

TARTU ÜLIKOOL
LOODUS- JA TÄPPISTEADUSTE VALDKOND
MATEMAATIKA JA STATISTIKA INSTITUUT

Iko Marten Kiisler
**Chevalley-Warningi teoreem polünoomidest üle
lõpliku korpuse**

Matemaatika
Bakalaureusetöö (9 EAP)

Juhendaja: Alvin Lepik

TARTU 2026

CHEVALLEY-WARNINGI TEOREEM POLÜNOOMIDEST ÜLE LÕPLIKU KORPUSE

Bakalaureusetöö

Iko Marten Kiisler

Lühikokkuvõte

Käesolevas bakalaureusetöös uuritakse mitmemuutuva polünoome, mis on defineeritud üle lõplike korpuste. Keskendutakse lahendite olemasolule ja arvule. Töö keskendub Chevalley-Warningi teoreemile ja sellega seotud tulemustele, mis annavad tingimused polünoomide ja nende süsteemide lahenduvusele. Antakse ülevaade lõplikest korpustest, mitmemuutja polünoomidest ja afinsetest alamruumidest ning nendega seotud tulemustest ja omadustest. Tõestatakse Chevalley teoreem, Warningi teoreem, Chevalley-Warningi teoreem ja lisaks teoreeme, mis annavad alumise piiri lahendite hulgale. Töö lõpus tehakse läbi ka selgitavad näited.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria

Märksõnad: Chevalley-Warningi teoreem, lõplikud korpused, mitmemuutja polünoomid

CHEVALLEY-WARNING THEOREM OF POLYNOMIALS OVER A FINITE FIELD

Bachelor thesis

Iko Marten Kiisler

Abstract

This bachelor's thesis studies multivariable polynomials defined over finite fields. The main focus is on the existence and number of solutions. The thesis concentrates on the Chevalley–Warning theorem and related results that provide conditions for the solvability of polynomials and systems of polynomials. An overview of finite fields, multivariable polynomials, and affine subspaces together with their related results and properties is given. The thesis proves Chevalley's theorem, Warning's theorem, the Chevalley–Warning theorem, as well as additional theorems that establish lower bounds for the number of solutions. Explanatory examples are also presented at the end of the thesis.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory

Key Words: Chevalley-Warning theorem, finite fields, multivariable polynomials

Sisukord

Sissejuhatus	4
1 Põhimõisted ja -tulemused	5
1.1 Lõplikud korpused	5
1.2 Polünoomid	7
1.3 Afiinsed alamruumid	10
2 Chevalley-Warningi teoreem	14
Kokkuvõte	24
Kasutatud allikad	25

Sissejuhatus

Käesolev töö keskendub lõplikele korpustele ning nendes moodustatud mitmemuutuja polünoomidele ja nendest süsteemidele. Töö põhiliseks küsimuseks on, kas on tingimusi, millal polünoomidel ja ka nende süsteemidel leidub lahendeid ning kui neid leidub, siis kui palju neid on. Töös tõestatakse tulemusi, mis seavad lahendite arvule alumise tõkke.

Töö kõige olulisem teoreem on tuntud Chevalley-Warningi teoreemi nime all. Seda seetõttu, et Claude Chevalley ja Ewald Warning avaldasid 1935. aastal samas ajakirjanumbris artiklid, millest kujunes välja tänapäeval nende nimede järgi tuntud teoreem [1].

Töö esimeses osas tutvustatakse hilisemate tõestuste mõistmiseks vajalikke mõisteid ja tulemusi. Defineeritakse lõplikud korpused ning käsitletakse nende omadusi. Tutvustatakse mitmemuutuja polünoomide ringi moodustamist ja polünoomide omadusi. Antakse ka ülevaade afiinsetest alamruumidest.

Töö teises osas tõestatakse Warningi teoreem, Chevalley teoreem, Chevalley-Warningi teoreem ja lisaks veel paar teoreemi, mis piiravad polünoomide ja nende süsteemide lahendite arvu. Vaadeldakse ka paar näidet, mis illustreerivad tõestatud teoreemide toimimist ja seatud piiride optimaalsust.

Bakalaureusetöö on referatiivne ning põhiliseks allikaks on Rudolf Lidli ja Harald Niederreiteri õpik "Finite Fields"[4]. Lisaks on kasutatud ka teiste autorite teoseid: Paul R. Halmose [2], S. Langi [3] ja Gary L. Mullen ja Daniel Panario [5].

1 Põhimõisted ja -tulemused

Enne selle töö põhilise osa juurde asumist on vaja meil sõnastada mõned definitsioonid ja tulemused, mida on hiljem tõestustes tarvis.

1.1 Lõplikud korpused

Definitsioon 1.1 ([4, Definitsioon 1.28.]). **Ringiks** $(R, +, \cdot)$ nimetatakse hulka R , millel on defineeritud kaks kahekohalist algebralist tehet $+$ ja $\cdot$ nii, et

1. R on $+$ tehte osas Abeli rühm.
2. $\cdot$ on assotsiatiivne ehk $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ kõigi $a, b, c \in R$ korral.
3. Kehtib distributiivsuse seadus ehk kõigi $a, b, c \in R$ korral $a \cdot (b+c) = a \cdot b + a \cdot c$ ja $(b+c) \cdot a = b \cdot a + c \cdot a$.

Definitsioon 1.2 ([4, Definitsioon 1.29.]). 1. Öeldakse, et ring on **ühikelementaarne ring**, kui leidub element e nii, et $ae = ea = a$ iga $a \in R$ korral.

2. Öeldakse, et ring on **kommutatiivne**, kui $\cdot$ tehe on kommutatiivne.
3. Ringi nimetatakse **integriteetkonnaks**, kui tegemist on kommutatiivse ringiga, millel on olemas ühikelement $e \neq 0$, kus võrdusest $ab = 0$ järeldub, et $a = 0$ või $b = 0$.
4. Ringi nimetatakse **kaldkorpuseks**, kui tema nullist erinevad elemendid moodustavad $\cdot$ suhtes rühma.
5. Kommutatiivset kaldkorpust nimetatakse **korpuseks**.

Definitsioon 1.3. Lõpliku arvu elementidega korpust nimetatakse **lõplikuks korpuseks**.

