802328A LUKUTEORIAN PERUSTEET
Merkintöjä ja Algebrallisia rakenteita

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

SYKSY 2018

$$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$$

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}.$

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}.$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{\text{kokonaisluvut}\}.$

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}.$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{\text{kokonaisluvut}\}.$

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N}\backslash\{0\} = \{\text{positiiviset kokonaisluvut}\}.$

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}.$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{\text{kokonaisluvut}\}.$

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N}\backslash\{0\} = \{\text{positiiviset kokonaisluvut}\}.$

$\mathbb{Z}^- = \{-1, -2, -3, \ldots\} = \mathbb{Z}\backslash\mathbb{N} = \{\text{negatiiviset kokonaisluvut}\}.$

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}.$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}.$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{\text{kokonaisluvut}\}.$

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N}\backslash\{0\} = \{\text{positiiviset kokonaisluvut}\}.$

$\mathbb{Z}^- = \{-1, -2, -3, \ldots\} = \mathbb{Z}\backslash\mathbb{N} = \{\text{negatiiviset kokonaisluvut}\}.$

$\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\} = \{\text{rationaaliluvut}\}.$

$$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$$

$$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$$

$$\mathbb{C} = \mathbb{R}(i) = \{a + ib |\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$$

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$

$\mathbb{C} = \mathbb{R}(i) = \{a + ib |\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{ Irrationaaliluvut }\}.$

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$

$\mathbb{C} = \mathbb{R}(i) = \{a + ib |\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{ Irrationaaliluvut }\}.$

$\mathbb{Z}_{\geq m} = \{k \in \mathbb{Z} |\ k \geq m\}.$

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$

$\mathbb{C} = \mathbb{R}(i) = \{a + ib |\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{ Irrationaaliluvut }\}.$

$\mathbb{Z}_{\geq m} = \{k \in \mathbb{Z} |\ k \geq m\}.$

$\mathbb{R}_{\leq 0} = \{r \in \mathbb{R} |\ r \leq 0\}, \ldots$

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}.$

$\mathbb{C} = \mathbb{R}(i) = \{a + ib |\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{ Irrationaaliluvut }\}.$

$\mathbb{Z}_{\geq m} = \{k \in \mathbb{Z} |\ k \geq m\}.$

$\mathbb{R}_{\leq 0} = \{r \in \mathbb{R} |\ r \leq 0\}, \ldots$

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\},$

$\exists!$ $\Leftrightarrow \exists$ täsmälleen yksi.

$\exists!$ $\Leftrightarrow \exists$ täsmälleen yksi.

$\#A = |A| =$ Joukon A alkioiden lukumäärä.

$\exists!$ $\Leftrightarrow \exists$ täsmälleen yksi.

$\#A = |A| =$ Joukon A alkioiden lukumäärä.

Olkoot a, b lukuja sekä A, J lukujoukkoja:

$$aJ + b = \{aj + b \mid j \in J\}$$

$$a^J = \{a^j | j \in J\}$$

$$A^J = \{a^j | a \in A, j \in J\}$$

$\exists!$ $\Leftrightarrow \exists$ täsmälleen yksi.

$\#A = |A| =$ Joukon A alkioiden lukumäärä.

Olkoot a, b lukuja sekä A, J lukujoukkoja:

$$aJ + b = \{aj + b \mid j \in J\}$$
$$a^J = \{a^j | j \in J\}$$
$$A^J = \{a^j | a \in A, j \in J\}$$

Esimerkki 1

$J = \mathbb{Z},\ b \in \mathbb{Z},\ n \in \mathbb{Z}^+$, tällöin merkitään

$$\overline{b} = n\mathbb{Z} + b,$$

joka on jakojäännösluokka (mod n) ja

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{b} \mid b \in \{0, 1, \ldots, n-1\}\},$$

