TARTU ÜLIKOOL
MATEMAATIKA-INFORMAATIKATEADUSKOND
Matemaatika instituut

Kätlin Loit

Täisarvuliste maatriksite Smithi normaalkuju

Bakalaureusetöö

Juhendaja: Lauri Tart

Autor: . . . . . .

Juhendaja: . . . . . .

Lubatud kaitsmisele
Matemaatika instituudi juhataja: . . . . . .

TARTU 2013

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö üldiseks valdkonnaks on algebra ja täpsemalt vaadeldakse maatriksalgebrat üle täisarvude ringi. Töö peamiseks eesmärgiks on anda täisarvuliste maatriksite ühe kanoonilise kuju, niinimetatud *Smithi normaalkuju*, olemasolu üksikasjalik tõestus ning illustreerida seda näidete ja rakendustega.

Üks maatriksalgebra tüüpiline lähenemisviis on viia maatriks endaga "ekvivalentsele", kuid lihtsamale kujule, säilitades seejuures algse maatriksi olulised omadused. Esimesena kasutas nüüd tema nime kandvat normaalkuju H.J.S. Smith oma 1861. aasta artiklis [6], kus ta uuris diofantiliste võrrandite lahenduvust. Smithi normaalkuju on teatud diagonaalmaatriks, mis saadakse esialgset maatriksit vasakult ja paremalt sobivate maatriksitega korrutades. Tõsiasi, et mistahes täisarvulisel maatriksil on olemas üheselt määratud Smithi normaalkuju on üks maatriksalgebra olulisemaid põhitulemusi. Maatriksalgebra rakendusvaldkonnad on väga laialdased ja ka Smithi normaalkuju ei ole erand. Seda kasutatakse näiteks diofantiliste võrrandisüsteemide lahendamisel, diofantilises analüüsis, täisarvulises programmeerimises, lineaarses süsteemiteoorias ja mooduliteoorias üle nulliteguriteta peaideaaliringide.

Antud bakalaureusetöö on referatiivne ning selles on kasutatud peamiselt kahte allikat, milleks on Morris Newmani monograafia "*Integral Matrices*" [5] ja W. Holtzmanni loengumärkmed "*Classification of finetely generated Abelian groups*" [1] . Lisaks oli materjali läbitöötamisel abiks M. Kilbi õpik "*Algebra I*" [3]. Peale eeltoodud algallikates esitatud tulemuste detailsemale lahtikirjutamisele on käesoleva töö autor neile lisanud üksikasjalikud arvulised näited.

Bakalaureusetöö koosneb kolmest peatükist. Esimeses neist on ära toodud maatriksalgebra põhidefinitsioonid ja tulemused. Teises peatükis vaadeldakse täisarvuliste maatriksite ekvivalentsust ja tõestatakse bakalaureusetöö põhitulemus Smithi normaalkuju olemasolust. Lisaks seotakse selle normaalkujuga mõned maatriksite ekvivalentsuse invariandid ja näidatakse nende abil, et Smithi normaalkuju on üheselt määratud. Kolmandas peatükis kirjaldatakse kolme Smithi normaalkuju rakendust: diofantilise võrrandisüsteemi lahendamine, teatud liiki kombinatoorikaülesannete uurimine ja lõplikult moodustatud Abeli rühmade ehituse kirjeldamine. Esimene neist on samuti illustreeritud arvulise näitega.

1 Põhimõisted

Kõigepealt toome ära töös kasutatavad maatriksalgebra ja arvuteooria põhimõisted ning lihtsamad tulemused. Need või nende prototüübid võib leida allikatest [2]-[4].

Definitsioon 1.1. Lõpliku mittetühja hulga A elementide järjendit, mis sisaldab iga elementi täpselt üks kord, nimetatakse **permutatsiooniks** hulga A elementidest. Kõigi n-elemendilise hulga permutatsioonide hulka tähistatakse sümboliga S_n.

Bakalaureusetöö põhiliseks uurimisobjektiks on maatriksid üle täisarvude ringi. Seetõttu meenutame, et täisarvude hulk, mis tähistatakse sümboliga $\mathbb{Z}$, on kommutatiivne taandamisega nulliteguriteta ring. Täpsemalt öeldes, hulgal $\mathbb{Z}$ on defineeritud liitmistehe $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ja korrutamistehe $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ nii, et kehtivad järgmised seosed:

- $(a+b)+c = a+(b+c) \quad \forall a,b,c \in \mathbb{Z}$ (liitmise assotsiatiivsus);
- $\exists 0 : a+0 = a = 0+a \quad \forall a \in \mathbb{Z}$ (nullelemendi olemasolu);
- $\exists (-a) \in \mathbb{Z} : a+(-a) = 0 = (-a)+a \quad \forall a \in \mathbb{Z}$ (vastandelemendi olemasolu);
- $a+b = b+a \quad \forall a,b \in \mathbb{Z}$ (liitmise kommutatiivsus);
- $(ab)c = a(bc) \quad \forall a,b,c \in \mathbb{Z}$ (korrutamise assotsiatiivsus);
- $\exists 1 \in \mathbb{Z} : a1 = a = 1a \quad \forall a \in \mathbb{Z}$ (ühikelemendi olemasolu);
- $ab = ba \quad \forall a,b \in \mathbb{Z}$ (korrutamise kommutatiivsus);
- $a(b+c) = ab+ac \quad \forall a,b,c \in \mathbb{Z}$ (liitmise distributiivsus korrutamise suhtes);
- $ac = bc \wedge c \neq 0 \Longrightarrow a = b \quad \forall a,b,c \in \mathbb{Z}$ (taandamine);
- $ab = 0 \Leftrightarrow (a = 0 \vee b = 0) \quad \forall a,b \in \mathbb{Z}$ (nullitegurite puudumine);
- $ab = 1 \Leftrightarrow (a = b = 1 \vee a = b = -1) \quad \forall a,b \in \mathbb{Z}$ (ainsad pööratavad elemendid on 1 ja -1).

Märkus 1.2. Kuna ringi $\mathbb{Z}$ pööratavad elemendid on 1 ja -1, siis täisarvude $a_1, \ldots, a_n$ suurim ühistegur, mida me tähistame sümboliga $\mathrm{SÜT}(a_1, \ldots, a_n)$, on määratud märgi täpsusega.

Edaspidi tähistame sümboliga $\mathrm{Mat}_n(\mathbb{Z})$ kõigi $n \times n$ maatriksite ringi üle ringi $\mathbb{Z}$.

Definitsioon 1.3. Maatrikseid hulgast $\mathrm{Mat}_n(\mathbb{Z})$, mille determinant on kas 1 või -1, nimetatakse **unimodulaarseteks** maatriksiteks.

Definitsioon 1.4. Maatriksit $A \in \mathrm{Mat}_n(\mathbb{Z})$ nimetatakse **pööratavaks**, kui tal leidub pöördmaatriks $A^{-1} \in \mathrm{Mat}_n(\mathbb{Z})$.

Lause 1.5. *Maatriks $A \in \mathrm{Mat}_n(\mathbb{Z})$ on pööratav parajasti siis, kui tema determinant $|A| \in \{1, -1\}$.*

TÕESTUS. *Tarvilikkus.* Olgu maatriks $A \in \mathrm{Mat}_n(\mathbb{Z})$ pööratav. Siis $A \cdot A^{-1} = E$, kus E on $n \times n$ ühikmaatriks. Seega

$$|A| \cdot |A^{-1}| = |A \cdot A^{-1}| = |E| = 1.$$

Kuna $|A|, |A^{-1}| \in \mathbb{Z}$, siis kas $|A| = 1$ või $|A| = -1$, sest 1 ja -1 on ringi $\mathbb{Z}$ ainsad pööratavad elemendid.

Piisavus. Olgu $|A| = \pm 1$. Algebra kursusest (õpiku [3] teoreem 4.7.10) teame, et maatriksil A eksisteerib reaalarvuline pöördmaatriks A^{-1}, kusjuures

$$A^{-1} = \frac{1}{|A|} \cdot \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix},$$

kus A_{ij} on elemendi a_{ij} algebraline täiend, st $A_{ij} = (-1)^{i+j} M_{ij}$, kus M_{ij} on elemendi a_{ij} täiendusmiinor. Kuna täiendusmiinor M_{ij} on täisarvulise $(n-1)\times(n-1)$ maatriksi determinant, siis $M_{ij} \in \mathbb{Z}$ ning seega ka $A_{ij} \in \mathbb{Z}$, iga $i, j \in \{1, \ldots, n\}$ korral. Eelduse kohaselt $|A| \in \{1, -1\}$, seega $\dfrac{1}{|A|} \in \{1, -1\}$ ja pöördmaatriks A^{-1} peab samuti olema täisarvuline. □

Järeldus 1.6. *Unimodulaarsed täisarvulised maatriksid on parajasti pööratavad täisarvulised maatriksid.*

Definitsioon 1.7. Maatriksi $A \in \mathrm{Mat}_n(\mathbb{Z})$ k. järku **miinoriks** nimetatakse sellise k. järku ruutmaatriksi determinanti, mis saadakse maatriksist A k rea ja k veeru väljavalimisel (ilma elementide vastastikust asendit muutmata).

Definitsioon 1.8. Maatriksi **astakuks** nimetatatakse selle maatriksi nullist erinevate miinorite kõrgeimat järku. Maatriksi A astakut tähistatakse sümboliga $\mathrm{rank}(A)$.

Definitsioon 1.9. Olgu $k \in \mathbb{Z} \setminus \{0\}$ ja $i, j \in \{1, \ldots, n\}$, $i \neq j$. Vaatleme $n \times n$ maatrikseid

$$E_i(k) = \begin{pmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & k & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i\text{-s rida} \\ \\ \\ \end{matrix}$$

ja

$$
E_{ij}(k) = \begin{pmatrix}
1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\
0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & 1 & \dots & k & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & 0 & \dots & 1 & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & 0 & \dots & 0 & \dots & 1
\end{pmatrix} \begin{matrix} \\ \\ \\ i\text{-s rida.} \\ \\ \\ \\ \\ \end{matrix}
$$

(veeru k kohal: j-s veerg)

Elementaarmaatriksiteks nimetatakse järgmiseid maatrikseid

- **I tüüpi** elementaarmaatriksid on maatriksid $E_i(k)$;
- **II tüüpi** elementaarmaatriksid on maatriksid, mis on saadud maatriksitest $E_i(k)$ kahe rea äravahetamisel;
- **III tüüpi** elementaarmaatriksid on maatriksid $E_{ij}(k)$.

Definitsioon 1.10. Täisarvulise maatriksi **elementaarteisendusteks** nimetatakse järgmisi teisendusi:

- **I tüüpi** elementaarteisendus on maatriksi mingi rea või veeru korrutamine nullist erineva täisarvuga;
- **II tüüpi** elementaarteisendus on maatriksi kahe rea või veeru omavaheline vahetamine;
- **III tüüpi** elementaarteisendus on maatriksi ühele reale või veerule mingi nullist erineva täisarvuga korrutatud teise rea või veeru liitmine.