Märkus 1.4. Kirjapildiga Na , kus a on korpuse element ja $N \in \mathbb{N}$, tähistame me N liidetavaga summat, kus iga liidetav on a .

Olgu F korpus ja K selle korpuse alamhulk. Kui K on ise samade tehete osas korpus nagu F , siis öeldakse, et K on korpuse F **alamkorpus**. Korpust F nimetatakse korpuse K **ülemkorpuseks**.

Definitsioon 1.5 ([4, Definitsioon 1.6.]). **Lõpliku rühma G järguks** nimetatakse selle rühma elementide arvu $|G|$.

Definitsioon 1.6 ([5, Definitsioon 2.1.40]). **Elemendi $a \in G$ järguks** nimetatakse vähimat positiivset täisarvu n nii, et $a^n = e$, kus e on rühme G ühikelement.

Definitsioon 1.7 ([5, Definitsioon 2.1.6]). Ringi R **karakteristikaks** nimetatakse vähimat sellist positiivset täisarvu n , mille korral $nr = 0$ iga $r \in R$ puhul. Kui sellist täisarvu ei leidu, siis öeldakse, et ringi karakteristika on null.

Lemma 1.8 ([4, Lemma 2.3.]). *Kui F on lõplik korpus, kus on q elementi, siis iga $a \in F$ korral $a^q = a$*

Teoreem 1.9 ([4, Teoreem 1.14.]). *Lõpliku rühma mistahes alarühma järk on selle rühma järgu jagaja. Muuhulgas lõpliku rühma iga elemendi järk on selle rühma järgu jagaja.*

Definitsioon 1.10 ([4, lk 50]). Lõpliku korpuse $\mathbb{F}_q$ **multiplikatiivseks rühmaks** nimetatakse rühma, kuhu kuuluvad kõik korpuse elemendid peale nullelemendi, ja tähistatakse $\mathbb{F}_q^\times$.

Definitsioon 1.11 ([4, Definitsioon 1.3.]). Rühm G on **tsükliline**, kui leidub element $a \in G$ nii, et iga $b \in G$ korral leidub mingi täisarv j nii, et $b = a^j$. Sellist elementi a nimetatakse selle tsüklilise rühma **moodustajaks** ja kirjutatakse $G = \langle a \rangle$.

Definitsioon 1.12 ([4, Definitsioon 2.9.]). Tsüklilise rühma $\mathbb{F}_q^\times$ moodustajat nimetatakse selle rühma **primitiivseks** elemendiks.

Teoreem 1.13 ([4, Teoreem 2.8.]). *Lõpliku korpuse multiplikatiivne rühm on tsüklikiline.*

Definitsioon 1.14 ([4, Definitsioon 2.27.]). Olgu $\alpha \in \mathbb{F}_{q^m} = F$ ja $K = \mathbb{F}_q$. Elemendi α norm $N_{F/K}(\alpha)$ üle korpuse K avaldub kujul

$$\alpha \cdot \alpha^q \cdot \dots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$$

ning tähistatakse $N_{F/K}(\alpha)$.

Lemma 1.15 ([4, Teoreem 2.28.]). *Olgu $\mathbb{F}_{q^m} = F$ ja $K = \mathbb{F}_q$. Kehtivad järgmised väited.*

1. Iga $\alpha, \beta \in F$ korral $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$
2. $N_{F/K}$ kujutab korpuse F korpusele K ja rühma $F^\times$ rühmale $K^\times$
3. Iga $a \in K$ korral $N_{F/K}(a) = a^m$
4. Iga $\alpha \in F$ korral $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$

Definitsioon 1.16 ([4, Definitsioon 2.17.]). Olgu $\mathbb{F}_{q^m}$ korpuse $\mathbb{F}_q$ laiend ja olgu $\alpha \in \mathbb{F}_q$. Siis elemente $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^m}$ nimetatakse elemendi α kaaselementideks korpuse $\mathbb{F}_q$ suhtes.

1.2 Polünoomid

Definitsioon 1.17 ([4, Definitsioon 1.49. ja lk 19]). Olgu R ring. Funktsiooni $f : R \rightarrow R$, mis defineeritakse eeskirjaga

$$f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n,$$

nimetatakse ühemuutuja **polünoomiks** üle ringi R . Polünoomi f **astmeks** nimetatakse arvu n , kui $a_n \neq 0$, ja tähistatakse sümboliga $\deg(f)$.

Järgnev osa n -muutuja polünoomide ringi moodustamisest on kirjutatud [4, lk 28] põhjal.

Selleks, et moodustada n -muutuja polünoom on meil vaja moodustada selleks sobiv polünoomide ring. Olgu R kommutatiivne ring koos ühikelemendiga ja $t_1, \dots, t_n$ on muutujad. Polünoomide ringi $R[t_1]$ moodustatakse tavapärasel viisil. Mitme muutujaga polünoomide ringi moodustame rekursiivselt. Ringi $R[t_1, \dots, t_n] = R[t_1, \dots, t_{n-1}][t_n]$ moodustame vaadeldes polünoome muutujaga t_n üle ringi $R[t_1, \dots, t_{n-1}]$. Ringi $R[t_1, \dots, t_n]$ elemendid on siis kujul

$$f = f(t_1, \dots, t_n) = \sum a_{i_1, \dots, i_n} t_1^{i_1} \dots t_n^{i_n},$$

kus kordajad $a_{i_1, \dots, i_n} \in R$. Sellist avaldist nimetatakse **polünoomiks** muutujatega $t_1, \dots, t_n$ üle ringi R .

Definitsioon 1.18 ([4, Definitsioon 1.72.]). Olgu $f \in R[t_1, \dots, t_n]$ antud kujul

$$f(t_1, \dots, t_n) = \sum a_{i_1, \dots, i_n} t_1^{i_1} \dots t_n^{i_n}.$$

Kui $a_{i_1 \dots i_n} \neq 0$, siis $a_{i_1 \dots i_n} t_1^{i_1} \dots t_n^{i_n}$ nimetatakse polünoomi f **liikmeks** ja $i_1 + \dots + i_n$ nimetatakse **liikme astmeks**. Sellise **polünoomi astmeks** loetakse tema liikmete astmete maksimumi. Polünoomi astet tähistatakse $\deg(f)$. Kui $f = 0$, siis defineerime, et $\deg(f) = 0$. Kui $f = 0$ või kõik liikmed on sama astmega, siis öeldakse, et polünoom on **homogeenne**.

