Eötvös Loránd Tudományegyetem
Természettudományi Kar

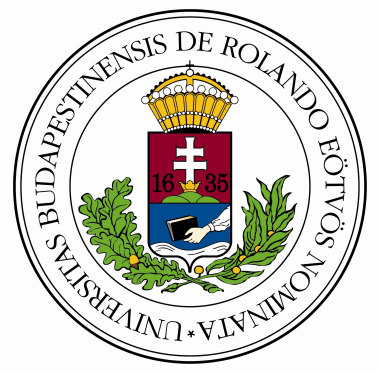
Véges Testek

Szakdolgozat

Boldizsár Dóra
Matematika Bsc
Alkalmazott matematikus szakirány

Témavezető:

Fialowski Alice
Algebra és Számelmélet Tanszék



Budapest
2017

Tartalomjegyzék

Bevezetés

A véges testek elmélete hatalmas irodalommal rendelkezik. Az alkalmazások sora egyre bővül. A kódelmélet, kriptográfia, computer-algebra, információelmélet, statisztikai módszerekbeli alkalmazások mellett a CD és DVD lejátszók, okos telefonok, tabletek működésében is használják, éppúgy, mint kísérletek tervezésében vagy a populáció-genetikában. Az alkalmazásoknak is nagy irodalma van, lásd például a [12] irodalmat.

Dolgozatomban a véges testek elméletének egy fontos fejezetével, a véges test feletti csoportok illetve vektorterek reprezentációival foglalkozom, a teljesség igénye nélkül. A moduláris reprezentációelmélet véges csoportok lineáris reprezentációival foglalkozik. Ha a test karakterisztikája nem osztja a csoport rendjét, akkor a reprezentáció teljesen reducibilis (Dickson 1902). Ha a karakterisztika osztja a csoport rendjét, a reprezentációkat Brauer kezdte tanulmányozni 1935-ben.

Az első fejezetben egy, a véges testekre vonatkozó rövid történeti áttekintést adok, melyhez az [1] irodalmat használtam fel, utána az alapvető fogalmakat foglalom össze.

A második fejezetben véges kommutatív csoportok karaktereit vizsgálom.

A harmadik fejezetben a csoportreprezentáció alapfogalmait és tulajdonságait vezetem be.

Ezután térek rá a véges test feletti vektorterek reprezentációira. Külön foglalkozom a Weil-reprezentációval.

Az utolsó fejezetben a Heisenberg-csoport reprezentációit vizsgálom véges test felett.

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Fialowski Alice-nak, hogy időt szakított rám, észrevételeivel és útmutatásával segítette a munkám, valamint rendelkezésemre bocsátotta a dolgozat elkészüléséhez szükséges szakirodalmat.

Köszönöm a családomnak és a barátaimnak, akik mindvégig támogattak, jóban s rosszban egyaránt.

1. Alapvető ismeretek véges testekről

1.1. Történelmi áttekintés

A véges testek elméletének eredete visszavezethető egészen a 17. századig, de önálló tudományágként csak a 19. század végén terjedt el. Ekkor élt és alkotott a modern algebra egyik megalapítója, Évariste Galois. Galois 1830-ban publikált tanulmánya, melyben lefektette a véges testek elméletének alapjait, igazi mérföldkőnek számít a véges testek elméletében.
Megmutatta, hogy minden p prímre és n egész számra pontosan egy p^n elemű véges test van, és a nemnulla elemek multiplikatív csoportjának az elemszáma $p^n - 1$. Galois eredményeinek nagy részét az 1790-es évek második felében Gauss is leírta, azonban ő nem tette közzé a munkáját.

