

Abstraktse algebra põhimõisteid

Definitsioon 1. Olgu A mittetühi hulk. Kujutust $\omega : A^n \rightarrow A$ nimetatakse n -kohaliseks algebraliseks tehteks hulgal A .

Definitsioon 2. Rühmaks nimetatakse hulka A , millel on defineeritud üks kahekohaline tehe $*$ (tähistame $*(a, b) = a * b$), nii et

G1. $(\forall a, b, c \in A)((a * b) * c = a * (b * c))$ (assotsiatiivsus);

G2. $(\exists e \in A)(\forall a \in A)(a * e = e * a = a)$ (leidub ühikelement);

G3. $(\forall a \in A)(\exists a^{-1} \in A)(a * a^{-1} = a^{-1} * a = e)$ (igal elemendil leidub pöördelament).

Õeldakse, et A on rühm tehete $*$ suhtes ja kirjutatakse $(A, *)$.

Kui hulgal A on defineeritud kahekohaline tehe, mis on assotsiatiivne, siis A on poolrühm. Kui poolrühmas leidub ühikelement, siis teda nimetatakse monoidiks.

Kahekohaline tehe $*$ hulgal A on kommutatiivne, kui kehtib samasus

COMM. $(\forall a, b \in A)(a * b = b * a)$.

Rühma, mille tehe on kommutatiivne, nimetatakse kommutatiivseks ehk Abeli rühmaks.

Tihti tähistatakse Abeli rühma tehet märgiga “+” ja nimetatakse liitmiseks. Sellisel juhul võtavad Abeli rühma aksioomid järgmise kuju:

AG1. $(\forall a, b, c \in A)((a + b) + c = a + (b + c))$ (assotsiatiivsus);

AG2. $(\exists 0 \in A)(\forall a \in A)(a + 0 = a)$ (leidub nullelement);

AG3. $(\forall a \in A)(\exists -a \in A)(a + (-a) = 0)$ (igal elemendil leidub vastandelement);

AG4. $(\forall a, b \in A)(a + b = b + a)$ (kommutatiivsus).

Definitsioon 3. Ringiks nimetatakse hulka R , millel on defineeritud kaks kahekohalist tehet, $+$ (liitmine) ja \cdot (korrutamine), nii et

R1. $(R, +)$ on Abeli rühm;

R2. (R, \cdot) on monoid;

R3. $(\forall a, b, c \in R)(a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + b \cdot c)$ (distributiivsus).

(Tihti defineeritakse ringid ilma nõudeta R2. Sellisel juhul kutsutakse meie poolt vaadeldavaid ringe assotsiatiivseteks ühikelemendiga ringideks.) (Kui mingis algebralises struktuuris kõneldakse korrutamistest \cdot , siis enamasti jäetakse tehemärk ära ning kirjutatakse $a \cdot b$ asemel lihtsalt ab .)

Definitsioon 4. Ringi $(R, +, \cdot)$ nimetatakse korpuseks, kui igal nullist erineval elemendil on olemas pöördelament. Sel juhul $(R \setminus \{0\}, \cdot)$ on rühm.

Ringi (korpust) nimetatakse kommutatiivseks, kui tema korrutamine on kommutatiivne.

Ringi R nullist erinevat elementi a nimetatakse nulliteguriks, kui leidub selline nullist erinev element $b \in R$, et $ab = 0$.

Lause 1. Korpuses ei ole nullitegureid.

Definitsioon 5. *Vektorruumiks* üle korpuse K nimetatakse mittetühja hulka V , millel on defineeritud üks kahekohaline tehe $+$ (liitmine) ning iga $k \in K$ ja $a \in V$ korral on defineeritud korrutis $ka \in V$, nii et

VS1. $(V, +)$ on Abeli rühm;

VS2. $(\forall a, b \in V)(\forall k \in K)(k(a + b) = ka + kb)$;

VS3. $(\forall a \in V)(\forall k, l \in K)((k + l)a = ka + la)$;

VS4. $(\forall a \in V)(\forall k, l \in K)((kl)a = k(la))$;

VS5. $(\forall a \in V)(1a = a)$.

Vektorruumi V elemente kutsutakse *vektoriteks* ning korpuse K elemente *skalaarideks*.

Definitsioon 6. Olgu G_1 ja G_2 rühmad. Kujutust $\varphi : G_1 \rightarrow G_2$ nimetatakse (rühmade) *homomorfismiks*, kui

HG. $(\forall a, b \in G_1)(\varphi(ab) = \varphi(a)\varphi(b))$. (korrutamise säilitamine)

Definitsioon 7. Olgu R_1 ja R_2 ringid ühikelementidega 1 ja $1'$, vastavalt. Kujutust $\varphi : R_1 \rightarrow R_2$ nimetatakse (ringide) *homomorfismiks*, kui

HR1. $(\forall a, b \in R_1)(\varphi(a + b) = \varphi(a) + \varphi(b))$; (liitmise säilitamine)

HR2. $(\forall a, b \in R_1)(\varphi(ab) = \varphi(a)\varphi(b))$; (korrutamise säilitamine)

HR3. $\varphi(1) = 1'$. (ühikelemendi säilitamine)

Definitsioon 8. Olgu V_1 ja V_2 vektorruumid üle korpuse K . Kujutust $\varphi : V_1 \rightarrow V_2$ nimetatakse (vektorruumide) *homomorfismiks* ehk *linearkujutuseks*, kui

HVS1. $(\forall a, b \in V_1)(\varphi(a + b) = \varphi(a) + \varphi(b))$; (liitmise säilitamine)

HVS2. $(\forall a \in V_1)(\forall k \in K)(\varphi(ka) = k\varphi(a))$. (skalaariga korrutamise säilitamine)

Algebraaliste struktuuride *isomorfismiks* nimetatakse nende bijektiivset homomorfismi. Kui leidub isomorfism ühest algebraalisest struktuurist teise, siis neid struktuure nimetatakse *isomorfseteks*. Korpuse loetakse isomorfseteks, kui nad on isomorfsetes kui ringid.

