Ewa Kozłowska-Walania
Zakład Algebry, Instytut Matematyki UG

Wykład fakultatywny
(semestr letni)

Kodowanie algebraiczne

Często może nam się wydawać, że mało wspomina się o zastosowaniach abstrakcyjnej algebry we współczesnym nam świecie i w innych dziedzinach matematyki. Tymczasem niektóre działy matematyki oraz informatyki wymagają znajomości bardziej zaawansowanych metod algebraicznych - przykładem może tu być teoria kodowania i kryptografia. W dzisiejszych czasach szybkiego rozwoju technik komputerowych i teleinformatycznych duże znaczenie mają metody ochrony informacji przed błędami oraz przed nielegalnym dostępem. Świetnym przykładem takiej sytuacji może być tutaj przesyłanie zdjęć z kosmosu. Informację I, którą chcemy przesłać przekazujemy do kanału transmisyjnego. Po przesłaniu informacji I, po drugiej stronie kanału otrzymujemy jakąś informację odebraną $T(I)$. Zależy nam, aby zachodziła równość $T(I) = I$. Bardziej prawdopodobne jest jednak, że $T(I) \neq I$. Chcemy w takiej sytuacji móc w jakiś sposób odtworzyć wysłaną oryginalną informację I. Podczas wykładu zajmiemy się głównie teorią kodów korekcyjnych, która opiera się na algebrze ciał skończonych.

Orientacyjny zakres wykładu:

(1) Przypomnienie podstawowych wiadomości z algebry liniowej i algebry abstrakcyjnej, ciała proste i struktura ich rozszerzeń, wielomiany nad ciałami skończonymi, wielomiany pierwotne, wielomiany minimalne.
(2) Wprowadzenie do teorii kodowania: kody blokowe, kody liniowe, kody grupowe, kody macierzowe, kody doskonałe
(3) Kody Hamminga
(4) Sekwencje pseudolosowe
(5) Kody cykliczne, kody BCH, kody Hadamarda

Literatura:

1. W. Mochnacki, Kody korekcyjne i kryptografia, Wrocław 2000.
2. G. Birkhoff, T. C. Bartee, Współczesna algebra stosowana, Warszawa 1983.
3. J. Adamek, Foundations of coding, 1991.
4. E. R. Berlekamp, Algebraic coding theory, 2nd edition, 2015.
5. E. R. Berlekamp, A survey of algebraic coding theory, 1970.