Ewa Kozłowska-Walania
Zakład Algebry, Instytut Matematyki UG

Seminarium magisterskie

Algebra i jej zastosowania

Algebra abstrakcyjna posiada bardzo bogate zastosowania w wielu dziedzinach matematyki, ale nie tylko - w związku z rozwojem technik komputrowych również informatyka często czerpie z metod algebraicznych. Jak wiadomo, u podstaw chociażby teorii kodowania czy kryptografii leży arytmetyka modularna i teoria ciał skończonych. Ponadto, w dzisiejszych czasach istotnie rozwija się zastosowanie krzywych eliptycznych i hipereliptycznych w kryptografii, które pozwala na korzystne skrócenie kluczy a więc obniżenie wymagań odnośnie pamięci i procesora w stosunku chciażby do szeroko stosowanego kryptosystemu RSA. Z kolei teoria kodowania algebraicznego pozwala na wychwycenie błędów pojawiających się podczas transmisji danych. Podczas seminarium zajmiemy się różnymi zastosowaniami metod algebraicznych, zaś tematy prac uwzględnią zarówno zagadnienia czysto algebraiczne, jak i te bardziej nastawione na zastosowania w teorii kodowania czy kryptografii.

Orientacyjny zakres seminarium:

(1) Algebry skończenie wymiarowe, liczby hiperzespolone, algebry kwaternionów i oktonionów Cayley'a, pierścienie noetherowskie, bazy Gröbnera i algorytm Buchbergera, algebry Boole'a, monoidy i automaty, kwadraty łacińskie, konstrukcje geometryczne.
(2) Elementy teorii kodowania, kody blokowe, kody liniowe, kody grupowe, kody macierzowe, kody doskonałe, kody Hamminga, sekwencje pseudolosowe, kody cykliczne, kody BCH, kody Hadamarda.
(3) Elementy kryptografii z kluczem publicznym.
(4) Krzywe eliptyczne i hipereliptyczne wraz z ich zastosowaniem w kryptografii, arytmetyka na krzywej eliptycznej i hipereliptycznej, iloczyn Weila, logarytm dyskretny, algorytmy Schoofa, Elkiesa i Atkina.

Literatura:

1. N. Koblitz, Algebraiczne aspekty kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2000.
2. I. Blake, G. Seroussi, N. Smart, Krzywe eliptyczne w kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
3. W. J. Gilbert, W. K. Nicholson, Algebra współczesna z zastosowaniami, WNT, Warszawa, 2008.
4. M.Ch. Klin, R. Poeschel, K. Rosenbaum, Algebra stosowana dla matematyków i informatyków, WNT, Warszawa, 1992.
5. I.L. Kantor, A.S. Solodovnikov, Hypercomplex Numbers. An elementary introduction to algebras. Springer-Verlag, 1989.
6. J.H. Conway, D.A. Smith, On quaternions and Octanions: Their Geometry, Arithmetic and Symmetry, A K Peters, Ltd. 2003.
7. D. Joyner, R. Kreminski, J. Turisco, Applied abstract algebra, John Hopkins University Press, Baltimore and London, 2004.
8. G. Birkhoff, T. C. Bartee, Współczesna algebra stosowana, Warszawa 1983.
9. E. R. Berlekamp, Algebraic coding theory, 2nd edition, 2015.