Gauss "Disquisitiones Arithmeticae" című munkája korszakalkotó volt a matematikában. Ebben teljesen új ötletek és igényes bizonyítások szerepelnek. Bevezette a kongruenciára máig használt jelölést, a $\equiv$ –t. A tanulmánynak lett volna egy 8. fejezete is, ami helytakarékossági okokból kimaradt. A kézirat hiányzó részét Gauss halála után találták meg, és saját jegyzeteivel kiegészítve Dedekind publikálta 1863-ban "Disquisitiones Generales de Congruentiis" címmel, melyet 1889-ben Günther Frei németre is lefordított. A 8. fejezet jelentős hatással volt a véges testek korai elméletére.
A véges testek korai elméletének alakításában fontos szerepe volt még Theodor Schönemann-nak. 1845-ös tanulmányát egy bocsánatkéréssel kezdi, elismerve, hogy Gauss kiadatlan 8. fejezete tartalmazza a magasabb fokú kongruenciák elméletét, melynek néhány eredményét esetleg újra felfedezhette. Ennek ellenére munkája újítónak számított, melyet többek között Kronecker is felhasznált a 19. század második felében. A 19. század vége felé a véges testek kiemelt szerepet kaptak az algebrai kutatásokban. Jordan a klasszikus csoportokat vizsgálta, mint az általános lineáris csoport részcsoportjait. Moore pedig megjegyezte, hogy az ilyen konstrukciókat ki lehetne terjeszteni tetszőleges véges testre.

Galois munkásságának fontosságát jelzi, hogy a véges test megjelölés szinonimájaként máig használatban van a Galois test elnevezés is, melyet Moore vezetett be Galois tiszteletére, és $GF(q^n)$-nel jelölte, ahol q prím és n pozitív egész.

1.2. Algebrai összefoglaló

A fejezet megírásához a [2], [3], [4] és a [6] irodalmat használtam fel, valamint a saját kézzel írt jegyzeteimet.
Ebben a fejezetben a későbbiekben használt fogalmakat és összefüggéseket foglalom össze.

1.1. Tétel. *Minden véges kommutatív csoportnak van bázisa (minden elem egyértelműen előáll a báziselemek hatványszorzataként).*

1.2. Definíció. Egy R gyűrű *karakterisztikája* az a legkisebb pozitív egész m, melyre $m \cdot r = 0$ minden $r \in R$ gyűrűelemre. Ha nincs ilyen legkisebb pozitív egész m, akkor azt mondjuk, hogy az R gyűrű karakterisztikája 0.

1.3. Definíció. A *test* egy olyan $(T; +, \cdot)$ kétműveletes algebrai struktúrát jelöl, ahol T kommutatív csoportot alkot az összeadásra nézve, a szorzás kommutatív, asszociatív, minden nem nulla elemnek van inverze a szorzásra nézve, továbbá a szorzás disztributív az összeadásra nézve.

1.4. Definíció. Legyen K részteste L-nek. Ekkor azt mondjuk, hogy az L *testbővítése* K-nak, vagy $K \leq L$ testbővítés.

1.5. Definíció. Legyen L és K test, L pedig testbővítése K-nak. Ekkor *a bővítés foka* az L, mint K feletti vektortér dimenziója, melyet $|L\colon K|$-val jelölünk.

1.6. Tétel. *Legyen T test, e az egységeleme. Ekkor létezik T-nek egy legszűkebb P részteste (ami T minden résztestének részteste), melyre $e \in P$.*
Ha T karakterisztikája $p > 0$, akkor

$$P = \{0, e, 2e, \ldots, (p-1)e\} \cong \mathbb{Z}_p.$$

Ha T karakterisztikája 0, akkor

$$P = \left\{ \frac{me}{ne} \colon\ m, n \in \mathbb{Z},\ n \neq 0 \right\} \cong \mathbb{Q}$$

1.7. Definíció. Az előző tételben szereplő legszűkebb P résztestet a T test *prímtestének* nevezzük.

1.8. Definíció. Legyen $P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ polinom a K test felett. Ennek *kísérőmátrixa*:

$$C_P = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{bmatrix}$$

1.9. Állítás. *P a C_P mátrix karakterisztikus polinomja.*

Bizonyítás. A karakterisztikus polinomot adó determinánsokban alulról minden sor x-szeresét a fölötte lévőhöz adjuk.

