Peatükk 1

Üldise algebra põhimõisteid ja põhikonstruktsioonid

Meenutusi varasemast

Olgu A mittetühi hulk ehk $A \neq \emptyset$. Olgu n suvaline naturaalarv, hulga A n-**ndaks otseastmeks** nimetatakse hulga A elementidest koosnevate järjestatud vektorite hulka.

$$A^n = A \times A \times ... \times A = \{(a_1, \cdots, a_n) | a_i \in A\}.$$

Inglise keelses kirjanduses kasutatakse tähist n-*tuple*. Märgime veel, et $A^0 = \{\emptyset\}$, seega $|A^0| = 1$.
Kujutustust

$$\omega : A^n \to A$$

nimetatakse n-**naarseks** ehk n-**kohaliseks** algebraliseks tehteks hulgal A.
Levinumad n-aarsete tehete nimetused:

1. n=2: binaarne tehe, paneb kahele kindlas järjekorras võetud elemendile vastavusse elemendi samast hulgast.

2. n=1: unaarne tehe, paneb hulga elemendile vastavasse mingi selle sama hulga elemendiga.

3. n=0: nullarne tehe, tõlgendatav kui ühe kindla elemendi fikseerimine

1.1 Ω-algebra

Definitsioon 1.1.1. Hulka Ω nimetakse **tüübiks** ehk **signatuuriks** kui ta on esitatud mittelõikuvate alamhulkade $\Omega_0, \Omega_1, \Omega_2, ...$ ühendina.

Definitsioon 1.1.2. Olgu Ω tüüp. Mittetühja hulka A nimetatakse **Ω-algebraks**, kui iga a korral igale $\omega \in \Omega_n$ vastab n-aarne tehe hulgal A, mida tähistatakse sama sümboliga ω.

Ehk, kui A on Ω-algebra, siis iga $\omega \in \Omega_n$ ja suvaliste $a_1, a_2, ..., a_n \in A$ korral on üheselt määratud element $\omega(a_1, a_2, ..., a_n) \in A$.
Kui tahetakse rõhutada, mis tüüpi algebraga on tegemist, siis tähistatakse Ω algebrad paarina $(A; \Omega)$.

Meenutusi varasemast

Algebralised põhistruktuurid.

I Rühmoid - mittetühi hulk, millel defineeritud kahekohaline tehe.

II Poolrühm - rühmoid, mille tehe on assotsiatiivne.

III Monoid - poolrühm, milles leidub ühikelement.

IV Rühm - monoid, mille igal elemendil leidub pöördelement.

V Abeli rühm - rühm on Abeli rühm, kui tema tehe on kommutatiivne.

VI Ring - hulka R nimetatatkse ringiks, kui tal on defineeritud liitmine ja korrutamine, kusjuures R on liitmiise suhtes Abeli rühm ja liitmine ja korrutamine on distributiivsed. Tihti lisatakse ka nõue ühikelemende olemasoluks.

VII Korpus - ring, mille nullist erinevad elemendid moodustavad rühma korrutamise suhtes.

Näited

I Rühmoid - hulk ühe binaarse tehtega, see tähendab $\Omega = \Omega_2 = \{*\}$.

II Poolrühm - signatuur analoogne rühmoidi signatuuriga.

III Monoid - ühikelemendiga poolrühm, vaatame seda tihti laiema signatuuriga, $\Omega = \Omega_0 \cup \Omega_2$, kus $\Omega_0 = \{1$ (ühikelemendi fikseerimine)$\}$ ja $\Omega_2 = \{*\}$.

IV Rühm - saab kirjeldada eelnevate signatuuride kaudu, aga parem kirjeldada järgnevalt: $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, kus $\Omega_0 = \{1\}$, $\Omega_1 = \{^{-1}$ (pöördelemendi leidmine)$\}$ ja $\Omega_2 = \{*\}$.

V Ring - algebraline struktuur signatuuriga: $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, kus $\Omega_2 = \{+, *\}$, $\Omega_1 = \{-$ vastandelemendi leidmine$\}$ ja $\Omega_0 = \{0$ (nullelemendi fikseerimine)$, 1\}$.

VI Vektorruum üle korpuse $\mathbb{K}$ - struktuur signatuuriga: $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, kus $\Omega_2 = \{+\}$, $\Omega_1 = \{-\} \cup \{\alpha * | \alpha \in \mathbb{K}\}$, $\Omega_0 = \{0\}$. Paneme tähele, et kui oleme sisse toonud skalaariga korrutamise ei ole rangelt võttes vaja ei nullelemendi fikseerimist ega vastandelemendi leidmist - need tehted võime defineerida läbi skalaariga korrutamise. Ehk alternatiivne signatuur oleks järgmine: $\Omega = \Omega_1 \cup \Omega_2$, kus $\Omega_2 = \{+\}$, $\Omega_1 = \{\alpha * | \alpha \in \mathbb{K}\}$.

1.2 Morfismid

Definitsioon 1.2.1. Olgu meil Ω-algebra A ja Ω-algebra B. Kujutust ϕ nimetatakse **homomorfismiks**, kui iga n, iga $\omega \in \Omega_n$ ja suvaliste $a_1, ..., a_n \in A$ korral kehtib võrdus

$$\phi(\omega(a_1, ..., a_n)) = \omega(\phi(a_1), ..., \phi(a_n)).$$

Defineerime kõikide A ja B vaheliste homomorfismide hulga järgnevalt - $\{\phi | \phi$ on homoformism algebrast A algebrasse B $\}$, sellist hulka tähistatakse sümboliga $\mathrm{Hom}(A, B)$.

Näited

I Olgu A ja B rühmad. Meenutame, et rühma saab kirjeldada järgneva signatuuri abil: $\Omega = \{1\} \cup \{^{-1}\} \cup \{*\}$. Olgu meil järgnev kujutus:

$$\phi : A \to B$$

Veendumaks, et ϕ on homomorfism tuleb veenduda selles, et ϕ säilitab kõik tehted. Teisisõnu:

$$\phi \text{ on homomorfism } \iff \begin{cases} \phi(1) = 1 \\ \phi(x^{-1}) = \phi(x)^{-1} \\ \phi(xy) = \phi(x)\phi(y) \end{cases}$$

Tõestame, et rühmade A ja B vaheline kujutus on homomorfism siis ja ainult siis kui kehtib kolmas tingimus ($\phi(xy) = \phi(x)\phi(y)$).

Tõestus. Kehtigu kolmas tingimus, see tähendab $\phi(xy) = \phi(x)\phi(y)$. Veendume, et sellest järeldub esimese kahe tingimuse kehtivus.

$$\phi(1) = \phi(1*1) = \phi(1)\phi(1) \implies \phi(1)\phi(1)^{-1} = \phi(1)\phi(1)\phi(1)^{-1} \implies 1 = \phi(1)*1 = \phi(1)$$

$$\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1) = 1 \implies \phi(x)^{-1} = \phi(x^{-1})$$

□

Niisiis taandub kujutuse homomorfismiks olemise kontroll kolmanda omanduse kehtimise kontrollimisele.

II Lineaarkujutis on vektorruumide isomorfism.

III Olgu meil Ω-algebrad A, B ja C ning nende homomorfismid $\phi : A \to B$, $\psi : B \to C$. Defineerime kujutuse $\upsilon : A \to C$ järgnevalt: $\upsilon = (\psi\phi) = \psi(\phi(x)), x \in A$. Siis see kompositsioon on samuti homoformism (kui teda saab nii defineerida).Sõnastame eelneva lausena ja veendume, et see nii on.

Lause 1.2.2. *Kui Ω-algebrate homomorfismide korrutis on defineeritud, siis on see ise ka Ω-algebrate homomorfism.*

Tõestus. Peame veenduma sellest, et $(\psi\phi)(\omega(a_1, \cdots, a_n)) = \omega((\psi\phi)(a_1, \cdots, a_n))$. See on samaväärne sellega, te $\psi(\phi(\omega(a_1, \cdots, a_n))) = \omega(\psi(\phi(a_1)), \cdots, \psi(\phi(a_n)))$. Kuna ϕ on homomorfism, siis kehtib $\psi(\phi(\omega(a_1, \cdots, a_n))) = \psi(\omega(\phi(a_1), \cdots, \phi(a_n))$. Kuna ka ψ on homomorfism, siis saame kirjutada: $\omega(\psi(\phi(a_1)), ..., \psi(\phi(a_n)))$.

□

Definitsioon 1.2.3. Homomorfismis mingist Ω-algebrast iseendasse nimetatakse selle algebra **endomorfismiks**. Kõikide endomorfismide hulka $\mathrm{Hom}(A, A)$ tähistame sümboliga $\mathrm{End}(A)$.

Lause 1.2.4. *Iga Ω-algebra A korral on hulk End(A) monoid kujutuste korrutamise (järjest rakendamise) suhtes.*

Tõestus. Tõestuseks piisab veenduda, et leidub ühikelement ja kujutuste järjest rakendamine on assotsiatiivne. Veendume ühikelemendi olemasolus, selleks sobib kujutus $id_A : A \to A, id_A(x) = x, x \in A$. On selge, et selline kujutus on ka homomorfism, mistõttu ta kuulub hulka End(A). Assotatiivsuses veendumiseks piisab tähele panna, et $(\phi\psi)\,x$ on defineeritud kui $\phi\,(\psi\,(x))$. Seega $(\phi\psi)\,\upsilon\,(x) = \phi\,(\psi\,(\upsilon\,(x))) = \phi\,(\psi\upsilon)\,(x)$. □

Definitsioon 1.2.5. Bijektiivset homomorfismi nimetatakse **isomorfismiks**.

Definitsioon 1.2.6. Ω-algebraid A ja B nimetatakse nimetatakse **isomorfseteks**, kui leidub isomorfism $\phi : A \to B$.

Seda, et Ω-algebrad A ja B on isomorfsed, tähistatakse sümboliga $A \simeq B$.

Lause 1.2.7. *Isomorfism on ekvivalentsiseos kõigi Ω-algebrade klassil, ehk ta on refleksiivne, sümmeetriline ja transitiivne.*

Tõestus. Veendume, et isomorfism on refleksiivne, sümeetriline ja transitiivne. Olgu A, B, C Ω-algebrad.

I Refleksiivsus, ehk A $\simeq$ A. Lihte on nähe, et sobivaks isomorfismiks osutub $id_A : A \to A$.