Lause 1.11. *Elementaarmaatriksite ja elementaarteisenduste vahel kehtivad järgmised seosed:*

1) I tüüpi elementaarteisenduse tegemine maatriksiga A on sama, mis maatriksi A vasakult (reateisendus) või paremalt (veeruteisendus) korrutamine I tüüpi elementaarmaatriksiga;

2) II tüüpi elementaarteisenduse tegemine maatriksiga A on sama, mis maatriksi A vasakult (ridade vahetamine) või paremalt (veergude vahetamine) korrutamine II tüüpi elementaarmaatriksiga, mis on saadud elementaarmaatriksist kujul $E_i(1)$;

3) III tüüpi elementaarteisenduse tegemine maatriksiga A on sama, mis maatriksi A vasakult (rea liitmine) või paremalt (veeru liitmine) korrutamine III tüüpi elementaarmaatriksiga.

Märkus 1.12. Paneme tähele, et II ja III tüüpi elementaarteisenduste korral korrutatakse maatriksit A unimodulaarse maatriksiga.

Lemma 1.13. *Olgu $a_i, b_j, a_{st} \in \mathbb{Z}, i, j, s = 1, \ldots, n; t = 2, \ldots, n$. Siis kehtib võrdus*

$$\begin{vmatrix} a_1 + b_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_n + b_n & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_1 & a_{21} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{2n} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} b_1 & a_{21} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_n & a_{2n} & \cdots & a_{nn} \end{vmatrix}.$$

Järgeneva teoreemi saab tõestada analoogiliselt loengukonspekti [4] teoreemiga 1.7.

Teoreem 1.14. *Olgu $a_1, \ldots, a_n \in \mathbb{Z}$. Siis diofantilisel võrrandil*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

tundmatute $x_1, \ldots, x_n$ suhtes leidub täisarvuline lahend parajasti siis, kui

$$\text{SÜT}(a_1, a_2, \ldots, a_n) \mid c.$$

Lemma 1.15. *Olgu $a_1, \ldots, a_n \in \mathbb{Z}$, kusjuures vähemalt üks neist arvudest ei ole 0. Siis leiduvad täisarvud $k_1, \ldots, k_n$ nii, et*

$$a_1k_1 + a_2k_2 + \cdots + a_nk_n = \text{SÜT}(a_1, a_2, \ldots, a_n) \tag{1}$$

ja $\text{SÜT}(k_1, \ldots, k_n) = 1$.

TÕESTUS. Tingimust (1) rahuldavate täisarvude $k_1, \ldots, k_n$ olemasolu on tõestatud õpiku [3] teoreemis 6.3.5.

Oletame vastuväiteliselt, et $e := \text{SÜT}(k_1, k_2, \ldots, k_n) > 1$. Kuna $x_1 = a_1, \ldots, x_n = a_n$ on diofantilise võrrandi

$$k_1x_1 + k_2x_2 + \cdots + k_nx_n = \text{SÜT}(a_1, a_2, \ldots, a_n)$$

lahend, siis teoreemi 1.14 kohaselt $e \mid \text{SÜT}(a_1, \ldots, a_n)$. Paneme tähele, et $x_1 = \dfrac{k_1}{e}, \ldots,$ $x_n = \dfrac{k_n}{e} \in \mathbb{Z}$ on diofantilise võrrandi

$$a_1x_1 + \cdots + a_nx_n = \frac{\text{SÜT}(a_1, \ldots, a_n)}{e}$$

lahend. Jällegi teoreemi 1.14 kohaselt $\text{SÜT}\,(a_1, a_2, \ldots, a_n) \mid \dfrac{\text{SÜT}\,(a_1, a_2, \ldots, a_n)}{e}$, mis on vastuolus sellega, et $\text{SÜT}(a_1, a_2, \ldots, a_n) > \dfrac{\text{SÜT}(a_1, a_2, \ldots, a_n)}{e}$ (viimane võrratus kehtib seetõttu, et $\text{SÜT}(a_1, a_2, \ldots, a_n) \neq 0$). Järelikult $\text{SÜT}(k_1, \ldots, k_n) = e = 1$. $\square$

2 Smithi normaalkuju

Alljärgnevas peatükis on meie eesmärgiks tõestada käesoleva töö põhiteoreem Smithi normaalkuju olemasolust ja ühesusest. Lisaks vaatleme selle normaalkujuga seotud invariante ja leiame ühe konkreetse maatriksi Smithi normaalkuju.

2.1 Täisarvuliste maatriksite ekvivalentsus

Kõigepealt toome sisse täisarvuliste maatriksite ekvivalentsuse mõiste ja tõestame mõned selle omadused.

Definitsioon 2.1. Olgu A, B maatriksid ringist $\mathrm{Mat}_n(\mathbb{Z})$. Öeldakse, et maatriks B on maatriksiga A vasakult (paremalt) **ekvivalentne**, kui leidub unimodulaarne maatriks $U \in \mathrm{Mat}_n(\mathbb{Z})$ nii, et

$$B = UA \quad (B = AU).$$

Öeldakse, et maatriks B on **ekvivalentne** maatriksiga A, kui leiduvad unimodulaarsed maatriksid $U, V \in \mathrm{Mat}_n(\mathbb{Z})$ nii, et

$$B = UAV.$$

Definitsioon 2.2. Olgu A, B maatriksid ringist $\mathrm{Mat}_n(\mathbb{Z})$. Öeldakse, et maatriks B on maatriksi A **kordne**, kui leiduvad sellised maatriksid $P, Q \in \mathrm{Mat}_n(\mathbb{Z})$ nii, et

$$B = PAQ.$$

Märkus 2.3. Maatriksite (ühepoolne) ekvivalentsus ja kordsus on ekvivalentsusseosed.

Märkus 2.4. Ekvivalentsed maatriksid on alati teineteise kordsed.

Lemma 2.5. *Maatriks, mis saadakse maatriksist $A \in \mathrm{Mat}_n(\mathbb{Z})$ kas II või III tüüpi elementaarteisenduste abil, on ekvivalentne maatriksiga A.*

TÕESTUS. Märkuse 1.12 kohaselt on II ja III tüüpi elementaarteisendustes kasutatavad maatriksid unimodulaarsed. Paneme tähele, et tehes maatriksiga A kas II või III tüüpi elementaarteisenduse, saame tulemuseks maatriksi $AU = EAU$ või $UA = UAE$, kusjuures maatriks U ja ühikmaatriks E on mõlemad unimodulaarsed. □

Tähistame sümboliga $Q_{k,n}$ kõigi selliste järjendite $(i_1, i_2, \ldots, i_k)$ hulka, kus $i_1, i_2, \ldots, i_k$ on niisugused täisarvud, et $1 \leq i_1 < i_2 < \cdots < i_k \leq n$.

Definitsioon 2.6. Olgu $A = (a_{ij}) \in \mathrm{Mat}_n(\mathbb{Z})$. Kui $\omega = (l_1, \ldots, l_k), \tau = (p_1, \ldots, p_k)$ on hulga $\{1, \ldots, n\}^k$ elemendid, siis sümboliga $A(\omega, \tau)$ tähistame sellise k. järku maatriksi determinanti, mille i. rea ja j. veeru element on a_{l_i, p_j}.

Teoreem 2.7. *(Cauchy-Binet) Olgu $A, B \in \mathrm{Mat}_n(\mathbb{Z})$ ja k selline täisarv, et $1 \leq k \leq n$. Kui C=AB, siis*

$$C(\omega, \tau) = \sum_{\alpha \in Q_{k,n}} A(\omega, \alpha) B(\alpha, \tau)$$

mistahes $\omega, \tau \in Q_{k,n}$ korral.

TÕESTUS. Olgu $\omega = (m_1, \ldots, m_k) \in Q_{k,n}, \tau = (l_1, \ldots, l_k) \in Q_{k,n}$. Kui $C = AB$, siis korrutise definitsiooni ja lemma 1.13 abil saame, et

$$C(\omega, \tau) = \begin{vmatrix} \sum\limits_{i_1=1}^{n} a_{m_1,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_1,i_k} b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ \sum\limits_{i_1=1}^{n} a_{m_k,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_k,i_k} b_{i_k,l_k} \end{vmatrix}$$

$$= \begin{vmatrix} a_{m_1,1} b_{1,l_1} + \sum\limits_{i_1=2}^{n} a_{m_1,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_1,i_k} b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ a_{m_k,1} b_{1,l_1} + \sum\limits_{i_1=2}^{n} a_{m_k,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_k,i_k} b_{i_k,l_k} \end{vmatrix}$$

$$= \begin{vmatrix} a_{m_1,1} b_{1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_1,i_k} b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ a_{m_k,1} b_{1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_k,i_k} b_{i_k,l_k} \end{vmatrix}$$

$$+ \begin{vmatrix} \sum\limits_{i_1=2}^{n} a_{m_1,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_1,i_k} b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ \sum\limits_{i_1=2}^{n} a_{m_k,i_1} b_{i_1,l_1} & \ldots & \sum\limits_{i_k=1}^{n} a_{m_k,i_k} b_{i_k,l_k} \end{vmatrix} = \cdots$$

$$= \sum_{i_1=1}^{n} \begin{vmatrix} a_{m_1,i_1}b_{i_1,l_1} & \dots & \sum\limits_{i_k=1}^{n} a_{m_1,i_k}b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ a_{m_k,i_1}b_{i_1,l_1} & \dots & \sum\limits_{i_k=1}^{n} a_{m_k,i_k}b_{i_k,l_k} \end{vmatrix} = \dots$$

$$= \sum_{i_1,\dots,i_k=1}^{n} \begin{vmatrix} a_{m_1,i_1}b_{i_1,l_1} & \dots & a_{m_1,i_k}b_{i_k,l_k} \\ \vdots & \ddots & \vdots \\ a_{m_k,i_1}b_{i_1,l_1} & \dots & a_{m_k,i_k}b_{i_k,l_k} \end{vmatrix}$$

$$= \sum_{i_1,\dots,i_k=1}^{n} \begin{vmatrix} a_{m_1,i_1} & \dots & a_{m_1,i_k} \\ \vdots & \ddots & \vdots \\ a_{m_k,i_1} & \dots & a_{m_k,i_k} \end{vmatrix} \cdot b_{i_1,l_1} \cdot b_{i_2,l_2} \cdot \ldots \cdot b_{i_k,l_k}.$$

Paneme tähele, et kui $i_s = i_t$ mingite $s, t \in \{1, \dots, n\}$, $s \neq t$ korral, siis

$$\begin{vmatrix} a_{m_1,i_1} & \dots & a_{m_1,i_s} & \dots & a_{m_1,i_t} & \dots & a_{m_1,i_k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots \\ a_{m_k,i_1} & \dots & a_{m_k,i_s} & \dots & a_{m_k,i_t} & \dots & a_{m_k,i_k} \end{vmatrix} = 0,$$

sest selle determinandi kaks veergu on võrdsed. Seega

$$C(\omega, \tau) = \sum_{\substack{i_1,\dots,i_k=1 \\ i_s \neq i_t, \text{ kui } s \neq t}}^{n} A(\omega, (i_1, \dots, i_k)) \cdot b_{i_1,l_1} \cdot b_{i_2,l_2} \cdot \ldots \cdot b_{i_k,l_k}.$$

Kuna nüüd $i_s \neq i_t$, kui $s \neq t$, siis me võime arvud $i_1, \dots, i_k$ ümber järjestada ning saada arvud $j_1, \dots, j_k$ nii, et $1 \leq j_1 < j_2 < \dots < j_n \leq n$ ja $\{i_1, \dots, i_n\} = \{j_1, \dots, j_n\}$. Olgu vastav substitutsioon

$$\delta = \begin{pmatrix} j_1 \dots j_k \\ i_1 \dots i_k \end{pmatrix}.$$

Siis igale järjendile $(j_1, \dots, j_k)$, $1 \leq j_1 < \dots < j_k \leq n$, vastab $|S_k|$ järjendit $(i_1, \dots, i_k)$, $1 \leq i_s \leq n, s = 1, \dots, k, i_s \neq i_t$, kui $s \neq t$.