$$\chi_{C_P}(x) = \begin{vmatrix} -x & 0 & \cdots & 0 & -a_n \\ 1 & -x & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 - x \end{vmatrix} = \begin{vmatrix} 0 & 0 & \cdots & 0 & P(x) \\ 1 & 0 & \cdots & 0 & \cdot \\ 0 & 1 & \cdots & 0 & \cdot \\ \vdots & \vdots & \ddots & \vdots & \cdot \\ 0 & 0 & \cdots & 1 & -a_1 - x \end{vmatrix} = (-1)^n P(x)$$

□

1.10. Definíció. Legyen $A \in K^{n\times n}$. Az A *minimálpolinomja* egy olyan minimális fokszámú m_A főpolinom, 1 főegyütthatójú, melyre $m_A(A) = 0$.

1.11. Állítás. *A kísérőmátrix minimálpolinomja megegyezik a karakterisztikus polinomjával (-1) szorzó erejéig.*

Bizonyítás. Tetszőleges c_j nem mind 0 konstansokra $(j = 0, \ldots, n-1)$:

$$\left(\sum_{j=0}^{n-1} c_j {C_P}^j\right) e_1 = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$$

tehát nincs alacsonyabb fokú Q polinom, amire $Q(C_P) = 0$.
Tehát $m(C_P) = (-1)^n \chi_{C_P}$ □

1.12. Definíció. Legyen K test, $f \in K[x]$ n-edfokú polinom. Az f K *feletti felbontási teste* a K test legszűkebb olyan bővítése, amelyben f elsőfokú tényezők szorzatára bomlik.

1.13. Definíció. Tegyük fel, hogy a K véges test karakterisztikája p. Ekkor a $K \to K$, $\alpha \mapsto \alpha^p$ leképezés injektív homomorfizmus, és *Frobenius endomorfizmusnak* nevezzük.

Ebben a dolgozatban véges testekkel foglalkozunk.

1.14. Tétel. *Ha $\mathbb{F}$ véges test, akkor létezik p prímszám és létezik $n \in \mathbb{N}^+$ úgy, hogy $|\mathbb{F}| = p^n$.*

1.15. Tétel. (Wedderburn) *Ha $\mathbb{F}$ véges test, akkor $\mathbb{F}$ kommutatív.*

1.16. Lemma. *Véges test karakterisztikája prím.*

1.17. Tétel. (Véges testek létezése)

1. *Két azonos elemszámú véges test izomorf egymással.*

2. *Bármely $p > 0$ prímszám esetén és bármely $n > 0$ esetén létezik egy p^n elemű test, ami az $X^{p^n} - X \in \mathbb{Z}_p[X]$ polinom felbontási teste $\mathbb{Z}_p$ felett.*

Bizonyítás.

1. Legyen $q := p^n$, $K = \{a_1 = 0, a_2, \ldots, a_q\}$ és $K^* = K \backslash \{0\}$. A $(K^*, \cdot)$ csoportban minden $a_i \in K^*$ elem rendje osztja $q-1 = |K^*|$-ot, amiből az következik, hogy $a_i^{q-1} - a_i = 1$, minden $a_i \in K^*$-ra. Ebből következik, hogy $a_i^q - a_i = 0$ minden $a_i \in K$ esetén. Vagyis K minden eleme az $f := X^q - X$ $\mathbb{Z}_p[x]$-beli polinom gyöke, és f-nek nincs több gyöke a $\mathbb{Z}_p$ feletti felbontási testében. Ezért az f felbontási teste $\mathbb{Z}_p$ felett a K test. Kell még, hogy ez a test egyértelmű. Legyen L egy másik $q = p^n$ elemű test, ekkor $P(L) \cong \mathbb{Z}_p$, L pedig a $g = X^q - X \in P(L)[X]$ felbontási teste $P(L)$ felett. Ebből következik, hogy $K \cong L$.