II Sümmeetria. Peame veenduma, et kui eksisteerib isomorfism $\phi : A \to B$ isomorfism, siis sellest järeldub, et eksisteerib ka isomorfism $\psi : B \to A$. Valime selleks ϕ^{-1} ja näitame, et tegemist on tõepoolest isomorfismiga. Bijektiivsus on ilme, näidata tuleb, et ϕ^{-1} säilitab tehted. See tähendab, et peab kehtima järgnev : $\forall(b_1, \cdots, b_n) \in B$ korral $\phi^{-1}(\omega(b_1, \cdots, b_n)) = \omega(\phi^{-1}(b_1), \cdots, \phi^{-1}(b_n))$. Rakendame mõlemale poole kujutust ϕ. Saame $\phi\,(\phi^{-1}(\omega(b_1, \cdots, b_n))) = \phi\,(\omega\,(\phi^{-1}(b_1), \cdots, \phi^{-1}(b_n)))$. Arvestades seda, et ϕ on homomorfism saame kirjutada: $\phi\,(\phi^{-1}(\omega(b_1, \cdots, b_n))) = (\omega\,((\phi\phi^{-1})\,(b_1), \cdots, (\phi\phi^{-1})\,(b_n)))$. Kuna kujutuse ja tema pöördkujutuse järjest rakendamine on võrdne ühik teisendusega, siis on lihte näha, et võrdus kehtib. Siis aga ϕ injektiivsuse põhjal $\phi^{-1}(\omega(b_1, \cdots, b_n)) = \omega(\phi^{-1}(b_1), \cdots, \phi^{-1}(b_n))$, mida oligi tarvis näidata.

III Transitiivsus. Veendume, et kui leiduvad isomorfisimid $\phi : A \to B$ ja $\psi : B \to C$, siis leidub ka isomorfism $\upsilon : A \to C$. Valime kujutuseks υ

kujutuste ϕ ja *psi* järjest rakenduse $(\phi\psi) : A \to C$. Veendume, et nii defineeritud υ on isomorfism. On lihtne näha, et tegemist on bijektsiooniga. Lause 1.2.2 põhjal on υ ka homomorfism, seega oleme näidanud, et υ on isomorfism.

$\square$

Kui meid huvitab tehe ja tema omadused, siis need jäävad samaks isomorfismi klassi täpsusega. Seeläbi võime laiendada tehte kohta tehtud tähelepanekuid ühelt Ω-algebralt algebrade isomorfismiklassile.

Definitsioon 1.2.8. Bijektiivset endomorfismi nimetatakse automorfismiks.

Ω-algebra A kõigi automorfismide hulka tähistatakse sümboliga Aut$A$

Lause 1.2.9. *Iga Ω-algebra A korral on hulk AutA rühm kujutuste korrutamise (järjest rakendamise) suhtes.*

Tõestus. Olgu A suvaline Ω-algebra.Esiteks, tuletame meelde, et Lause 1.2.4 põhjal on kõikide A endomorfismide hulk monoid kujutuste korrutamise suhtes. Kuna Ω-algebra A kõikide automorfismide hulk Aut$A$ on endomorfismide hulga kinnine alamhulk, siis on tegemist samuti monoidiga. Hulga kinnisus tuleneb faktist, et bijektiivsete kujutuste korrutamise tulemus on bijektiivne kujutus. Tuletame meelde, et rühm on selline monoid, mille igal elemendil leidub pöördelement. Jääb veenduda, et iga hulga Aut$A$ elemendil leidub pöördelement. Selleks sobib aga elemendi pöördfunktsioon, nagu me Lause 1.2.7 tõestuse teises osas veendusime. Seega on lause tõestatud. $\square$

Näited automorfismidest

I Vaatleme kompleksarvude korpuse $\mathbb{C}$ peal defineeritud funktsiooni $\phi : C \to C, \phi(\alpha) = \overline{\alpha}$. On lihtne veenduda, et see funktsioon on automorfism.

II Olgu G suvaline rühm, fikseerime elemendi $g \in G$. Defineerime nüüd kujutuse $\phi : G \to G, \phi(x) = g^{-1}xg$. Nii defineeritud kujutis on automorfism.

1.3 Alamalgebra

Definitsioon 1.3.1. Ω-algebrat B nimetatakse Ω-algebra A alamalgebraks, kui $B \subseteq A$ ja iga $\omega \in \Omega$ korral tehe ω algebral B saadakse kui algebra A sama tehte ahend.

Eelnevat võib mõtestada järgnevalt : $B \subset A, b_1, \cdots, b_n : \omega^B(b_1, \cdots, b_n) = \omega^A(b_1, \cdots, b_n)(\in B)$. Ehk, sõnadesse panduna, siis tehte ω väärtus ei sõltu sellest, kas me vaatame teda algebras A või algebras B. Definitsioonist järjeldub, et algebra mittetühialamhulk, mis on kinnine tehete suhtes on alamalgebra. Paneme tähele, et kui me jätaksime ära nõude, et alamhulk peab olema mittetühi, siis kehtiks jägnev väide: olgu $(A; *)$ on poolrühm ja $B = \emptyset \subset A$, siis B rahuldab tingimust $x, y \in B \implies xy \in B$ ehk B on kinnine korrutamise suhtes. Samas B ei ole alamalgebra, seega on mittetühja alamhulga nõue oluline.
Seda, et Ω-algebra B on Ω-algebra A alamalgebra tähistame $B \leq A$.
Kui $B \leq A$, siis saab vaadelda sisestuskujutust $\tau : B \to A, \tau(x) = x, x \in B$. On selge, et $\tau \in Hom(B, A)$, samuti on lihte veenduda, et τ on injektiivne. Seega $B \simeq A$ Teatud mõttes kehtib ka vastupidine seos, seda näeme järgmises lauses.

Lause 1.3.2. *Kui A ja B on Ω-algebrad ning leidub üksühene homomorfism $\phi : B \to A$, siis kujutis $\phi(B)$ on A alamalgebra, mis on isomorfne algebraga B.*

Tõestus. Vaatleme hulka $\phi(B)$. Eelneva põhjal piisab selleks, et veenduda et $\phi(B)$ on A alamalgebra veenduda, et $\phi(B)$ on kinnine. On selge, et B on kinnine kõigi oma tehete suhtes, Ω-algebra definitsiooni põhjal. Kuna ϕ on homomorfism, siis ta säilitab teheted, kuna ta on ka injektiivne, siis on hulk $\phi(B)$ kinnine tehete suhtes, seega on hulk $\phi(B)$ algebra A alamalgebra. Kuna $\phi(B) = \{\phi(x) | x \in B\}$, siis on kujutus ϕ selle hulga suhtes pealekujutus. Seega on ϕ bijektsioon hulkade B ja $\phi(B)$ vahel ehk $B \simeq \phi(B)$.

□

Lause 1.3.3. *Olgu antud Ω-algebrate homomorfism $\phi : A \to B$ ning olgu antud alamalgebrad $C \leq A$ ja $D \leq B$. Siis $\phi(C) \leq B$ ja $\phi^{-1}(D) \leq A$.*

Tõestus. Veendume esiteks, et algebra B alamhulk $\phi(C)$ on kinnine. Valime suvaliselt mingi tehte $\omega \in \Omega_n$. Alamhulga kinnisus on samaväärne sellege,

et suvaliste $e_1, ..., e_n \in \phi(C)$ korral $\omega(e_1, ..., e_n) \in \phi(C)$. Märgime, et leiduvad $c_i \in C$,nii et $\phi(c_i) = e_i$. Kusjuures, leidub $c \in C$ niiviisi, et kehtib $\omega(c_1, ..., c_n) = c$. Seega, $\omega(e_1, ..., e_n) = \omega(\phi(c_1), ..., \phi(c_n)) = \phi(\omega(c_1, ..., c_n)) = \phi(c) \in \phi(C)$. Seega algebra B alamhulk $\phi(C)$ on kinnine ja seega algebra B alamalgebra.
Veendume nüüd, et algebra A alamhulk $\phi^{-1}(D)$ on kinnine. Valime taaskord suvaliselt mingi $\omega \in \Omega_n$. Piisab näidata, et $a_1, ..., a_n \in \phi^{-1}(D) \implies \omega(a_1, ..., a_n) \in \phi^{-1}(D) \iff \phi(\omega(a_1, ..., a_n)) \in D$. Leiduvad $d_1, ..., d_n$, nii et kehtib $\phi(a_i) = d_i$. Jällegi, kuna D on alamalgebra, siis kehtib järgnev: $d = \phi\left(\omega(a_1, ..., a_n)\right) = \omega(\phi(a_1), ..., \phi(a_n)) \in D$.

□

Lause 1.3.4. *Olgu antud Ω-algebra A alamalgebrate süsteem B_i, $i \in I$, kujsuures $B = \cap_{i \in I} B_i \neq \emptyset$. Siis $B \leq A$.*

Tõestus. Olgu $B_i \leq A, i \in I, \cap_{i \in I} B_i \neq \emptyset$. Olgu $\omega_n \in \Omega$, valime suvaliselt $x_1, ..., x_n$ hulgast $\cap_{i \in I} B_i$. Sellest järeldub otseselt, et $x_1, ..., x_n \in B_i$ $\forall i \in I$, kuna B_i on alamalgebra, siis $\omega(x1, ..., x_n) \in B_i \implies \omega(x_1, ..., x_n) \in \bigcap_{i \in I} B_i$, millest alamalgebra definitsioonist järeldub, et $\bigcap_{i \in I} B_i$ on alamalgebra. □

Vaatleme Ω-algebra A mittetühja alamhulka X. Näeme, et vähim X-i sisaldav alamalgebra $\cap\{B \mid X \subset B \leq A, B\} \neq \emptyset$. Vastavalt lausele 1.3.4 on tegemist alamalgebraga. Sellist alamalgebrad tähistatakse $\langle X \rangle$. Kui $\langle X \rangle = A$, siis öeldakse, et X on A moodustajate süsteem.
On võimalik näidata, et $\langle X \rangle$ koosneb täpselt algebra A neist elementidest, mis on selle algebra teheta abil (nende korduval rakendamisel) saadavad hulga B elementidest.

1.4 Faktoralgebra

Eesmärgiks on tükeldada Ω-algebra mittelõikuvateks osadeks, nii et nende osade hulgal saaks loomulikul viisil defineerida Ω-algebra struktuuri.

Definitsioon 1.4.1. Ekvivalentsiseost ρ Ω-algebral A nimetatakse selle algebra kongruentsiks, kui iga n, iga $\omega \in \Omega_n$ ja suvaliste $x_1, ..., x_n, y_1, ..., y_n \in A$ korral sellest, et

$$(x_1, y_1) \in \rho, ..., (x_n, y_n) \in \rho$$

järeldub

$$(\omega(x_1, ..., x_n), \omega(y_1, ..., y_n)) \in \rho.$$

Meenutusi varasemast

Ütleme, et ρ on hulga A ekvivalents ($\rho \in Eqv(A)$), kui $\rho \subset A \times A$ ja ρ on:

1. refleksiivne
2. sümmeetriline
3. transitiivne

Kui hulgal on antud ekvivalentsiseos ρ, siis iga $a \in A$ määrab ekvivalentsiklassi $\{x \in A \mid a\rho x\}$, mida me hakama tähistama a/ρ. Kõigi ρ-klasside hulka nimetatakse hulga A faktorhulgaks ekvivalentsi ρ järgi ja tähistatakse A/ρ. Paneme tähele, et kehtib $a_1/\rho = a_2/\rho \iff a_1\rho a_2$.