Kuna $A(\omega,(i_1,\ldots,i_k)) = A(\omega,(\delta(j_1),\ldots,\delta(j_k))) = \operatorname{sgn}\delta\cdot A(\omega,(j_1,\ldots,j_k))$ ja pöördelemendi leidmine on rühma S_n üksühene pealekujutus, siis saame, et

$$\begin{aligned}
& C(\omega,\tau) \\
= & \sum_{\delta\in S_k}\sum_{1\le j_1<\ldots<j_k\le n} A(\omega,(j_1,\ldots,j_k))\cdot\operatorname{sgn}\delta\cdot b_{\delta^{-1}(j_1),l_1}\cdot b_{\delta^{-1}(j_2),l_2}\cdot\ldots\cdot b_{\delta^{-1}(j_k),l_k} \\
= & \sum_{1\le j_1<\ldots<j\le n} A(\omega,(j_1,\ldots,j_k))\cdot\sum_{\delta\in S_k}\operatorname{sgn}\delta^{-1}\cdot b_{\delta^{-1}(j_1),l_1}\cdot\ldots\cdot b_{\delta^{-1}(j_k),l_k} \\
= & \sum_{1\le j_1<\ldots<j\le n} A(\omega,(j_1,\ldots,j_k))\cdot\sum_{\delta^{-1}\in S_k}\operatorname{sgn}\delta^{-1}\cdot b_{\delta^{-1}(j_1),l_1}\cdot\ldots\cdot b_{\delta^{-1}(j_k),l_k} \\
= & \sum_{1\le j_1<\ldots<j_k\le n} A(\omega,(j_1,\ldots,j_k))\cdot\sum_{\delta\in S_k}\operatorname{sgn}\delta\cdot b_{\delta(j_1),l_1}\cdot\ldots\cdot b_{\delta(j_k),l_k}.
\end{aligned}$$

Determinandi definitsiooni kohaselt

$$\sum_{\delta\in S_k}\operatorname{sgn}\delta\cdot b_{\delta(j_1),l_1}\cdot\ldots\cdot b_{\delta(j_k),l_k} = B(\alpha,(l_1,\ldots,l_k)) = B(\alpha,\tau),$$

seega

$$C(\omega,\tau) = \sum_{\alpha\in Q_{k,n}} A(\omega,\alpha)\cdot B(\alpha,\tau).$$

□

Lause 2.8. *Ekvivalentsetel täisarvulistel maatriksitel on võrdsed astakud.*

TÕESTUS. Olgu maatriksid $A,B\in\operatorname{Mat}_n(\mathbb{Z})$ ekvivalentsed. Siis $A=UBV$, kus U ja V on unimodulaarsed maatriksid. Järelikult $B=V^{-1}AU^{-1}$. Seetõttu iga $0\le r\le n$ korral kehtib järgmine implikatsioon:

$$\operatorname{rank}(A)\le r \Rightarrow \operatorname{rank}(B)\le r.$$

Tõepoolest, kui $r=n$, siis on väide ilmne. Kui $r<n$, siis iga $r<k\le n$ ja $\omega,\tau\in Q_{k,n}$ korral avalduvad maatriksi B kõik k. järku miinorid Cauchy-Binet' teoreemi põhjal järgmiselt:

$$B(\omega,\tau) = \sum_{\alpha\in Q_{k,n}} U^{-1}(\omega,\alpha)A(\alpha,\beta)V^{-1}(\beta,\tau) = 0,$$

sest $A(\alpha,\beta)$ on maatriksi A k. järku miinor ja $k>r\ge\operatorname{rank}(A)$. Järelikult $\operatorname{rank}(B)\le r$. Analoogiliselt saab näidata, et iga $0\le s\le n$ korral kehtib implikatsioon $\operatorname{rank}(B)\le s\Rightarrow\operatorname{rank}(A)\le s$. Võttes vastavalt $r=\operatorname{rank}(A)$ ja $s=\operatorname{rank}(B)$ saamegi, et $\operatorname{rank}(B)\le\operatorname{rank}(A)\le\operatorname{rank}(B)$. □

2.2 Smithi normaalkuju olemasolu

Käesolevas alapeatükis tõestame bakalaureusetöö põhiteoreemi täisarvuliste maatriksite Smithi normaalkuju olemasolust. Esmalt tõestame järgmise olulise vahetulemuse.

Teoreem 2.9. *Olgu $a_1 = a_2 \ldots = a_n$ täisarvud. Tähistame*

$$h := \begin{cases} 0, \quad \textit{kui} \quad a_1, \ldots, a_n = 0; \\ \text{SÜT}(a_1, \ldots, a_n), \textit{ vastasel juhul} \end{cases} \tag{2}$$

Siis leidub maatriks $D \in \mathrm{Mat}_n(\mathbb{Z})$, mille esimene rida on $(a_1, a_2, \ldots, a_n)$ ja mille determinant on h.

TÕESTUS. Tõestame teoreemi väite matemaatilise induktsiooniga n suhtes. Kui $a_1 = \ldots = a_n = 0$, siis võime maatriksiks võtta nullmaatriksi. Vastasel korral toimime alljärgnevalt: kui $n = 1$, siis võtame $D = (a_i)$. Kui $n = 2$, siis lemma 1.15 kohaselt leiduvad arvud $b, c \in \mathbb{Z}$ nii, et $ba_1 - ca_2 = h_2$. Seega determinandi arvutusvõtte kohaselt võime võtta

$$D = \begin{pmatrix} a_1 & a_2 \\ c & b \end{pmatrix}.$$

Oletame nüüd, et $n \geq 3$ ja teoreemi väide kehtib iga $1 \leq k < n$ korral. Tähistame

$$h_{n-1} := \begin{cases} 0, \quad \text{kui} \quad a_1 = \ldots = a_{n-1} = 0; \\ \text{SÜT}(a_1, \ldots, a_{n-1}), \text{ vastasel juhul} \end{cases} \tag{3}$$

Olgu $D_{n-1} = (d_{ij})$ selline maatriks, mille esimene rida on $(a_1, a_2, \ldots, a_{n-1})$ ja mille determinant on h_{n-1}. Kui $a_i = 0$ iga $i = 1, \ldots, n-1$ korral, siis $h_{n-1} = 0$ ja kuna suurim ühistegur on määratud märgi täpsusega, siis võime võtta $D = \begin{pmatrix} 0 & 0 & \cdots & a_n \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}$, sest $|D| \in \{a_n, -a_n\}$ ja $\ddot{\text{SÜT}}(0, 0, \cdots, a_n) = a_n$. Vastasel juhul $h_{n-1} \neq 0$. Kuna

$$h = \ddot{\text{SÜT}}(a_1, a_2, \ldots, a_n) = \ddot{\text{SÜT}}((a_1, a_2, \ldots, a_{n-1}), a_n) = \ddot{\text{SÜT}}(h_{n-1}, a_n),$$

siis leiduvad jälle täisarvud $b, c \in \mathbb{Z}$ nii, et $bh_{n-1} - ca_n = h_n$. Võtame

$$D_n = \begin{pmatrix} & & & a_n \\ & D_{n-1} & & 0 \\ & & & \vdots \\ & & & 0 \\ \frac{a_1 c}{h_{n-1}} & \frac{a_2 c}{h_{n-1}} & \cdots & \frac{a_{n-1} c}{h_{n-1}} \quad b \end{pmatrix}.$$

On selge, et $D_n \in \mathrm{Mat}_n(\mathbb{Z})$ ja tema esimene rida on $(a_1, a_2, \ldots, a_n)$. Kui arendada maatriksit D_n viimase veeru järgi, siis saame, et

$$\left|D_n\right| = \left|E_{n-1}\right| \cdot a_n \cdot (-1)^{n+1} + b \cdot (-1)^{2n} \cdot \left|D_{n-1}\right|, \tag{4}$$

kus E_{n-1} on maatriks, mis on saadud maatriksist D_n esimese rea ja viimase veeru ärajätmisel. Seega

$$\begin{aligned}
h_{n-1} \cdot E_{n-1} &= h_{n-1} \cdot \begin{pmatrix} d_{21} & \ldots & d_{2,n-1} \\ \vdots & \ddots & \vdots \\ d_{n-1,1} & \ldots & d_{n-1,n-1} \\ \dfrac{a_1}{h_{n-1}} \cdot c & \ldots & \dfrac{a_{n-1}}{h_{n-1}} \cdot c \end{pmatrix} \\
&= \begin{pmatrix} h_{n-1} \cdot d_{21} & h_{n-1} \cdot d_{22} & \ldots & h_{n-1} \cdot d_{2,n-1} \\ h_{n-1} \cdot d_{31} & h_{n-1} \cdot d_{32} & \ldots & h_{n-1} \cdot d_{3,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-1} \cdot d_{n-1,1} & h_{n-1} \cdot d_{n-1,2} & \ldots & h_{n-1} \cdot d_{n-1,n-1} \\ c \cdot d_{11} & c \cdot d_{12} & \ldots & c \cdot d_{1,n-1} \end{pmatrix} \\
&= \begin{pmatrix} 0 & h_{n-1} & 0 & \ldots & 0 \\ 0 & 0 & h_{n-1} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & h_{n-1} \\ c & 0 & 0 & \ldots & 0 \end{pmatrix} \cdot \begin{pmatrix} d_{11} & d_{12} & \ldots & d_{1,n-1} \\ d_{21} & d_{22} & \ldots & d_{2,n-1} \\ d_{31} & d_{32} & \ldots & d_{3,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n-1,1} & d_{n-1,2} & \ldots & d_{n-1,n-1} \end{pmatrix} \\
&= \begin{pmatrix} 0 & h_{n-1} & 0 & \ldots & 0 \\ 0 & 0 & h_{n-1} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & h_{n-1} \\ c & 0 & 0 & \ldots & 0 \end{pmatrix} \cdot D_{n-1}.
\end{aligned}$$