2. $f' = qX^{q-1} - 1 = -1$ az $f = X^q - X \in \mathbb{Z}_p[X]$ polinom formális deriváltja, ami azt igazolja, hogy f-nek q darab különböző gyöke van az $\mathbb{F} = \mathbb{F}_{f,\mathbb{Z}_p}$ felbontási testben. A $\psi\colon \mathbb{F} \mapsto \mathbb{F}$, $\psi(a) = a^q$ leképezés testautomorfizmus, mivel ψ a Frobenius automorfizmus n-edik hatványa. Az f polinom gyökei azonosak a ψ fixpontjaival. Tehát f gyökei egy q elemű $\mathbb{F}_0 \leq \mathbb{F}$ résztestet alkotnak. Ebből következik, hogy $\mathbb{F}_0 = \mathbb{F}_{f,\mathbb{Z}_p}$, tehát $|\mathbb{F}| = p^n$.

□

1.18. Tétel. *Minden véges test prímhatvány rendű.*

Bizonyítás. Minden R kommutatív gyűrűre van egyetlen $\mathbb{Z} \to R$ gyűrűhomomorfizmus, ami a következőképpen van megadva:

$$m \mapsto \begin{cases} \underbrace{1+1+\cdots+1}_{m\,db}, & ha\ \ m \geq 0, \\ -\underbrace{(1+1+\cdots+1)}_{|m|\,db}, & ha\ \ m < 0. \end{cases}$$

Ezt abban az esetben használjuk, amikor $R = \mathbb{F}$ egy véges test. A $\mathbb{Z} \to \mathbb{F}$ homomorfizmus magja nem nulla, mivel $\mathbb{Z}$ véges és $\mathbb{F}$ is véges. A magot írjuk fel $(m) = m\mathbb{Z}$ alakban egy $m > 0$ egészre, tehát $\mathbb{Z}/(m)$ beágyazható $\mathbb{F}$ részgyűrűjeként. Egy test bármely részgyűrűje integritási tartomány, tehát m-nek prímszámnak kell lennie, ekkor $m = p$. Következésképpen $\mathbb{Z}/(p) \hookrightarrow \mathbb{F}$ beágyazás. Nézzük $\mathbb{F}$-et, mint $\mathbb{Z}/(p)$ fölötti vektorteret, ez véges dimenziós, ha $\mathbb{F}$ véges. Legyen $n = \dim_{\mathbb{Z}/(p)}(\mathbb{F})$ és vegyünk egy $\{e_1, \ldots, e_n\}$ $\mathbb{F}$-beli bázist $\mathbb{Z}/(p)$ fölött. Ekkor $\mathbb{F}$ elemei egyértelműen felírhatók

$$c_1 e_1 + \ldots + c_n e_n$$

alakban, ahol $c_i \in \mathbb{Z}/(p)$. Minden tényezőre p választás van, így $|\mathbb{F}| = p^n$.

□

1.19. Lemma. *Ha $\mathbb{F}$ véges test, akkor az $\mathbb{F}^\times$ csoport ciklikus.*

1.20. Tétel. *Minden véges test izomorf $\mathbb{F}_p[x]/(\pi(x))$-el valamilyen p prímre és irreducibilis $\pi(x) \in \mathbb{F}_p[x]$-re.*