Märkus 1.19. Tavaliselt defineeritakse polünoomi $f = 0$ aste kui $\deg(f) = -\infty$. Käesolevas töös, aga defineerime, et $\deg(f) = 0$, sest sellisel juhul on arv $\deg(f)$ samastatav korpuse nullelemendiga.

Definitsioon 1.20 ([4, Definitsioon 1.90.]). Olgu $f \in F[t]$ positiivse astmega ja olgu K korpuse F ülemkorpuse. Öeldakse, et f **lahutub** korpuses K , kui leiduvad

elemendid $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ nii, et

$$f(x) = a(t - \alpha_1)(t - \alpha_2) \dots (t - \alpha_n),$$

kus a on pealiikme kordaja.

Definitsioon 1.21 ([4, Definitsioon 1.90.]). Polünoomi $f \in F[t]$ **lahutuskorpus** nimetatakse korpust K , kui polünoom f lahutub korpuses K ja K on vähim selline korpus, mis sisaldab kõiki polünoomi f juuri.

Teoreem 1.22 ([4, Teoreem 2.5.]). *Olgu p algarv ja n positiivne täisarv. Kehtivad järgmised väited.*

1. *Leidub lõplik korpus, milles on p^n elementi.*
2. *Mistahes p^n -elemendiline korpus on isomorfne polünoomi $t^{p^n} - t \in \mathbb{F}_p[t]$ lahutuskorpusega.*

Eelneva teoreemi tõttu tähistatakse (isomorfismi täpsuseni) üheselt määratud p^n -elemendilist korpust sümboliga $\mathbb{F}_{p^n}$ ja ka $GF(p^n)$. Erijuhul $n = 1$ on $\mathbb{F}_p$ isomorfne korpusega $\mathbb{Z}_p$.

Teoreem 1.23 ([4, Teoreem 1.50.]). *Olgu $f, g \in R[x]$, siis*

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(fg) \leq \deg(f) + \deg(g)$
3. *Kui R on integriteetkond, siis*

$$\deg(fg) = \deg(f) + \deg(g).$$

1.3 Afiinsed alamruumid

Definitsioon 1.24 ([4, lk 114, 273]). Vektorruumi V alamhulka W nimetatakse **afinseks alamruumiks**, kui leidub alamruum $U \subseteq V$ ja $a \in V$ nii, et

$$a + U = \{a + u \mid u \in U\} = W.$$

Afinse alamruumi W mõõtmelise $\dim W$ all peetakse silmas arvu $\dim U$. Öeldakse ka et affine alamruum $b + U$ on **paralleelne** alamruumiga W .

Töö põhiosas vajame mõningaid tehnilisi tulemusi afinsete alamruumide kohta. Esitame need käesolevas alapeatükis lemmadena. Esimene lemma on formuleeritud [4, Lemma 6.10] tõestuse esimese argumendi põhjal, mille kohaselt saame üldisust kitsendamata afinseid alamruume koordinaatide teisenduste abil sobival kujul esitada.

Lemma 1.25. *Olgu K korpus ja K^n vektorruum üle K . Kui $W_1 \neq W_2 \subseteq K^n$ on paralleelsed m -mõõtmelised afiinsed alamruumid, siis leidub koordinaatide teisendus nii, et*

$$\begin{aligned} W_1 &\mapsto \{(k_1, \dots, k_n) \in K^n \mid k_1 = k_2 = \dots = k_{n-m} = 0\}, \\ W_2 &\mapsto \{(k_1, \dots, k_n) \in K^n \mid k_1 = 1, k_2 = \dots = k_{n-m} = 0\}. \end{aligned}$$

Tõestus. Olgu U m -mõõtmeline vektoralamruum ja $\mathbf{a}_1 \neq \mathbf{a}_2 \in K^n$ sellised, et $W_i = \mathbf{a}_i + U$. Rakendame bijektiivset teisendust $\mathbf{x} \mapsto \mathbf{x} - \mathbf{a}_1$. Siis

$$W_1 \mapsto U \quad \text{ja} \quad W_2 \mapsto (\mathbf{a}_2 - \mathbf{a}_1) + U.$$

Valime alamruumi U baasi $\mathbf{u}_1, \dots, \mathbf{u}_m \in K^n$. Kui $\mathbf{a}_2 - \mathbf{a}_1 \in U$, siis $\mathbf{a}_2 = \mathbf{a}_1 + \mathbf{u}$ mingi $\mathbf{u} \in U$ korral, seega $\mathbf{a}_2 \in W_1$ ja $\mathbf{a}_1 \in W_2$, mis on vastuolus eeldusega $W_1 \neq W_2$. Eelduse kohaselt ka $\mathbf{a}_2 - \mathbf{a}_1 =: \mathbf{v} \neq 0$ ja seega süsteem $\mathbf{v}, \mathbf{u}_1, \dots, \mathbf{u}_m$ on lineaarselt

sõltumatu. Laiendame selle ruumi K^n baasiks

$$\mathbf{v}, \mathbf{b}_2, \dots, \mathbf{b}_{n-m}, \mathbf{u}_1, \dots, \mathbf{u}_m.$$

Defineerime nüüd lineaarteisenduse T nii, et

$$T(\mathbf{v}) = \mathbf{e}_1, \quad T(\mathbf{b}_i) = \mathbf{e}_i, \quad i = 2, \dots, n-m, \quad T(\mathbf{u}_i) = \mathbf{e}_{n-m+i}, \quad i = 1, \dots, m,$$

kus $\mathbf{e}_1, \dots, \mathbf{e}_n$ on ruumi K^n kanooniline baas. Kuna T kujutab baasi baasiks, siis ta on automorfism. Iga $\mathbf{u} \in U$ korral

$$\mathbf{u} = \sum_{i=1}^m k_i \mathbf{u}_i, \quad \text{seega} \quad T(\mathbf{u}) = \sum_{i=1}^m k_i \mathbf{e}_{n-m+i}.$$

Järeldame, et U kujutub alamruumiks

$$T(U) = \{(k_1, \dots, k_n) \in K^n \mid k_1 = \dots = k_{n-m} = 0\}$$

ja seega $\mathbf{v} + U$ kujutub paralleelseks afinseks alamruumiks

$$T(\mathbf{v} + U) = \mathbf{e}_1 + T(U) = \{(k_1, \dots, k_n) \in K^n \mid k_1 = 1, k_2 = \dots = k_{n-m} = 0\},$$

nagu tarvis. □

Lemma 1.26 ([2, Teoreem 2, lk 34]). *Olgu R n -mõõtmeline vektorruum ja S selle vektorruumi m -mõõtmeline alamruum. Siis faktorruumi R/S mõõde on $n - m$.*

Lemma 1.27. *Olgu $\mathbb{F}_q$ lõplik korpus ja $W \subseteq \mathbb{F}_q^n$ $(m-1)$ -mõõtmeline affine alamruum. Siis leidub täpselt*

$$\frac{q^{n-m+1} - 1}{q - 1}$$

m -mõõtmelist afinset alamruumi, mis sisaldavad W .

