H. Junnila: Johdatus Diskreettiin Matematiikkaan, s. 29 - 32

Määritelmä Joukko X on *äärellinen*, mikäli jollain $n \in \mathbb{N}$ on olemassa bijektio $[n] \to X$. Jos X ei ole äärellinen, niin sanomme, että X on *ääretön*.

Koska bijektion käänteiskuvaus on bijektio, joukko X on äärellinen jos ja vain jos jollain $n \in \mathbb{N}$ on olemassa bijektio $X \to [n]$.

Koska identtinen kuvaus on bijektio joukolta itselleen, näemme että joukot $[n]$ ovat äärellisiä. Erityisesti, tyhjä joukko $[0]$ on äärellinen. Myös jokainen yksiö $\{a\}$ on äärellinen, sillä ehto $1 \mapsto a$ määrittelee bijektion $[1] \to \{a\}$.

Todistamme nyt että bijektioita $[n] \to A$ voi olla olemassa vain yhdellä $n \in \mathbb{N}$. Tarvitsemme tähän aputulosta, jonka todistus perustuu seuraavaan luonnollisten lukujen ominaisuuteen (kyseessä on *induktioperiaatteen* yleinen muoto):

– *Jokaisessa* $\mathbb{N}$*:n epätyhjässä osajoukossa on pienin luku.*

Lemma *Olkoot* $n, k \in \mathbb{N}$ *ja* $k < n$. *Tällöin ei ole olemassa injektiota* $[n] \to [k]$.

Todistus. Meidän on osoitettava, että joukko

$$A = \{n \in \mathbb{N} : \exists \text{ injektio } [n] \to [k] \text{ jollain } k < n\}$$

on tyhjä. Teemme vastaväitteen: on voimassa $A \neq \emptyset$.

Yllä mainitun induktioperiaatteen nojalla on olemassa sellainen luku $m \in A$, että $m \leq n$ jokaisella $n \in A$. Koska $m \in A$, on olemassa $k < m$ ja injektio $\phi : [m] \to [k]$. Panemme merkille, että on voimassa $k > 0$ (koska $m > k \geq 0$ ja on olemassa kuvaus $[m] \to [k]$). Määrittelemme nyt kuvauksen $\psi : [m-1] \to [k]$ seuraavasti. Jos on voimassa $k \notin \phi([m-1])$, niin valitsemme ψ:ksi rajoittumakuvauksen $\phi|[m-1]$. Mikäli on olemassa sellainen $i \in [m-1]$, että $\phi(i) = k$, niin määrittelemme kuvauksen ψ asettamalla $\psi(i) = \phi(m)$ ja $\psi(j) = \phi(j)$ jokaisella $j \neq i$. Näemme helposti, että molemmissa tapauksissa kuvaus ψ on injektio $[m-1] \to [k-1]$. Tästä seuraa, että on voimassa $m - 1 \in A$, mutta tämä on ristiriidassa luvun m minimaalisuusominaisuuden kanssa. Täten vastaväite on väärä ja on voimassa $A = \emptyset$. □

Lause *Kun* A *on äärellinen joukko, niin vain yhdellä* $n \in \mathbb{N}$ *on olemassa bijektio* $[n] \to A$.

Todistus. Teemme vastaväitteen: on olemassa sellaiset luonnolliset luvut n ja k, että $k < n$ ja on olemassa bijektiot $f : [n] \to A$ ja $g : [k] \to A$. Kuvaus g^{-1} on bijektio $A \to [k]$ ja voimme määritellä kuvauksen $h : [n] \to [k]$ kaavalla $h(i) = g^{-1}(f(i))$. Bijektioiden yhdistämislauseen nojalla h on bijektio $[n] \to [k]$. Tämä on kuitenkin ristiriidassa edellisen lemman kanssa. $\square$

Olkoon A äärellinen joukko. Käytämme edellisen lauseen yksikäsitteiseksi todistamasta luvusta n merkintää $|A|$ ("A:n *alkioiden lukumäärä*" tai "A:n *koko*"). Kun $|A| = n > 0$, niin voimme esittää joukon A muodossa $A = \{a_1, ..., a_n\}$: asetamme $a_i = \varphi(i)$ jokaisella $i \in [n]$, kun φ on bijektio $[n] \to A$.

