Cvičení 17. 5. 2012

Každé konečné těleso má p^k prvků, kde p je prvočíslo. Navíc libovolná dvě konečná tělesa o stejném počtu prvků jsou isomorfní. Proto se někdy konečné těleso o p^k prvcích značí $GF(p^k)$.

Příklad 1. Je $\mathbb{Z}_2[x]/x^4 + x^2 + 1$ těleso?

Příklad 2. Nechť K je konečné těleso charakteristiky p. Dokažte, že pak je Frobeniův automorfismus $x \mapsto x^p$ skutečně automorfismem (tj. vnitřním isomorfismem) K.

Příklad 3. Popište grupu automorfismů tělesa:

1. $GF(13)$
2. $GF(9)$
3. $GF(8)$

Příklad 4. Buďte $K \leq L$ konečná tělesa. Dokažte, že řády (tj. počty prvků) K, L jsou mocninami stejného prvočísla p.

Pokud K je konečné těleso, tak grupa $K^\star = (K \setminus \{0\}, \cdot)$ je cyklická (to na přednášce asi nebylo). Prvky, které generují grupu $K^\star$, nazýváme primitivními prvky K.

Příklad 5. Najděte primitivní prvky tělesa $GF(16) \simeq \mathbb{Z}_2[x]/x^4 + x + 1$.