Järelikult

$$\left|h_{n-1} \cdot E_{n-1}\right| = \left| \begin{pmatrix} 0 & h_{n-1} & 0 & \cdots & 0 \\ 0 & 0 & h_{n-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & h_{n-1} \\ c & 0 & 0 & \cdots & 0 \end{pmatrix} \right| \cdot \left|D_{n-1}\right| = (-1)^{n-1+1} \cdot (h_{n-1})^{n-2} \cdot c \cdot h_{n-1}.$$

Kuna $\left|h_{n-1} \cdot E_{n-1}\right| = (h_{n-1})^{n-1} \cdot \left|E_{n-1}\right|$ ja $h_{n-1} \neq 0$, siis $\left|E_{n-1}\right| = (-1)^n \cdot c$

Asendades saadud seose võrdusesse (4) saame, et

$$\begin{aligned}\left|D_n\right| &= \left|E_{n-1}\right| \cdot a_n \cdot (-1)^{n+1} + b \cdot (-1)^{2n} \cdot \left|D_{n-1}\right| \\ &= (-1)^n \cdot c \cdot a_n \cdot (-1)^{n+1} + b \cdot (-1)^{2n} \cdot h_{n-1} \\ &= -c \cdot a_n + b \cdot h_{n-1} = b \cdot h_{n-1} - c \cdot a_n = h_n.\end{aligned}$$

□

Teoreem 2.10. ***(Smithi normaalkuju olemasolu)*** *Iga maatriksi $A \in \mathrm{Mat}_n(\mathbb{Z})$ korral leidub maatriksiga A ekvivalentne diagonaalmaatriks*

$$S = S(A) = \mathrm{diag}(s_1, s_2, \ldots, s_r, 0, 0, \ldots, 0),$$

kus r on maatriksi A astak ning $s_1, s_2, \ldots, s_r$ on positiivsed täisarvud omadusega $s_i | s_{i+1}$, kui $1 \leq i \leq r-1$.

TÕESTUS. Kui maatriks A on nullmaatriks, siis ta on juba soovitud kujul ja väide kehtib. Kui maatriks A ei ole nullmaatriks, siis leiduvad i, j nii, et $a = a_{ij} \neq 0$. Olgu $a = a_{ij}$. Siis me saame vahetada maatrika A esimese ja i. rea ja seejärel vahetada esimese ja j. veeru. Lemma 2.5 tõttu oleme saanud maatriksiga A ekvivalentse maatriksi

$$A' = \begin{pmatrix} a & \ldots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{n1} & \ldots & a'_{nn} \end{pmatrix}.$$

Olgu $(a, a_{21}, \ldots, a_{n1})^T$ maatriksi A' esimene veerg ja $d := \ddot{\mathrm{SUT}}(a, a'_{21}, \ldots, a'_{n1}) \neq 0$. Lemma 1.15 tõttu leiduvad täisarvud $k_1, k_2, \ldots, k_n$ nii, et $k_1 a + k_2 a'_{21} + \ldots + k_n a'_{n1} = d$ ja $\ddot{\mathrm{SUT}}(k_1, k_2, \ldots, k_n) = 1$. Teoreemi 2.9 tõttu leidub unimodulaarne maatriks K, mille esimene rida on $(k_1, k_2, \ldots, k_n)$. Korrutame maatriksi A' vasakult maatriksiga K ja saame maatriksiga A' ekvivalentse maatriksi:

$$\begin{pmatrix} k_1 & \ldots & k_n \\ k_{21} & \ldots & k_{2n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \ldots & k_{nn} \end{pmatrix} \begin{pmatrix} a & \ldots & a'_{1n} \\ a'_{21} & \ldots & a'_{2n} \\ \vdots & \ddots & \vdots \\ a'_{n1} & \ldots & a'_{nn} \end{pmatrix} = \begin{pmatrix} b & * & \ldots & * \\ b_2 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ b_n & * & \ldots & * \end{pmatrix} =: B,$$

kus

$$\begin{aligned} b_2 &= k_{21} a + k_{22} a'_{21} + \ldots + k_{2n} a'_{n1} \\ &\ldots \\ b_n &= k_{n1} a + k_{n2} a'_{21} + \ldots + k_{nn} a'_{n1}. \end{aligned}$$

Kuna $b = \ddot{\mathrm{SUT}}(a, a'_{21}, \ldots, a'_{n1})$, siis $b | a, b | a'_{21}, \ldots, b | a'_{n1}$. Seega $b | b_i$ iga $i = 2, \ldots, n$ korral. Lemma 2.5 abil saame maatriksi B viia ekvivalentsele kujule B', kus esimese

veeru elemendid peale kõige esimese on nullid. Analoogiliselt saab sobiva unimodulaarse maatriksiga paremalt korrutades muuta nullideks maatriksi B' esimese rea elemendid peale kõige esimese.

Eelneva protsessi tulemusena oleme saanud maatriksiga A ekvivalentse maatriksi

$$C = \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nn} \end{pmatrix}.$$

Seda protseduuri korduvalt rakendades on võimalik maatriks C viia kujule, kus esimeses reas ja esimeses veerus olev element jagab kõiki elemente alates teisest reast ja teisest veerust, mistõttu ta jagab kõiki selle maatriksi elemente. Nimelt oletame, et leidub element $c_{ij}, i, j \geq 2$, mille korral $c \nmid c_{ij}$. Liidame maatriksi C esimesele veerule j-da veeru. Viime saadud ekvivalentse maatriksiga läbi eelpool kirjeldatud protsessi. Tulemuseks saame maatriksiga C ekvivalentsed maatriksid

$$\begin{pmatrix} c & 0 & \cdots & 0 \\ c_{2j} & c_{22} & \cdots & c_{2n} \\ c_{3j} & c_{32} & \cdots & c_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{nj} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \longrightarrow \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & c'_{22} & \cdots & c'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c'_{n2} & \cdots & c'_{nn} \end{pmatrix},$$

kus $d = \ddot{\mathrm{SUT}}(c_{11}, c_{2j}, \ldots, c_{nj})$. Paneme tähele, et nüüd $d|c$ ja $d|c'_{ij}$ iga $i = 2, \ldots, n$ korral.

Sama mõttekäiku korrates saavutame olukorra, kus esimeses reas ja esimeses veerus olev element jagab maatriksi mistahes teist elementi ja kõik teised elemendid esimeses reas ja samuti esimeses veerus on võrdsed nulliga. Teisiti öeldes, maatriks A on ekvivalentne maatriksiga $D = (d_{ij})$, kus $d_{11}|d_{ij}$ iga i, j korral ja $d_{i1} = 0 = d_{1j}$ mistahes $2 \leq i, j \leq n$ puhul.

Nüüd viime sama protseduuri läbi alammaatriksiga $D_{n-1} = \begin{pmatrix} d_{22} & \cdots & d_{2n} \\ \vdots & \ddots & \vdots \\ d_{n2} & \cdots & d_{nn} \end{pmatrix}$. Paneme tähele, et siis selle alammaatriksiga tehtavatele teisendustele vastavad terve maatriksi korrutamised unimodulaarsete maatriksitega kujul

$$\begin{bmatrix} 1 & 0 \\ 0 & L \end{bmatrix},$$

kus L on alammaatriksiga tehtavale teisendusele vastav unimodulaarne maatriks. Muuseas jagab element d_{11} lõpptulemuseks oleva maatriksi kõiki elemente, sest kui $d_{11}|k_i$,

siis $d_{11} | \ddot{\mathrm{SUT}}(k_i)$ ja $d_{11} | \sum_{j=1}^{l} u_i k_i, i = 1, \ldots, l, 1 < l < n, u_i \in \mathbb{Z}$.
Analoogiliselt saab kogu protsessi korrata rangelt kahanevat järku alammaatriksitega, millega tehtavatele teisendustele vastavad korrutamised unimodulaarsete maatriksitega $\begin{pmatrix} E & \theta \\ \theta & L \end{pmatrix}$, kus E on ühikmaatriks, θ nullmaatriks ja L on alammaatriksiga tehtavale teisendusele vastav unimodulaarne maatriks. See protsess lõpeb, kui me mingis etapis jõuame kas nullmaatriksini või 1×1 maatriksini. Tähistame niiviisi leitud maatriksiga A ekvivalentset diagonaalmaatriksit $S' = \mathrm{diag}(s'_1, \ldots, s'_r, 0, \ldots, 0)$. Kui leidub element i nii, et $s'_i < 0$, siis korrutame maatriksit S' unimodulaarse maatriksiga $E_i(-1)$. Kõigi negatiivsete elementidega sedaviisi toimides saame nõutud omadustega maatriksi $S = \mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$, mis on ekvivalentne maatriksiga A. Jääb üle veel kontrollida, kas $r = \mathrm{rank}(A)$. Kuna maatriksid A ja S on ekvivalentsed ja $\mathrm{rank}(S) = r$, siis lause 2.8 põhjal $r = \mathrm{rank}(S) = \mathrm{rank}(A)$. □

Märkus 2.11. Mõnikord defineeritakse maatriksi A Smithi normaalkuju selliselt, et ei nõuta elementide $s_i, 1 \leq i \leq r$ positiivsust. Sellisel juhul mõistetakse ja uuritakse analoogiliselt suurima ühisteguri ühesusega.

Definitsioon 2.12. Teoreemis 2.10 konstrueeritud diagonaalmaatriksit $S(A)$ nimetatakse maatriksi A **Smithi normaalkujuks**.

2.3 Täisarvuliste maatriksite ekvivalentsuse invariandid

Selles alapeatükis vaatleme mõningaid täisarvuliste maatriksite invariante ja näitame nende abil, et Smithi normaalkuju on üheselt määratud.

