

Lõplikud korpused I  
1. praktikumi ülesanded  
Algebralised struktuurid.

1. Koostada ringi  $\mathbb{Z}_{26}$  pööratavate elementide rühma  $U(\mathbb{Z}_{26})$  Cayley tabel.
2. Leida rühma  $U(\mathbb{Z}_{26})$  kõik alamrühmad, nende järgud ja indeksid.
3. Leida järgmiste polünoomide suurim ühistegur ringis  $\mathbb{Z}_2[x]$ :

$$f(x) = x^5 + 2x^4 + 3x^3 + 3x^2 + 2x + 1$$

ja

$$g(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 4x^2 + 3x + 2 + 1.$$

4. Olgu  $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ . Tõestada, et  $K$  on korpus ja leida elemendi  $[x + 1] = x + (x^3 + x + 1)$  minimaalne polünoom üle  $\mathbb{F}_2$ .
5. Tõestada, et ringis  $R$  positiivse karakteristikaga  $m$  leidub iga  $0 < n \mid m$  jaoks  $n$ . järku element.
6. Olgu  $K$  kommutatiivne korpus, mille multiplikatiivne rühm  $K^*$  on tsükline. Tõestada, et  $K$  on lõplik.
7. Olgu  $K$  kommutatiivne korpus ja  $f(x), g(x), h(x) \in F[x]$ . Tõestada Eukleideese lemma polünoomide jaoks: kui  $f(x) \mid g(x) \cdot h(x)$  ja  $\gcd(f(x), g(x)) = 1$ , siis  $f(x) \mid h(x)$ .
8. Olgu  $K$  kommutatiivne korpus algarvulise karakteristikaga  $p$  ja olgu

$$f(x) = x^p + x - a, \quad 0 \neq a \in K,$$

selline polünoom, millel ei ole juuri korpuses  $K$ . Tõestada, et  $f$  on taandumatu.

- 9\*. Leida reaalarvu  $\sqrt[3]{3} + \sqrt[2]{5} + 1$  minimaalne polünoom üle  $\mathbb{Q}$ .