

**KRATKA VSEBINA**

Delo obravnava osnovne lastnosti končnih obsegov ter polinomov nad njimi.

Pri konstruiranju končnih obsegov in pri raziskavi njihove zgradbe so nerazcepni polinomi nepogrešljivi, zato obstajajo algoritmi za iskanje teh polinomov.

Vprašanje faktorizacije poljubnega polinoma nad nekim končnim obsegom na nerazcepne faktorje je rešeno z dvema algoritmoma. Prvi, t.j. *Berlekampov* algoritem, se uporablja v obsegih z majhnim številom elementov, drugi, t.j. *Zassenhausov* algoritem, pa se uporablja v obsegih, katerih število elementov je bistveno manjše od stopnje polinoma, ki ga faktoriziramo.

Iskanje ničel poljubnega polinoma je rešeno s pomočjo tako imenovanih *afinih* in *lineariziranih* polinomov.

## LITERATURA

1. Rudolf Lidl, Harald Niederreiter

**Introduction to finite fields and their applications**  
Cambridge University Press (1986)

2. Ivan Vidav

**Algebra**

Inštitut za matematiko, fiziko in mehaniko  
Univerze v Ljubljani (1972)