Definitsioon 2.13. Olgu $A \in \mathrm{Mat}_n(\mathbb{Z})$. Siis maatriksi A k. järku **determinandijagaja** $d_k(A)$ on defineeritud järgnevalt:

$$d_k(A) := \begin{cases} 0, & \text{kui} \quad A(\omega, \tau) = 0 \text{ iga } \omega, \tau \in Q_{k,n} \quad \text{korral;} \\ \ddot{\mathrm{SUT}}(A(\omega, \tau) \mid \omega, \tau \in Q_{k,n}), & \text{vastasel juhul.} \end{cases}$$

Lemma 2.14. *Olgu $A, B \in \mathrm{Mat}_n(\mathbb{Z})$ ja olgu maatriks B maatriksi A kordne. Siis iga $1 \leq k \leq n$ korral kehtivad järgmised väited:*

1) *kui $d_k(A) = 0$, siis $d_k(B) = 0$;*

2) *kui $d_k(A) \neq 0$, siis $d_k(A) | d_k(B)$.*

TÕESTUS. Definitsiooni kohaselt leiduvad sellised $P, Q \in \mathrm{Mat}_n(\mathbb{Z})$, et $B = PAQ$. Cauchy-Binet' teoreemist saame, et

$$B(\omega, \tau) = \sum_{\alpha, \beta \in Q_{k,n}} P(\omega, \alpha) A(\alpha, \beta) Q(\beta, \tau).$$

Kui $d_k(A) = 0$, siis $A(\alpha, \beta) = 0$ kõikide $\alpha, \beta \in Q_{k,n}$ korral. Seega sel juhul $P(\omega, \alpha)A(\alpha, \beta)Q(\beta, \tau) = 0$ ja seetõttu $B(\omega, \tau) = 0$ mistahes $\omega, \tau \in Q_{k,n}$ korral. Järelikult ka $d_k(B) = 0$.
Kui $d_k(A) \neq 0$, siis $d_k(A) \mid A(\alpha, \beta)$ mistahes $\alpha, \beta \in Q_{k,n}$ korral. Seega

$$d_k(A) \mid \sum_{\alpha,\beta \in Q_{k,n}} P(\omega, \alpha)A(\alpha, \beta)Q(\beta, \tau) \quad \text{ehk} \quad d_k(A)|B(\omega, \tau) \quad \forall \omega, \tau \in Q_{k,n}.$$

Suurima ühisteguri definitsiooni põhjal $d_k(A)|d_k(B)$, millega lemma ongi tõestatud. □

Lause 2.15. *Olgu $A, B \in \mathrm{Mat}_n(\mathbb{Z})$ ekvivalentsed maatriksid. Siis $d_k(A) = d_k(B)$ mistahes $1 \leq k \leq n$ korral.*

TÕESTUS. Kuna maatriksid A ja B on ekvivalentsed, siis leiduvad unimodulaarsed maatriksid $U, V \in \mathrm{Mat}_n(\mathbb{Z})$ nii, et $A = UBV$ ja $B = U^{-1}AV^{-1}$. Järelikult on maatriks A maatriksi B kordne ja maatriks B on maatriksi A kordne. Seega $d_k(A)|d_k(B)$ ja $d_k(B)|d_k(A)$, kust $d_k(A) = \pm d_k(B)$. Kuna suurim ühistegur on määratud märgi täpsusega, siis $d_k(A) = d_k(B)$. □

Teoreem 2.16. *Maatriksid $A, B \in \mathrm{Mat}_n(\mathbb{Z})$ on ekvivalentsed siis ja ainult siis, kui neil on märgi täpsusega samad determinandijagajad.*

TÕESTUS. Tarvilikkus on tõestatud lauses 2.15. Piisavuse jaoks leiame maatriksi A Smithi normaalkuju $S = S(A) = \mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$, kus $s_i > 0$ iga $i = 1, \ldots, r$ korral ja $r = \mathrm{rank}(A)$. Paneme tähele, et maatriksi S nullist erinevad k. järku miinorid on kujul

$$\begin{vmatrix} s_{i_1} & 0 & 0 & 0 \\ 0 & s_{i_2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & s_{i_k} \end{vmatrix} = s_{i_1} \cdot \ldots \cdot s_{i_k},$$

kus $1 \leq i_1 < i_2 < \cdots < i_k \leq r$. Tõepoolest, need on miinorid, mis saadakse maatriksist S ridade $i_1, \ldots, i_r$ ja veergude $i_1, \ldots, i_r$ fikseerimisel. Mistahes neist erineva k. järku miinori korral, mis on saadud maatriksist S ridade $u_1, \ldots, u_k$ ja veergude $v_1, \ldots, v_k$ fikseerimisel, leidub indeks i_0 nii, et $u_{i_0} \notin \{v_1, \ldots, v_k\}$. Seega selle miinori u_{i_0}-s rida koosneb nullidest ja terve miinor on võrdne nulliga. Eelneva põhjal $d_k(S) = \text{SÜT}\{s_{i_1}, \ldots, s_{i_k} |\, 1 \leq i_1 < i_2 < \ldots < i_k \leq r\}$. Kuna $s_k \mid s_l$, kui $l \geq k$, siis

$$\begin{array}{ll} s_1|s_{i_1}, & \text{kui } i_1 \geq 1 \\ s_2|s_{i_2}, & \text{kui } i_2 \geq 2 \\ \quad\vdots & \\ s_k|s_{i_k}, & \text{kui } i_k \geq k. \end{array}$$

Järelikult $s_1 s_2 \cdots s_k \mid s_{i_1} s_{i_2} \cdots s_{i_k}, 1 \leq i_1 < i_2 < \ldots < i_k \leq r$ korral. Seega $s_1 s_2 \ldots s_k | d_k(S)$. Veelgi enam, $s_1 s_2 \ldots s_k \in \{s_{i_1} s_{i_2} s_{i_k} |\ 1 \leq i_1 < i_2 < \ldots < i_k \leq r\}$, mistõttu $d_k(S) \mid s_1 \ldots s_k$ ja järelikult $|d_k(S)| = s_1 s_2 \ldots s_k$ ehk

$$s_1 = |d_1(S)|, s_1 s_2 = |d_2(S)|, \ldots, s_r = |d_r(S)|, \ldots, 0 = |d_{r+1}(S)| = \ldots = |d_n(S)|,$$

sest $r = \operatorname{rank}(A)$. Kuna maatriksid S ja A on ekvivalentsed, siis lause 2.15 tõttu $|d_i(S)| = |d_i(A)|$ iga $1 \leq i \leq n$ korral, kust

$$\begin{aligned} s_1 &= |d_1(S)| = |d_1(A)|, \\ s_1 s_2 &= |d_2(S)| = |d_2(A)|, \\ &\vdots \\ s_1 s_2 \cdots s_r &= |d_r(S)| = |d_r(A)|. \end{aligned}$$

Järelikult maatriks A on ekvivalentne diagonaalmaatriksiga

$$S(A) = \operatorname{diag}(|d_1(A)|, \left|\frac{d_2(A)}{d_1(A)}\right|, \left|\frac{d_3(A)}{d_2(A)}\right|, \ldots, \left|\frac{d_r(A)}{d_{r-1}(A)}\right|, |d_{r+1}(A)|, \ldots, |d_n(A)|).$$

Analoogiliselt, maatriks B on ekvivivalentne diagonaalmaatriksiga

$$S(B) = \operatorname{diag}(|d_1(B)|, \left|\frac{d_2(B)}{d_1(B)}\right|, \left|\frac{d_3(B)}{d_2(B)}\right|, \ldots, \left|\frac{d_r(B)}{d_{r-1}(B)}\right|, |d_{r+1}(B)|, \ldots, |d_n(B)|),$$

sest lause 2.8 põhjal $\operatorname{rank}(A) = \operatorname{rank}(B)$. Kuna lause 2.15 tõttu $|d_i(A)| = |d_i(B)|$ iga $1 \leq i \leq n$ korral, siis $S(A) = S(B)$ ja seega on maatriks A ekvivalentne maatriksiga B. □

Järeldus 2.17. *Maatriksi $A \in \operatorname{Mat}_n(\mathbb{Z})$ Smithi normaalkuju on üheselt määratud.*

TÕESTUS. Eelneva põhjal $S(A) = \operatorname{diag}(|d_1(A)|, \left|\frac{d_2(A)}{d_1(A)}\right|, \ldots, \left|\frac{d_r(A)}{d_{r-1}(A)}\right|, 0, \ldots, 0)$, kus $r = \operatorname{rank}(A)$. □

Definitsioon 2.18. Suuruseid

$$s_k(A) = \frac{d_k(A)}{d_{k-1}(A)}$$

nimetatakse maatriksi A **invariantseteks teguriteks**.

Märkus 2.19. Maatriksi A Smithi normaalkuju $S(A)$ on kujul

$$S(A) = \operatorname{diag}(|s_1(A)|, \ldots, |s_r(A)|, 0, \ldots, 0).$$

Järeldus 2.20. *Maatriksid $A, B \in \operatorname{Mat}_n(\mathbb{Z})$ on ekvivalentsed siis ja ainult siis, kui neil on märgi täpsusega samad invariantsustegurid.*

Märkus 2.21. Eelnevas vaatlesime ainult $n \times n$ maatrikseid. Smithi normaalkuju olemasolu, ühesus ja invariandid on defineeritavad ja tõestatavad ka $m \times n$ ristkülikmaatriksi jaoks. Sel juhul $A = UBV$, kus $A, B \in \operatorname{Mat}_{mn}(\mathbb{Z}), m, n \in \mathbb{N}$, ning $U \in \operatorname{Mat}_m(\mathbb{Z})$ ja $V \in \operatorname{Mat}_n(\mathbb{Z})$ on $m \times m$ ja $n \times n$ järku unimodulaarsed maatriksid.

2.4 Maatriksi Smithi normaalkuju leidmisest

Antud alapeatükis illustreerime teoreeme 2.9 ja 2.10 ühe konkreetse täisarvulise maatriksi Smithi normaalkuju leidmisega.

Näide 2.22. Leiame maatriksi $A = \begin{pmatrix} 3 & 0 & -2 & 1 \\ -1 & -5 & 4 & -2 \\ -1 & 5 & -6 & 3 \\ 5 & -5 & 0 & 0 \end{pmatrix}$ Smithi normaalkuju.

Teoreemi 2.9 tõttu leidub unimodulaarne maatriks, millega maatriksit A vasakult korrutades saame esimese rea ja esimese veeru elemendiks $\ddot{\mathrm{SUT}}(3, 0, -2, 1) = 1$. Sellise maatriksi konstrueerimiseks avaldame kõigepealt maatriksi A esimese veeru elementide suurima ühisteguri kujul $h_4 = 1 = \ddot{\mathrm{SUT}}(3, -1, -1, 5) = 3a_1 - 1a_2 - 1a_3 + 5a_4$. Me võime valida kordajateks u, v, s, t arvud $0, 0, 4, 1$, seega otsitava maatriksi esimene rida on $(0, 0, 4, 1)$. Esimene nullist erinev arv selles reas on 4, seega võime lähtuda 3×3 maatriksist $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$, kus üks kõrvaldiagonaali element on valitud negatiivne, et determinant $h_3 = 4 = \ddot{\mathrm{SUT}}(0, 0, 4)$ tuleks positiivne. Nüüd leiame arvud $b, c \in \mathbb{Z}$ nii, et $b \cdot h_3 - c \cdot 1 = h_4 = 1$. Nendeks sobivad $b = 0$ ja $c = -1$. Otsitava maatriksi viimase rea elemendid on $\frac{a_{11} \cdot c}{h_3}, \frac{a_{12} \cdot c}{h_3}, \frac{a_{13} \cdot c}{h_3}, b$ ja viimase veeru puuduvad elemendid on võrdsed nulliga. Seega on see maatriks $U_1 = \begin{pmatrix} 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

Maatriksit A maatriksiga U_1 vasakult korrutades on tulemuseks:

$$\begin{pmatrix} 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & -2 & 1 \\ -1 & -5 & 4 & -2 \\ -1 & 5 & -6 & 3 \\ 5 & -5 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 15 & -24 & 12 \\ -1 & -5 & 4 & -2 \\ -3 & 0 & 2 & -1 \\ 1 & -5 & 6 & -3 \end{pmatrix}.$$

Paneme tähele, et kuna $\ddot{\mathrm{SUT}}(1, 21, -24, 12) = 1$, siis ei ole vaja tulemust uuesti paremalt unimodulaarse maatriksiga korrutada. Muudame esimese rea ja esimese veeru ülejäänud elemendid nullideks III tüüpi elementaarteisenduste abil:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 15 & -24 & 12 \\ 1 & 5 & -4 & 2 \\ 3 & 0 & -2 & 1 \\ 1 & -5 & 6 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & -15 & 24 & -12 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 10 & -20 & 10 \\ 0 & 45 & -70 & 35 \\ 0 & -20 & 30 & -15 \end{pmatrix}.$$

Tähistame $A' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 10 & -20 & 10 \\ 0 & 45 & -70 & 35 \\ 0 & -20 & 30 & -15 \end{pmatrix}$. Alammaatriksi $\begin{pmatrix} 10 & -20 & 10 \\ 45 & -70 & 35 \\ -20 & 30 & -15 \end{pmatrix}$ sobivale kujule viimiseks vajaliku unimodulaarse maatriksi saame leida analoogiliselt eelnevaga ja selleks võib võtta $\begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ maatriksi.