Bizonyítás. Legyen $\mathbb{F}$ véges test, melynek rendje p^n valamilyen p prímre és n pozitív egészre, és legyen $\mathbb{F}_p \hookrightarrow \mathbb{F}$ test beágyazás. Az $\mathbb{F}^\times$ csoport ciklikus az 1.19 Lemma miatt. Legyen γ az $\mathbb{F}^\times$ egy generátora. Tekintsük az $f(x) \mapsto f(\gamma)$ értékelő leképezést (evaluation map). Ez egy $\mathrm{ev}_\gamma \colon \mathbb{F}_p[x] \to \mathbb{F}$ gyűrűhomomorfizmus, ami helyben hagyja $\mathbb{F}_p$-t. Mivel $\mathbb{F}$-ben minden szám 0 vagy a γ hatványa, $0 = \mathrm{ev}_\gamma(0)$, és $\gamma^r = \mathrm{ev}_\gamma(x^r)$ bármely $r \geq 0$-ra. Ekkor $\mathbb{F}_p[x]/\ker \mathrm{ev}_\gamma \cong \mathbb{F}$. Az ev_γ leképezés magja maximális ideál $\mathbb{F}_p[x]$-ben, tehát kell lennie irreducibilis $\pi(x)$-nek $\mathbb{F}_p[x]$-ben. $\square$

2. Véges Abel-csoport karakterei

A fejezet megírásához a [3] és az [5] irodalmat használtam fel.

Abel-csoportként tekinthetjük egy vektortér additív csoportját.
Az alábbiakban $\varepsilon_k^{(n)} = \left(\varepsilon_1^{(n)}\right)^k = \left(1, k\frac{2\pi}{n}\right)$ a $k\frac{2\pi}{n}$ szöghöz tartozó n-edik komplex egységgyök.

2.1. Definíció. Legyen $\mathcal{G}$ kommutatív csoport, χ a $\mathcal{G}$-nek a komplex számok multiplikatív félcsoportjába való nem azonosan nulla félcsoport-homomorfizmusa. Ekkor χ a $\mathcal{G}$ *karaktere*.

2.2. Példa. $\mathcal{G}$ triviális karaktere az $1_{\mathcal{G}}$ homomorfizmus, ami definíció szerint $1_{\mathcal{G}}(g) = 1$ minden $g \in \mathcal{G}$-re.

2.3. Tétel. *Legyen χ a $\mathcal{G}$ kommutatív csoport karaktere, ekkor*

1. *Minden $g \in \mathcal{G}$-re $\chi(g) \neq 0$;*
2. *$\chi(e) = 1$, ahol e a $\mathcal{G}$ egységeleme;*
3. *Minden $g \in \mathcal{G}$-re $\chi(g^{-1}) = (\chi(g))^{-1}$;*
4. *ha $g \in \mathcal{G}$-re $o(g) = n \in \mathbb{N}^+$, akkor $\chi(g) = \varepsilon_k^{(n)} = \left(\varepsilon_1^{(n)}\right)^k$ (ebből következik, hogy $|\chi(g)| = 1$) egy $n > k \in \mathbb{N}$ egésszel; véges $\mathcal{G}$ esetén $|\chi|$ az azonosan 1 függvény, így χ korlátos;*
5. *ha χ korlátos, akkor minden $g \in \mathcal{G}$-re $|\chi(g)| = 1$.*
6. *ha $|\chi(g)| = 1$, akkor $\chi(g^{-1}) = \overline{\chi(g)}$.*

Bizonyítás.

1. Tetszőleges $\mathcal{G}$-beli g-hez adott h esetén van olyan g', hogy $hg' = g$. Ha $\chi(h) = 0$, akkor

$$\chi(g) = \chi(hg') = \chi(h)\chi(g') = 0 \cdot \chi(g') = 0.$$

   Tehát χ azonosan nulla, ami ellentmond a definíciónak.

2. Az előző pont alapján $\chi(e) \neq 0$, ezért

$$1 \cdot \chi(e) = \chi(e) = \chi(e^2) = \chi(e \cdot e) = \chi(e) \cdot \chi(e).$$

$\chi(e)$-vel egyszerűsíthetünk, és ekkor $\chi(e) = 1$.

3. $\chi(g^{-1})\chi(g) = \chi(g^{-1}g) = \chi(e) = 1$, amiből következik az állítás.