Olkoon $A = \{a_1, ..., a_m\}$, tällöin

$$\sum_{a \in A} f(a) = f(a_1) + ... + f(a_m),$$

$$\prod_{a \in A} f(a) = f(a_1) \cdots f(a_m).$$

Tyhjä summa ja tulo: Jos $A = \emptyset$, niin

$$\sum_{a \in A} f(a) = 0, \quad \prod_{a \in A} f(a) = 1$$

Olkoon $A = \{a_1, ..., a_m\}$, tällöin

$$\sum_{a \in A} f(a) = f(a_1) + ... + f(a_m),$$

$$\prod_{a \in A} f(a) = f(a_1) \cdots f(a_m).$$

Tyhjä summa ja tulo: Jos $A = \emptyset$, niin

$$\sum_{a \in A} f(a) = 0, \quad \prod_{a \in A} f(a) = 1$$

Edelleen "Summaus n. tekijöiden yli"

$$\sum_{d|n} f(d) = f(d_1) + ... + f(d_k),$$

missä $d_i \in \mathbb{Z}^+$ ovat n:n erilliset tekijät. "Summaus n. alkutekijöiden yli"

$$\sum_{p|n} f(p) = \sum_{p|n, p \in \mathbb{P}} f(p).$$

"T[illegible]"

Binary relation

Let A be a non-empty set. A binary operation/laskutoimitus denoted by $*$ is a mapping/kuvaus

$$* : A \times A \to A, \quad (a, b) \to a * b$$

meaning that $a * b \in A$, whenever $a \in A$ ja $b \in A$.

Binary relation

Let A be a non-empty set. A binary operation/laskutoimitus denoted by $*$ is a mapping/kuvaus

$$* : A \times A \to A, \quad (a, b) \to a * b$$

meaning that $a * b \in A$, whenever $a \in A$ ja $b \in A$.

Particular cases:

Binary relation

Let A be a non-empty set. A binary operation/laskutoimitus denoted by $*$ is a mapping/kuvaus

$$* : A \times A \to A, \quad (a, b) \to a * b$$

meaning that $a * b \in A$, whenever $a \in A$ ja $b \in A$.

Particular cases:

multiplication/kertolasku denoted by $\cdot$

Binary relation

Let A be a non-empty set. A binary operation/laskutoimitus denoted by $*$ is a mapping/kuvaus

$$* : A \times A \to A, \quad (a, b) \to a * b$$

meaning that $a * b \in A$, whenever $a \in A$ ja $b \in A$.

Particular cases:

multiplication/kertolasku denoted by $\cdot$

yhteenlasku/addition denoted by $+$

Identity axioms

(a) $\forall\ a :$ $a = a.$

Identity axioms

(a) $\forall\ a :$ $\qquad a = a.$

(b) $\forall\ a_1, a_2, b_1, b_2 :$ $\quad a_1 = b_1,\ a_2 = b_2 \quad \Rightarrow \quad (a_1 = a_2 \ \Leftrightarrow\ b_1 = b_2).$

Identity axioms

(a) $\forall\ a :\qquad a = a.$

(b) $\forall\ a_1, a_2, b_1, b_2 :\quad a_1 = b_1,\ a_2 = b_2 \quad \Rightarrow \quad (a_1 = a_2 \ \Leftrightarrow\ b_1 = b_2).$

(c) $\forall\ a_1, a_2, b_1, b_2 :\quad a_1 = b_1,\ a_2 = b_2 \quad \Rightarrow \quad a_1 * a_2 = b_1 * b_2.$

Corollaries of the identity relation axiom (c)

Seuraus 1

Identiteetin

$$a = b \tag{1}$$

molemmat puolet saa kertoa samalla alkiolla c/You may multiply the both sides of the identity (1) *by the same element c, jolloin/whereupon*

$$c \cdot a = c \cdot b. \tag{2}$$

Seuraus 2

Identiteetin

$$a = b \tag{3}$$

molemmille puolin saa lisätä saman alkion c/You may add the same element c on the both sides of the identity (3)*, jolloin/whereupon*

$$a + c = b + c. \tag{4}$$

Group

Let G be a non-empty set with a multiplication

$$\cdot : G \times G \to G, \quad (a, b) \to a \cdot b.$$

Group

Määritelmä 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

Group

Määritelmä 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$ (assosiativity).

Group

Määritelmä 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$ (assosiativity).

(b) There exists a unit-element $1 \in G$, satisfying
$1 \cdot a = a \cdot 1 = a$ for all $a \in G$.

Group

Määritelmä 1

A pair $(G, \cdot)$ is a group, if the multiplication satisfies the following axioms:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$ (assosiativity).

(b) There exists a unit-element $1 \in G$, satisfying
$1 \cdot a = a \cdot 1 = a$ for all $a \in G$.

