

Bibliografie:

J. W. S. Cassels, A. Frohlich, *Algebraic Number Theory*, Thompson Book Company, 1967

J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften, 322, Springer-Verlag, 1999

J. Neukirch: *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften, 280. Springer-Verlag, 1986.

3.2. **Teza Tate.** In incercarea sa de a rescrie teoria corpului de clase fara analiza matematica (adica de a elimina toate demonstratiile in care se foloseau proprietati analitice ale functiei zeta a corpurilor de numere), Chevaley a introdus notiunea de adele (produsul corpurilor $\mathbb{Q}_p$ pentru toti p (inclusiv ∞)) si idele (produsul grupurilor $\mathbb{Q}_p^*$ pentru toti p (inclusiv ∞)).

Tate, in teza de doctorat din 1950, a rescris demonstratia ecuatiei functionale a functiei zeta a corpurilor de numere intr-un limbaj al analizei pe

grupurile topologice ale adelor si idelelor (analiza matematica revine deci). Faptul este important pentru ca este prima demonstratie in care poate numerele prime p (inclusiv ∞) au un rol simetric, spre deosebire de demonstratiile precedente, in care numarul prim $p = \infty$ avea un rol privilegiat (adica corpul $\mathbb{R}$ avea un rol privilegiat fata de corpurile $\mathbb{Q}_p$).

Bibliografie: Teza originala a lui Tate, inclusa in J. W. S. Cassels, A. Frohlich, *Algebraic Number Theory*, Thompson Book Company, 1967.

3.3. **Analogia arithmetic geometric.** Scoala germana de la inceputul secolului 20 (Hasse, Artin) a observat utilitatea analogiei intre corpuri de numere si corpuri de functii de o variabila peste un corp finit, adica corpurile functiilor rationale peste o curba peste un corp finit. $\mathbb{F}_p(X)$ este exemplul cel mai simplu, constituind corpul functiilor rationale peste dreapta proiectiva peste corpul finit $\mathbb{F}_p$. Cand curba nu mai este dreapta proiectiva ci are un gen superior, lucrurile sunt mai complica dar si mult mai interesante. Numim pe scurt pe scurt aici corpuri de functii corpuri de functii de o variabila peste un corp finit. Corpurile de numere si corpurile de functii de o variabila peste un corp finit sunt numite impreuna corpuri globale.

Orice enunt arithmetic, adica un enunt formulat peste un corp de numere, are un analog geometric, adica acelasi enunt in care inlocuim corpul de numere cu un corp de functii. Vorbim de cazul aritmetic si de cazul geometric. Evident, cazul geometric e intotdeauna mai simplu, caci toate obiectele sunt varietati, fascicule, sectiuni, etc. peste un acelasi corp de baza (corpul finit) si se pot folosi toate teoremele geometriei algebrice.

Bibliografie:
Andre Weil, articolul 1939a din Andre Weil, *Collected Papers*, Springer-Verlag, 1979
K. Iwasawa, *Analogies between number fields and function fields*, Some Recent Advances in the Basic Sciences 2, 1969, 203-208.

3.4. **Ipoteza Riemann in cazul geometric.** Enuntul analogului ipotezei Riemann pentru cazul geometric a fost scris de scoala germana la inceputul secolului 20. Demonstratia a fost data de Hasse in cazul g=1 (curbe eliptice) in 1930 si de Weil in anul 1947 pentru curbe de orice gen. Pentru aceasta demonstratie, Weil a fost nevoit sa rescrie geometria algebrica trecind de la coeficienti $\mathbb{C}$ la coeficienti in orice corp. A fost primul care a considerat varietatile abeliene si jacobiana unei curbe in acest context.

Bibliografie: A. Weil, *Courbes algebriques et varieties abeliennes*, Hermann, 1948.

4. Problemele mari ale teoriei numerelor contemporane

4.1. **Ipoteza Riemann.** Functia zeta Riemann este un invariant care codifica informatia despre distributia numerelor prime. Ipoteza Riemann afirma ca toate zerourile netrivilale ale acesteia sunt numere complexe cu partea

reala $1/2$. Serre a legat varianta geometrica a enuntului, pentru curba proiectiva peste un corp finit corespunzatoare corpului de functii, de o teorie Hodge conjecturala pe respectiva curba proiectiva.