Järelikult peame maatriksi A' läbi korrutama maatriksiga $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -10 & 20 & -10 \\ 0 & -45 & 70 & -35 \\ 0 & -20 & 30 & -15 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & -10 & 5 \\ 0 & -10 & 20 & -10 \\ 0 & -20 & 30 & -15 \end{pmatrix}.$$

Jälle ridade ja veergudega elementaarteisendusi tehes saame, et

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & -10 & 5 \\ 0 & -10 & 20 & -10 \\ 0 & -20 & 30 & -15 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -10 & 5 \end{pmatrix}.$$

Lõpuks teisendame tulemuse diagonaalmaatriksiks:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -10 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Korrutades kokku kõik vahesammudes paremalt ja vasakult korrutamiseks kasutatud maatriksid, saame unimodulaarsed maatriksid

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$
$$\cdot \begin{pmatrix} 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 4 & 1 \\ -1 & 0 & 2 & 1 \\ -4 & 0 & 3 & 3 \\ -2 & -1 & 0 & 1 \end{pmatrix}$$

ja

$$V = \begin{pmatrix} 1 & -15 & 24 & -12 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -15 & 3 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

Seega

$$U \cdot \begin{pmatrix} 3 & 0 & -2 & 1 \\ -1 & -5 & 4 & -2 \\ -1 & 5 & -6 & 3 \\ 5 & -5 & 0 & 0 \end{pmatrix} \cdot V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

ja järelikult maatriksi A Smithi normaalkuju on

$$S(A) = UAV = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathrm{diag}(1, 5, 5, 0).$$

3 Rakendused

Selles peatükis tutvume mõnede Smithi normaalkuju rakendustega erinevatest matemaatika valdkondadest.

3.1 Diofantiline analüüs

Smith kasutas nüüd tema järgi nimetatud normaalkuju just diofantiliste võrrandite uurimiseks. Näitame siinkohal, kuidas rakendada Smithi normaalkuju diofantiliste võrrandite süsteemi lahendamisel. Olgu meil antud järgmine lineaarvõrrandisüsteem:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = c_1 \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = c_m, \end{cases} \tag{5}$$

kus $m \leq n, a_{ij}, c_i \in \mathbb{Z}, 1 \leq i, j \leq m$ ja $x_1, \ldots, x_n$ on tundmatud. Vaatleme $m \times n$ täisarvulist maatriksit $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$ ja võtame $c = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$. Siis süsteemi (5) lahendamiseks tuleb lahendada maatriksvõrrand

$$Ax = c \tag{6}$$

Üldsust kitsendamata eeldame, et maatriksi A astak on m. Siis leiduvad täisarvulised unimodulaarsed maatriksid U, V nii, et U on $m \times m$ maatriks, V on $n \times n$ maatriks ja UAV on maatriksi A Smithi normaalkuju

$$S = S(A) = \operatorname{diag}(s_1, s_2, \ldots, s_m),$$

kus $s_i | s_{i+1}$ iga $1 \leq i \leq m-1$ korral. Tähistame $y := V^{-1}x$ ja $d := Uc$. Sel juhul võrrand (6) on samaväärne võrrandiga

$$Sy = d. \tag{7}$$

Kui $y = (y_1, y_2, \ldots, y_n)^T$ ja $d = (d_1, d_2, \ldots, d_m)^T$, siis muutujate $y_1, y_2, \ldots, y_m$ väärtused peavad võrrandi (7) tõttu rahuldama võrrandeid

$$s_i y_i = d_i, \quad 1 \leq i \leq m. \tag{8}$$

Kuna maatriksi S viimases $n-m$ veerus on nullid, siis maatriksvõrrand $Sy = d$ on rahuldatud muutujate $y_{r+1}, y_{r+2}, \ldots, y_n$ mistahes täisarvuliste väärtuste korral. Järelikult võrrandi (7) mistahes lahend avaldub kujul $y = (y_1, \ldots, y_m)^T$, kus $y_1, \ldots, y_m$ on võrrandite (8) lahendid ja $y_{m+1}, \ldots, y_n$ väärtused on vabalt valitud täisarvud. Sellega oleme ära lahendanud maatriksvõrrandi (7), kust maatriksvõrrandi (6) ja järelikult võrrandisüsteemi (5) lahendid saame seose $x = Vy$ abil.

Näide 3.1. Lahendame diofantilise lineaarvõrrandisüsteemi

$$\begin{cases} 2x_1 - 2x_2 - 4x_3 + 4x_4 = 4 \\ -8x_1 + 2x_2 - 14x_3 + 2x_4 = 8 \\ 10x_1 - 4x_2 + 10x_3 + 3x_4 = -4 \end{cases} \tag{9}$$

Olgu

$$A = \begin{pmatrix} 2 & -2 & -4 & 4 \\ -8 & 2 & -14 & 2 \\ 10 & -4 & 10 & 2 \end{pmatrix} \quad \text{ja} \quad c = \begin{pmatrix} 4 \\ 8 \\ -4 \end{pmatrix}.$$

Tänu märkusele 2.21 leiduvad sellised unimodulaarsed maatriksid $U \in \mathrm{Mat}_3(\mathbb{Z})$ ja $V \in \mathrm{Mat}_4(\mathbb{Z})$, et maatriksi A Smithi normaalkuju on $S(A) = UAV$, st

$$\begin{aligned} S(A) &= \begin{pmatrix} -1 & 2 & 2 \\ -4 & 9 & 8 \\ 1 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 & -4 & 4 \\ -8 & 2 & -14 & 2 \\ 10 & -4 & 10 & 2 \end{pmatrix} \cdot \begin{pmatrix} 131 & 25 & -38 & 27 \\ -34 & -7 & 10 & -7 \\ -106 & -21 & 31 & -22 \\ -188 & -37 & 55 & -39 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Siis $d = Uc = \begin{pmatrix} 4 \\ 24 \\ 0 \end{pmatrix}$. Võrrandi (8) tõttu peavad kehtima võrdused

$$2 \cdot y_1 = 4, \qquad 6 \cdot y_2 = 24,$$

seega

$$y_1 = 2, \qquad y_2 = 4$$

Järelikult

$$x = Vy = V \begin{pmatrix} 2 \\ 4 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 363 - 38y_3 + 27y_4 \\ -96 + 10y_3 - 7y_4 \\ -296 + 31y_3 - 22y_4 \\ -524 + 55y_3 - 39y_4 \end{pmatrix}.$$

Kokkuvõttes avalduvad võrrandisüsteemi (9) kõik lahendid kujul

$$\begin{aligned} x_1 &= 363 - 38y_3 + 27y_4, \\ x_2 &= -96 + 10y_3 - 7y_4, \\ x_3 &= -296 + 31y_3 - 22y_4, \\ x_4 &= -524 + 55y_3 - 39y_4, \end{aligned}$$

kus $y_3, y_4 \in \mathbb{Z}$.

3.2 Kombinatoorikaülesannetest

Osutub, et Smithi normaalkuju on võimalik rakendada ka teatud kombinatoorikaülesannete lahendamisel.

Orienteeritud graafi G **intsidentsusmaatriksiks** nimetatakse $n \times m$ maatriksit $A = (a_{ij})$, kus $a_{ij} = 1$ parajasti siis, kui tipp v_i on kaare e_j otstipp.

Permutatsioonimaatriks on maatriks, mille igas reas ja veerus on täpselt üks nullist erinev erinev element, milleks on 1.

Üks oluline kombinatoorikas esinev ülesanne on kindlaks teha, millal etteantud intsidentsusmaatriks on saadud mingist teisest maatriksist ridade ja veergude permuteerimise teel. Teisisõnu, kui A ja B on $m \times n$ intsidentsusmaatriksid, siis öeldakse, et maatriksid A ja B on **permutatsioonekvivalentsed**, kui leiduvad $m \times m$ maatriks P ja $n \times n$ maatriks $Q \in \mathrm{Mat}_n(\mathbb{Z})$ nii, et

$$B = PAQ.$$

Maatriksite A ja B on permutatsioonekvivalentsuse kindlakstegemiseks otse definitsiooni järgi oleks vaja moodustada $m! \cdot n!$ korrutis PAQ ja kontrollida, kas maatriks B kuulub nende hulka. Selline lähenemine pole aga $m! \cdot n!$ suuruse tõttu üldiselt otstarbekas. On selge, et kui maatriksid A ja B ei ole ekvivalentsed, siis ei saa nad olla ka permutatsioonekvivalentsed. Järelikult üks kasulik kriteerium selle näitamiseks, et maatriksid ei ole permutatsioonekvivalentsed, on vaadelda nende determinandijagajaid. Kui maatriksitel A ja B ei ole samad determinandijagajad, siis nad ei ole permutatsioonekvivalentsed.

3.3 Lõplikult moodustatud Abeli rühmad

Selle alapeatüki eesmärgiks on tõestada lõplikult moodustatud Abeli rühmade põhiteoreem Smithi normaalkuju abil. Selle teoreemi kohaselt on iga lõplikult moodustatud Abeli rühm isomorfne täisarvude rühma ja jäägiklassirühmade teatud lõpliku otsesummaga.

Definitsioon 3.2. Abeli rühma A nimetatakse **lõplikult moodustatuks**, kui leidub lõplik arv elemente $a_1, a_2, \ldots, a_n \in A$, mis tekitavad A, see tähendab, et

$$A = \langle a_1, \ldots, a_n \rangle = \{z_1 a_1 + \cdots + z_n a_n | z_1, \ldots, z_n \in \mathbb{Z}\}.$$

Definitsioon 3.3. Olgu $(A, +)$ ja $(B, +)$ Abeli rühmad. Kujutist $f : A \longrightarrow B$ nimetatakse Abeli rühmade **homomorfismiks**, kui iga $a_1, a_2 \in A$ korral

$$f(a_1 + a_2) = f(a_1) + f(a_2).$$

Definitsioon 3.4. Abeli rühmade **isomorfismiks** nimetatakse bijektiivset Abeli rühmade homomorfismi.