4. A feltétel szerint $g^n = e$, ezért

$$(\chi(g))^n = \chi(g^n) = \chi(e) = 1.$$

$\chi(g)$ egy n-edik komplex egységgyök, ennek abszolút értéke viszont 1. Véges csoport minden eleme véges rendű, tehát minden csoportbeli elemen a karakter értékének abszolút értéke 1, ami egyben korlátosságot is jelent.

5. Legyen g a $\mathcal{G}$-nek olyan eleme, amelyre $|\chi(g)| \neq 1$. Ekkor g rendje végtelen. Ha $|\chi(g)| < 1$, akkor a 3. pont alapján $|\chi(g^{-1})| > 1$, ezért feltehetjük, hogy $|\chi(g)| > 1$. Ekkor bármely $n \in \mathbb{N}$-re

$$|\chi(g^n)| = |(\chi(g))^n| = |\chi(g)|^n,$$

és ez tart a végtelenhez, vagyis a karakter nem korlátos.

6. $\chi(g^{-1}) = (\chi(g))^{-1}$, és egységnyi hosszúságú komplex szám inverze a szám konjugáltja.

□

2.4. Állítás. *Legyen $\mathcal{G}$ kommutatív csoport. Ha χ_1, χ_2, χ a $\mathcal{G}$ karakterei, akkor a*

$$g \mapsto \chi_1(g)\chi_2(g),$$
$$g \mapsto \chi(g^{-1}),$$
$$g \mapsto \overline{\chi(g)}$$

leképezések karaktert definiálnak.
Amennyiben χ korlátos, akkor a két utóbbi karakter egybeesik.

Bizonyítás.

(1) $\chi_1(g)$ és $\chi_2(g)$ minden g-re értelmezett és nem nulla komplex szám, ezért a szorzatuk is egy nullától különböző komplex szám, továbbá χ_1 és χ_2 egy g-hez egyértelműen rendel egyetlen komplex számot. Ezek szorzata is egyértelműen meghatározott, így az első szabály egy leképezést definiál $\mathcal{G}$-ről $\mathbb{C}^\times$-be. Komplex számok szorzása kommutatív és asszociatív,

$$\chi_1(g_1g_2)\chi_2(g_1g_2) = (\chi_1(g_1)\chi_1(g_2))(\chi_2(g_1)\chi_2(g_2)) = (\chi_1(g_1)\chi_2(g_1))(\chi_1(g_2)\chi_2(g_2)),$$

így g_1g_2 képe a g_1 és g_2 képének szorzata. A leképezés művelettartó.

(2) g egyértelműen meghatározza az inverzét, ehhez χ egyértelműen rendel egy nem nulla komplex számot. Ez minden g-re érvényes, így $g \mapsto \chi(g^{-1})$ a $\mathcal{G}$-nek $\mathbb{C}^\times$-be való leképezése.

$$\chi((g_1g_2)^{-1}) = \chi(g_2^{-1}g_1^{-1}) = \chi(g_2^{-1})\chi(g_1^{-1}) = \chi(g_1^{-1})\chi(g_2^{-1}),$$

így a leképezés homomorfizmus.

(3) Minden $g \in \mathcal{G}$-re $\chi(g)$ létezik és egyértelmű nem nulla komplex szám, de akkor ez igaz a konjugáltjára is, hiszen a konjugálás automorfizmus $\mathbb{C}$-n. Mivel szorzat konjugáltja a konjugáltak szorzata, ezért ez ismét homomorfizmus.

(4) Ha a feltétel teljesül, akkor a 2.3 Tétel 5. és 6. pontja alapján a $\mathcal{G}$ minden g elemére teljesül, hogy $\chi(g^{-1}) = \overline{\chi(g)}$, de ekkor a két függvény megegyezik.