4.2. **Demonstratia ecuatiei functionale a functiei zeta a unei varietati aritmetice.** Functia zeta a varietatii aritmetice codifica informatie pentru toate numerele prime p si pentru toate reducerile modulo p ale varietatii aritmetice de la $\mathbb{Z}$ la $\mathbb{F}_p$. Serre a conjecturat o ecuatie functionala a functiei zeta a fiecarei varietati aritmetice. In cazul (primul caz netrivial) in care varietatea in cauza este o curba eliptica, problema este echivalenta cu teorema demonstrata de Wiles (orice curba eliptica definita peste $\mathbb{Q}$ este dominata de o curba modulara) si care implica teorema lui Fermat.

4.3. **Valorile functie zeta ale unei varietati aritmetice in intregi: conjectura Bloch-Kato.** Dirichlet a exprimat reziduul in $s = 1$ al functiei zeta al unui corp de numere in functie de mai multi invarianti ai corpului: numarul de radacini ale unitatii incluse in corp, cardinalul grupului de clase (citul intre grupul tuturor idealelor si grupul idealelor principale), etc. Conjectura Bloch-Kato (1990) generalizeaza acest enunt la orice varietate aritmetica si la orice valoare intreaga a lui s. Formulari partiale au fost scrise de Lichtenbaum, Deligne si Beilinson. Cand $s = 1$ si cand varietatea este curba eliptica, enuntul este celebra conjuctura Birch - Swinnerton Dyer. In linii mari, conjectura exprima echivalenta unor invarianti de natura diferita asociati varietatilor aritmetice.

5. Teme ale teoriei numerelor contemporane

5.1. **Curbe modulare, forme modulare, varietati Shimura, forme automorfe.** O curba modulara este un cit al semi-spatiului Poincare printr-un grup de congruente (adica un subgrup de indice finit al lui $SL_2(\mathbb{Z})$). O forma modulara este foarte aproape de o functie rationala pe o curba modulara. Mai precis este o sectiune a unui fibrat inversibil amplu pe curba modulara (asa cum un polinom omogen de grad k in 2 variabile este o sectiune a fibratului $\mathcal{O}(k)$ si aproape o functie rationala pe dreapta proiectiva).

Putem abstractiza definitia curbei modulare in doua etape, ceea ce va fi util la generalizarea in dimensiune superioara si la programul Langlands. In primul rand semi-spatiul Poincare se mai scrie $O(2) \setminus SL_2(R)$, citul la actiunea la stinga a subgrupului $O(2)$ pe $SL_2(\mathbb{R})$, deci o curba modulara se poate scrie $O(2) \setminus SL_2(\mathbb{R})/\Gamma$, pentru Γ un grup de congruente. E un principiu in aritmetica acela ca numerele prime p (inclusiv ∞) trebuie sa joace un rol simetric. In aceasta idee, putem rescrie citul de mai sus in forma $O(2)\setminus SL_2(\mathbb{A})/G$, unde $\mathbb{A}$ reprezinta adelele, deci $SL_2(\mathbb{A})$ este produsul dupa toate numerele prime p (inclusiv ∞) ale grupurilor $SL_2(\mathbb{Q}_p)$, iar G este un subgrup de indice finit in $SL_2(\mathbb{Q})$.

Dupa aceasta abstractizare putem generaliza. O varietate Shimura este un cit dublu $O(n)\setminus SL_n(\mathbb{R})/\Gamma$, unde Γ este un subgrup de indice finit in $SL_n(\mathbb{Z})$,

sau, echivalent, un cit dublu $O(n) \setminus SL_n(\mathbb{A})/G$, unde G este un subgrup de indice finit in $SL_n(\mathbb{Q})$. O forma automorfa este aproape o functie rationala pe o varietate Shimura.

Bibliografie: P. Deligne, *Travaux de Shimura*, Seminaire Bourbaki, nr. 389, anul 1970/1971.