Definitsioon 9. Olgu (G, \cdot) rühm. Mittetühja hulka $H \subseteq G$ nimetatakse rühma G *alamrühmaks*, kui

SG1. $(\forall a, b \in H)(ab \in H)$; (kinnisus korrutamise suhtes)

SG2. $(\forall a \in H)(a^{-1} \in H)$. (kinnisus pöördlemendi võtmise suhtes)

Kui a on rühma G mingi fikseeritud element, siis hulk $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, 1 = a^0, a, a^2, \dots\} \subseteq G$ on rühma G alamrühm. Seda alamrühma nimetatakse *elemendi a poolt moodustatud (tekitatud) alamrühmaks*. Kui see rühm on lõpmatu, siis öeldakse, et element a on *lõpmatut järku*. Kui aga see rühm on lõplik, siis leidub selline naturaalarv m , et $\langle a \rangle = \{a, a^2, \dots, a^{m-1}, a^m = 1\}$. Kui m on vähim sellise omadusega naturaalarv, siis öeldakse, et elemendi a *järk* rühmas G on m ning tähistatakse $\text{ord}_G(a) = m$. Kui rühm G on moodustatud ühe elemendi poolt, s.t. kui $G = \langle a \rangle$, siis öeldakse, et rühm G on *tsükliline*.

Lõpliku rühma *järguks* nimetatakse tema elementide arvu. Seega elemendi järk on tema poolt moodustatud alamrühma järk.

Teoreem 1. (Lagrange) *Lõpliku rühma mistahes alamrühma järk on selle rühma järgu jagaja.*

Definitsioon 10. Olgu $(R, +, \cdot)$ ring ühikelemendiga 1. Mittetühja alamhulka $R' \subseteq R$ nimetatakse ringi R *alamringiks*, kui

SR1. $(\forall a, b \in R')(a + b \in R')$; (kinnisus liitmise suhtes)

SR2. $(\forall a \in R')(-a \in R')$; (kinnisus vastandelemendi võtmise suhtes)

SR3. $(\forall a, b \in R')(ab \in R')$; (kinnisus korrutamise suhtes)

SR4. $1 \in R'$. (kinnisus ühikelemendi suhtes)

Definitsioon 11. Olgu $(K, +, \cdot)$ korpus. Mittetühja alamhulka $K' \subseteq K$ nimetatakse korpuse K *alamkorpuseks*, kui

SF1. $(\forall a, b \in K')(a + b \in K')$; (kinnisus liitmise suhtes)

SF2. $(\forall a \in K')(-a \in K')$; (kinnisus vastandelemendi võtmise suhtes)

SF3. $(\forall a, b \in K')(ab \in K')$; (kinnisus korrutamise suhtes)

SF4. $(\forall a \in K' \setminus \{0\})(a^{-1} \in K')$. (kinnisus pöördelemendi võtmise suhtes)

Definitsioon 12. Olgu V vektorruum. Mittetühja alamhulka $U \subseteq V$ nimetatakse vektorruumi V *alamruumiks*, kui

SVS1. $(\forall a, b \in U)(a + b \in U)$; (kinnisus liitmise suhtes)

SVS2. $(\forall a \in U)(\forall k \in K)(ka \in U)$. (kinnisus skalaariga korrutamise suhtes)

Definitsioon 13. Rühma G alamrühma N nimetatakse *normaalseks alamrühmaks* ehk *normaaljagajaks*, kui

NSG. $(\forall a \in G)(\forall b \in N)(a^{-1}ba \in N)$.

Olgu N rühma G normaaljagaja. Alamhulki $aN = \{ab \mid b \in N\}$, kus $a \in G$, nimetatakse *kõrvalklassideks* normaaljagaja N järgi. Tähistame kõigi kõrvalklasside hulga $\{aN \mid a \in G\} = G/N$ ning defineerime sellel hulgal korrutamistehte võrdusega

$$(a_1N)(a_2N) = a_1a_2N.$$

Saab näidata, et G/N on rühm selle tehte suhtes. Seda rühma G/N nimetatakse rühma G *faktorrühmaks* normaaljagaja N järgi.

Definitsioon 14. Ringi R mittetühja alamhulka I nimetatakse *ideaaliks*, kui

I1. $(\forall a, b \in I)(a + b \in I)$;

I2. $(\forall a \in R)(\forall i \in I)(ai, ia \in I)$.

Olgu I ringi R ideaal. Alamhulki $a + I = \{a + i \mid i \in I\}$, kus $a \in R$, nimetatakse kõrvalklassideks ideaali I järgi. Tähistame kõigi kõrvalklasside hulga $\{a + I \mid a \in R\} = R/I$ ning defineerime sellel hulgal korrutamise- ja liitmistehte võrdustega

$$\begin{aligned}(a_1 + I) + (a_2 + I) &= (a_1 + a_2) + I; \\ (a_1 + I)(a_2 + I) &= (a_1a_2) + I.\end{aligned}$$

Saab näidata, et R/I on ring nende tehete suhtes. Seda ringi R/I nimetatakse ringi R *faktoringiks* ideaali I järgi.