Tõestus. Eelduse kohaselt leidub $(m-1)$ -mõõtmeline vektoralamruum U ja $\mathbf{a} \in \mathbb{F}_q^n$

nii, et $W = \mathbf{a} + U$. Kui W' on m -mõõtmeline afinne alamruum, mis sisaldab W , siis leidub m -mõõtmeline vektoralamruum U' ja vektor $\mathbf{b}$ nii, et

$$\mathbf{a} + U = W \subseteq W' = \mathbf{b} + U',$$

seega ka $\mathbf{a} = \mathbf{b} + \mathbf{v}$ mingi $\mathbf{v} \in U'$ korral. See tähendab, et piisab kokku lugeda kõik m -mõõtmelised vektoralamruumid, mis sisaldavad U . Selleks näitame, et on üksühene vastavus m -mõõtmeliste vektoralamruumide, mis sisaldavad U , ja faktorrüümi $\mathbb{F}_q^n/U$ 1-mõõtmeliste alamruumide vahel. Olgu V m -mõõtmeline vektoralamruum, mis sisaldab U . Valime alamruumi U baasi $\mathbf{u}_1, \dots, \mathbf{u}_{m-1}$ ning laiendame selle alamruumi V baasiks

$$\mathbf{v}, \mathbf{u}_1, \dots, \mathbf{u}_{m-1},$$

kus $\mathbf{v} \in V \setminus U$. Vaatleme nüüd kujutust, mis kujutab sellise alamruumi V alamruumiks $\text{span}(\mathbf{v} + U)$ vektorruumis $\mathbb{F}_q^n/U$.

Kujutus on injektiivne, sest kui kaks alamruumi V_1, V_2 peaksid kujutuma samaks 1-mõõtmeliseks alamruumiks faktorrüümis, siis on nende baasivektorid vastavalt $\mathbf{v}_1, \mathbf{u}_1, \dots, \mathbf{u}_{m-1}$ ja $\mathbf{v}_2, \mathbf{u}_1, \dots, \mathbf{u}_{m-1}$. Need baasivektorid peavad rahuldama tingimust, et $\mathbf{v}_1 + U = c(\mathbf{v}_2 + U)$ mingi $c \neq 0$ korral. See tähendab, et $\mathbf{v}_1 - c\mathbf{v}_2 \in U$, mistõttu $\mathbf{v}_1 \in \text{span}(U, \mathbf{v}_2) = V_2$. Analoogiliselt saame ka $V_2 \subseteq V_1$ ja seega $V_1 = V_2$.

Näitame sürjektiivsust. Olgu $S \subseteq \mathbb{F}_q^n/U$ suvaline 1-mõõtmeline alamruum. Siis leidub $\mathbf{v} \notin U$ nii, et $S = \text{span}(\mathbf{v} + U)$. Alamruum $V := \text{span}(U, \mathbf{v})$ on m -mõõtmeline alamruum, mis sisaldab alamruumi U , ning konstrueeritud kujutuse korral kujutub V alamruumiks S . Seega iga faktorrüümi $\mathbb{F}_q^n/U$ 1-mõõtmeline alamruum on mingi m -mõõtmelise alamruumi kujutis. Järelikult on kujutus sürjektiivne ning seega ka bijektiivne.

Lemma 1.26 põhjal on $\dim(\mathbb{F}_q^n/U) = n - (m - 1) = n - m + 1$. Ühemõõtmelise alamruumi leidmiseks valime suvalise nullist erineva vektori, selleks on $q^{n-m+1} - 1$ valikut. Selle vektori kollineaarseid nullist erinevaid vektoreid on kokku $q - 1$,

seega 1-mõõtmelisi alamruume on kokku

$$\frac{q^{n-m+1} - 1}{q - 1},$$

nagu tarvis.

□

2 Chevalley-Warningi teoreem

Lemma 2.1 ([4, Lemma 6.3]). *Olgu k mittenegatiivne täisarv. Kehtib võrdus*

$$\sum_{x \in \mathbb{F}_q} x^k = \begin{cases} 0, & k = 0 \quad \text{või} \quad q-1 \nmid k \\ -1, & k > 0 \quad \text{ja} \quad q-1 \mid k \end{cases}.$$

Tõestus. Loeme, et $0^0 = 1$, siis juhul $k = 0$ väide kehtib. Olgu $k > 0$ ja $a \in \mathbb{F}_q$ primitiivne. Kuna 0 võime ära jätta, siis saame võrdused

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} x^k &= \sum_{x \in \mathbb{F}_q^\times} x^k = \sum_{i=0}^{q-2} (a^i)^k = \sum_{i=0}^{q-2} (a^k)^i \\ &= 1 + a^k + a^{2k} + \dots + a^{(q-2)k}. \end{aligned}$$

Kui lisaks $q-1 \mid k$, siis kõigi indeksite korral $a^{ik} = 1$. Seda seetõttu, et Lemma 1.8 tõttu teame, et $a^q = a$ ning sellest järeldub, et $a^{q-1} = 1$. Summas on kokku $q-1$ liiget, seega need summeeruvad elemendiks -1 korpusel $\mathbb{F}_q$. Kui aga $q-1 \nmid k$, siis elemendid a^{ik} katavad ära kõik rühma $\mathbb{F}_q^\times$ elemendid. Ringi kõikide elementide summa on võrdne nullelemendiga. $\square$