Kun A on äärellinen joukko ja $|A| = n$, niin sanomme, että A on *n-joukko* tai *n-alkioinen joukko.* Käytämme seuraavassa sekä merkintää "$|B| = n$" että sanontoja "B on n–joukko" ja "B on n-alkioinen joukko" lyhennyksenä ilmaisulle "B on äärellinen joukko ja n on luonnollinen luku, jolle on voimassa $|B| = n$".

Tyhjä joukko on ainoa 0–joukko. Yksiö on sama asia kuin 1-joukko. Jokaisella $n \in \mathbb{N}$ on voimassa $|[n]| = n$, koska joukon identtinen kuvaus on aina bijektio joukolta itselleen.

Osoitamme nyt, että joukkojen välinen bijektio "säilyttää" joukkojen äärellisyyden ja niiden koon.

Lause *Olkoot A ja B sellaisia joukkoja, että on olemassa bijektio $A \to B$. Jos joko A tai B on äärellinen, niin tällöin sekä A että B ovat äärellisiä ja on voimassa $|A| = |B|$.*

Todistus. Olkoon f bijektio $A \to B$.

Oletamme, että joukko A on äärellinen. Tällöin on olemassa $n \in \mathbb{N}$ ja bijektio $\varphi : [n] \to A$. Näemme helposti, että kaavan $h(k) = f(\varphi(k))$ määrittämä kuvaus h on bijektio $[n] \to B$. Täten B on äärellinen ja on voimassa $|B| = n = |A|$.

Koska kuvaus f^{-1} on bijektio $B \to A$, edellä esitetystä seuraa, että jos B on äärellinen, niin tällöin A on äärellinen ja $|A| = |B|$. $\square$

Seuraavaksi osoitamme, että äärellisten joukkojen osajoukot ovat äärellisiä. Todistamme tämän ensin joukkojen $[n]$, $n \in \mathbb{N}$, osajoukoille.

Lemma *Olkoon n luonnollinen luku ja olkoon A joukon $[n]$ aito osajoukko. Tällöin jollain $k < n$ on olemassa bijektio $[k] \to A$.*

Todistus. Merkitsemme E:llä niiden lukujen $n \in \mathbb{N}$ muodostamaa joukkoa, joilla on olemassa sellainen $A \subsetneq [n]$, että millään $k < n$ ei ole olemassa bijektiota $[k] \to A$. Haluamme osoittaa, että on voimassa $E = \emptyset$.

Käytämme jälleen epäsuoraa todistusta ja induktioperiaatetta. Oletamme, että $E \neq \emptyset$. Induktioperiaatteen nojalla joukossa E on pienin luku m. Koska $m \in E$, on olemassa sellainen joukko $A \subsetneqq [m]$, että millään $k < m$ ei ole olemassa bijektiota $[k] \to A$. Koska tyhjällä joukolla $[0]$ ei ole aitoja osajoukkoja, on voimassa $m > 0$ ja koska m on joukon E pienin luku, on voimassa $m - 1 \notin E$.

Merkitsemme $B = A \cap [m-1]$ eli $B = A \setminus \{m\}$. Jos olisi voimassa $B = [m-1]$, niin tällöin olisi voimassa $A = [m-1]$ ja identtinen kuvaus olisi bijektio $[m-1] \to A$, ristiriidassa joukon A ominaisuuden kanssa. Näin ollen on voimassa $B \subsetneqq [m-1]$. Koska $m - 1 \notin E$, on olemassa $\ell < m-1$ ja bijektio $\varphi : [\ell] \to B$. Edellisestä seuraa, että on voimassa $B \neq A$ eli $m \in A$. Jatkamme nyt kuvauksen φ kuvaukseksi $\bar{\varphi} : [\ell+1] \to A$ asettamalla $\bar{\varphi}(\ell+1) = m$. Näemme helposti, että $\bar{\varphi}$ on bijektio $[\ell+1] \to A$, mutta tämä on ristiriidassa joukon A ominaisuuden kanssa, koska $\ell + 1 < m$.

Vastaväite johti ristiriitaan, joten se on väärä ja on voimassa $E = \emptyset$. $\square$

Lause *Olkoon A äärellinen joukko ja olkoon B A:n aito osajoukko. Tällöin B on äärellinen ja $|B| < |A|$.*

Todistus. Koska A on äärellinen, on olemassa $n = |A|$ ja bijektio $f : A \to [n]$. Merkitään $C = f(B) = \{f(b) : b \in B\}$. Koska f on bijektio ja $B \subsetneqq A$, on voimassa $C \subsetneqq [n]$. Edellisen lemman nojalla on olemassa $k < n$ ja bijektio $g : C \to [k]$. Kuvaus $\varphi : B \to [k]$, missä $\varphi(b) = g(f(b))$ jokaisella $b \in B$, on bijektio. Täten B on äärellinen ja $|B| = k < n = |A|$. $\square$

Todistamme seuraavaksi tärkeän "summalauseen".

