Algebra I/Kevät 2009
Täydennystä luentomateriaaliin (JL)

Sivulle 110, Esim., e) Pätee: $f \in \mathbb{R}[x]$ on jaoton $\iff \deg(f) = 1$ tai $\deg(f) = 2$ ja f:llä ei ole nollakohtia $\mathbb{R}$:ssä.

($\Longleftarrow$: Selvä.
$\Longrightarrow$: Olkoon $f \in \mathbb{R}[x]$ jaoton. Jos $\deg(f)$ on pariton, niin kurssin Analyysi I perusteella f:llä on nollakohta, joten $\deg(f) = 1$. Olkoon sitten $\deg(f)$ parillinen, jolloin $n = \frac{1}{2}\deg(f) \in \mathbb{N}_+$, eikä f:llä ole nollakohtia $\mathbb{R}$:ssä. Algebran peruslauseen nojalla f:llä tulkittuna $\mathbb{C}$-kertoimiseksi polynomiksi on nollakohdat $c_k = a_k + ib_k \in \mathbb{C}$, $1 \leq k \leq n$ ($a_k, b_k \in \mathbb{R}$ ja $b_k > 0$, kun $1 \leq k \leq n$), moninkertaiset nollakohdat luettuina kertalukunsa mukaisesti, niin että myös $\overline{c}_k = a_k - ib_k$ on f:n nollakohta, kun $1 \leq k \leq n$, ja niin että eräällä $a \in \mathbb{R} \setminus \{0\}$ on

$$f = a\prod_{k=1}^{n}((x - c_k)(x - \overline{c}_k)) = a\prod_{k=1}^{n}((x - a_k)^2 + b_k^2).$$

Koska tässä $(x - a_k)^2 + b_k^2 \in \mathbb{R}[x]$, kun $1 \leq k \leq n$, niin on oltava $n = 1$.)

Sivun 113 loppuun. Jälkimmäinen väite voidaan todistaa helposti ja jopa vahvemmassa muodossa:

Väite. Olkoon L äärellinen kunta ja $q = \mathrm{char}(L)$ (siis q alkuluku). Tällöin additiivinen ryhmä $(L, +)$ on isomorfinen tuloryhmän $((\mathbb{Z}_q)^n, +)$ kanssa eräällä $n \in \mathbb{N}_+$, jolloin $|L| = q^n$.

Tod. Kunnalla L on alikuntanaan $K = \mathbb{Z}_q$. Tulos seuraisi heti lineaarialgebrasta: Kunta L on K-kertoiminen vektoriavaruus, joka on äärellinen ja siis äärellisulotteinen; jos nyt $n = \dim_K(L) \in \mathbb{N}_+$, niin K-vektoriavaruudet L ja K^n ovat tällöin isomorfiset. Mutta todistetaan tulos suoraan ryhmäteoreettisesti.

Huomataan, että joukko $V = \{a_1, \ldots, a_k\} \subset L$, jossa $k = |V|$, virittää additiivisen ryhmän L (eli $L = \langle V\rangle = \{\sum_{i=1}^{k} m_i a_i \mid m_i \in \mathbb{Z}, \text{ kun } 1 \leq i \leq k\}$) jos ja vain jos

$$L = \{\textstyle\sum_{i=1}^{k} m_i a_i \mid m_i \in K, \text{ kun } 1 \leq i \leq k\}.$$

Tietysti L on itsensä virittämä. Siis $\mathbb{N}_+$:n osajoukko

$$A = \{|V| \mid V \subset L \text{ virittää } L\text{:n}\}$$

on epätyhjä. Olkoon $n = \min A$. Valitaan L:n virittävä joukko $V = \{a_1, \ldots, a_n\}$, jolla $|V| = n$. Tällöin kuvaus $f\colon K^n \to L$, $(m_i)_{1\leq i\leq n} \mapsto \sum_{i=1}^{n} m_i a_i$, on selvästi surjektiivinen ryhmähomomorfismi. Osoitetaan, että $\mathrm{Ker}(f) = \{0\}$; tällöin f on myös injektio ja siis ryhmäisomorfismi. Olkoon siis $(m_i)_{1\leq i\leq n} \in K^n$ ja $\sum_{i=1}^{n} m_i a_i = 0$. Jos $m_j \neq 0$ jollain $1 \leq j \leq n$, niin $a_j = \sum_{i=1, i\neq j}^{n}(-m_j^{-1}m_i)a_i$, joten jo joukko $V' = V \setminus \{a_j\}$ virittää L:n, kuten olisi helposti osoitettavissa. Mutta $|V'| = n - 1 < n = \min A$, ristiriita. Siis $m_i = 0$, kun $1 \leq i \leq n$. ■