Näiteid kongruentsidest

I Olgu meil rühm $(\mathbb{Z}, +)$, $n \in \mathbb{Z}$ ja ekvivalents ρ_n: $a\rho_n b \iff n|a - b$. Siis $\mathbb{Z} = \{0/\rho, 1/\rho, ..., n-1/\rho\}$, kusjuures $a\rho = \{a + kn|k \in \mathbb{Z}\}$. Sellist faktorhulka $\mathbb{Z}/\rho$ nimetatakse jäägiklassiringiks. Lihtne on veenduda, et ρ on tõepoolest kongruents.

II Olgu meil rühm $(\mathbb{Z}, +)$ ja ekvivalents ρ: $= \begin{cases} -1\rho x, \; x < 0 \\ 0\rho x, x = 0 \\ 1\rho x, x > 0 \end{cases}$ Paneme tähele, et tegemist ei ole kongruentsiga. Tõepoolest, $(1, 1), (-2, -1) \in \rho, (-1, 0) \notin \rho$.

III Paneme samas tähele, et eelnevalt defineeritud ekvivalents on kongruents rühma $(\mathbb{Z}, \cdot)$.

Definitsioon 1.4.2. Ω-algebra A faktoralgebraks kongruentsi ρ järgi nimetatakse faktorhulka A/ρ, mille tehted $\omega \in \Omega$ on defineeritud valemiga

$$\omega(a_1/\rho, ..., a_n/\rho) = (\omega(a_1, ..., a_n))/\rho$$

Olgu $\rho \in Eqv(a)$. Saab defineerida kujutise $\pi : A \to A/\rho$, $\pi(a) = a/\rho$. Seda kujutust nimetatakse loomulik kujutus faktorhulgale või ka loomulikuks projektsiooks. Kuna iga ρ-klass koosneb hulga a elementidest, siis on kujutus π sürjektiivne.

Lause 1.4.3. *Kui A on Ω-algebra ja ρ tema kongruents, siis loomulik kujutus $\pi : A \to A/\rho$ on Ω-algebrate sürjektiivne homomorfism.*

Tõestus. Olgu A Ω-algebra ja ρ tema kongruents. Veendume, et loomulik kujutus $\pi : A \to A/\rho$ on sürjektiinve homomorfism. Sürjektiivsus on ilmne - iga ekvivalentsiklass sisaldab hulga A element. Veendume, et π on homomorfism. Valime suvaliselt $\omega \in \Omega$, veendume, et $\omega\left(\pi\left(a_1\right), ..., \pi\left(a_n\right)\right) = \pi\left(\omega\left(a_1, ..., a_n\right)\right)$. Loomuliku kujutuse ja faktoralgebra definitsioonide põhjal saame kirjutada : $\omega\left(\pi\left(a_1\right), ..., \pi\left(a_n\right)\right) = \omega\left(a_1/\rho), ..., a_n/\rho\right) = \left(\omega\left(a_1, ..., a_n\right)\right)/\rho = \pi\left(\omega\left(a_1, ..., a_n\right)\right)$. $\square$

Definitsioon 1.4.4. Kujutuse $\phi \colon A \to B$ tuumaks nimetatakse binaarset seost ρ hulgal A, mis on defineeritud eeskirjaga:

$$(x, y) \in \rho \iff \phi\left(x\right) = \phi\left(y\right)$$

On kerge kontrollida, et iga kujutuse $\phi \colon A \to B$ tuum on ekvivalentsiseos hulgal A.

Lause 1.4.5. *Iga Ω-algebrate homomorfismi $\phi \colon A \to B$ tuum on algebra A kongruents.*

Tõestus. Veendume, et homomorfismi$\phi \colon A \to B$ tuum on kongruents. Teame, et tegemist on ekvivalentsiga, seega jääb kontrollida, et suvaline $\omega \in \Omega$ korral kui $\left(a_1, b_1\right), ..., \left(a_n, b_n\right)$ siis ka $\left(\omega\left(a_1, ..., a_n\right), \omega\left(b_1, ..., b_n\right)\right)$, mis on samaväärne sellega, et kui $\phi\left(a_1\right) = \phi\left(b_1\right), ..., \phi\left(a_n\right) = \phi\left(b_n\right)$ siis ka $\phi\left(\omega\left(a_1, ..., a_n\right)\right) = \phi\left(\omega\left(b_1, ..., b_n\right)\right)$. Kuna ϕ on homomorfism, siis:

$$\phi\left(\omega\left(a_1, ..., a_n\right)\right) = \omega\left(\phi\left(a_1\right), ..., \phi\left(a_n\right)\right) = \omega\left(\phi\left(b_1\right), ..., \phi\left(b_n\right)\right) = \phi\left(\omega\left(b_1, ..., b_n\right)\right)$$

$\square$

Lause 1.4.6. *Kui ρ on Ω-algebra A kongruents, siis loomuliku homomorfismi $\pi \colon A \to A/\rho$ tuum on ρ.*

Tõestus. Veendume, et $Ker\,(\pi) = \rho$. Veendume, et $Ker\,(\pi) \subset \rho$. Olgu $(a,b) \in Ker\,(\pi) \implies \pi\,(a) = \pi\,(b) \implies a/\rho = b/\rho \implies (a,b) \in \rho$. Teistpidi, olgu $(a,b) \in \rho$, siis $a/\rho = b/\rho \implies \pi\,(a) = \pi\,(b) \implies (a,b) \in Ker\,(\pi)$. $\square$

Teoreem 1.4.7. *Kui ϕ: $A \to B$ on Ω-algebrate sürjektiinve homomorfism ja ρ on ϕ tuum, siis $B \simeq A/\rho$*

Tõestus. Defineerime $\psi : A/\rho \to B, \psi\,(a/\rho) := \phi\,(a)$. Kas on definitsioon on korrektne, st kas ψ on üheselt määratud ? Ehk kas $a_1/\rho = a_2/\rho \iff \phi\,(a_1) = \phi\,(a_2)$. Siit saaksime kätte ka injektiivsuse. Piisab arvesse võtta, et eelnev tähendab, et $a_1/\rho = a_2/\rho \iff a_1\rho a_2$, ning kuna ρ on ϕ tuum, siis $(a_1, a_2) \in Ker\,(\phi)$. ψ sürjektiivsus tuleneb otse ϕ sürjektiivsusest. Järelikult on ψ bijektsioon. Kas ψ on homoformism ? Olgu $\omega \in \Omega_n$ ja $a_1, ..., a_n \in A$.

$$\psi\,(\omega\,(a_1/\rho, ..., a_n/\rho)) = \psi\,(\omega\,(a_1, ..., a_n)\,/\rho) = \phi\,(\omega\,(a_1, ..., a_n)) = \\ = \omega\,(\phi\,(a_1)\,, ..., \phi\,(a_n)) = \omega\,(\psi\,(a_1/\rho)\,, ..., \psi\,(a_n/\rho))$$

$\square$

Lause 1.4.8. *EI SAA ARU Olgu ρ Ω-algebra A kongruents, $D \leq A/\rho$ ning π kongurgentsi ρ tuum. Siis $D \simeq C/\rho|_C$, kus $C = \pi^{-1}(D)$.*

Tõestus. Olgu $\pi^{-1}(D) = C \leq A$. Olgu α π ahend C-le ($\alpha = \pi|_C$). Siis $\alpha : C \to D$, α on homomorfism. Väidame, et α on sürjektiinve. Kuna π oli sürjektiinve, siis $\forall y \in A/\rho\ \exists x \in A, \pi(x) = y$. Seega $\alpha(x) = y$. $\square$

Viimane lause näitab, et mistahes algebra A faktoralgebra alamalgebra on alati isomorfne sama algebra A mingi alamalgebra faktoralgebraga. Vastupidine ei ole üldiselt võimalik.

1.5 Faktoralgebra faktoriseerimine

Tekib küsimus, kui kaks korda faktoriseerime, mis siis juhtub, kas me saame midagi uut ? Tuleb välja, et kahekordset faktoriseeringut on võimalik asendada isomorfismi täpsuseni üks kord faktoriseerimisega.
Olgu antud ρ ja σ Ω-algebra A kongruentsid, kusjuures $\rho \leq \sigma, (x,y) \in \rho \implies (x,y) \in \sigma$. Defineerime faktoralgebral A/ρ binaarse seose:

$$\sigma/\rho = \{(x/\rho, y/\rho)\,|(x,y) \in a\sigma\}$$

Võime veenduda, et nii defineertus seos σ/ρ on faktoralgebra A/ρ kongruents.

Teoreem 1.5.1. *Olgu A Ω-algebra, $\rho, \sigma \in Con(A)$, kusjuures $\rho \leq \sigma$. Siis σ/ρ on faktoralgebra A/ρ kongruents. Veel enam, faktoralgebra A/ρ iga kongruents omab kuju σ/ρ, kus $\sigma \in Con(A)$ ja $\rho \leq \sigma$. Sealjuures algebrad $(A/\rho)/(\sigma/\rho)$ ja A/σ on isomorfsed.*

Tõestus. Veendume esimese s väites. Tõepoolest, pannes tähele, kuidas on defineeritud faktoralgebra tehted, on lihtne veenduda, et tõepoolest σ/ρ on faktoralgebra kongruents. Olgu $\omega \in \Omega_n$, $(a_i/\rho, b_i/\rho) \in \sigma/\rho \implies (a_i, b_i) \in \sigma \implies (\omega(a_i), \omega(b_i)) \in \sigma \implies (\omega(a_i)/\rho, \omega(b_i))/\rho \in \sigma/\rho$. Teoreemi teise osa tõestus: Olgu $\tau \in Con(A/\rho)$. Defineerime kongruentsi σ_0 järgnevalt: $(x, y) \iff (\pi(x), \pi(y))$. Lihtne on veenduda, et $\sigma_0 \in \mathrm{Con}(A)$. Tõepoolest, see, et $\sigma_0 \in \mathrm{Eqv}(A)$ on ilmne. Veendume, et $\omega \in \Omega_n$ korral $(a_i, b_i) \in \sigma_0 \implies (\omega(a_i), \omega(b_i))$. Olgu $(a_i, b_i) \in \sigma_0$, vastavalt definitsioonile siis $(\pi(a_i), \pi(b_i)) \in \tau$, kuna τ on kongruents, siis ka $(\omega(a_i)/\rho, \omega(b_i)/\rho) \in \tau$, seega ka $(\omega(a_i), \omega(b_i)) \in \sigma_0$. Viimase osa tõestuseks paneme tähele, et A/ρ faktoriiseerimine a/ρ järgi kitsendab ekvivalentsiklasse ning loomulik kujutus $\pi\colon A/\rho \to (A/\rho)/(\sigma/\rho)$ on homomorfism. □

Järeldus 1.5.2. *Olgu A Ω-algbra ja $\rho \in Con(A)$. Siis on olemas sisalduvusega kooskõlas olev üksühene vastavus faktoralgebra A/ρ kõig kongruentside ja algebra A kõigi nende kongruentside vahel, mis sisaldavad kongruentsi ρ*

Tõestus. küsi, ei tea □

Igas hulgal A on kaks erilist ekvivalentsiseosst: $\triangle_A$ ja $\bigtriangledown_A$. Esimene neist on võrdusseos hulgas A: $\triangle_A = \{(a, a) \mid a \in A\}$, teine aga kogu otsekorrutis $A \times A$. On selge, et $\triangle_A$ ja $\bigtriangledown_A$ on vastavalt vähim ja suurim ekvivalentsiseos hulgal A. Samuti on lihtne veenduda, et kui A on Ω-algebra, siis need kaks ekvivalentsiseost on selle algebra kongruentsid.