Polünoomide analüüsimisel piisab linearsuse tõttu tihti analüüsida, kuidas käituvad üksliikmed. Distributiivsuse põhjal kehtib võrdus

$$\sum_{x_1, \dots, x_n \in \mathbb{F}_q} x_1^{k_1} \dots x_n^{k_n} = \prod_{i=1}^n \left(\sum_{x_i \in \mathbb{F}_q} x_i^{k_i} \right). \quad (1)$$

Lemma 2.2 ([4, Lemma 6.4]). *Olgu $P \in \mathbb{F}_q[t_1, \dots, t_n]$ ja $\deg(P) < n(q-1)$. Kehtib võrdus*

$$\sum_{x_1, \dots, x_n \in \mathbb{F}_q} P(x_1, \dots, x_n) = 0.$$

Tõestus. Vaatleme üksliiget $x_1^{k_1} \dots x_n^{k_n}$, kus $\sum k_i < n(q-1)$. Võrratuse tõttu leidub

indeks, mille korral $k_j < q - 1$. Selle väite kehtivuse nägemiseks oletame vastuväiteliselt, et iga j korral $k_j \geq q - 1$. Sellisel juhul oleks üksliikme aste:

$$\sum_{i=1}^n a_i \geq \sum_{i=1}^n (q - 1) = n(q - 1).$$

Seega oleme saanud vastuolu, sest teame, et üksliikme aste ei saa olla suurem kui $(q - 1)n$. Vastav tegur esituses (1) on siis lemma 2.1 tõttu võrdne nulliga. Suvalise polünoomi P saame esitada lineaarkombinatsioonina üksliikmetest. $\square$

Järgnevat teoreemi tuntakse Warningi teoreemina.

Teoreem 2.3 ([4, Teoreem 6.5]). *Olgu $P \in \mathbb{F}_q[t_1, \dots, t_n]$ ja $\deg(P) < n$. Siis polünoomi P juurte arv hulgas $\mathbb{F}_q^n$ jagub korpuse $\mathbb{F}_q$ karakteristikaga p .*

Tõestus. Vaatleme polünoomi $F = 1 - P^{q-1}$, kus sümboli 1 all mõistame konstantset polünoomi, mille väärtus on $1 \in \mathbb{F}_q$. Kui $\mathbf{x} \in \mathbb{F}_q^n$ ei ole polünoomi P juur, siis $P(\mathbf{x})^{q-1} = 1$ ja seega $F(\mathbf{x}) = 0$. Vastasel juhul $F(\mathbf{x}) = 1$. Niisiis

$$\sum_{x_1, \dots, x_n \in \mathbb{F}_q} F(x_1, \dots, x_n) = N1,$$

kus N on polünoomi P juurte arv. Et $\deg(P) < n$, siis $\deg(F) < n(q - 1)$ ja seega lemma 2.2 põhjal $N1 = 0$ korpuses $\mathbb{F}_q$. Järelikult arv N peab jaguma arvuga p . $\square$

Järeldusena Warningi teoreemist saame ühe Chevalley teoreemi.

Järeldus 2.3.1 ([4, Järeldus 6.6]). *Olgu $P \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $P(0, \dots, 0) = 0$ ja $\deg(P) < n$. Siis polünoomil P on mittetriviaalne juur.*

Tõestus. Eelduse tõttu on polünoomil P vähemalt üks juur. Teoreemi 2.3 tõttu aga peab kõikide juurte arv jaguma arvuga $p \geq 2$. $\square$

Warningi ja Chevalley teoreemid saab hõlpsasti ka üldistada polünoomide süsteemidele ning järgmine tulemus ongi tuntud Chevalley-Warningi teoreemina.

Teoreem 2.4 ([4, Teoreem 6.8]). Olgu $P_1, \dots, P_m \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $\sum \deg(P_i) < n$. Siis süsteemi

$$P_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, m, \quad (2)$$

lahendite arv jagub korpuse $\mathbb{F}_q$ karakteristikaga p .

Tõestus. Eeldame, et $x \in \mathbb{F}_q$. Siis saame, et

$$x^{q-1} = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0. \end{cases}$$

Moodustame nüüd polünoomi L nii, et

$$L := \prod_{j=1}^r (1 - P_j^{q-1}) \in \mathbb{F}_q[t_1, \dots, t_n].$$

Nüüd saame, et

$$L(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} \text{ on süsteemi (2) lahend} \\ 0, & \mathbf{x} \text{ ei ole süsteemi (2) lahend} \end{cases}.$$

See seos tuleneb asjaolust, et kui $\mathbf{x}$ on polünoomide süsteemi lahend, siis $P_j^{q-1}(\mathbf{x}) = 0$ iga indeksi j korral ning seetõttu võrdub korrutis ühikelemendiga. Kui $\mathbf{x}$ ei ole lahend, siis vähemalt ühe indeksi j korral $P_j^{q-1}(\mathbf{x}) = 1$ (see tuleneb omakorda polünoomi x^{q-1} omadusest) ning seetõttu võrdub korrutis nulliga.

Olgu polünoomide süsteemi lahendite arv N . Siis saame, et

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} L(\mathbf{x}) = N1$$

Kuna korpuse $\mathbb{F}_q$ karakteristika on p , siis näeme $p \mid N$ kehtib siis ja ainult siis kui

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} L(\mathbf{x}) = 0 \text{ korpuses } \mathbb{F}_q.$$

Seda seetõttu, et kui $N1 = 0$ korpuses $\mathbb{F}_q$, siis peab karakteristika definitsiooni põhjal N olema p kordne ning seega $p \mid N$. Lisaks märkame ka, et

$$\deg(L) = \sum_{j=1}^r \deg(1 - P_j^{q-1}) = (q-1) \sum_{j=1}^r d_j < (q-1)n$$

Võrduse $\sum_{j=1}^r \deg(1 - P_j^{q-1}) = (q-1) \sum_{j=1}^r d_j$ kehtivust saab kontrollida kasutades Teoreemi 1.23, mille põhjal kui f_j aste on d_j , siis f_j^{q-1} aste on $(q-1)d_j$.