5.2. **Programul Langlands.** A cunoaste abelianizatul unui grup Galois G (de exemplu $Gal(\mathbb{Q})$) e tot una cu a cunoaste caracterele lui, adica morfismele $G \to GL_1(\mathbb{C}) = \mathbb{C}^*$. Am vrea sa stim (cu aplicatii pe probleme diofantiene explicite, de exemplu teorema Fermat, inca de la cazul $n = 2$) care sunt reprezentarile de dimensiune n ale lui G, adica morfismele $G \to GL_n(\mathbb{C})$. Analogia cu caracterele (GL_1) ne spune ca trebuie inteles intii cazul local, adica in exemplul $Gal(\mathbb{Q})$ reprezentarile de dimensiune n ale lui $Gal(\mathbb{Q}_p)$.

In cazul GL_1 pentru un corp local K, una din formularile teoriei corpului de clase este o corespondenta intre caracterele lui $Gal(K)$ si caracterele lui K^* (grupul inversibelelor lui K). Langlands a conjecturat in anii 60, pentru K corp local, o corespondenta intre reprezentarile de dimensiune n ale lui $Gal(K)$, adica morfisme $Gal(K) \to GL_n(\mathbb{C})$, si anumite reprezentari ale lui $GL_n(K)$ (infinit dimensionale in majoritatea lor). Aceasta este conjectura Langlands locala. A fost demonstrata de Harris-Taylor in 2000.

Conjecturile de tip Langlands global sunt mai dificil de exprimat la un nivel elementar. O conjectura tip (nu cea mai generala) este de genul: orice reprezentare de grad n a lui $Gal(\mathbb{Q})$, adica un morfism $Gal(\mathbb{Q}) \to GL_n(\mathbb{C})$, se corespunde cu o reprezentare automorfa, adica cu un sistem de reprezentari ale lui $Gl_n(\mathbb{Q}_p)$ pentru fiecare p si o reprezentare a lui $GL_n(\mathbb{R})$, care satisfac anumite compatibilitati. In plus, reprezentarile automorfe sunt in stransa legatura cu formele automorfe. Programul Langlands este departe de a fi incheiat.

Bibliografie:
(cazul $n = 2$) R. Taylor, *Representations of Galois groups associated to modular forms*, Proceedings of ICM 1994
A. Borel, *Formes automorphes et serie de Dirichlet*, Seminaire Bourbaki nr. 466, anul 1974-1975
Stephen Gelbart, *An Elementary Introduction to the Langlands Program*, Bulletin of the AMS 10, 1984, p. 177-219

5.3. **Ciclotomie, sau teorie Iwasawa.** In demonstratia lui Weil la ipoteza Riemann in cazul geometric (sectiunea 3.4), este esentiala folosirea jacobienei curbei in cauza. Mai precis, jacobiana curbei este o varietate abeliana de dimensiune g peste corpul finit. Putem considera extinderea sa peste inchiderea algebrica a corpului finit. Punctele de l^n-torsiune ale acesteia din urma pentru l un numar prim fixat, diferit de caracteristica corpului finit, iar n un numar natural oarecare, formeaza un grup V_l izomorf cu $(\mathbb{Q}_l/\mathbb{Z}_l)^{2g}$.

Endomorfismele acestui grup sunt date de $M_{2g}(\mathbb{Z}_l)$ (matricile $2g$ x $2g$ cu coeficienti in $\mathbb{Z}_l$), iar automorfismele de grupul $GL_{2g}(\mathbb{Z}_l)$. Automorfismul Frobenius actioneaza liniar pe V_l, deci da un element in $M_{2g}(\mathbb{Z}_l)$. Polinomul caracteristic al acestei matrici este functia zeta a curbei. Este o justificare pentru cautarea analogului aritmetic al jacobienei.

Cautarea analogului aritmetic al Jacobienei si al altor notiuni in cazul aritmetic care sa fie traduceri de notiuni binecunoscute in cazul geometric a fost un proiect inceput de Weil si desfasurat de Iwasawa, intr-un efort de 20 de ani. Analogul grupului V_l de mai sus pentru corpul de numere $\mathbb{Q}$ este limita inductiva V_l a grupurilor Cl_n, unde Cl_n este grupul corpurilor de clase (ideale/ideale principale) ale corpului $K_n = \mathbb{Q}(\mu_{l^n})$ (aditionarea radacinii de ordin l^n a unitatii la corpul $\mathbb{Q}$), iar analogul actiunii automorfismului Frobenius este dat de actiunea pe V_l a grupului Galois al lui $K_\infty = \mathbb{Q}(\mu_\infty)$ (reuniunea tuturor K_n peste $\mathbb{Q}$).