Definitsioon 1.5.3. Algebrat, millel on täpselt kaks kongruentsi: $\triangle_A$ ja $\bigtriangledown_A$, nimetatakse lihtsaks.

Järeldusest 1.5.2 tuleneb otseselt järgmine järeldus.

Järeldus 1.5.4. *Faktoralgebra A/ρ on lihtne parajasti siis, kui kongruents ρ on maksimaalne.*

1.6 Rühmade, ringide ja vektorruumid faktoriseerimine

Definitsioon 1.6.1. Olgu G rühm ja H tema alamrühm. Siis hulki $aH = \{ah | h \in H\}$ $(Ha = \{ha | h \in H\})$, kus $a \in G$, nimetatakse alamrühma H vasakpoolseks (parempoolseks) kõrvalklassideks rühmas G.

Definitsioon 1.6.2. Rühma G alamrühm H nimetatakse normaalseks, kui iga $a \in G$ ja $h \in H$ korral $a^{-1}ha \in H$.

Lause 1.6.3. *Rühma G alamrühm H on normaalne parajasti siis, kui iga $a \in G$ korral $aH = Ha$.*

Tõestus. Olgu H normaalne, s.t. $\forall a \in G,\ h \in H \implies a^{-1}ha \in H$. Fikseerime $a_0 \in G$, veendume, et $a_0H = Ha_0$. Olgu $z \in H \implies az \in aH$, $az = aza^{-1}a$. H normaalsuse tõttu $y = aza^{-1} \in H$, seega $az = ya$ ehk $aH \subset Ha$. Analoogiliselt saame näidata ka et $Ha \subset aH$. Olgu nüüd $aH = Ha$ ja olgu $ah \in aH$, siis $\exists h' \in H\colon ah = h'a$. Korrutame mõlemat poolt a pöördelemendiga, saame, et $aha^{-1} = h' \in H$. □

Teoreem 1.6.4. *Kui ρ on rühma G kongruents, siis G ühikelementi sisaldav ρ-klass $1/\rho$ on rühma G normaalne alamrühm. Vastupidi, kui H on rühma G normaalne alamrühm, siis leidub täpselt üks rühma G kongruents rho, mille korral $1/\rho = H$. Selle kongruentsi klassid on täpselt H kõrvalklassid rühmas G, täpsemalt, iga $a \in G$ korral $a/\rho = aH$.*

Tõestus. Esimest poolt lihtne näidata: $(x,1) \in \rho, (y,1) \in \rho \implies (x \cdot y, 1 \cdot 1 = 1), (x,1) \in \rho \implies (x^{-1}, 1^{-1} = 1) \in \rho$, $(a^{-1}, a^{-1}) \in \rho, (x,1) \in \rho, (a,a) \in \rho \implies (a^{-1}xa, a^{-1}1a = a^{-1}a = 1) \in \rho$. Teine pool:Olgu H normaalne alamrühm. Veendume, et kõrvalklassid on lõikumatud. Tõepoolest, olgu $aH \cap bH \neq \emptyset$. Siis leidub $c \in aH \cap bH$, s.t $c = ah_0 = bh_1$, seega $a = bh_1h_0^{-1} = bh_2 \in bH$, $z \in H, az = bh_2z = bh_3 \in bH$, analoogiliselt saame näidata teistpidist sisalduvust, seega $aH = bH$. Defineerime $a\rho_0 b \iff aH = bH$. Paneme tähele, et siis $1/\rho = H$. Veendume, et defineeritu on kongruents: $a_iH = b_iH \implies a_i = b_ih_i$, siis $a_1a_2 = b_1h_1b_2h_2 = b_1b_2\left(b_2^{-1}h_1b_2\right)h_2 = b_1b_2h_0h_2 = b_1b_2h_0 \in b_1b_2H$. Miks teisiti ei saa kongruentsi defineerida?. □

See teoreem ütleb, et iga rühma G korral on olemas üksühene vastavus normaalsete alamrühmade ja kongruentside vahel. Järelikult võime rääkida faktorrühma moodustamisest sellele alamrühmale vastava kongruentsi järgi. Seda arvestades jõuame järgmise definititsioonini.

Definitsioon 1.6.5. Rühma G faktorrühmaks normaalse alamrühma H järgi nimetatakse rühma, mille elementideks on H kõrvalklassid rühmas G, kusjuures nende korrutamine toimub jargimse eeskirja kohaselt: $aH \cdot bH = (ab)H$. Seda rühma tähistatakse G/H.

Samuti, arvestades üksühest vastavust rühma kongruentside ja normaalsete alamrühmade vahel võib rühmade homomorfismi tuuma defineerida mitte kui kongruentsi vaid kui selle ühikelementi sisaldavat klassi. Nii rühmateoorias ka tavaliselt tehakse.
Seega, kui $\phi\colon G \to H$ on rühmade homomorfism, siis ϕ tuumaks nimetatakse G normaalset alamrühma $\{x \in G|\phi(x) = 1\}$, mida tähistatakse $\mathrm{Ker}(\phi)$.
Saame ümber sõnastada kaks Ω-algebrate jaoks tõestatud tulemust:

Lause 1.6.6. *Kui H on rühma G normaalne alamrühm, siis loomulik homomorfism $\pi\colon G \to G/H$ tuum on H.*

Teoreem 1.6.7. *Kui $\phi\colon G \to H$ on rühmade sürjektiivne homomorfism, siis $G \simeq H/Ker(\phi)$,*

1.6.1 Lagrange'i teoreem

Lõpliku rühma järk(elementide arv) jagub tema iga alamhulga järguga.

1.6.2 Ω-algebrate otsekorrutis

Viis kuidas saada mitmest algebrast uus algebra.
Võime defineerida funktsioonid, mis kirjeldavad jadasid. $\phi : \mathbb{N} \to \cup_{i\in\mathbb{N}} A_i$, mis rahuldab tingimust $\phi(i) \in A_i$, iga $i \in \mathbb{N}$ korral.
Projektsioonid - seavad jadale vastavuse mingi kindla elemendi. Tähistame π_i.

1.6.1

Tõestus $\omega \in \Omega_n, a^1 = (a_i^1)_{i\in I}, ..., a^n = (a_i^n)_{i\in I} ...$

1.6.3 Võred

(Osaliselt) Järjestatud hulk Binaarne seas, mis on refleksiivne, transitiivne ja antism̈eetriline. Lineaarselt järjestatud hulk on selline, kus iga element on mingis seoses iga teisega.

Teoreem 2.2.1

Tõestus 4) Neeldevus (absorbtion)
Tarvilikkus:
$x \leq y \iff x = xaluminerajay$

1.7 Loeng V

$[a, b] = \{x \in L | a \leq x \leq b\}$
$Con(A/\rho) \longleftrightarrow \{\sigma \in Con(A) | \rho \leq \sigma\}$

Teoreem 2.2.2 Distributiivsed võred.

Lause 2.3.1 Ahelad on distributiivsed võred.

Lause 2.3.2 Tähtis distributiivne võre $(P(A);\ intersection; union)$
Isendega duaalsus.

Lause 2.3.3

Järeldus 2.3.1

Teoreem 2.3.1 Võre on modulaarne parajasti siis, kui ta ei oma võrega N_5 isomorfset alamvõret. Modulaarne võre on distributiivne parajasti siis, kui ta ei oma võrega M_3 isomorfset alamvõret.

Tõestus. Võrk on modulaarne $\implies$ võrk ei ma N_5 isomorfset alamvõret.
$\forall a, b, c \in L\ a \leq b \implies aylemineraja(baluminerajac) = balumeineraja(aylemінerajac)$
Vastuolu!

$\square$

Tõestus Riina esitab seminaris.

Teorem 2.4.1 Võre on distributiivne parajasti siis, kui ta on isomorfne mingi hulga kõigi alamhulkade võre mingi alamvõrega.

Definitsioon 2.4.1 Võre mittetühja alamhulka F nimetatakse filtriks, kui ta on kinnine alumise raja võtmise suhtes ja koos iga elemendiga a sisaldab ka võre L kõik elemendist a suuremad elemendid.

Märkus Filtri ja algfiltri duaalsed mõisted on vastavalt ideaal ja algideaal.

Definitsioon 2.4.2 Võre L filtrit F nimetatakse algfiltriks, kui sellest, et $aVb \in F$, kus $a, b \in L$, järjeldub $a \in F$ või $b \in F$. Algfilter $F \neq L$.

Zorni lemma Olgu meil järjestatud hulk A. Eeldame, et iga hulga A alamhulk omab ülemist tõket hulgas A. Siis sellest järeldub, et A omab vähemalt ühte maksimaalset elementi. $C \subset Aalamhulk : x, y \in C \implies x \leq y \vee y \leq x$.

Lause 2.4.1 Distributiivse võre iga kahe erivena elemendi jaoks leidub algfilter, mis sisaldab täpselt ühte neist kahest.

Tõestus

Teoreem 2.4.1 Võre on distributiivne parajasti siis, kui ta on isomorfne mingi hulga kõigi alamhulkade võre mingi alamvõrega

Selgitus Olgu L distributiivne võre. Vaja ledia hulk A ja üksühene homomorfism $\Phi : L \to P(A), \Phi(L) \leq P(A), Lisomm\Phi(L)$.

Tõestus

1.8 Rühmad

1.8.1 Faktorrühma faktoriseerimine

Isomorfismiteoreem Olgu H rühma G normaalne alamrühm, B rühma G alamrühm ning A rühma B normaalne alamrühm. Siis $BH/AHisomB/(A(ByhisosaH))$.

Järeldus 3.2.1. Olgu H rühma G normaalne alamrühm ja A rühma G alamrühm. Siis $BH/HisomB/(ByhisosaH)$.

Teoreem 3.2.2. (Zassenhausi lemma) Kui H, H', K ja K' on rühma G alamrühmad, kusjuures H' on normaalne alamrühm rühmas H ja K' on normaalne alamrühm rühmas K, siis
$(HyhisK)H'/(HyhisK')H'isom(KyhisH)K'/(KyhisH')K'$.