Vaatleme Abeli rühmade $A_\alpha, \alpha \in I$ otsekorrutises $\prod\limits_{\alpha \in I} A_\alpha$ alamhulka $\oplus \sum\limits_{\alpha \in I} A_\alpha$, mis koosneb jadadest, millel on vaid lõplik arv nullist erinevaid komponente. Siis hulk $\oplus \sum\limits_{\alpha \in I} A_\alpha$ on Abeli rühm komponentviisilise liitmise suhtes, seetähendab, et liitmine on seotud seosega

$$(\ldots, x_\alpha, \ldots) + (\ldots, y_\alpha, \ldots) = (\ldots, x_\alpha + y_\alpha, \ldots).$$

Definitsioon 3.5. Abeli rühma $\oplus \sum\limits_{\alpha \in I} A_\alpha$ nimetatakse Abeli rühmade $A_\alpha, \alpha \in I$, **otsesummaks**.

Vaatleme täisarvude hulga $\mathbb{Z}$ n-dat otseastet

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n} = \{(z_1, \ldots, z_n) | z_1, \ldots, z_n \in \mathbb{Z}\}.$$

Olgu B Abeli rühm ja A rühma B alamrühm. Siis elemendi b kõrvalklassiks alamrühma A järgi nimetatakse hulka $b + A := \{b + a \mid a \in A\}$. Kõigi kõrvalklasside hulk $B/A := \{b + A \mid b \in B\}$ on Abeli rühm liitmistehte

$$(b + A) + (b' + A) := (b + b') + A.$$

suhtes (õpiku [3] lause 6.1.17). Seda Abeli rühma nimetatakse rühma B **faktorrühmaks** alamrühma A järgi.

Tähistame sümboliga e_i hulga $\mathbb{Z}^n$ selliseid elemente, mille i-s komponent on 1 ja ülejäänud komponendid on nullid, st

$$e_i = (0, 0, \ldots, \underset{i}{1}, 0, \ldots, 0)$$

Definitsioon 3.6. Olgu $f : A \longrightarrow A'$ Abeli rühmade homomorfism. Siis homomorfismi f **tuumaks** nimetatatakse hulka

$$\operatorname{Ker} f = \{a \in A |\ f(a) = 0\}$$

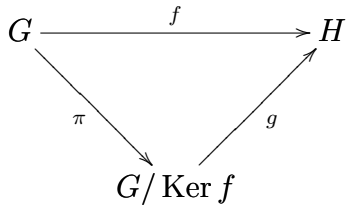
Homomorfismi f tuum Abeli rühma A alamrühm ([3] lemma 6.2.2).

Iga faktorrühma korral saab defineerida **loomuliku projektsiooni** $\pi : B \longrightarrow B/A$ seosega

$$\pi(b) = b + A.$$

Loomulik projektsioon on alati sürjektiivne homomorfism (õpiku [3] lause 6.1.14).
Edasises on meil vaja õpiku [3] teoreeme 6.2.4 ja 6.2.5.

Teoreem 3.7. ***(Rühmade homomorfismiteoreem)*** *Olgu $f : G \longrightarrow H$ rühmade homomorfism. Siis leidub üksühene homomorfism $g : G/\operatorname{Ker} f \longrightarrow H$ nii, et $f = g\pi$, kus $\pi : G \longrightarrow G/\operatorname{Ker} f$ on loomulik projektsioon.*



Teoreem 3.8. ***(Rühmade isomorfismiteoreem)*** *Olgu G ja H rühmad. Kui homomorfism $f : G \longrightarrow H$ on pealekujutus, siis*

$$H \cong G/\operatorname{Ker} f.$$

Lause 3.9. *Abeli rühm A on lõplikult moodustatud parajasti siis, kui leidub sürjektiivne homomorfism $f : \mathbb{Z}^n \longrightarrow A$.*

TÕESTUS. *Tarvilikkus.* Eeldame, et A on lõplikult moodustatud Abeli rühm. Siis leiduvad $a_1, \ldots, a_n \in A$ nii, et $A = \langle a_1, a_2, \ldots, a_n \rangle$. Defineerimine kujutuse $f : \mathbb{Z}^n \longrightarrow A$ võrdusega

$$f(z_1, \ldots, z_n) = z_1 a_1 + \cdots + z_n a_n.$$

Iga rühma A element $a \in A$ avaldub kujul $a = z_1 a_1 + \cdots + z_n a_n = f(z_1, \ldots, z_n)$, mingite
$z_1, \ldots, z_n \in \mathbb{Z}$ korral. Seega on f sürjektiivne kujutus.

Meil on veel vaja näidata, et kujutus f on kooskõlas liitmisega. Olgu $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ ja $(z'_1, \ldots, z'_n) \in \mathbb{Z}^n$. Siis

$$\begin{aligned} f((z_1, \ldots, z_n) + (z'_1, \ldots, z'_n)) &= f(z_1 + z'_1, \ldots, z_n + z'_n) \\ &= (z_1 + z'_1)a_1 + \cdots + (z_n + z'_n)a_n \\ &= z_1a_1 + z'_1a_1 + \cdots + z_na_n + z'_na_n \\ &= f(z_1, \ldots, z_n) + f(z'_1, \ldots, z'_n). \end{aligned}$$

Järelikult on f tõepoolest sürjektiivne homomorfism.

Piisavus. Eeldame, et leidub sürjektiivne homomorfism $f : \mathbb{Z}^n \longrightarrow A$. Vaatleme elemente

$$a_i := f(e_i) \in A,$$

kus $i = 1, \ldots, n$. Kuna kujutus f on sürjektiivne, siis iga $a \in A$ korral saame leida $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ nii, et $a = f(z_1, \ldots, z_n)$. Järelikult

$$\begin{aligned} a = f(z_1, z_2, \ldots, z_n) &= f((z_1, 0, 0, \ldots, 0) + (0, z_2, 0, \ldots) + \cdots + (0, 0, 0, \ldots, z_n)) \\ &= f(z_1e_1 + z_2e_2 + \ldots + z_ne_n) \\ &= f(z_1e_1) + f(z_2e_2) + \cdots + f(z_ne_n) \\ &= z_1f(e_1) + \cdots + z_nf(e_n) = z_1 \cdot a_1 + \cdots + z_n \cdot a_n. \end{aligned}$$

Seega $A = \langle a_1, \ldots, a_n \rangle$ on lõplikult moodustatud. □

Lemma 3.10. *Olgu K rühma $\mathbb{Z}^n$ alamrühm, $A \in \mathrm{Mat}_{mn}(\mathbb{Z})$ ja $U \in \mathrm{Mat}_m(\mathbb{Z})$ ning $V \in \mathrm{Mat}_n(\mathbb{Z})$, kusjuures maatriksid U ja V on unimodulaarsed. Siis maatriksvõrrandite süsteem*

$$xA = k, k \in K, \tag{10}$$

on lahenduv parajasti siis, kui maatriksvõrrandite süsteem

$$yUAV = l, l \in L = KV = \{kV \mid k \in K\}, \tag{11}$$

on lahenduv.

TÕESTUS. *Piisavus.* Olgu maatriksvõrrandite süsteem (10) lahenduv. Vaatleme maatriksvõrrandeid

$$yUAV = l, l \in KV.$$

Olgu $l = k \cdot V, k \in K$. Tähistame $x := yU$. Siis $xAV = yUAV = l = kV$, kust V pööratavuse tõttu $xA = k$. Eelduse kohaselt on see maatriksvõrrand lahenduv.

Tarvilikkus. Olgu maatriksvõrrandite süsteem (11) lahenduv. Vaatleme maatriksvõrrandit

$$x \cdot A = k, k \in K.$$

Tähistame $y := xU^{-1}$. Siis $yUAV = (xU^{-1})(UAV) = (xA)V = kV = l \in KV$, mis on eelduse kohaselt lahenduv.

□

Lause 3.11. *Olgu K rühma $\mathbb{Z}^n$ alamrühm. Siis kas $K = \{0\}$ või $K = \langle s_1v_1, \ldots, s_rv_r\rangle$, kus $\mathbb{Z}^n = \langle v_1, \ldots, v_r\rangle, 1 \leq r \leq n, s_i > 0$ ja $s_i|s_{i+1}$, kui $1 \leq i \leq r$.*

TÕESTUS. Lause 3.13 põhjal kas $K = \{0\}$ või $K = \langle a_1, \ldots, a_t\rangle, a_1, \ldots, a_t \in \mathbb{Z}^n$, $1 \leq t \leq n$. Oletame, et $K \neq \{0\}$. Tähistame

$$\begin{aligned}
a_1 &= (a_{11}, \quad a_{12}, \quad \ldots, \quad a_{1n}),\\
a_2 &= (a_{21}, \quad a_{22}, \quad \ldots, \quad a_{2n}),\\
a_3 &= (a_{31}, \quad a_{32}, \quad \ldots, \quad a_{3n}),\\
&\quad\ \vdots\\
a_t &= (a_{t1}, \quad a_{t2}, \quad \ldots, \quad a_{tn}),
\end{aligned}$$

kus $a_{ij} \in \mathbb{Z}, 1 \leq i \leq t, 1 \leq j \leq n$. Olgu $A = (a_{ij}) \in \mathrm{Mat}_{tn}(\mathbb{Z})$. Siis iga $(k_1, \ldots, k_n) \in K$ korral leiduvad $z_1, \ldots, z_n \in \mathbb{Z}$ nii, et

$$(k_1, \ldots, k_n) = \sum_{i=1}^{t} z_i a_i = (z_1, \ldots, z_t) \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ddots & \ldots \\ a_{t1} & \ldots & a_tn \end{pmatrix}.$$

On lihtne näha, et alamrühm K on moodustatud elementide $a_1, \ldots, a_n$ poolt parajasti siis, kui kõik maatriksvõrrandid $k = xA, k \in K, x = (x_1, \ldots, x_n)^T$, on lahenduvad tundmatute $x_1, \ldots, x_n$ suhtes. Olgu

$$S = S(A) = \mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$$

maatriksi A Smithi normaalkuju. Siis $A = USV$, kus U, V on unimodulaarsed maatriksid. Tõepoolest, kui $t = 0$, siis $1 \leq r \leq t$ ja järelikult ka maatriksi A astak oleks null, seega A oleks nullmaatriks, mis on vastuolus eeldusega, et $K \neq \{0\}$. Kuna maatriks $S \in \mathrm{Mat}_{tn}(\mathbb{Z})$ ja $t \leq n$, siis $r = \mathrm{rank}\, S \leq \min(t, n) = t$. Lisaks $s_i > 0$ ja $s_i|\ s_{i+1}$, kui $1 \leq i < r$.