□

2.5. Definíció. Legyen χ_1, χ_2 a $\mathcal{G}$ kommutatív csoport karaktere.
Ekkor a $g \mapsto \chi_1(g)\chi_2(g)$ karakter *a χ_1 és χ_2 karakterek szorzata*, a $g \mapsto \chi(g^{-1})$ karakter *a χ karakter inverze*, a $g \mapsto \overline{\chi(g)}$ karakter a *a χ karakter konjugáltja.*
Az első jele $\chi = \chi_1\chi_2$, a másodiké χ^{-1}, az utolsóé $\overline{\chi}$.
$\mathcal{G}$ karaktereinek halmazát $\widehat{\mathcal{G}}$-vel jelöljük.

2.6. Tétel. *Tetszőleges $\mathcal{G}$ kommutatív csoport esetén $\widehat{\mathcal{G}}$ kommutatív csoport a karakterszorzással.*

Bizonyítás.

1. $\widehat{\mathcal{G}}$ nem üres: ha minden g-hez 1-et rendelünk, akkor ez egy leképezés $\mathcal{G}$-ről $\mathbb{C}$-be, nem azonosan nulla, és szorzattartó. Tehát karakter.
   Jelöljük ezt χ_0-val.

2. A karakterszorzás asszociatív: ha χ_1, χ_2 és χ_3 karakterek, akkor tetszőleges g-re

$$\begin{aligned}((\chi_1\chi_2)\chi_3)(g) &= ((\chi_1\chi_2)(g))\,\chi_3(g) = (\chi_1(g)\chi_2(g))\,\chi_3(g) = \chi_1(g)\,(\chi_2(g)\chi_3(g)) \\ &= \chi_1(g)\,((\chi_2\chi_3)(g)) = (\chi_1(\chi_2\chi_3))\,(g)\end{aligned}$$

tehát $(\chi_1\chi_2)\chi_3 = \chi_1(\chi_2\chi_3)$.

3. Bármely χ karakterrel a $\mathcal{G}$ minden g elemére

$$(\chi_0\chi)(g) = \chi_0(g)\chi(g) = 1 \cdot \chi(g) = \chi(g),$$

így $\chi_0\chi = \chi$, tehát χ_0 bal oldali egységelem $\widehat{\mathcal{G}}$-ben.

4. Tetszőleges $\chi \in \widehat{\mathcal{G}}$-vel és $g \in \mathcal{G}$-vel

$$(\chi^{-1}\chi)(g) = \chi^{-1}(g)\chi(g) = \chi(g^{-1})\chi(g) = \chi(g^{-1}g) = \chi(e) = 1 = \chi_0(g),$$

azaz a karakterekre átírva $\chi^{-1}\chi = \chi_0$.

Az eddigiek együtt biztosítják, hogy $\widehat{\mathcal{G}}$ csoport a χ_0 egységelemmel és χ^{-1}-gyel mint inverzzel.
Ezt a csoportot $\widehat{\mathcal{G}}$-vel fogjuk jelölni.

5. $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \chi_2(g)\chi_1(g) = (\chi_2\chi_1)(g)$,
mivel $\mathbb{C}$-ben a szorzás kommutatív, így $\chi_1\chi_2 = \chi_2\chi_1$, a karakterszorzás kommutatív.

□

2.7. Definíció. Ha $\mathcal{G}$ Abel-csoport, és $\chi_0 \colon \mathcal{G} \to \mathbb{C}^\times$ olyan, hogy minden $\mathcal{G}$-beli g-re $\chi_0(g) = 1$, akkor χ_0 a *főkarakter*.