Tõestus Idee: näitame, et mõlemad on isomorfsed $HyhisK/(H'yhisK)(HyhisK')$. $H'(HyhisK)/H'(HyhisK')isomHyhisK/(H'yhisK)(HyhisK')$. Kasutame isomorfismiteoreemi. Võtame B rolli $HyhisK$, H rolli sobib H', A rolli võtame $HyhisK'$. Lisaks vaatama G rollis H-d. Kas $hyhisK'normaalnealamryhmHyhisK$?

1.8.2 Normaal- ja kompositsioonijadad

Schreieri teoreem Antud rühmas suvalised kaks normaaljada omavad ekvivalentseid tihedusi.

Tõestus $\{1\} = H_0 < dH_1 < dH_2 ... H_m = G$
$\{1\}]K_0 < dK_1 < dK_2 ... < dH_n = G$
Defineerime $H_{ij} = H_i(H_{i+1}yhisosaK_j)$ ja $K_{ji} = K_j(K_{j+1}yhisosaH_i)$.
Miks $H_{ij} < dH_{i,j+1}$?
Miks $H_i(H_{i+1}yhisosaK_j) < dH_i(H_{i+1}yhisosaK_{j+1})$?

Näide Olgu $m = 2, n = 3$. Siis peavad eelneva põhjal ekvivalentsed olema $H_0 = H_{00} \leq H_{01} \leq H_{02} \leq H_{03} = H_1 = H_{10} \leq H_{11} \leq H_{12} \leq H_{13} = H_2 = G$ ja $K_0 = K_{00} \leq K_{01} \leq K_{02} = K_1 = K_{10} \leq K_{11} \leq K_{12} = K_2 = K_{20} \leq K_{21} \leq K_{22} = K_3 = G$.
Veenduda Sachenhausi lemma põhjal.
$H_{01}/H_{00}isomorfneK_{01}/K_{00}$
$H_{02}/H_{01}isomorfneK_{11}/K_{10}$
$H_{03}/H_{02}isomorfneK_{21}/K_{20}$
$H_{11}/H_{10}isomorfneK_{02}/K_{01}$
$H_{12}/H_{11}isomorfneK_{12}/K_{11}$
$H_{13}/H_{12}isomorfeK_{22}/K_{12}$

1.9 Lihtsad rühmad

Lause 3.4.1 Abeli rühm on lihtne siis ja ainult siis, kui tema järk on algarv

Tõestus Kuna alamrühma järk jagab rühma järke, siis algarvulise järguga rühmal saab olla ainult 2 alamrühma - kogu rühm ja 1 elemendiline rühm. Teistpidi, olgu A lihtne Abeli rühm. $(A,+)$,$0 \neq a \in A$, $\{na|n \in \mathbb{Z}\}$. Kusjuures, kui $n > 0$ siis $na = a + a + ... + a$, kui $n = 0$ siis $0a = 0$. Ja kui $n < 0$ siis $(-n) * a = -(na)$. Elemendi A poolt tektitatdu tsükliline alamrühm. Abeli rühma alamrühm on lihte, seega $A =< a >$.

Teoreem 3.4.1 Kui $n = 3$ või $n \geq 5$, siis rühm A_n on lihtne

Teoreem 3.4.2 Kui $n > 2$ või $n = 2$ ja $|K| > 3$, siis projektiivne spetsiaalne lineaarrühm PSL(n,K) on lihtne.

1.10 Lahenduvad rühmad

Definitsioon 3.5.1. Rühma, mis omab normaaljada, mille kõik faktorid on Abeli rühmad, nimetatakse lahenduvaks.

Teoreem 3.5.1 Lahenduva rühma alamrühmad ja faktorrühmad on lahenduvad.

Tõestus Olgu meil lahenduv rühm G. Kehtigu $\{1\} = H_0 < dH_1 < dH_2 < d... < dH_m = G$. H_{i+1}/H_i on Abeli rühm $i = 0, ..., n-1$.
$A \leq G$, $A_i = AyhiosaH_i$, $A_0 = Ayhisosa\{1\} = \{1\}$, $A_n = AyhisosaG = A$, $i \leq j \implies A_i \leq A_j$.

Teoreem X Iga paaritu arvulise järguga rühm on lahenduv

Tõestus Olgu $|G|$ paaritu. $\{1\} = H_0 < dH_1 < dH_2 < d... < dH_n = G$. Kõik jada faktorit lihtsad lõplikud rühmad. Alamrühma järk jagab rühma järku $\implies$ alamrühmade järgud on paaritud.

1.11 Faktorringi faktoriseerimine

Lause 4.1.1 Kõik korpused on lihtsad ringid. Iga lihtne kommutatiivne ring on korpus.

Tõestus $\{0\} \neq I < dK$. I - ideaal. ...

Lause 4.1.2 Täielik maatriksring $Mat_n(K)$ on lihtne iga naturaalarve n ja korpuse K korral.
AlI - iga vektorruum omab baasi lõplikul juhul lõpmatu mõõtmelise baasi lin sõltumatus - kõik lõpblikud alamhulgad sõltumatud. T.4.4.2 $S = \{X|X \subset V, X on lin.soltumatu\}$ Zorni lemma eeldute kontroll. $\{X_i|i \in I\}, X_i \in S$ Otsime suurimat elementi $X = \sup_{i \in I} X_i$. Kas X kuulub hulka S? ... Zorni lemma eeldus täidetud. S omab maksimaalset elementi, olgu selleks Z. Z on V baas ? Valime $v \in V$, kas $v \in L(Z)$. Oletame, et $v \notin V$, siis $Z \sup \{v\}$ on lin sõltumatu, see on aga vastuolu.
V vektorruum üle K $ei, i \in I$ -V baas. $V isom ringpluss \sum\limits_{i \in I} K_i \; ringpluss \sum\limits_{i \in I} K_i = \{(k_i)_{i \in I}|k_i \in K, |\{j \in L|k_j = 0\}| < \infty\}$
defineerime $\phi : V \to ringpluss \sum\limits_{i \in I} K_i$ nii, et $\phi(v) = (l_i)_{i \in I}, l_i = \begin{cases} k_i, \text{kui} i \in \{i_1, i_2, ..., i_n\} \\ 0, \text{kui} i \notin \{i_1, i_2, ..., i_n\} \end{cases}$

1.12 Ringide esitused ja moodulid

D 4.5.1
A Abeli rühm, End(A) on rühm. Liitimine defineeritud kui $(\phi + \psi)(a) = \phi(a) + \psi(a)$.
T 4.5.1 $\phi : R \to End(M; +)$, iga $r \in R$ kollab tekib loomulik kujutus $l_2 : M \to M, x \to rx$. Sellest võime mõelda kui vasaknihkest. $\phi(r) = l_r$. Veendume, kas definitsioon on korrektne. Esiteks, kas $l_r \in$ End$(M; +)$? $l_2(x + y) = r(x + y) = rx + ry = l_r(x) + l_r(y)$. Veel, $\phi(rs) = \phi(r) * \phi(s)$, $\phi(1) = 1_M$, $l_{r+s} = l_r + l_s$.
D 4.5.2
$\phi : R \to$ End(A). Oletame, et ϕ on üksühene, oletame, et r kuulub Ker(ϕ), $\phi(r) = 0 = \phi(0) \implies r = 0$, seega Ker$(\phi)$ ....
R-moodul M on täpne $\implies$ vastav esitus on täpne. $\phi : R \to$ End$(M; +)$, $\phi(r) = l_r$, Ker$(\phi) = \{0\}$, $l_r(x) = 0 \forall x \in M \iff r = 0$
T 4.5.2 $R isom \phi(R) \leq$ End$(M; +)$.
Ainult null element anuleerib kõik mooduli elemendid.

1.13 Abeli rühmad

POLE SLAIDIL! Idee: näidata, et mooduli ehitus võib olla keerulisem.
Tsükliline R-moodul
Def. R-moodulit nimetatakse tsükliliseks, kui ta on tekitatud ühe elemendi poolt.
Olgu M tsükliline R-moodul, see tähendab $\exists a \in M, M =< a >$. $M = Ra = \{ar | r \in R\}$. $RA \subset < a >$. $ra + sa = (r + s)a$, $s(ra) = (sr)a$. $a = 1 * a \in Ra$.
L. Iga tsükliline R-moodul on isomorfne R-mooduli R faktormooduliga.

Tõestus. $M = Ra$. $\phi : R \to Ra$. $\phi(r) = ra$. Kontrollida homomorfismi. Sürjektiivne, homomorfismi teoreemi põhjal M isomorfne $R/\mathrm{Ker}\,(\phi)$.

□

L 4.5.1
$A \simeq \mathbb{Z}_{k_1} + ring... + ring\mathbb{Z}_{k_n}$
$k, l \in \mathbb{N}, \text{SÜT}(k, l) = 1$ $\mathbb{Z}_{kl} \simeq \mathbb{Z}_k + ring\mathbb{Z}_l$ $\phi(\overbrace{x_k l}) = (\overbrace{x_k}, \overbrace{x_l})$ .... $phibijektsioon$
$|\mathbb{Z}_k l| = kl = |\mathbb{Z}_k + ring\mathbb{Z}_l|$
Lemma 4.6.1
Tõestus: M -[täpne] taandamatu(=lihtne) R-moodul $K = End_R M$, $(K, +, *)$, $\phi, \psi \in K$, liitmine punktikaupa, korrutamine järjest rakendamine. Fikseerime $0 \neq \phi \in K, \phi(M) = \{\phi(m) | m \in m\}, 0 \neq \phi(M) \leq M/implies(eeldus, lihtne)\phi(M) = M$. Uurime ϕ tuuma. $\mathrm{Ker}\phi = \{x \in M | \phi(x) = 0\}$. $\mathrm{Ker}\phi \neq M \implies \mathrm{Ker}\phi = \{0\} \iff \phi$ on bijektsioon.
L 4.7.1
T 4.7.1
Tõestus : M täpne taandumatu R-mooduls. $K = \mathrm{End}_R M$, k^M ruut... , $f \in End_k M, S \subset M$ - lõplik, $\exists a \in R \forall s \in S f(s) = rs$. S võib kästleda kui lõpliku mõõtmelise moodustjaga alamruumi. Tõestuse idee: induktsiooni alamruumi mõõtme järgi. Baas : $S = \{0\}$. $X \subset M$, $\{a \in R | \forall x \in X ax = 0\} = \mathrm{Anh}(X) = X^t agurpidiT$ $Y \subset R. \{m \in M | \forall y \in Y my = 0\} = \mathrm{Anh}(Y) = Y^t agurpidiT$ S lõplik alamruum , $f \in \mathrm{End}_k M \implies r \in R, \forall s \in S, f(s) = rs$, $(f - r) - = 0$. $(f - r)S = 0$.
Tehniline abvahend induktsiooni jaoks: $(S^{tagurpidiT})^t agurpidiT = S$ Olgu väide tõestatud S jaoks, $a \in M\S$, $T = S + Ka = \{s + ka | s \in S, k \in K\}$.
$dim_K T = dim_K S + 1$
$f \in End_K M$ $r \in R, (f - r)S = 0$ leida $r' \in R$, nii et $(f - r')T = 0$, $b = (e - r)e$, leida $u \in R$, nii et $nS = 0$ ja $na = b$. $S^{tagurpidiT} a \subset M$,

