

Vladimir Božović

Faktorizacija konačnih grupa

Apstrakt

Pod faktorizacijom konačne grupe G podrazumijevamo kolekciju njenih podskupova $[B_1, B_2, \dots, B_k]$ tako da se svaki element $g \in G$ može predstaviti na jedinstven način $g = s_1 s_2 \cdots s_k$, $s_i \in B_i$, $1 \leq i \leq k$. Grupovne faktorizacije, kao veoma privlačna tema na teorijskom nivou, se pojavljuje u aplikacijama, i to u kriptografiji, teoriji grafova i kodiranja. Konstrukcija i opis faktorizacija za datu grupu su u principu teški problemi, koji su samo u specijalnim slučajevima potpuno riješeni. To se posebno odnosi na neke komutativne grupe. Predstavićemo elemente teorije grupovnih faktorizacija i dati pregled osnovnih rezultata. Posebno, neki novi rezultati u faktorizaciji nekomutativnih grupa će biti prezentovani.