Esimerkkejä kuntalaajennuksista polynomirenkaissa

Esimerkki. Tutkitaan reaalilukujen kuntaa $(\mathbb{R},+,\cdot)$. Olkoon $p(x)=x^2+1$. Kuten sivulla Esimerkkejä polynomirenkaista todettiin on $p(x)$ jaoton yli kunnan $\mathbb{R}$. Merkitään $I=<x^2+1>$. Sivun Polynomirenkaan jäännösluokkarenkaasta perusteella saadaan siis kunta

$$\mathbb{R}[x]/I=\{a+bx+I \mid a,b\in\mathbb{R}\},$$

jonka operaatiot ovat, kun $a+bx+I, a'+b'x+I\in\mathbb{R}[x]/I$,

$$\begin{aligned}(a+bx+I)+(a'+b'x+I) &= (a+a')+(b+b')x+I,\\ (a+bx+I)\cdot(a'+b'x+I) &= (aa'-bb')+(ab'+a'b)x+I.\end{aligned}$$

Tuloa laskettaessa vähennettiin jäännösluokan edustaja $bb'(x^2+1)$. Sivun Kuntalaajennus polynomirenkaassa lauseen mukaan polynomilla x^2+1 on nollakohta kuntalaajennuksessa $\mathbb{R}[x]/I$.

Saatu kunta on kompleksilukujen kunta $(\mathbb{C},+,\cdot)$. Yhteyden näkee helpoiten, kun merkitään $a+bx+I=a+bi$.

Sivun Kuntalaajennus polynomirenkaassa lauseen todistuksen perusteella polynomin y^2+1 nollakohta kunnassa $(\mathbb{R}[x]/I,+,\cdot)$ on $x+I$, siis $0+1\cdot i=i$, kuten pitääkin.

Esimerkki. Polynomi $p(x)=x^2+x+\overline{1}$ on jaoton yli kunnan $(\mathbb{Z}_2,+,\cdot)$, sillä $p(\overline{0})=\overline{1}$ ja $p(\overline{1})=\overline{1}$. Täten saadaan kunta, kun merkitään $I=<p(x)>$,

$$\begin{aligned}\mathbb{Z}_2[x]/I &= \{a+bx+I \mid a,b\in\mathbb{Z}_2\}\\ &= \{I,\overline{1}+I,x+I,\overline{1}+x+I\}.\end{aligned}$$

Kyseessä on siis neljän alkion kunta. (Tämä on *Galois'n kunta* $GF(2^2)$.) Jos kunnan alkioita merkitään seuraavasti: $0=I$ (nolla-alkio), $1=\overline{1}+I$ (ykkösalkio), $\alpha=x+I$ ja $\beta=\overline{1}+x+I$, saadaan additiiviselle ja multiplikatiiviselle ryhmälle seuraavat taulut.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	1	α	β
1	1	α	β
α	α	β	1
β	β	1	α

Taulussa esimerkiksi tulo $\alpha\beta$ laskettiin seuraavasti:

$$\alpha\beta=(x+I)(\overline{1}+x+I)=x(\overline{1}+x)+I=x+x^2+I=-\overline{1}+I=\overline{1}+I=1.$$

Tauluja apuna käyttäen todetaan, että α on polynomin $x^2+x+\overline{1}$ nollakohta. Nimittäin

$$\alpha^2+\alpha+\overline{1}=\beta+\alpha+\overline{1}=\overline{1}+\overline{1}=\overline{0}.$$

Linkit:
Esimerkkejä polynomirenkaista
Polynomirenkaan jäännösluokkarenkaasta
Kuntalaajennus polynomirenkaassa