Nüüd saame Lemma 2.2 põhjal, et iga polünoomi $P \in \mathbb{F}_q[t_1, \dots, t_n]$, mille aste on väiksem kui $(q-1)n$, korral $\sum_{\mathbf{x} \in \mathbb{F}_q^n} P(x) = 0$ korpuses $\mathbb{F}_q$. Kuna polünoomi L aste on väiksem kui $(q-1)n$, siis olemegi saanud, et $\sum_{\mathbf{x} \in \mathbb{F}_q^n} L(\mathbf{x}) = 0$

Nüüd kuna oleme saanud, et $\sum_{\mathbf{x} \in \mathbb{F}_q^n} L(\mathbf{x}) = 0$ korpuses $\mathbb{F}_q$, siis olemegi näidanud, et $p \mid N$.

□

Järeldus 2.4.1. Olgu $P_1, \dots, P_m \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $P_i(0, \dots, 0) = 0$ iga i korral ja $\sum \deg(P_i) < n$. Siis süsteemil (2) on mittetriviaalne lahend.

Märkus 2.5. Aastal 1935 püstitas Artin hüpoteesi, et lõplikud korpused on kvaasi-algebralised kinnised. See tähendab, et üle lõpliku korpuse mistahes n -muutuva homogeenisel polünoomil astmega $d < n$ on olemas mittetriviaalne juur [3]. Hüpoteesi juured on projektiivses geomeetrias, mida me käesolevas töös täpsemalt ei käsitle. Küll aga järeldub Chevalley-Warningi teoreemist, et lõplikel korpustel on eelnimetatud omadus.

Ehkki süsteemi (2) lahendite arv jagub arvuga p , sellest ei järeldu, et lahendeid leidub. Polünoomide süsteem ei tarvitse ka olla omadusega järelduse 2.4.1 sõnas-

tuses. Osutub siiski, et kui süsteem (2) teoreemi 2.4 eeldustel on lahenduv, siis tal on palju lahendeid.

Lemma 2.6 ([4, Lemma 6.10]). *Olgu $P_1, \dots, P_m \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $\sum \deg(P_i) < n$. Olgu $d := \sum \deg(P_i)$ ja Z süsteemi (2) lahendite hulk. Kui W_1 ja W_2 on vektorruumi $\mathbb{F}_q^n$ d -mõõtmelised afiinsed alamruumid, siis*

$$|W_1 \cap Z| \equiv |W_2 \cap Z| \pmod{p}.$$

Tõestus. Võime eeldada, et $W_1 \neq W_2$. Lemma 1.25 põhjal saame üldisust kitsendamata defineerida alamruumid W_1 ja W_2 järgnevalt

$$\begin{aligned} W_1 &= \{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid x_1 = \dots = x_{n-d} = 0\} \\ W_2 &= \{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid x_1 = 1, x_2 = \dots = x_{n-d} = 0\}, \end{aligned}$$

sest leidub bijektiivne kujutus $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, mis kujutab afiinsed alamruumid vastavale kujule. Kuna T on bijektsioon, siis piisab näidata, et $|T(W_1 \cap Z)| \equiv |T(W_2 \cap Z)| \pmod{p}$. Kujutuse T rakendamisel ei muutu ka polünoomide astmed.

Defineerime polünoomi G võrdusega

$$G(x_1, \dots, x_n) = (-1)^{n-d} \left(x_1^{q-2} + \dots + x_1 + 1 \right) \left(x_2^{q-1} - 1 \right) \dots \left(x_{n-d}^{q-1} - 1 \right).$$

Märgime, et $\deg(G) = (n-d)(q-1) - 1$. Defineerime veel polünoomi

$$H := G \prod_{i=1}^m \left(1 - P_i^{q-1} \right)$$

ning märgime, et

$$\deg(H) \leq d(q-1) + (n-d)(q-1) - 1 = n(q-1) - 1 < n(q-1)$$

ning

$$H(\mathbf{x}) = \begin{cases} -1, & \mathbf{x} \in W_1 \cap Z \\ 1, & \mathbf{x} \in W_2 \cap Z \\ 0, & \text{muidu} \end{cases}.$$

Järelikult

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} H(\mathbf{x}) = (|W_2 \cap Z| - |W_1 \cap Z|)1.$$

Lemma 2.2 tõttu on aga see summa võrdne nulliga korpuses $\mathbb{F}_q$. Järelikult arv $|W_2 \cap Z| - |W_1 \cap Z|$ jagub arvuga p , nagu tarvis. $\square$

Teoreem 2.7 ([4, Teoreem 6.11]). *Olgu $P_1, \dots, P_m \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $d = \sum \deg(P_i) < n$. Kui süsteem (2) on lahenduv, siis lahendite arv on vähemalt q^{n-d} .*

Tõestus. Tähistame süsteemi (2) lahendite hulka sümboliga Z . Vaatleme kahte juhtu. Esiteks, leidugu ruumi $\mathbb{F}_q^n$ d -mõõtmeline afinne alamruum W_1 , mille korral $|W_1 \cap Z| \not\equiv 0 \pmod{p}$. Siis mistahes afinse alamruumiga W_1 paralleelse alamruumi W_2 korral $|W_2 \cap Z| \not\equiv 0 \pmod{p}$ tänu lemmale 2.6. Järelikult ka $|W_2 \cap Z| \geq 1$. Nüüd saame hulga Z esitada lõikumatu ühendina

$$Z = \bigcup_W (W \cap Z),$$

üle kõikide alamruumiga W_1 paralleelsete alamruumide. Kuna neid on täpselt q^{n-d} , siis

$$|Z| = \sum_W |W \cap Z| \geq q^{n-d}.$$

Vastasel juhul mistahes d -mõõtmelise afinse alamruumi W korral jagub arv $|W \cap Z|$ arvuga p . Olgu siis $1 \leq k \leq d$ vähim selline arv, mille korral mistahes k -mõõtmelise afinse alamruumi V korral $|V \cap Z| \equiv 0 \pmod{p}$. Minimaalsuse tõttu leidub $(k-1)$ -mõõtmeline afinne alamruum U , mille korral $|U \cap Z| \not\equiv 0 \pmod{p}$, valimegi siis U sellise. Afinseid alamruume V mõõtmega k , mis sisaldavad U , on Lemma 1.27

põhjal täpselt

$$\frac{q^{n-k+1} - 1}{q - 1} = q^{n-k} + \dots + q + 1.$$

Iga sellise alamruumi V korral kehtib

$$|(V \setminus U) \cap Z| = |V \cap Z| - |U \cap Z| \not\equiv 0 \pmod{p},$$

järelikult $|(V \setminus U) \cap Z| \geq 1$. Sellest järeldame, et

$$|Z| = |U \cap Z| + \sum_V |(V \setminus U) \cap Z| \geq q^{n-k} + \dots + q + 2 > q^{n-d},$$

nagu tarvis. □

Järgmisena vaatame kahte näidet, mis näitavad Chevalley-Warningi teoreemi eelduste ja lahendite arvu alumise tõkke optimaalsust.