In linii mari, in notatiile de mai sus, teoria Iwasawa studiaza proprietati ale extinderii K_∞ peste $\mathbb{Q}$, pentru l un numar prim fixat. In elaborarea teoriei sale Iwasawa a folosit sau regasit rezultate demonstrate de Kummer cu 120 de ani inainte.

Conjectura principala Iwasawa vorbeste de egalitatea a doua functii zeta p-adice. Functia zeta p-adica este un obiect care interpoleaza (codifica), pe de o parte, congruentele modulo p ale valorilor rationale ale functie zeta Riemann in intregii negativi. Pe de alta parte, e un obiect care codifica grupul V_p descris in paragraful precedent (am schimbat notatia, inlocuind l cu p) cu actiunea lui $Gal(K_\infty/\mathbb{Q})$. Egalitatea celor doua functii zeta p-adice a fost demonstrata de Mazur si Wiles in 1972 folosind tehnici de curbe modulare si, mai simplu in anii 1990 de Kolivagin si Rubin, folosind doar tehnici de teorie Iwasawa.

Generalizari. Putem inlocui corpul $\mathbb{Q}$ cu un corp de numere arbitrar L si putem studia extinderea K_∞/L , unde $K_\infty = L(\mu_\infty)$. Putem, mai mult, sa inlocuim corpul $\mathbb{Q}$, care se corespunde cu $Spec\mathbb{Z}$, cu orice alta varietate aritmetica. Putem sa consideram de exemplu o curba eliptica definita peste $\mathbb{Q}$ si sa studiem limita inductive a grupurilor Selmer (invarianti coomologici atasati unei curbe eliptice peste un corp de numere) Sel_n ale curbei definite peste $K_n = \mathbb{Q}(\mu_\infty)$. Functia zeta p-adica atasata acestui grup este conjectural egala cu o functie zeta p-adica obtinuta prin interpolarea valorilor functiei zeta ai curbei eliptice in intregi negativi. E o teorema foarte dificila demontrata de Kato in anii 2000. Numim astfel de enunturi tot conjectura principala Iwasawa.

Bibliografie:

(pentru analogia arithmetic-geometric) K. Iwasawa, *Analogies between number fields and function fields*, Some Recent Advances in the Basic Sciences 2, 1969, p. 203-208

(pentru analogul arithmetic al jacobienei) J. Coates, *K-theory and Iwasawa's analogue of the jacobian* in *Algebraic K-theory, II*, Lecture Notes in Mathematics, 342, Springer-Verlag, 1973, p. 502-520

(teoria ciclotomica) L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, 1997

(pentru generalizari) R. Greenberg, *Iwasawa Theory past and present*, in *Class Field Theory–Its Centenary and Prospect*, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, p. 335-385.

5.4. **Reprezentari galoisiene l-adice si p-adice.** Pentru o curba eliptica definita peste $\mathbb{Q}$, putem considera punctele ei de l^∞ torsiune peste inchiderea algebrica a lui $\mathbb{Q}$. Formeaza un grup abelian izomorf cu $(\mathbb{Q}_l/\mathbb{Z}_l)^2$, pe care $Gal(\mathbb{Q})$ actioneaza. Endomorfismele grupului $(\mathbb{Q}_l/\mathbb{Z}_l)^2$ sunt descrise de grupul $GL_2(\mathbb{Z}_l)$, deci obtinem o reprezentare $Gal(\mathbb{Q}) \to GL_2(\mathbb{Z}_l)$. Practic toate proprietatile aritmetice l-adice (adica cele care tin de divizibilitatea cu l) ale curbei sunt codificate de acest morfism. Grupul $Gal(\mathbb{Q})$ este prea complicat pentru a putea folosi in practica aceasta reprezentare. Insa pentru fiecare prim p avem o incluziune (determinata pina la o conjugare) a lui $Gal(\mathbb{Q}_p)$ in $Gal(\mathbb{Q})$. Restrictionind la $Gal(\mathbb{Q}_p)$ obtinem o reprezentare $Gal(\mathbb{Q}_p) \to GL_2(\mathbb{Z}_l)$. Grupurile $Gal(\mathbb{Q}_p)$ sunt mult mai tractabile decit $Gal(\mathbb{Q})$ si putem obtine multa informatie din aceste reprezentari.