(c) For all $a \in G$ there exists an inverse-element $a^{-1} \in G$, satisfying
$a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Abelian group

In the case of commutative group the addition notation is familiar.
Olkoon A epätyhjä joukko, jossa on määritelty yhteenlasku/addition

$$+ : A \times A \to A, \quad (a, b) \to a + b.$$

Abelian group

Määritelmä 2

Pari $(A, \cdot)$ on Abelin ryhmä, jos yhteenlasku toteuttaa seuraavat aksiomit eli ehdot:

Abelian group

Määritelmä 2

Pari $(A, \cdot)$ on Abelin ryhmä, jos yhteenlasku toteuttaa seuraavat aksiomit eli ehdot:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in A$ (liitännäisyys).

Abelian group

Määritelmä 2

Pari $(A, \cdot)$ on Abelin ryhmä, jos yhteenlasku toteuttaa seuraavat aksiomit eli ehdot:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in A$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in A$ (vaihdannaisuus/commutativity).

Abelian group

Määritelmä 2

Pari $(A, \cdot)$ on Abelin ryhmä, jos yhteenlasku toteuttaa seuraavat aksiomit eli ehdot:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in A$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in A$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in A$, jolle $0 + a = a$ kaikilla $a \in A$.

Abelian group

Määritelmä 2

Pari $(A, \cdot)$ on Abelin ryhmä, jos yhteenlasku toteuttaa seuraavat aksiomit eli ehdot:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in A$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in A$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in A$, jolle $0 + a = a$ kaikilla $a \in A$.

(d) Kaikilla $a \in A$ on olemassa vasta-alkio/additive inverse $-a \in A$, jolle $a + (-a) = 0$.

Ring

In this course we are studying commutative rings with unity.
Olkoon R joukko, jossa on ainakin kaksi alkiota, $\#R \geq 2$. Oletetaan, että joukossa R on määritelty yhteenlasku:

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

missä $a + b \in R$, kun $a \in R$ ja $b \in R$ sekä

Ring

In this course we are studying commutative rings with unity.
Olkoon R joukko, jossa on ainakin kaksi alkiota, $\#R \geq 2$. Oletetaan, että joukossa R on määritelty yhteenlasku:

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

missä $a + b \in R$, kun $a \in R$ ja $b \in R$ sekä

kertolasku $*$:

$$* : R \times R \to R, \quad (a, b) \to a * b,$$

missä $a * b \in R$, kun $a \in R$ ja $b \in R$.

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in R$, jolle $0 + a = a$ kaikilla $a \in R$.

Commutative ring with unity

Määritelmä 3

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in R$, jolle $0 + a = a$ kaikilla $a \in R$.

(d) Kaikilla $a \in R$ on olemassa vasta-alkio/inverse $-a \in R$, jolle $a + (-a) = 0$.

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

(a) $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in R$.

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

(a) $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in R$.

4. $0 \neq 1$.

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Mutta $R = (R, *)$ EI/NOT ole kertolaskun $*$ suhteen (välttämättä/necessarily) ryhmä/group.

Määritelmän 3 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Mutta $R = (R, *)$ EI/NOT ole kertolaskun $*$ suhteen (välttämättä/necessarily) ryhmä/group. Kertolaskun neutraalialkio on ykkös-alkio 1.

Merkintä 1

Yleensä kertolasku $*$ jätetään merkitsemättä eli tehdään samaistus:

$$a * b = ab.$$

Määritelmä 4

Olkoon R ykkösellinen rengas. Joukko

$$R^* = \{\textit{yksiköt}\} = \{u \in R \mid \exists\ u^{-1} \in R :\ \ uu^{-1} = 1\} \tag{5}$$

on renkaan R yksikköryhmä (unit group).

Usein käytetään esitystä

$$R^* = \{u \in R \mid \exists\ v \in R :\ \ uv = 1\}, \tag{6}$$

jolloin pätee

$$u \in R^* \quad \Rightarrow \quad 1 = uv, \quad u, v \in R^*. \tag{7}$$

Jos $R = K$ kunta/field, niin $K^* = K \backslash \{0\}$.

Määritelmä 5

Renkaan R alkio $a \neq 0$ on nollantekijä (zero divisor), jos $\exists\ b \in R \backslash \{0\}$ s.e. $ab = 0$ tai $ba = 0$.

Määritelmä 6

Kommutatiivinen ykkösellinen rengas D on kokonaisalue/integral domain, mikäli D:ssä ei ole nollantekijöitä eli ehdosta $ab = 0$, $a, b \in D$ aina seuraa $a = 0$ tai $b = 0$.