$S \subset M \implies S^{tagurpidiT} \subset R$. Kas $S^{tagurpidiT}a \leq_R M$? $x, y \in S^{tagurpidiT} \implies x, y \in S^{tagurpidiT}$, $s \in S, xs = ys = 0 \implies (x+y)a \in S^{tagurpidiT}a$. $x \in S^{tagurpidiT}, r \in R, s \in S$, $(rx)s = r(xs) = r0 = 0 \implies rx \in S^{tagurpidiT}, ...$
1) $S^{tagurpidiT}a = M$ 2) $S^{tagurpidiT}a = \{0\}$.
$a \in (S^{tagurpidiT})^{tagurpidiT} = S$, vastuolu. $t \in T$, $t = s + ka$, $s \in S$, $k \in K$ $(r+u)t = (r+n)(s+ka) = rs + r(ka) + ns + n(ka) = f(s) = k(ra+na) = f(s) + k(ra + (fa) = f(s) + (ka) = f(s-ka) = f(t), r' = r+n$. Jääb näidata, et $T^{tagurpidiTtagurpidiT} = T$.
$T? = T^{tagurpidiTtagurpidiT}$ $T \leq M$ $T^{tagurpidiT} \subset R$ $T^{tagurpidiTtagurpidiT} \subset M$
$TsubsetT^{tagurpidiTtagurpidiT}$ ilmne $T^{tagurpidiTtagurpidiT}?subsetT$
$T = S + Ka$ $a \in M$
S $K = End_R M$ $S^{tagurpidiTtagurpidiT} = S$ $b \in (S^{tagurpidiT}yhisosaa^{tagurpidiT})^{tagurpidiT} \subset M$ $\phi : S^{tagurpidiT}a \to S^{tagurpidiT}b$ $\phi(xa) = xb, x \in S^{tagurpidiT}$. $S^{tagurpidiT}a = \left\{xa | x \in S^T\right\} \leq_R M$ $S^{tagurpidiT}b \leq_R M$ $x, y \in S^{tagurpidiT} \implies x - y \in S$ $xa = ya \implies x - y \in a^{tagurpidiT} \implies x - y \in S^{tagurpidiT}yhisosaa^{tagurpidiT} \implies (x-y)b = 0$ ....
Teoreem 4.8.1

Tõestus. 1) $\implies$ 2) $RprimitiivneArtiniring$ $M - t2pnetaandumatuR-moodul$ $K = End_R korpus$ (üldises mõttes) $\phi : R \to End_K M$ $\phi(r) = l_r$ M - ruutvorm üle K. K^M - lõplikumõõtmeline ? Oletame, et leidub $e1, e2, e3, ...$ lineaarselt sõltumatu süsteem vektorruumis K^M. $S_i =< e_1, e_2, ... > \leq K^M$. $A_1 = S_i^{tagurpidiT} = \{x \in R | xS_i = 0\}, i = 1, 2, 3....$ $\forall i \exists \phi \in EndK^M, \phi(e_i) = 0, \phi(e_{i+1}) \neq 0$ A_i $A_{i+1} \exists r \in R, ...$ $A_i - Rvpidevadi = 1, 2, 3, ..$ A_1 $/...A_2$ $e1, ..., en - K^M baas$ $f \in EndK^M$ $\exists r \in Rre_i = f(ei), i = 1, 2, 3..., n$ $l_2 = \phi(r) = f$.
2) $\implies$ 3) Olgu $Mat_n(K), K$ korpus. Väide: R on lihtne. $\{0\} \neq InormaalnealamruhmR \implies I = R$. $\exists A = (a_{ij}) \in I$ Toome sisse maatriksid $E_{ij} = \begin{cases} e_{ij} = 1 \\ e_{kl} = 0, k \neq ivoil \neq j \end{cases}$ $E_{ij}A = A1ridaAE_{ij} = A1veergiE_{kk}AE_{ll} = a_{kl}E_{kl}$ $a_{kl}^{-1}EE_{kk}AE_{ll} = E_{kl}$ $E_{ij}E_{jm} = E_{im} \forall i, j \in E_{ij} \in I$ $\forall \alpha \in K \forall i, j \alpha E_{ij} \in I$
3) $\implies$ 1 Olgu r lihtne Artini ring, näitame, et ta on primitiivne. R on vasakpoolne moodul üle iseenda. Selle R-mooduli alamoodulid on parajasti R vasakpoolsed ideaalid. Kasutame Artini tingimust, kuna R on Artini ringi siis R omab minimaalset vasakpoolset ideaali (Ei ole nullideaal). $\{0\} \leq L \leq K$. $L - vpideaalid \implies L = \{0\} voiL = \{K\}$. $K - R$-moodul, K on lihtne R-moodul. Kas R-moodul K on täpne? Vaatame hulka $I =$

$\mathrm{Anh}K = \{x \in R | xK = 0\}$. I on R vasakpoolne ideaal, veendume, et I on ka parempoolne ideaal. $x \in I, r \in R$, kas siis $xr \in I$? $(xr)k = x(rk) = 0$, siis kas $I = \{0\}$ või $I = R$. $I = R \implies R \cdot K = \{0\}$... □

Def Ringi nimetatatkse poollihtsaks, kui tema taandumatute moodulite annullaatorite ühisosa on null.
Poollihtsat Artini ringi nimetatakse klassikaliselt poollihtsaks ringiks.
Primitiivne ring on poollihtne.
$R \to \mathrm{End}(M; +)$ $\forall i$ $R \to (\phi_i)\mathrm{End}(M_i; +)$ $\phi : R \to \mathrm{End}(M_1; +)!otsekorrutis...!otsekorrutis\mathrm{End}(M_n$
$\phi(r) = 0 \iff (\phi_1(r), \phi_2(r), ..., \phi_n(r)) = (0, 0, ..., 0)$
$\phi(R) \leq \phi_1(R)!otsekorrutis\phi_2(R)!otsekorrutis...!otsekorrutis\phi_n(R)$
Teoreem 4.8.2 (Artin-Weddenburni teoreem) Ring on klassikaliselt poollihtne parajasti siis, kui ta on isomorfne lõpliku arvu lihtsate Artini ringide otsekorrutisega.

1. Primitiivne ring on poolihtne

2. Primitiivne ringide otsekorrutis on pooltühi ring

   Tõestus. Tõestus Olgu $R = R_1!otsekorrutis...!otsekorrutisR_N$, $R_i - primitiivsedringid$, M_i täpne taandumatu R_i-moodul. $M_1, m \in M_1, r \in R, r = (r1, ..., r2), r_i \in R_i$, $rm = r_1 m$, $l_r : M \to M$.

   R^{M_1} alamoodulid on mooduli $R_1^{M_1}$ alusmooulid ja vastupidi.

   $R \leq \cap AmR^{M_i}, r = (r_1, ..., r_n)$

   $m \in M_i, 0 = rm = (r1, ..., rn)m = r_i m \implies r = 0$ □

3. Olgu R ringide otsekorrutis, $R = R_1!otsekorrutis...!otsekorrutisR_n$. Moodul R vasakpoolsed (parempooled, kahepoolsed) on parajasti R alamhulgad kujul $X_1!otsekorrutis...!otsekorrutisX_n$, kus $X_i \mathrm{on} R_i$ vasakpooled ideaalid.

   Tõestus. $X_i - R_i$... $X\mathrm{on}R_1!otsekorrutis...!otsekorrutisR_n$ vasakpoolne ideaal. $\pi_i : R \to R_i, \pi_i(r_1, ..., r_n) = r_i$, $X_i = \pi_i(X)$, $i \in \{1, 2, ..n\}$. $X = X_1!otsekorrutis...!otsekorrutisX_N, \leq onilmne, x \in X, x = (x_1, ..., x_n), x_i \in R_i$, $x_i = \pi_i(x) \in X_i$. $X_i onR_i$ vasakpoolsed ideaalid ? $r_i \in R_i, x_i \in X_i$. Kas $r_i x_i \in X_i$? $r = (0, ..., r_i, 0, ..., 0) \in R$ $x = (x_1, ..., x_i, ..., x_n) \in X$ $rx = (0, ..., 0, r_1 x_i, 0, ...0) \in X$ $r_i x_i \in X_i$ Kas $X_1!otsekorrutis...!otsekorrutis \subset X$? Valime suvalise elemendi $(X_1, ..., X_n) \in X_1!otsekorrutis...!otsekorrutisX_n$.

Kas sellest järeldub, et $(x_1, 0, ..., 0) \in X$? $(x_1, x_2', ..., x_n') \in X, x_2' \in R_{j1} \geq 2$. $(1, 0, ..., 0)(x_1, x_2', ..., x_n') = (x_1, 0, 0, ...0) \in X$. $\square$

4. Lõpliku arvu Artini ringide otsekorrutis on ka Artini ring.

   Tõestus. Olgu $R1, ..., R_n$ Artini ringid, $R = R_1!otsekorrutis...!otsekorrutisR_n$. $X^{(1)} \subset X^{(2)} \subset ... \subset X^{(n)}$ - kahanev vasakpoolsete ideaalide jada. $X^{(j)} = X_1^{(j)}!otsekorrutis...!otsekorrutisX_n^{(j)}, X_i^{(j)}$...... $\square$

5. Kui meil on L minimaalne vasakpoolne ideaal, kusjuures $L^2 \neq 0$, siis leidub $1 \in L$, nee et $e = e^2$ ja $L = Le = Re_n$.

   Tõestus. $L^2 \neq 0 \implies \exists a \in L, La \neq 0$, $La \subset L$, La on mooduli R vasakpolone ideaal - $x \in La$, $r \in R, \exists y = ya, rx = r(ya) = (ry)a \in La$, sest $ry \in L$. Kas $La = L$? $\exists e \in L, ea = a$. $ea = e(ea) = e^2a, (e - e^2)a = 0, e - e^2 \in \mathrm{Anh}\,(a)!yhisosaL$ vasakpoolne ideaal. $\{x \leq R | xa = 0\}$, $Rv.pideaal$ ..... $\square$

6. Kui I on Artini ringi minimaalne ideaal ja $I^2 \neq 0$, siis leidub $e \in I$, nii et $e' = e$ ja $\forall x \in I$, $exe = x$.