Mai general, numim reprezentare l-adica a lui $Gal(K)$, pentru K un corp local (de exemplu $\mathbb{Q}_p$), un morfism $Gal(K) \to GL_n(\mathbb{Z}_l)$ sau un morfism $Gal(K) \to GL_n(\mathbb{Q}_l)$. Exista o teorie generala pentru aceste reprezentari. Teoria e mult mai dificila cand $l = p$, adica atunci cand numarul prim l coincide cu caracteristica reziduala a corpului local K (definita ca fiind caracteristica corpului finit O/m, O fiind inelul local al corpului K iar m idealul maximal (in cazul $K = \mathbb{Q}_p$, $O = \mathbb{Z}_p$, O/m este $\mathbb{F}_p$, caracteristica reziduala este p)).

Pentru o varietate proiectiva lisa X peste $\mathbb{Q}_p$ si pentru un numar natural i avem un grup de coomologie etala $H^i_{et}(X, \mathbb{Q}_p)$ si un grup de coomologie de Rham $H^i_{dR}(X, \mathbb{Q}_p)$, fiecare cu diverse structuri aditionale. Teoria reprezentarilor de la paragraful precedent permite identificarea acestor grupuri cu aceste structuri. Prin comparatia grupurilor $H^i_{et}(X, \mathbb{Z}_p)$ si $H^i_{dR}(X, \mathbb{Z}_p)$ se obtine un numar p-adic a carui valuare este legata de valuarea p-adica a functiei zeta a varietatii in $1 - i$ (conjectura Bloch-Kato).

5.5. **Deformari de reprezentari Galoisiene.** Teoria studiaza reprezentari ale lui $Gal(\mathbb{Q})$. Vom exemplifica pe teorema lui Wiles. Acesta a demonstrat ca orice curba eliptica definita peste $\mathbb{Q}$ este modulara (adica exista un morfism surjectiv de la o curba modulara la ea). Demonstratia acestui enunt fusese redusa anterior la demonstratia faptului ca, pentru un numar prim l, reprezentarea lui $Gal(\mathbb{Q})$ asociata curbei eliptice ca in sectiunea precedenta este aceeasi cu reprezentarea lui $Gal(\mathbb{Q})$ asociata (intr-un anume mod pe care nu il detaliem) unei forme modulare.

Morfismul canonic (reducerea modulo l) de la $\mathbb{Z}_l$ la $\mathbb{F}_l$ induce un morfism canonic $GL_2(\mathbb{Z}_l) \to GL_2(\mathbb{F}_l)$. O reprezentare R a lui $Gal(\mathbb{Q})$ in $GL_2(\mathbb{Z}_l)$ induce prin acest morfism o reprezentare R' a lui $Gal(\mathbb{Q})$ in $GL_2(\mathbb{F}_l)$. Spunem ca R este o deformare a lui R' (asa cum $\mathbb{Z}_l$ este o deformare a lui F_l, intr-un sens pe care nu il precizam).

Primul pas in demonstratia lui Wiles a fost sa demonstreze ca reprezentarea $Gal(\mathbb{Q}) \to Gl_2(\mathbb{F}_l)$ asociata unei curbe eliptice este modulara, adica coincide cu reprezentarea asociata unei forme modulare. Era o teorema a lui Serre pentru anumite numere prime l mici (3, 5). Partea care tine de teoria deformarilor a fost urmatoarea. Pentru o reprezentare $Gal(\mathbb{Q})$ in $GL_2(\mathbb{F}_l)$ despre care stim ca e modulara, calculam spatiul tuturor reprezentarilor $Gal(\mathbb{Q}) \to GL_2(\mathbb{Z}_l)$ care deformeaza reprezentarea data si spatiul tuturor reprezentarilor modulare $Gal(\mathbb{Q}) \to GL_2(\mathbb{Z}_l)$ care deformeaza reprezentarea data. Demonstram ca cele doua spatii sunt identice demonstrind ca sunt aproape netede si ca "spatiile lor tangente" coincid.