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa nolla-alkio $0 \in K$, jolle $0 + a = a$ kaikilla $a \in K$.

Määritelmä 7

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa nolla-alkio $0 \in K$, jolle $0 + a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K$ on olemassa vasta-alkio $-a \in K$, jolle $a + (-a) = 0$.

2. Kertolaskun aksiomit:

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle
$1 * a = a$ kaikilla $a \in K$.

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle
$1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle
$a * a^{-1} = 1$.

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle $1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle $a * a^{-1} = 1$.

3. Osittelulaki:

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle $1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle $a * a^{-1} = 1$.

3. Osittelulaki:

(a) $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in K$.

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Edelleen, aksiomit 2a–d sanovat, että $(K^*, *)$ on Abelin ryhmä, jonka laskutoimitusta $*$ kutsutaan kertolaskuksi.

Määritelmän 7 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Edelleen, aksiomit 2a–d sanovat, että $(K^*, *)$ on Abelin ryhmä, jonka laskutoimitusta $*$ kutsutaan kertolaskuksi.
Sanotaan siis, että $(K^*, *)$ on kunnan K kertolaskuryhmä, jonka neutraalialkio on ykkös-alkio 1.

LYHYESTI: Kolmikko $(K, +, \cdot)$, $\#K \geq 2$ on *kunta*, jos:

1. $(K, +)$ on Abelin ryhmä (additiivinen ryhmä),
2. $(K^*, *)$ on Abelin ryhmä (multiplikatiivinen ryhmä), $K^* = K \backslash \{0\}$.
3. $a(b + c) = ab + ac, \ \forall a, b, c \in K$.

Erityisesti, kunta on kommutatiivinen ykkösellinen rengas.
Edelleen kunnassa on aina vähintään kaksi alkiota, nimittäin $0, 1 \in K$, $0 \neq 1$.

Esimerkki 2

Field K is an integral domain.
Proof: Let

$$ab = 0, \tag{8}$$

where $a, b \in K$. Antithesis: $a \neq 0$ and $b \neq 0$.
Because K is a field, then $a^{-1} \in K$. Multiplying (8) by a^{-1} gives

$$a^{-1}ab = a^{-1} \cdot 0 \quad \Rightarrow \quad b = 0. \tag{9}$$

A contradiction. □

Esimerkki 3

The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$, where $p \in \mathbb{P}$, are integral domains.

Esimerkki 4

Any subring S of a field K is an integral domain.

Esimerkki 5

$\mathbb{Z}$ is an integral domain.

Esimerkki 6

The set

$$\mathbb{Z}[i] = \{a + ib |\ a, b \in \mathbb{Z}\} \tag{10}$$

of Gaussian integers is an integral domain and its unit group is

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{11}$$

Esimerkki 7

The set

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\} \tag{12}$$

is an integral domain and its unit group is

$$\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}. \tag{13}$$

Karakteristika

Määritelmä 8

Kunnan K karakteristika

$$char\ K = \begin{cases} p \Leftrightarrow \exists\ p \in \mathbb{P} :\ \ p1 = 0; \\ 0 \Leftrightarrow \nexists\ n \in \mathbb{Z}^+ :\ \ n1 = 0. \end{cases}$$

Esimerkki 8

Kompleksilukujen kunta $\mathbb{C}$.
Luvun $z = a + ib$ kompleksikonjugaatti on luku $\overline{z} = a - ib$ ja pituus $|\overline{z}| = \sqrt{a^2 + b^2}$.

$$\overline{\overline{z}} = z, \quad \overline{zw} = \overline{z}\,\overline{w}, \quad z\overline{z} = |z|^2. \tag{14}$$

$$\overline{z} = z \quad \Leftrightarrow \quad z \in \mathbb{R}. \tag{15}$$

$$a = \frac{z + \overline{z}}{2}, \quad b = \frac{z - \overline{z}}{2i}. \tag{16}$$

$$|z + \overline{z}| \leq 2|z|, \quad |z - \overline{z}| \leq 2|z|. \tag{17}$$

$$z + \overline{z} \leq 2|z|. \tag{18}$$

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Kuvaus $f : A \to B$ on

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Kuvaus $f : A \to B$ on

INJEKTIO: $f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2;$

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Kuvaus $f : A \to B$ on

INJEKTIO: $f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2;$

SURJEKTIO: $f(A) = B;$

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Kuvaus $f : A \to B$ on

INJEKTIO: $f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2$;

SURJEKTIO: $f(A) = B$;

BIJEKTIO=INJEKTIO+SURJEKTIO.