   Tõestus. $L \subset I$, vähim vasakpoolne ideaal. Veendume, et $L^2 \neq 0$. Kõigepealt, $LI \neq 0$. Kui $LI = 0$, siis $L \subset \mathrm{Anh}\,(I)!yhisosaI$, $\mathrm{Anh}\,(I)$ on R vasapoolne ideaal. $x \in \mathrm{Anh}\,(I)\,, r \in R$ Kas $xr \in \mathrm{Anh}\,(I)$? Olgu $y \in I$, $(xl)y = x(ly) = 0$, kuna $xin\mathrm{Anh}\,(I)$. $\mathrm{And}\,(I)!yhisosaI$, I on vähim ideaal, yhisosa on ideaal, järelikult $\mathrm{Anh}\,(I)!yhisosaI = I$.... Kas $Re_1 + Re_2 + ... + Ren = I$? Kuna $e_3(e_1 + e_2 - e_1e_2)$... $I = Re_1!otsesumma(\mathrm{Anh}\,(e_1)!yhisosaI)$

   (a) $Re_1!yhisosa(\mathrm{Anh}\,(e_1)!yhisosaI) = \{0\}$

   (b) $I = Re_1 + (\mathrm{Anh}\,(e_1)!yhisosaI)$

   $\mathrm{Anh}\,(e_1)!yhisosaI = Re_2!otsesumma(\mathrm{Anh}\,(e_1, e_2)!yhisosaI)$ $\mathrm{Anh}\,(X) = \{r \in R | \forall x \in Xrx = 0\}$ $\mathrm{Anh}_v(X)$ - vasakapoolne anhilaator $\mathrm{Anh}_p(X)$ - parempoolne anhilaator Olgu $I = Re, e^2 = e$ $R = I!otsesumma\mathrm{Anh}_v(e), j := \mathrm{Anh}_v(e)$ $x \in I$ $ex - x \in I$ Kas $ex - x = 0$? $y \in I$ $\exists l \in R, y = re$ $y\,(ex - x) = re\,(ex - x) = re^2x - rex = 0$ $ex - x \in \mathrm{Anh}_p(I)!yhisosaI$ Kas $\mathrm{Anh}_p(I)!normaalne_alamryhmR$? $x \in \mathrm{Anh}_p(I)$ $y \in I, r \in R$ $y\,(rx) =$

$(yr)\,x = 0$, kuna $(yr) \in I ...$ $I = eRe = eIe$, $eIe \subset eRe\ subsetI$ $x \in I, x = xe = e(xe)$ ... $1 \in R$ $1 = a - b, a \in I, b \in J$ $x \in R, x = y + z, y \in I, z \in J$ $x = x \cdot 1 = (y+z)(a+b) = ya + yb + za + zb$, $yb, ze \in I!yhisosaJ \implies yb, za = 0$, $ya + yb + za + zb = ya + zb$, $ya \in I, zb \in J \implies y = yb, z = zb$. Sarnase arutluskaigu alusel, $y = ay, z = bz$, seega $a = e$,... $R!isomeetrilineI!otsekorrutisJ$ $x \to (y,z), (y,z) \to x$ □

7. Teoreemi toestus

Tõestus. Olgu $R!isomeetirilneMat_{m_1}(K_1)!otsekorrutis...!otsekorrutisMat_{m_n}(K_n)$ Kas R on klassikaline poollihtne ?

(a) R on Artini ring Kas $R = Mat_m(K)$ on Artini ring ? $L \subset R$, vasakpoolsed ideaalid, $A \in L$, $\alpha \in K$, $(\alpha E)A = \alpha EA = \alpha A\ inR...$

(b) R on poollihtne Piisavus $\exists$täpne taandumatu R_i maadul M_i, $i \in \{1,2,...,n\}$. $i = 1$. $x \in M_1, r \in R$ $r = (r_1, ..., r_n)$ $rx := r_1 x$ R-moodul M_1 alammoodulid $= R_1$ moodul M_1 alammoodulid. $!yhisosa!limits_{i=1}^{n}\mathrm{Anh}_R(M_i) = \{0\}$ $r \in R, r \in !yhisosa!limits_{i=1}^{n}\mathrm{Anh}_R(M_i)$... Tarvilikus Eeldame, et R on klassikaliselt poollihte ring.R on Artini ring (vastavalt defile). $I!normaalnealamryhmR$, I minimaalne vasakpoolne ideaal. Kas $I^2 \neq 0$. Eeldame vastuväiteliselt, et $I^2 = 0$. $\exists$ taandumatu R-moodul M, nii et $IM \neq 0$. (Muidu vastuolu millegagi) $\exists m \in M, Im \neq 0$, siis Im on R-mooduli M alammoodul. Kaks võimalust, kas $Im = M, Im = \{0\}$, teine variant eelduse kohaselt ei sobi. Vaatleme esimest varianti, olgu $a \in M, x \in I$, $\exists y \in I, a = ym$, $xa = x\,(ym) = (xy)\,m = 0m = 0 \implies IM = 0$, mis on vastuolu. Saame kasutada eelnevalt tõestatud.

$R!isomeetrilineI!otsekorrutisJ$ $R = I!otsesummaJ$, $J!normaalnealamryhm$ I on ... Artini ring. On Artini Ring? $L \subset I, I$ on vasakpoolne ideaal. $x \in Z, r \in R, r = a + l, a \in I$ $rx = (a+b)x = ax + bx = ax \in L$ L - R minimaalne vasakpoolne ideaal,... I-s. $IL \neq 0$, L - taandumatu R-moodul. L on vaadelduav kui I-moodul.Kas I-moodul on täpne ja taandumatu ? $0 = l \in L$. Kas $Il = L$? , IL on R-vasakpoolneideaal, järelikul $Il = L$, kuna puuduvad mittetirivaalsed R-vasakpoolsed ideaalid. Kas $\mathrm{Anh}_I\,(LI = \{0\})$? $\mathrm{Anh}_R\,(R)!yhisosaI!normalanealamryhmi \subset I$, peab olema I. $R = R_1!otsekorrutisT_1, R_1 = Mat_{m_1}\,(K_1)\,, Anh_R R_1 = T_1$ □

1.14 Väändeta ja perioodiline Abeli rühmad

Olgu A Abeli rühm. Siis iga element $a \in A$ moodustab A alamrühma - $< a > \leq A$. 0 järk on 1.
def perioodiline - rühm on perioodiline, kui tema kõik elemendid on lõpliku järku.
def Rühm, mille kõIk elemendid peale ühikelemine on lõpmatut järku, nimetatatkse väändeta rühmaks.
def Segarühm ei ole kumbagi.
Näited $(R;+)$ väändeta rühm? Koik lõplikud rühmad on perioodilised.
$Z_n!isomA_i, i \in I$ (Lõpmatu). $!otsesumma \sum_{i \in I} A_i$ - lõpmatu perioodiline rühm.
$R* = R$
$\{0\}, (R*, \cdot), -1$ rikub ära ja teeb segarühmaks. $(C*, \cdot)\alpha \in C* \exists n \in N \alpha n = 1$.
def Rühma A perioodiliseks osaks nimetatakse tema kõigi lõpliku järku elementide hulk.
lause Abeli rühma perioodiline osa on selle rühma alamrühm.

Tõestus. $(A;+)$ Abeli rühm. $T(A)$ - A perioodiline osa. $a, b \in T(A)$. $a \in T(A) \iff \exists n \in N, na = 0$ $\exists m, n \in N, ma = 0 = nb$ $ms \in N$ $mn(a+b) = mna + mnb = n(ma) + m(nb) = 0$ $a + b \in T(A)$. □

Lause Abeli rühma faktorrühm on oma perioodilise osa järgi on väändeta rühm.

Tõestus. $(A;+)$ Abeli rühm. $a \in A, a + T(A) \in A/T(A)$ $a \notin T(A)$. $n \in N, n\,(a + T\,(A)) = 0 + T(A)$ Samas, $na + TA = n\,(a + T\,(A))$, $na \in na - 0 \in T(A)$. $\exists n \in N(mn)a = m(na) = 0$. □

A Abeli rühm. $B \leq A$ $A = B!plusspunktT(A)$ $B!isomorfneA/T(A)$
p algarv
def Abeli rühma p-komponendks nimetatakse selle rühma kõigi nende elementide hulka mille järk on p aste.
Lause. Abeli rühma kõik p-komponendid on selle rühma alamrühmadega.

Tõestus. $T_p(A)$- A p-komponent. $a, b \in T_p(A)$. a jark p^m b jark p^n. $p^m a = 0 = p^n b$ $m \leq n$ $p^n(a+b) = p^n + p^n b = 0$ Vaja naidate, et $< a + b >$ $!isomorfne\mathbb{Z}_{p^k}$. Oletus: $a + b$ jark on l. $p^k = ql + r$, $q, r \in \mathbb{Z}, 0 \leq r < l$ $0p^k(a+b) = gl(a+b) + r(a+b) = r(a+b) \implies r = 0$ □

Teoreem Iga perioodiline Abeli rühm on oma p-komponentide otsesumma.

Tõestus. Olgu $p_1 = 2, p_2 = 3, p_3 = 5,... T_i(A) = T_{p_i}(A)$ Kas $A =! sisemineotsesumma \sum_{i \in N} T_i(A)$? Kas $A \subset ! sisemineotsesumma \sum_{i \in N} T_i(A)$? Teistpidi ilmne. $a \in A, \exists n \in N, na = 0, n = p_1^{k_1}, ..., p_n^{k_n}$ $n_i = \frac{n}{p_i^{k_i}}$. SÜT$(n_1, ..., n_k) = 1$ $\exists t_1, ..., t_k \in \mathbb{Z}, 1 = t_1 n_1 + ... + t_k n_k$. $a = 1 \cdot a = (t_1 n_1 + ... + tkn_k)a = t_1(n_1 a) + ... + t_k(n_k a)$ Kas $n_i a \in T_i(A)$? $t_i(n_i a) \in T_i$........... ☐

1.15 Poolrühmad

1.15.1 Teisinustes poolrühmad

Cayle teoreem - iga rühm on isomorfne mingi teisenduste rühmaga. $(G; \cdot)$ - rühm. Vastavalt Cayle teoreerimle $\exists A, G! isomorfne$ rühma $S(A)$ (kõik bijektiivsed teisenudse) alamrühmaga.

Tõestus. $A = G$ sobib, $g \in, lg : G \to G, l_g(x) = gx, lg \in S(G)$. $\phi : G \to S(G)$ $\phi(g) = l_g$. Kas phi on injetiivne? $g, h \in G, l_g = l_h$ $g = g \cdot 1 = l_g(1) = l_h(1) = h \cdot 1 = h$ $l_{gh} = l_g l_h$ $x \in G$ $l_{gh}(x) = (gh)x = g(bx(= l_g(l_h(x)) = (l_g l_h)(x)$ $T(A) =$ kõigi teisenduste hulk hulgal A. ☐

....

1.15.2 Vabad poolrühmad

F vaba poolrühm baasgia B. $B = \{b_1, ..., b_n\}$ F elemenidid - sõned tähestikus B. B tähestiks F_B - kõigi lõpliku sõnade hulk tähestikus B Miks poolrühm on vaba ?