Näide 2.8 ([4, Näide 6.7]). Olgu $n \in \mathbb{N}$ ja olgu $\{\alpha_1, \dots, \alpha_n\}$ üle korpuse $\mathbb{F}_q$ moodustatud ülemkorpuse $E = \mathbb{F}_{q^n}$ baas.

Vaatleme polünoomi

$$f(x_1, \dots, x_n) = \prod_{j=0}^{n-1} (\alpha_1^{q^j} x_1 + \dots + \alpha_n^{q^j} x_n).$$

Kuna $\alpha_i^{q^j}, j = 0, 1, \dots, n-1$ on α_i kaaselemendid $\mathbb{F}_q$ suhtes, siis polünoomi f kordajad on korpuse $\mathbb{F}_q$ elemendid. Lihtne on näha, et $\deg(f) = n$. Olgu $(c_1, \dots, c_n) \in \mathbb{F}_q^n$ ja olgu $\gamma = c_1 \alpha_1 + \dots + c_n \alpha_n \in E$. Siis

$$f(c_1, \dots, c_n) = \prod_{j=0}^{n-1} (\alpha_1^{q^j} c_1 + \dots + \alpha_n^{q^j} c_n) = \prod_{j=0}^{n-1} (\alpha_1 c_1 + \dots + \alpha_n c_n)^{q^j} = N_{E/\mathbb{F}_q}(\gamma)$$

Seega saame, et $f(c_1, \dots, c_n) = 0$ on samaväärne võrdusega $N_{E/\mathbb{F}_q}(\gamma) = 0$. See on aga võimalik ainult juhul kui $\gamma = 0$, seega $c_1 = \dots = c_n = 0$. Seega võrrandil $f(x_1, \dots, x_n) = 0$ ainukeseks lahendiks korpuses $\mathbb{F}_q^n$ on $(0, \dots, 0)$. Seega oleme

näidanud, et teoreemis 2.3 ja järelduses 2.3.1 saadud tulemused ei kehti polünoomi f korral.

Näide 2.9 ([4, Näide 6.12.]). Teoreemis 2.7 antud võrratus $N \geq q^{n-d}$ on parim võimalik, isegi juhul $m = 1$, selles mõttes, et kõikide positiivsete täisarvude d ja n nii, et $d < n$ korral leidub polünoom $f_1 \in \mathbb{F}_q[x_1, \dots, x_n]$ astmega d nii, et võrrandil $f_1(x_1, \dots, x_n) = 0$ on täpselt q^{n-d} lahendit ruumis $\mathbb{F}_q^n$. Olgu $g \in \mathbb{F}_q[x_1, \dots, x_n]$ defineeritud peaaegu täpselt samamoodi nagu näites 2.8 aga n asemel on d ehk

$$g(x_1, \dots, x_n) = \prod_{j=0}^{d-1} (\alpha_1^{q^j} x_1 + \dots + \alpha_d^{q^j} x_d).$$

Võtame nüüd, et $f_1(x_1, \dots, x_n) = g(x_1, \dots, x_n)$ nii, et muutujaid $x_{d+1}, \dots, x_n$ ei esine polünoomis f_1 . Näite 2.8 põhjal teame, et $f_1(c_1, \dots, c_n) = 0$ ainult siis, kui $c_1 = \dots = c_d = 0$. Kuna $c_{d+1}, \dots, c_n$ saavad olla suvalised korpuse $\mathbb{F}_q$ elemendid, on võrrandil $f_1(x_1, \dots, x_n) = 0$ täpselt q^{n-d} lahendit ruumis $\mathbb{F}_q^n$.

Teoreem 2.10 ([4, Teoreem 6.13]). Olgu $P \in \mathbb{F}_q[t_1, \dots, t_n]$ nii, et $\deg(P) = d \geq 1$. Siis võrrandil $P(x_1, \dots, x_n) = 0$ on ülimalt dq^{n-1} lahendit.

Tõestus. Tõestame väite induktsiooniga muutujate arvu n ja polünoomi astme d järgi. Olgu $d = 1$, siis

$$P(x_1, \dots, x_n) = a_1 x_1 + \dots + a_n x_n + b = 0$$

ning lahendite arv on q^{n-1} , sest leidub $a_i \neq 0$ ja kui ülejäänud $n - 1$ muutujat väärtustada, siis x_i väärtus on üheselt määratud. Juhul $n = 1$ on väite kehtivus selge.

Olgu nüüd $n > 1$ ja $d > 1$ ning eeldame, et teoreemi väide kehtib kõigi mittekons-tantsete

- i) ülimalt n muutujaga astmega ülimalt $d - 1$ polünoomide korral;

ii) ülimalt $n - 1$ muutujaga astmega ülimalt d polünoomide korral.

Vaatleme kahte juhtu.

Esiteks, oletame, et leidub $c \in \mathbb{F}_q$ nii, et

$$P(x_1, \dots, x_n) = (x_1 - c)Q(x_1, \dots, x_n) \quad (3)$$

mingi $Q \in \mathbb{F}_q[t_1, \dots, t_n]$ korral, mille korral $\deg(Q) \leq d - 1$. Induktsiooni eelduse põhjal on võrrandil $Q(x_1, \dots, x_n) = 0$ ülimalt $(d - 1)q^{n-1}$ lahendit. Kuna korpuses pole nullitegureid, siis (3) põhjal on lahendeid ülimalt

$$(d - 1)q^{n-1} + q^{n-1} = dq^{n-1}.$$

Teiseks, kui sellist $c \in \mathbb{F}_q$ ei leidu, siis iga $c \in \mathbb{F}_q$ korral $P(c, t_2, \dots, t_n)$ on $n - 1$ muutuja polünoom, mille aste on ülimalt d . Induktsiooni eelduse põhjal on võrrandil $P(c, x_2, \dots, x_n) = 0$ ülimalt dq^{n-2} lahendit ruumis $\mathbb{F}_q^{n-1}$. Kuna c valikuks on q varianti, siis esialgsel võrrandil on lahendeid ülimalt $q \cdot dq^{n-2} = dq^{n-1}$. $\square$

Vaatame nüüd ühte näidet polünoomist, millel on dq^{n-1} lahendit.