5.6. **K-teorie, motive, complexe motivice, polilogaritmi.** K-teoria algebrica este o teorie coomologica care asociaza unui inel si mai general unei scheme X invarianti grupuri abeliene $K_n(X)$ pentru fiecare numar natural n. A fost definita in anii 1970. Observatia ca ordinul subgrupului de torsiune al grupului $K_n(\mathbb{Z})$ este legat de valoarea functiei zeta Riemann in $1-n$ a fost o surpriza. Grupurile de K-teorie calculeaza deci invarianti aritmetici.

Deja in anii 1960 s-a observat ca nu exista o teorie buna de coomologie cu valori in $\mathbb{Q}$-spatii vectoriale pentru varietati algebrice proiective lise peste corpuri generale (adica functori H^i de la varietatile algebrice proiective lise la $\mathbb{Q}$-spatii vectoriale) care sa satisfaca anumite axiome firesti. Cu atit mai putin exista o buna teorie de coomologie coeficienti in grupuri abeliene, caci daca am avea o astfel de teorie am tensoriza coeficientii cu $\mathbb{Q}$ si am obtine teoria dorita in Q-spatii vectoriale. Explicatia euristica este ca varietatile algebrice sunt mult mai rigide decit varietatile diferentiabile. De aceea a aparut ideea unei categorii abeliene universale in care acesti functori cu axiome firesti sa existe. Numim conjectural aceasta categorie categoria motivelor pure, daca ne restringem la varietati proiective lise, sau categoria abeliana a motivelor mixte, daca ne referim la toate varietatile algebrice. Prototipul unui motiv mixt (pur) este un obiect $H^i(X)$ in una dintre aceste categorii abeliene, pentru X o varietate (proiectiva lisa).

Grupurile de K-teorie algebrica ale varietatii pot fi vazute ca grupuri Ext^i in categoria abeliana a fascicolelor motivice peste X (un fascicol motivic peste X este fata de un motiv ceea ce este un fascicul in grupuri abeliene peste o varietate fata de un grup abelian). Complexele motivice $\mathbb{Z}(n)$ sunt, cite unul pentru fiecare numar natural n, complexe de fascicule in grupuri abeliene peste o varietate algebrica X, care verifica anumite proprietati, cea mai importanta fiind ca hipercoomologia acestui complex calculeaza grupurile de K-teorie ale lui X. Complexele motivice nu sunt triviale cind schema X este spectrul unui corp caci nici K-teoria unui corp nu este.

$n-$logaritmii sunt, pentru fiecare numar natural n, functii complexe multivaluate de o variabila complexa ($\mathbb{C} \to \mathbb{C}$), generalizind functia logaritm. 1-logaritmul este logaritmul clasic. Asa cum logaritmul are ecuatia functionala $log(xy) = logx + logy$, n-logaritmii au mai multe ecuatii functionale. Structura combinatorica a acestora este cunoscuta complet in cazul $n = 2$ si aproape complet in cazul $n = 3$. Cind varietatea algebrica X este spectrul unui corp, un complex de fascicule pe ea este un complex de grupuri abeliene. Deci complexul motivic $\mathbb{Z}(n)$ trebuie sa fie un complex de grupuri abeliene. Conjectural, $\mathbb{Z}(n)$ este un anumit complex de grupuri abeliene, in care fiecare din grupurile abeliene are o prezentare explicita cu generatori si relatii, care copiaza relatiile functionale ale functiei n-logaritm.

5.7. **Valori speciale ale functiilor zeta (vezi** 4.3**).** Un prim rezultat contemporan de acest tip este un corolar la teorema Mazur-Wiles citata in sectiunea 5.3. Teorema Mazur-Wiles da valuarea p a valorii functiei zeta Riemann in $1 - n$, n natural, pentru fiecare numar prim p, in functie de ordinul unor grupuri coomologice. Punand impreuna toate valuarile pentru toti p gasim acest numar rational, pana la un semn. Acesta este exprimat in functie de ordinul unor grupuri coomologice (obtinute punand impreuna toate grupurile coomologice de mai sus pentru toti p) de tip coomologie etala.

