Domácí úloha z 20. listopadu 2015 (odevzdává se 27. listopadu 2015)

a) Nechť $K = \mathbb{Z}_p(c)$ je libovolné konečné těleso mající p^m prvků, kde p je prvočíslo. Označme f minimální polynom prvku c nad $\mathbb{Z}_p$, tedy $\operatorname{st} f = m$. Nechť L je také konečné těleso mající p^m prvků. Na přednášce jsme dokázali, že pak $K \cong L$, neboť obě tělesa mají stejný počet prvků. Protože polynom f má kořen c v tělese K, musí mít také nějaký kořen d v tělese L. Víme, že $1, c, c^2, \ldots, c^{m-1}$ je bází K jakožto vektorového prostoru nad $\mathbb{Z}_p$, proto každý prvek tělesa K lze napsat jediným způsobem ve tvaru $a_0 + a_1 c + a_2 c^2 + \cdots + a_{m-1} c^{m-1}$, kde $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_p$, tedy ve tvaru $r(c)$, kde $r \in \mathbb{Z}_p[x]$, $\operatorname{st} r < m$. Dokažte, že zobrazení $\varphi : K \to L$ určené předpisem $\varphi(r(c)) = r(d)$ pro každý polynom $r \in \mathbb{Z}_p[x]$, $\operatorname{st} r < m$, je izomorfismus těles.

b) Nechť p je libovolné prvočíslo, $a \in \mathbb{Z}_p$, $a \neq 0$. Dokažte, že polynom $x^p - x + a \in \mathbb{Z}_p[x]$ je ireducibilní nad $\mathbb{Z}_p$.

[Návody:

a) Patrně jediné obtížné místo důkazu se týká toho, zda zobrazení φ zachovává součin. Lze postupovat tak, že nejprve dokážete, že zobrazení φ splňuje $\varphi(r(c)) = r(d)$ pro každý polynom $r \in \mathbb{Z}_p[x]$, tedy i pro polynomy splňující $\operatorname{st} r \geq m$.

b) Zvolme libovolný normovaný ireducibilní polynom f, který je dělitelem daného polynomu $x^p - x + a$. Sestrojme těleso $L = \mathbb{Z}_p[x]/(f)$ a označme $\alpha = x + (f)$. Pak α je kořenem polynomu f, a tedy i polynomu $x^p - x + a$. Opakovaně užijte úvahu, že obraz kořene polynomu f ve Frobeniově automorfismu je opět kořen polynomu f, k tomu, abyste ukázali, že polynom f má alespoň p různých kořenů, a tedy $\operatorname{st} f \geq p$. Odtud odvoďte $f = x^p - x + a$.]