Lause *Olkoot A ja B keskenään erillisiä äärellisiä joukkoja. Tällöin joukko $A \cup B$ on äärellinen ja*

$$\boxed{|A \cup B| = |A| + |B|\,.}$$

Todistus. Olkoon $|A| = n$ ja $|B| = k$ ja olkoot $\phi : [n] \to A$ ja $\psi : [k] \to B$ bijektioita. Määrittelemme nyt kuvauksen $\theta : [n+k] \to A \cup B$ seuraavasti: $\theta(i) = \phi(i)$ jos $i \leq n$ ja $\theta(i) = \psi(i-n)$ jos $i > n$. Näemme helposti, että θ on bijektio $[n+k] \to A \cup B$. $\square$

Seuraus *Olkoon A äärellinen joukko ja $B \subset A$. Tällöin*

$$\boxed{|A \setminus B| = |A| - |B|\,.}$$

Todistus. Äärellisen joukon A osajoukot B ja $A \setminus B$ ovat äärellisiä; lisäksi ne ovat erillisiä, joten edellisen lauseen nojalla on voimassa $|B| + |A \setminus B| = |B \cup (A \setminus B)| = |A|$; tästä seuraa yhtälö $|A \setminus B| = |A| - |B|$. □

Seuraus *Olkoot A ja B äärellisiä joukkoja. Tällöin joukko $A \cup B$ on äärellinen ja*

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B| \,.}$$

Todistus. On voimassa $A \cup B = A \cup (B \setminus A)$ ja tästä seuraa edellisten tulosten nojalla, koska joukot A ja $B \setminus A$ ovat äärellisiä ja $A \cap (B \setminus A) = \emptyset$, että joukko $A \cup B$ on äärellinen ja $|A \cup B| = |A| + |B \setminus A|$. Koska $B \setminus A = B \setminus (A \cap B)$ ja $A \cap B \subset B$, niin edellisen seurauslauseen nojalla on voimassa $|B \setminus A| = |B| - |A \cap B|$. Näinollen on voimassa

$$|A \cup B| = |A| + |B \setminus A| = |A| + |B| - |A \cap B| \,. \qquad \square$$

Edellisiä kahden joukon yhdisteen kokoa koskevia tuloksia on helppo yleistää kolmelle, neljälle, viidelle,... joukolle. Jos esimerkiksi A, B ja C ovat keskenään erillisiä äärellisiä joukkoja, niin tällöin $A \cup B$ on aikaisemman nojalla $|A| + |B|$-joukko; soveltamalla tulosta toistamiseen, näemme että joukko $(A \cup B) \cup C$, eli joukko $A \cup B \cup C$ on $|A| + |B| + |C|$-joukko. Käyttämällä hyväksi tätä kolmea joukkoa koskevaa tulosta näemme vastaavalla tavalla, että jos jos joukot A, B, C ja D ovat keskenään erillisiä äärellisiä joukkoja, niin $A \cup B \cup C \cup D$ on $|A| + |B| + |C| + |D|$-joukko.

Koska voimme jatkaa edellistä päättelyä loputtomiin, tuntuu itsestään selvältä, että seuraava tulos on voimassa: jos $n \in \mathbb{N}$ ja jos joukot $A_1, A_2, ..., A_n$ ovat keskenään erillisiä äärellisiä joukkoja, niin joukko $A_1 \cup A_2 \cup \cdots \cup A_n$ on äärellinen ja $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$. Jos kuitenkin haluamme todistaa tuon tuloksen täsmällisesti, niin emme voi vedota siihen, että "voimme jatkaa edellistä päättelyä loputtomiin". Täsmälliseen todistukseen tarvitsemme jo aikaisemmin pari kertaa kohtaamaamme "induktioperiaatetta".

Ilmaisemme erillisten joukkojen yhdisteeseen liittyvän tuloksen yleisessä muodossa käyttämällä yleistettyjä yhdistys- ja summamerkintöjä. Teemme seuraavat sopimukset koskien "tyhjää summaa" ja "tyhjää yhdistettä": $\sum_{i \in \emptyset} r_i = 0$ ja $\bigcup_{i \in \emptyset} A_i = \emptyset$.