Lemma 3.10 tõttu on maatriksvõrrandite süsteem $xA = k, k \in K$ lahenduv parajasti siis, kui on lahenduv maatriksivõrrandite süsteem $yUAV = yC = l, l \in LV$. Paneme jälle tähele, et selline süsteemi lahenduvus on samaväärne sellega, et

$$K \cdot V = \langle s_1e_1, \ldots, s_re_r\rangle \text{ ehk } K = \langle s_1(e_1V^{-1}), \ldots, s_t(e_tV^{-1})\rangle.$$

Nüüd on vaja vaid näidata, et $\langle e_1V, \ldots, e_tV\rangle = \mathbb{Z}^n$. Olgu $(z_1, \ldots, z_n) \in \mathbb{Z}^n$. Tähistame $(z'_1, \ldots, z'_n) = (z_1, \ldots, z_n)V$. Siis

$$\begin{aligned}
(z_1, \ldots, z_n) &= ((z_1, \ldots, z_n)V)V^{-1} = (z'_1, \ldots, z'_n)V^{-1}\\
&= (\sum_{i=1}^{n} z'_ie_i)V^{-1} = \sum_{i=1}^{n} z'_i(e_iV^{-1}).
\end{aligned}$$

Järelikult tõepoolest $\mathbb{Z}^n = \langle e_1V^{-1}, \ldots, e_nV^{-1}\rangle$. □

Ei ole keeruline näidata, et kehtib järgmine lause (vt. loengumärkmete [1] teoreemi tõestus).

Lause 3.12. *Olgu $\mathbb{Z}^n = \langle v_1, \ldots, v_n\rangle$, kus $v_1, \ldots, v_n \in \mathbb{Z}^n$, siis Abeli rühmad $\mathbb{Z}^n/\langle s_1v_1, \ldots, s_rv_n\rangle$ ja $\mathbb{Z}_{s_1} \oplus \ldots \oplus \mathbb{Z}_{s_r} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ on isomorfsed.*

Lause 3.13. *Iga rühma $\mathbb{Z}^n$ alamrühm K on kas nullrühm $\{0\}$ või ülimalt n elemendi poolt moodustatud rühm.*

TÕESTUS. Tõestame väite induktsiooniga n järgi. Olgu K rühma $\mathbb{Z}^n$ alamrühm. Eeldame, et $K \neq \{0\}$, sellisel juhul leidub $i_0 \in \{1, \ldots, n\}$ nii, et leiduvad $l_1, \ldots, l_n \in \mathbb{Z}, l_{i_0} \neq 0$ ja $(l_1, \ldots, l_n) \in K$. Üldsust kitsendamata oletame, et $i_0 = 1$. Vaatleme alamrühma K kõigi elementide esimeste komponetide hulka, st

$$F := \{f \in \mathbb{Z} |\ \exists a_1, \ldots, a_n \in \mathbb{Z} : (f, a_2, \ldots, a_n) \in K\}.$$

Olgu $f, f' \in F$, siis leiduvad $a_2, \ldots, a_n, a'_2, \ldots, a'_n$ nii, et $(f, a_2, \ldots, a_n) \in K$ ja $(f', a'_2, \ldots, a'_n) \in K$. Kuna K on rühma $\mathbb{Z}^n$ alamrühm, siis

$$(-f', -a'_2, \ldots, -a'_n) = -(f', a'_2, \ldots, a'_n) \in K \quad \text{ja}$$

$$(f, a_2, \ldots, a_n) + (-f', -a'_2, \ldots, -a'_n) = (f - f', a_2 - a'_2, \ldots, a_n - a'_n) \in K.$$

Järelikult $f - f' \in F$. Sellega oleme näidanud, et hulk F on täisarvude rühma $(\mathbb{Z}, +)$ alamrühm.

Paneme tähele, et $F \neq \{0\}$, sest $(l_1, \ldots, l_n) \in K, l_1 \neq 0$. Seega hulgas F leidub positiivseid elemente, sest kas $l_1 > 0$ või $l_1 < 0$. Teisel juhul $-(l_1, \ldots, l_n) \in K$, sest K on $\mathbb{Z}^n$ alamrühm, seega $0 < -l_1 \in F$. Olgu d hulga F vähim positiivne element. Võtame hulga K suvalise elemendi $k = (k_1, \ldots, k_n)$. Jagades arvu k_1 jäägiga arvuga d, saame, et $k_1 = d \cdot q_k + r_k$, kus $q_k, r_k \in \mathbb{Z}, 0 \leq r_k < d$. Kuna $d \in F$, siis leiduvad $d_2, \ldots, d_n \in \mathbb{Z}$ nii, et $d = (d, d_2, \ldots, d_n) \in K$. Jälle, hulk K on rühma $\mathbb{Z}^n$ alamrühm, seega $(k_1, \ldots, k_n) - (d, d_2, \ldots, d_n)q_k \in K$. Kuna

$$\begin{aligned}(k_1, \ldots, k_n) - (d, d_2, \ldots, d_n) \cdot q_k &= (k_1, \ldots, k_n) - (dq_k, \ldots, d_nq_k)\\ &= (k_1 - dq_k, k_2 - d_2q_k - \ldots - k_n - d_nq_k)\\ &= (r_k, k_2 - d_2q_k, \ldots, k_n - d_nq_k),\end{aligned}$$

siis $r_k \in F$.

Definitsiooni kohaselt on d hulga F vähim positiivne element, seega juhul $r_k > 0$ kehtib võrratus $d < r_k$. Eelneva põhjal aga $0 \leq r_k < d$, järelikult $r_k = 0$. Seega $k_1 = d \cdot q_k$. Seetõttu võime alamrühma K suvalise elemendi $(k_1, \ldots, k_n)$ kirja panna järgmiselt :

$$(k_1, \ldots, k_n) = q_k \cdot (d, d_2, \ldots, d_n) + (0, k_2 - q_k \cdot d_2, \ldots, k_n - q_k \cdot d_n).$$

Ei ole raske näidata, et hulk

$$R = \{(k_2 - q_k d_2, k_3 - q_k d_3, \ldots, k_n - q_k d_n) | k_2, \ldots, k_n \in \mathbb{Z}\}$$

on rühma $\mathbb{Z}^{n-1}$ alamrühm. Induktsiooni eelduse kohaselt on see alamrühm kas $\{0\}$ või lõplikult moodustatud ülimalt $n-1$ elemendi poolt, see tähendab, et

$$\{k_2 - q_k d_2, k_3 - q_k d_3, \ldots, k_n - q_k d_n\} = \langle a_2, \ldots, a_l \rangle,$$

kus $a_i = (a_{i_1}, \ldots, a_{i_n}), a_{ij} \in \mathbb{Z}, 2 \leq i \leq l, 2 \leq j \leq l, l \leq n$. Siis suvaline element hulgast K avaldub kujul

$$(k_1, \ldots, k_n) = q_k \cdot (d, d_2, \ldots, d_n), \text{ kui } R = \{0\} \text{ või}$$

$$(k_1, \ldots, k_n) = q_k \cdot (d, d_2, \ldots, d_n) + z_2(0, a_{22}, \ldots, a_{2n}) + \cdots + z_l(0, a_{l2}, \ldots, a_{ln}),$$

kui $R \neq \{0\}$, kus $l \leq n$. Järelikult $k = \langle \bar{d} \rangle$ või $K = \langle \bar{d}, a_2, \ldots, a_l \rangle, l \leq n$, ehk K on lõplikult moodustatud ülimalt n elemendi poolt. □

Teoreem 3.14. ***(Lõplikult moodustatud Abeli rühmade põhiteoreem)*** *Olgu A lõplikult moodustatud Abeli rühm. Siis*

$$A \cong \mathbb{Z}_{s_1} \oplus \ldots \oplus \mathbb{Z}_{s_r} \oplus \mathbb{Z}, s_i |\ s_{i+1}, \ldots, s_{r-1} |\ s_r,$$

kus $s_i \in \mathbb{Z}, s_i > 0$ ja $s_i | s_{i+1}$, kui $1 \leq i < r$.

TÕESTUS. Lõplikult moodustatud Abeli rühma A korral leidub lause 3.9 põhjal sürjektiivne homomorfism $f : \mathbb{Z}^n \longrightarrow A$. Järelikult isomorfismiteoreemi 3.8 tõttu $A \cong \mathbb{Z}^n / \operatorname{Ker} f$. Kuna $K := \operatorname{Ker} f$ on rühma $\mathbb{Z}^n$ alamrühm, siis lause 3.11 kohaselt kas $K = \{0\}$ või $K = \langle s_1 v_1, \ldots, s_r v_r \rangle, 1 \leq r \leq n$, kus $\mathbb{Z}^n, v_1, \ldots, v_n \in \mathbb{Z}^n$. Järelikult kas $\mathbb{Z}^n / K = \mathbb{Z}^n / \{0\} \cong \mathbb{Z}^n$ või lause 3.12 kohaselt $\mathbb{Z}^n / K \cong \mathbb{Z}_{s_1} \oplus \ldots \oplus \mathbb{Z}_{s_r} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$. □

Smith Normal Form of Integral Matrices

Bachelor's Thesis

Kätlin Loit

Summary

This bachelor's thesis gives an overview of the Smith normal form for integral matrices, i.e. matrices whose entries are integers. This normal form is a diagonalization that exists for any integral matrix and, moreover, is uniquely determined. It was first used in the 1861 paper by H.J.S. Smith which considered solving linear diophantine equations and congruences. The Smith normal form has seen an extensive number of applications since then, including diophantine analysis, integer programming, linear systems theory and module theory over principal ideal domains.

The thesis itself is a review of fundamentals and contains no original research, but it does strive to be as elementary and self-contained as possible. There are altogether three chapters. The first one introduces a number of definitions and results from elementary matrix algebra and number theory that will be needed later on. The second chapter introduces the notion of equivalent matrices. It also contains the main result of the thesis, the proof that every integral matrix has a Smith normal form, i.e. is equivalent to a specific kind of diagonal matrix. There is also a subchapter on certain invariants of equivalent matrices, namely determinantal divisors and invariant factors, which are used to prove that the Smith normal form is unique. Finally, the process of finding the Smith normal form of an integral matrix is illustrated by a simple numerical example. The last chapter contains an overview of three applications: solving linear diophantine equations, a method for analysing a certain class of combinatorial problems and the fundamental theorem of finitely generated Abelian groups.

Kasutatud kirjandus

[1] W. Holtzmann, Classification of finetely generated Abelian groups, elektroonilised loengumärkmed, http://www.cs.uleth.ca/∼holzmann/notes/abelian.pdf (viimati vaadatud 19.02.2013).

[2] R. Howard, Rings, determinants and the Smith normal form, elektroonilised loengumärkmed, http://www.math.sc.edu/∼howard/Classes/700b/notes.pdf (viimati vaadatud 24.10.2012).

[3] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005, 311 lk.

[4] V. Laan, Arvuteooria, elektroonilised loengumärkmed, http://math.ut.ee/pmi/kursused/arvuteooria/kon.pdf (viimati vaadatud 01.06.2013).

[5] M. Newman, *Integral Matrices*, Academic Press, New York, 1972, 224 lk.

[6] H.J.S. Smith, On systems of linear indeterminate equations and congruences, *Phil. Trans. R. Soc. Lond* **151**(1), 1861: 293–326.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Kätlin Loit (sünnikuupäev 09.10.1989),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Täisarvuliste maatriksite Smithi normaalkuju", mille juhendaja on Lauri Tart,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus 04. juunil 2013.a.