Lemma 1

Olkoon

$$\#A = \#B < \infty$$

ja

$$f : A \to B$$

injektio.

Lemma 1

Olkoon

$$\#A = \#B < \infty$$

ja

$$f : A \to B$$

injektio.

Tällöin $f : A \to B$ *on bijektio.*

Polynomijoukko

Olkoon R ykkösellinen rengas. Tällöin R-kertoimisten polynomien joukolle käytetään merkintää

$$R[x] = \{P(x) \mid P(x) = \sum_{k=0}^{n} p_k x^k;\ p_k \in R,\ n \in \mathbb{N}\}.$$

Polynomia

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{19}$$

kutsutaan nollapolynomiksi ja polynomia

$$1(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{20}$$

ykköspolynomiksi. Ne ovat erikoistapauksia vakiopolynomista

$$c(x) = c + 0 \cdot x + 0 \cdot x^2 + \ldots, \quad c \in R. \tag{21}$$

Laskutoimitukset

Määritelmä 9

Olkoot $P(x) = \sum_{k=0}^{n} p_k x^k, \quad Q(x) = \sum_{k=0}^{n} q_k x^k \in R[x]$, *jolloin asetetaan*

$$P(x) = Q(x) \Leftrightarrow \forall k(p_k = q_k);$$

$$P(x) + Q(x) = \sum_{k \geqslant 0} (p_k + q_k) x^k;$$

$$P(x) \cdot Q(x) = \sum_{k \geqslant 0} r_k x^k,$$

$$r_k = \sum_{i=0}^{k} p_i q_{k-i} = \sum_{i+j=k} p_i q_j, \tag{22}$$

joka on Cauchyn kertosääntö.

Polynomial ring/degree

Lause 1

Tällöin $(R[x], +, \cdot)$ *on rengas, missä* $0(x)$ *on yhteenlaskun nolla-alkio ja* $1(x)$ *on kertolaskun ykkösalkio.*

Määritelmä 10

Jos $p_n \neq 0$, *niin polynomin* $P(x) = \sum_{k=0}^{n} p_k x^k$ *aste on*

$$\deg P(x) = n, \tag{23}$$

lisäksi asetetaan

$$\deg 0(x) = -\infty. \tag{24}$$

Jakoalgoritmi

Lause 2

Olkoon K kunta ja $P(x), Q(x) \in K[x]$. Tällöin

$$\deg P(x)Q(x) = \deg P(x) + \deg Q(x). \tag{25}$$

Lause 3

Jakoalgoritmi.
Olkoon $a(x), b(x) \in K[x]$, $a(x)b(x) \neq 0(x)$ ja $\deg b(x) \leq \deg a(x)$.
Tällöin $\exists\ q(x), r(x) \in K[x]$ s.e.

$$[J.A.] \quad a(x) = q(x)b(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{26}$$

Määritelmä 11

Jos $\alpha \in K$ *ja*

$$(x-\alpha)^m \| p(x),\ m \in \mathbb{Z}^+,$$

niin $m = m(\alpha)$ *on polynomin* $p(x)$ *nollakohdan* α *kertaluku/order of the zero. Nollakohtien lukumäärä/number of zeros* n_p *on summa kertaluvuista/is sum of orders eli*

$$n_p = \#\{\alpha |\ p(\alpha) = 0\} := \sum_{p(\alpha_i)=0} m(\alpha_i).$$

Lause 4

Olkoon K *kunta ja* $p(x) \in K[x]$, $p(x) \neq 0(x)$. *Tällöin* $n_p \leq \deg p(x)$.

Esimerkki 9

- *a) Olkoon* $p(x) = (x-1)^3(x+1/2)^5$. *Polynomin* $p(x)$ *nollakohdat ovat* $\alpha_1 = 1$ *ja* $\alpha_2 = -1/2$. *Nollakohtien kertaluvut ovat* $m(\alpha_1) = 3$ *ja* $m(\alpha_2) = 5$, *ja nollakohtien lukumäärä* $n_p = 3 + 5 = 8$.
- *b) Olkoon* $(x^2+1)(x^2-1) \in \mathbb{R}[x]$. *Nyt nollakohtien lukumäärä* $n_p = m(-1) + m(1) = 2 < 4 = deg(p(x))$.