Näide 2.11 ([4, Näide 6.14.]). Ülemine piir dq^{n-1} , mis on toodud välja teoreemis 2.10, on saavutatav ainult juhul kui $d \leq q$. Vaatame polünoomi

$$f(x_1, \dots, x_n) = (x_1 - c_1)(x_1 - c_2) \dots (x_1 - c_d),$$

kus $c_1, c_2, \dots, c_d \in \mathbb{F}_q$ on kõik erinevad elemendid. Selle polünoomi aste on d ja on lihtne veenuda, et võrrandil $f(x_1, \dots, x_n) = 0$ on täpselt dq^{n-1} lahendit korpuses $\mathbb{F}_q^n$. Selleks, et $(x_1 - c_1)(x_1 - c_2) \dots (x_1 - c_d) = 0$ peab x_1 võrduma c_i -ga, kus $i = 1, 2, \dots, d$ ning teised muutujad võivad võtta mis tahes väärtuse korpusest $\mathbb{F}_q$. Seega iga c_i puhul on q^{n-1} lahendit ning kokku on d erinevat väärtust, mis muutujal x_1 saab olla. Seega on kokku dq^{n-1} lahendit.

Teoreem 2.12 ([4, Teoreem 6.15.]). Olgu $P \in \mathbb{F}_q[t_1, \dots, t_n]$ mittekonstantne homogeenne d -astme polünoom. Siis võrrandil $P(x_1, \dots, x_n) = 0$ on ülimalt $d(q^{n-1} - 1)$ mittetriviaalset lahendit.

Tõestus. Tõestus topeltinduktsiooniga nii nagu teoreemi 2.10 tõestuses. Baasjuhitudel $d = 1$ või $n = 1$ on väite kehtivus selge ning olgu induktsiooni eeldus sõnasstatud samamoodi nagu teoreemi 2.10 tõestuses. Vaatleme kahte juhtu.

Esiteks, kui leidub polünoom $Q \in \mathbb{F}_q[t_1, \dots, t_n]$, mis on mittekonstantne, homogeenne ja väiksema astmega kui d nii, et

$$P(x_1, \dots, x_n) = x_1 Q(x_1, \dots, x_n),$$

siis induktsiooni eelduse põhjal on võrrandil $P(x_1, \dots, x_n) = 0$ ülimalt

$$(q^{n-1} - 1) + (d - 1)(q^{n-1} - 1) = d(q^{n-1} - 1)$$

mittetriviaalset lahendit.

Vastasel juhul sellist polünoomi Q ei leidu. Siis fikseeritud $c \neq 0$ korral on $P(c, x_2, \dots, x_n)$ $(n-1)$ -muutuja polünoom astmega d . Teoreemi 2.10 põhjal on võrrandil $P(x_1, \dots, x_n) = 0$ ülimalt $(q-1)dq^{n-2}$ lahendit kujul $(c_1, \dots, c_n)$, kus $c_1 \neq 0$. Teisalt, $P(0, x_2, \dots, x_n)$ on $(n-1)$ -muutuja homogeenne polünoom, mille aste on d . Induktsiooni eelduse kohaselt on võrrandil $P(x_1, \dots, x_n) = 0$ ülimalt $d(q^{n-2} - 1)$ mittetriviaalset lahendit kujul $(0, c_2, \dots, c_n)$. Niisiis, n -muutuja homogeense d -astme polünoomi korral saab vastaval võrrandil olla mittetriviaalseid lahendeid ülimalt

$$(q-1)dq^{n-2} + d(q^{n-2} - 1) = d(q^{n-1} - 1),$$

nagu tarvis. □

Kokkuvõte

Käesolevas bakalaureuse töös käsitleti lõplikel korpustel defineeritud polünoome ja nendest polünoomidest moodustatud süsteeme.

Bakalaureuse töö esimeses peatükis tutvustasime töö mõistmiseks vajalike tulemusi ja definitsioone. Selgitasime lõplikke korpuseid ja nende olulisemaid omadusi. Käsitlesime mitmemuutuja polünoomide ringe ning polünoomidega seotud põhilisi omadusi ja mõisteid. Viimasena andsime ülevaate afinsetest alamruumidest.

Teises osas tõestasime Warningi teoreemi, Chevalley teoreemi ja Chevalley-Warningi teoreemi. Need teoreemid andsid meile tingimused, mille korral leiduvad polünoomidel ja nende süsteemidel lahendeid. Seejärel tõestasime teoreeme, mis andsid lahendite arvule alumise tõkke ning tegime läbi ka paar selgitavat näidet.

Kasutatud allikad

- [1] Pete L. Clark, Tyler Genao ja Frederick Saia. “Chevalley–Warning at the boundary”. *Expositiones Mathematicae* 39.4 (2021), lk. 604–623. ISSN: 0723-0869. DOI: <https://doi.org/10.1016/j.exmath.2021.03.005>. URL: <https://www.sciencedirect.com/science/article/pii/S0723086921000207>.
- [2] Paul R. Halmos. *Finite-Dimensional Vector Spaces*. Undergraduate Texts in Mathematics. Springer-Verlag, 1974. ISBN: 9783540900931.
- [3] S. Lang. “On quasi algebraic closure”. *Ann. of Math (2)* 55 (1952), lk. 373–390.
- [4] Rudolf Lidl ja Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996.
- [5] Gary L. Mullen ja Daniel Panario. *Handbook of Finite Fields*. Chapman ja Hall/CRC, 2013. DOI: [10.1201/b15006](https://doi.org/10.1201/b15006). URL: <https://doi.org/10.1201/b15006>.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Iko Marten Kiisler,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose Chevalley-Warningi teoreem polünoomidest üle lõpliku korpuse, mille juhendaja on Alvin Lepik, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.
2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commons'i litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.
3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.
4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Iko Marten Kiisler

27.05.2026