Generalizarea enuntului din paragraful precedent de la functia zeta Riemann la functia zeta asociata oricarui corp de numere este conjectura Lichtenbaum. Exista o exprimare paralela care foloseste in loc de grupuri de coomologie etala grupuri de K-teorie (5.6). Echivalenta acestor doua enunturi a fost problema deschisa pina la rezultatul lui Voevodski din 1996.

Cele de mai sus sunt rezultate si conjecturi pentru functia zeta asociata corpurilor de numere. Cind trecem la functia zeta asociata varietatilor aritmetice, pentru a formula conjectural valoarea acestei functii in $1 - n$, n numar natural, avem nevoie de o intreaga familie de grupuri abeliene si de morfisme intre ele: grupuri de K-teorie, grupuri de coomologie etala si grupuri de coomologie de Rham. Acest enunt complex poarta numele de conjectura Bloch-Kato si este un subiect intens cercetat. Este demonstrat doar pentru functia zeta a corpurilor de numere abeliene si pentru functia zeta a unei curbe eliptice.

Bibliografie:

(pentru partea de pina la conjectura Lichtenbaum) Manfred Kolster, *K-theory and arithmetic* in *Contemporary developments in algebraic K-theory*, ICTP Trieste, 2002

(pentru partea Bloch-Kato) S.Bloch, K.Kato, *L Functions and Tamagawa numbers of motives* in *The Grothendieck Festchrift*, Birkhuser, Basel, 1990, vol. 1, p. 333-400.

5.8. **Teoria corpului de clase in dimensiune superioara, adele si teoria Tate in dimensiune superioara.** In incercarea de a demonstra problema 4.2 cu metoda Tate citata in sectiunea 3.2. s-a definit grupul adelelor

peste scheme de dimensiune superioara, cazul classic Tate fiind vazut ca grupul adelelor peste schema de dimensiune 1 $Spec\mathbb{Z}$. Teoria este strans legata de extinderea teoriei corpului de clase de la corpuri de numere, vazuta ca o teorie de dimensiune 1 asociata inelului de intregi al acestor corpuri de numere, la scheme de orice dimensiune (de exemplu o curba eliptica definita peste $\mathbb{Z}$ este o suprafata, are dimensiunea Krull 2). Cele doua teorii au fost realizate. Lipseste inca conectarea lor cu functiile zeta.

Bibliografie: I. Fesenko, M. Kurihara. *Invitation to higher local fields* in *Geometry and Topology Monographs*, vol. 3, Warwick, 2000

5.9. **Teorii combinatorice pentru grupul Galois absolut. Geometria anabeliana.** Am vazut deja ce importanta este intelegerea reprezentarilor grupului Galois absolut $Gal(\mathbb{Q})$. Grothendieck a fost primul care a scris o schita de proiect pentru intelegerea directa, combinatorica, a grupului $Gal(\mathbb{Q})$. Grupul combinatoric cu care $Gal(\mathbb{Q})$ este comparat este construit cu ajutorul grupurilor fundamentale ale spatiilor de moduli de curbe algebrice.

Exista o notiune de grup fundamental al unei scheme, analoaga notiunii de grup fundamental din topologie. Cind schema este spectrul unui corp, grupul sau fundamental este grupul Galois al corpului. Intrebarea cat de mult din strucrura unei varietati se poate reconstrui din cunoasterea grupului sau fundamental este o tema contemporana de reflectie.

