Alkukunta

Lause. Kaikilla kunnilla $(K,+,\cdot)$ on alikuntana $(P,+,\cdot)$, missä

$$P \simeq \begin{cases} \mathbb{Z}_p, & \text{jos } \operatorname{char}(K) = p, \\ \mathbb{Q}, & \text{jos } \operatorname{char}(K) = 0. \end{cases}$$

Todistus. Todistetaan, että kunnaksi $(P,+,\cdot)$ voidaan ottaa sivun Huomioita alikunnasta lauseen mukainen kunta $(K_D,+,\cdot)$, missä $(D,+,\cdot)$ on saman sivun lemman mukainen kokonaisalue.

Jos $\operatorname{char}(K) = p$, niin $D \simeq \mathbb{Z}_p$. Siis D on äärellinen ja sivun Kunta lauseen mukaan $(D,+,\cdot)$ on kunta, joten se sisältää alkioidensa osamäärät ja täten $D = K_D$. Silloin kunnalla $(K,+,\cdot)$ on alikunta $(K_D,+,\cdot)$, missä $K_D \simeq \mathbb{Z}_p$.

Oletetaan nyt, että $\operatorname{char}(K) = 0$. Silloin

$$D = \{n1_K \mid n \in \mathbb{Z}\} \simeq \mathbb{Z} \quad \text{ja} \quad K_D = \left\{ \frac{n1_K}{m1_K} \mid n,m \in \mathbb{Z},\ m \neq 0 \right\},$$

siis $K_D \simeq \mathbb{Q}$. □

Määritelmä. Kuntaa sanotaan *alkukunnaksi (prime field),* jos sillä ei ole aitoja alikuntia.

Lause. (i) Kaikki alkukunnat (isomorfiaa vaille) ovat kunnat $(\mathbb{Z}_p,+,\cdot)$, missä p on alkuluku ja $(\mathbb{Q},+,\cdot)$.

(ii) Jokaisella kunnalla $(K,+,\cdot)$ on alikuntana yksikäsitteinen alkukunta $(P,+,\cdot)$, missä P on kuten edellisessä lauseessa.

Todistus. (i) Todistetaan ensin, että $(\mathbb{Q},+,\cdot)$ on alkukunta. Oletetaan, että kunta $(F,+,\cdot)$ on kunnan $(\mathbb{Q},+,\cdot)$ alikunta. Koska $1 = 1_{\mathbb{Q}} \in F$, niin $n \cdot 1 \in F$ kaikilla $n \in \mathbb{Z}$. Siis $\mathbb{Z} \subseteq F$. Koska F on kunta, niin $\frac{a}{b} \in F$ kaikilla $a,b \in \mathbb{Z}$, $b \neq 0$. Siis $\mathbb{Q} \subseteq F$. Täten $F = \mathbb{Q}$. Siis kunnalla $(\mathbb{Q},+,\cdot)$ ei ole aitoja alikuntia.

Todistetaan toiseksi, että kunta $(\mathbb{Z}_p,+,\cdot)$ on alkukunta. Jos $(F,+,\cdot)$ on kunnan $(\mathbb{Z}_p,+,\cdot)$ alikunta, niin $(F,+)$ on ryhmän $(\mathbb{Z}_p,+)$ aliryhmä. Lagrangen lauseen mukaan aliryhmän kertaluku jakaa ryhmän kertaluvun, joten $\sharp F \mid \sharp\mathbb{Z}_p$. Koska $\sharp\mathbb{Z}_p = p$ ja $\sharp F \geq 2$ (koska $(F,+,\cdot)$ on kunta), niin $\sharp F = p$ ja siis $F = \mathbb{Z}_p$.

Se, ettei ole olemassa muita alkukuntia seuraa kohdasta (ii).

(ii) Olkoon $(K,+,\cdot)$ kunta. Silloin edellisen lauseen mukaan kunnalla K on alikunta $(P,+,\cdot)$, jossa $P \simeq \mathbb{Z}_p$ tai $P \simeq \mathbb{Q}$ kunnan K karakteristikan mukaan. Edellä todistetun mukaan nämä ovat alkukuntia.

Osoitetaan vielä yksikäsitteisyys (tästä seuraa myös (i)-kohdan loppuosa). Olkoot alkukunnat $(P_1,+,\cdot)$ ja $(P_2,+,\cdot)$ kunnan $(K,+,\cdot)$ alikuntia. Sivun Alikunta lauseen mukaan $(P_1 \cap P_2,+,\cdot)$ on myös kunta. Se on siis kuntien P_1 ja P_2 alikunta. Koska nämä molemmat ovat alkukuntia, on $P_1 = P_1 \cap P_2 = P_2$. □

Edellinen lause osoittaa, että kunnan karakteristika on ratkaisevassa osassa määritettäessä kunnan tyyppiä. Lauseesta seuraa myös, että kunnalla ja sen alikunnalla on sama alkukunta.

Linkit:
Huomioita alikunnasta

Kunta

Lagrangen lause

Alikunta