Tõestus. S suvaline poolrühm. $s_1, ..., s_n \in S$ Kas leidub homomorfism $\phi : F_B \to S$, nii et $f(b_i) = s_i$? $\phi(b_{i_1}, ..., b_{i_m}) = s_{i_1} ... s_{i_m}$ ....

☐

def 6.1.1 $F_X ! yhend \{\emptyset\}$ $S =< a >$ poolrühm. $S = \{a^k | x \in \mathbb{N}\}$ $(N, +)$, $\phi : \mathbb{N} \to S$, $\phi(k) = a^k, \phi(k + l) = a^k \cdot a^l$
$K \neq l \implies a^k \neq a^l$, lõpmatu ... poolrühm , $! isom(\mathbb{N}, +)$. $\exists k, l, k \neq l, a^k = a^l$, valime miminaalse võimaliku k, valime minimaalse võimaliku l, $a, a^2, ..., a^k, a^{k+1}, ..., a^{l-1}$. $S = \{a, a^2, ..., a^{l-1}\}$. Kui kuskil $k \neq l$, $a^k = a^l$, siis see on lõplik.

$G = \left\{a^k, ..., a^l - 1\right\}$ $|G| = (l-1) - (k-1) = l - k = n$ $\phi : G \to (\mathbb{Z}_{\ltimes}, +)$
$\phi(a^i) =! j22giklassi$
Olertame, et $i, j \geq k, a^i = a^j \iff n|i - j$ $G!isomorfne(\mathbb{Z}, +)$
def 6.2.2
Lause 6.2.1

1.15.3 Regulaarsed ja inverssed poolrühmad

def 6.3.1
Lause 6.3.1

Tõestus. A hulk $T(A)$ kõigi teisenudse poolrühm hulgal A $\phi \in T(A)$ $\psi \in T(A), \phi = \phi\psi\phi$ $\forall a \in A, \phi(a) = \phi(\psi(\phi(a))))$ psi - paneb vastavusse ühe originaalidest, suvaline A element, kui argument ei oma originaali. □

Lause 6.3.2

Tõestus. $(Mat_n(K); \cdot), K$ korpus. Vaatleme maatrikseid kui lineaarteisendusi. $Mat_n(K)!isomEnd(V)$ $V-$ n-mõõtmeline vektorruum üle K. $\phi \in$End(V) $\psi \in End(V)$ $\phi = \phi\psi\phi$ $\forall x \in V, \phi(x) = \phi(\psi(\phi(x)))$ $Im(\phi) = W \leq V, Im(\phi) = \{\phi(x)|x \in V\}$ $\{e1, ..., e_n\} - Wbaas$ Valime iga i jaoks $a_i \in V$, nii et $\phi(a_i) = e_i$ $\psi(e_i)a_i, kuii \in \{1, .., m\}, else0$ $a \in V$ $\phi(a) \in Im(V)$ ... □

def 6.3.2
lause 6.3.3

Tõestus. S - reg. poolrühm $a \in S$ $\exists b, aba = e$ Kas $bab = b$? $c = bab$ $aca = ab(aba) = aba = a$ $cac = bab(aba)b = b(eba)b = bab = c$ □

def 6.3.3
näited:
rühm on inversne.
Rühm G $a, b \in G$ $aba = a \implies ab = 1 \implies b = a^{-1}$ $bab = b$
Olgu S poolvõre.
$a \in S$, $aaa = a$. Oletame, et $aba = a, bab = b$, $aba = a \implies a \leq b, bab = b \implies bleqa, \implies a = b$
Teoreem 6.3.1

Tõestus. Tarvilikkus: S on inversne poolrühm, $e, f \in S$, $e^2 = e, f^2 = f, x - ef$ ivresne element. $efxef = ef, xefx = x$, $fxe \cdot fxe = f(xefx)e = f(x)e$ Seega fxe on idempotent, fxe on fxe inversne element. $ef \cdot fxe \cdot ef = efxef = ef$ $fxe \cdot ef \cdot fxe = fxefke = fxe$, seega ef on fxe inverrse elment, seega $fxe = ef$. $ef = fxe = fef$, $ef = fxe = efe$, $fef = ef = efe$ Vahetades e ja f rollid, saame, te $ef = fe$. □

Teoreem 6.3.2

Tõestus. A hulk, $PT(A)$ - kõik osalised bijektsioonid Korrutis $g(f(x)), x \in A, f(x) \in Y, Y = \{y \in A | g(y) \in A\}$
Kas on regulaarne ? $(x \in S \implies \exists t \in S, s = sts$ Sobib pöördkujutis. $PT(A)$ idempotentidid ? Alamhulkade samasusteisendused. Oletame, et $\phi \in PT(A), \phi^2 = \phi, Dom(\phi^2) = Dom(\phi), In(\phi^2) = In(\phi)$. Seega, iga $b \in B\phi^2(b) = \phi(b)$, seega $\phi(\phi(b)) = \phi(b)$, üksühesuse põhjal $\phi(b) = b$. Miks nad kommuniteeruvad? Valime kaks alamhulka B, C, saame kaks idemponeti, mille korrutis on $id_B \cdot id_C = id_{B!yhisosaC}$. Oletame, et meil on $\phi, \psi \in PT(A)$, $Dom(\psi\phi) = \phi^{-1}(I_m\phi!yhisosaDom(\psi)$. Korrutise määramispiirkond $Dom(id_C \cdot id_B) = id_b^{-1}(C) = \{x \in B | id_B(x) \in C\} = B!yhisosaC$.
Teine pool: Olgu S inversne poolrühm, valime $A = S$. $s \in S$, $s \to l_s$, kus l_s on defineeritud teatul alamhulgal, nii et ta oleks bijektiivne. $Dom(l_s) = s'S$, s' elemendi s inversne element. $im(l_s) = sS$, $l_s : s'S \to sS$, vasaknihe, st $l_s(x) = sx, x \in s'S$, $x, y \in s'S$, kas $sx = sy \implies y = x$, $x = s'u$, $y = s'v$, $u, v \in S$, $ss'u = ss'v$, korrutame vasakult s', $s'ss'u = s'ss'v$, siit aga $s'u = s'v$, arvestades x, y def, olemig saanud implikatsiooni kehtivuse. Kas kujutus on sürjektiivne ? Võtame mistahes elemendi, $sx \in sS$, $sx = ss'sx = l_s(s'sx) \in s'S$. $\Phi : S \to PT(A)$, $\Phi(s) = l_s$, miks see kujutus on üksühene? Φ üksühesus: Olgu $s, t \in S, l_s = l_t$, siis $Dom(l_s) = Dom(l_t)$, arvestame, et $s'S = l_s$ ja $t'S = l_t$. $s = ss's = l_s(s's) = lt(s's) = ts's$, analoogiliselt $t = st't$, paneme kokku : $s = ts's = tt'ts's = t(t't)(s's)$, idempotent, kommunteerub, $(ts's')t't = st't = t$. Kas $l_st = l_s \cdot l_t$? Veendume, et $(st)'S = Dom(l_st) = Dom(l_s \cdot l_t) = l_t^{-1}(s'S)$. ABitulemus : $(st)' = t's'$, ühesuse põhjal piisab näidata, et sobib see element : $(t's')(st)(t's') = t'(s's)(tt')s' = (t'tt')(s'ss') = t's'$, $(st)(t's')(st) = st$. Kas $t's'S \subset l_t{-}1(s'S)$? Kas suvaline x kuulub sinna ? $x \in S, l_t(t's'x) = tt's'x = (tt')(s's)s'x = s'(stt's'x) \in s'S$. Kas $l_t^{-1}(s'S) \subset (st)'S$? $l_t^{-1}(s'S) = \{x \in t'S | tx \in s'S\}$ $x \in t'S$. Kas $tx \in s'S \implies x \in t's'S$? $x = t'y, y \in S$, $x = t'y = t'tt'y = t'tx = t's'z, z \in S, \in t's'S$.

□

1.16 Universaalalgebra

1.16.1 Alamotsekorrutis

Def 7.1.1
$A \le \prod\limits_{i \in I} A_i$ $\forall j \in I \forall x \in Aj$ $\exists (a_i)_{i \in I} \in A, a_j = x$ $A!otsekorrutisA$, alamotsekorrutis $\Delta_A = \{(a,a) | a \in A\}$
Teoreem 7.1.1

Tõestus. $\pi_j : \prod_{i \in I} A_i \to Aj$ $\alpha_j = \pi_j | A$, $\alpha_j : A \to A_j$, sürjektsioon. $\rho_j = \mathrm{Ker}(\alpha_j)$. Homomorfismiteoreem põhjal A $\rho_j!isomA_j$ $a = (a_i)_{i \in I}, b = (b_i)_{i \in I}, \in A$, $\forall j (a,b) \in \rho_j$..... Piisavus: Olgu $\phi : A \to \prod\limits_{i \in I} A/S_i$, $\phi(a) = (a/\rho_i)_{i \in I}$. I ω-algebrade homomorfism(tõestus rutiine). $A' = \phi(A) \le \prod_{i \in I} A/\rho_i$. $\phi(A)$ on $A/\rho_i, i \in I$, alamotsekorrutis. Paneme tähele, et $A!isom\phi(A)$, kui ϕ üksühene, siis sellest järeldub $A!isom\phi(A)$, $a, b \in A$, $\phi(a) = \phi(b)$, $\forall i \in a/\rho_i = b/\rho_i$.....
def 7.1.2
lause 7.1.1(1)
näited:

1. lihtsad on taandumatud.
2. $\mathbb{Z}_{p^n}, Z_{p^\infty}$, näiteks $\mathbb{Z}_8 \subset 2\mathbb{Z}_8 \subset 4\mathbb{Z}_8 \subset ...$

lemma 7.1.1

Tõestus. A algebra $a, b \in A, a \ne b$, $S = \{S \in Con(A) | (a,b) \notin S\}$ $S \ne \emptyset, \Delta_A \in S$, $(S, \le)$ järjestatud hulk. Näitame, et rahuldab Zorni lemma tingimusi. $C((ahend) \subset S$, $\rho, \sigma \in C \implies \rho \le \sigma$ või $\sigma \le \rho)$. $\tau = !yhendC = !yhend \{\rho | \rho \in C\}$, $(a,b), (b,c) \in \tau$. Kui meil on $n \in N4, \omega \in \Omega_n, a_1, ..., a_n, b_1, ..., b_n \in A$, $(a_i, b_i) \in \tau, i = 1, 2, ..., n \implies$ ..... Rahuldab Zorni lemma eeldust, leidub maksimaalne element, olgu ρ järjestatuh hulga $(S, \le)$ maksimaalne element. Miks $\tau \in S$? $(a,b) \in \tau \implies \exists \rho \in C, (a,b) \in \rho$, vastuolu. Maksimaalne element leidub, A/ρ on taandumatu.

$\square$

$\square$