Bibliografie:

Y. Ihara, *Braids, Galois groups and some arithmetical functions* in *Proceedings of the ICM 1990*

V. G. Drinfeld, *On quasitriangular quasi-Hopf algebras and a group closely connected with* $Gal(\mathbb{Q})$, Leningr. Math. J. 2, 1991, p. 829-860

A. Grothendieck, *Esquise dun Programme* in Schneps, Leila (ed.) et al., *Geometric Galois actions. 1. Around Grothendieck's "Esquisse d'un programme". Proceedings of the conference on geometry and arithmetic of moduli spaces, Luminy, France, August 1995*, Lond. Math. Soc. Lect. Note Ser. 242, Cambridge University Press. 1997, p. 5-48

G. Faltings, *Curves and their fundamental groups*, Seminarul Bourbaki nr. 840, anul 1997-1998

T. Szamuely, *Groupes de Galois de corps de type fini (d'apres Pop)*, Seminarul Bourbaki nr. 923, anul 2002-2003.

5.10. **Geometrie Arakelov.** Inaltimea (height) pentru o solutie a unui sistem diofantian este in linii mari suma modulelor valorilor absolute. De aici, mai general, putem definiti inaltimea unui punct pe o varietate aritmetica si chiar inaltimea unei subvarietati. Au fost dezvoltate tehnici de marginire a inaltimii punctelor si subvarietatilor varietatilor aritmetice. Geometria Arakelov a aparut ca o teorie care sa trateze sistematic definitia inaltimii si tehnicile de marginire ale acesteia.

Analogia aritmetic-geometric a fost apelata si in incercarea de demonstrare a conjecturii Mordel (demonstrata de Faltings in 1983). Analogul geometric a fost demonstrat in anii 1960, iar demonstratia conecteaza notiunea de inaltime cu teoria intersectiei (ajunge sa consideram teoria intersectiei divizorilor pe o suprafata proiectiva lisa peste un corp algebric inchis). De unde cautarea unei teorii de intersectie in cazul arithmetic. Stim din geometria algebrica ca pentru a avea o teorie de intersectie trebuie sa lucram cu varietati proiective = compacte (pentru a nu pierde intersectia la infinit, pentru a avea o teorema Bezout, de exemplu). Deci trebuie sa "compactificam" varietatile aritmetice. Convenim sa compactificam $Spec\mathbb{Z}$ adaugindu-i inca un punct, valuarea infinita. Analogia cu cazul geometric este urmatoarea: pentru orice functie rationala nenula pe o curba proiectiva numarul zerourilor cu multiplicitati coincide cu numarul polilor cu multiplicitati; pentru orice numar nenul intr-un corp de numere produsul valuarilor sale in toate primele (inclusiv infinitul) este 1. Articolul citat al lui Weil explica foarte bine aceasta analogie.

Daca avem o suprafata aritmetica, adica o schema lisa de dimensiune 2 impreuna cu un morfism proiectiv peste $Spec\mathbb{Z}$ (fibrele sunt deci curbe), ca sa o compactificam convenim sa ii adaugam o intreaga fibra deasupra punctului infinit cu care compactificam $Spec\mathbb{Z}$, iar aceasta fibra este schema initiala tensorizata peste $Spec\mathbb{Z}$ cu $Spec\mathbb{C}$. Va fi o curba proiectiva peste $\mathbb{C}$. Putem copia teoria intersectiei de la suprafetele proiective din geometria algebrica la teoria suprafetelor aritmetice astfel compactificate, cu conditia sa adaugam metrici pe fibra infinita adaugata. Sunt necesare tehnici de analiza complexa. Teoria se generalizeaza la varietati de dimensiune superioara. Multe din rezultatele din geometria algebrica se transfera fara probleme aici, altele in mod surprinzator de greu (de exemplu teorema Riemann-Roch unde apar surprinzator termeni suplimentari care contin derivate ale functiei zeta Riemann in $1-n$, n numar natural). Teoria a fost folosita in cea de-a doua demonstratie a lui Faltings la conjectura Mordel.

Desi a inceput ca instrument pentru marginirea inaltimii punctelor varietatilor aritmetice, odata cu dezvoltarea teoriei in dimensiuni superioare interesul s-a mutat catre faptul ca produce obiecte intermediare intre K-teorie si coomologia Deligne-Beilinson.

Bibliografie:

(pentru teoria originala a lui Arakelov, pentru suprafete) G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. 119, 1984, p. 387424

(pentru teoria Arakelov in orice dimensiune) H. Gillet, *A Riemann-Roch Theorem in Arithmetic Geometry*, in *Proceedings of the ICM 1990.*

Institutul de Matematica al Academiei Romane, Calea Grivitei 21, Bucuresti 010702, Romania

E-mail address: nd@nicusordan.ro