2.8. Tétel. *Ha $\mathcal{G}$ véges Abel-csoport, akkor $\widehat{\mathcal{G}} \cong \mathcal{G}$.*

Bizonyítás. Legyen $B = \{b_i \mid r \geq i \in \mathbb{N}^+\}$, ahol $o(b_i) = n_i \in \mathbb{N}^+$, a véges $\mathcal{G}$ Abel-csoport bázisa. Nyilvánvaló, hogy $\widehat{\mathcal{G}}$ véges, mivel $\mathcal{G}$ minden eleméhez csak véges sok érték rendelhető, hiszen $g \in \mathcal{G}$-re tetszőleges χ karakterrel $\chi(g)$ egy véges fokú komplex egységgyök valamilyen hatványa, és ilyen csak véges számú van, a

kommutativitást pedig már beláttuk. Így $\widehat{\mathcal{G}}$ véges kommutatív csoport, ezért van bázisa. Legyen $r \geq i \in \mathbb{N}^+$-ra $\chi_i \colon \mathcal{G} \to \mathbb{C}$ olyan, hogy $b_j \in B$-re $\chi_i(b_j) = \varepsilon_1^{(n_i)}$, ha $i = j$, egyébként $\chi_i(b_j) = 1$. Továbbá, ha $g = \prod_{t=1}^{r} b_t^{k_t}$, akkor

$$\chi_i(g) = \chi_i\left(\prod_{t=1}^{r} b_t^{k_t}\right) = \prod_{t=1}^{r} \left(\chi_i(b_t)\right)^{k_t} = \left(\varepsilon_1^{(n_i)}\right)^{k_i}.$$

Igazoljuk, hogy ekkor $\widehat{B} = \{\chi_i \mid r \geq i \in \mathbb{N}^+\}$ egy bázis $\widehat{\mathcal{G}}$-ben.

a) Az $\left(1, k\frac{2\pi}{n}\right) = \left(1, \frac{2\pi}{n}\right)^k = 1 = (1, 0)$ akkor és csak akkor teljesül, ha $k\frac{2\pi}{n} = t \cdot 2\pi$, ami ekvivalens azzal, hogy $n \mid k$, és így $\varepsilon_1^{(n_i)}$ rendje n_i.

b) χ_i karakter. Ugyanis a definícióból következik, hogy minden csoportelemre az értéke egy nullától különböző komplex szám. A g-hez rendelt komplex szám egyértelmű, mivel g felírása a bázis elemeivel egyértelmű.

Legyen $g_1 = \prod_{t=1}^{r} b_t^{k_t{}^{(1)}}$ és $g_2 = \prod_{t=1}^{r} b_t^{k_t{}^{(2)}}$ két elem a csoportból. Ekkor $g_1 g_2 = \prod_{t=1}^{r} b_t^{k_t}$, ahol $r \geq t \in \mathbb{N}^+$, $n_t > k_t \in \mathbb{N}$ és $k_t \equiv k_t{}^{(1)} + k_t{}^{(2)}(n_t)$. Továbbá,

$$\chi_i(g_1 g_2) = \left(\varepsilon_1{}^{(n_i)}\right)^{k_i}$$
$$\chi_i(g_1)\chi_i(g_2) = \left(\varepsilon_1{}^{(n_i)}\right)^{k_i{}^{(1)}} \left(\varepsilon_1{}^{(n_i)}\right)^{k_i{}^{(2)}} = \left(\varepsilon_1{}^{(n_i)}\right)^{k_i{}^{(1)} + k_i{}^{(2)}}$$

a két komplex szám azonos a k-kra vonatkozó kongruencia miatt.

c) Legyen χ a $\mathcal{G}$ egy karaktere. A b_i rendje n_i, ezért $\chi(b_i) = \left(\varepsilon_1{}^{(n_i)}\right)^{m_i}$ valamilyen $n_i > m_i \in \mathbb{N}$ egésszel.

Tekintsük a $\chi' = \prod_{t=1}^{r} \chi_t{}^{m_t}$ karaktert, ekkor $\chi'(b_i) = \prod_{t=1}^{r} \chi_t{}^{m_t}(b_i) = \left(\varepsilon_1{}^{(n_i)}\right)^{m_i}$.
Amennyiben $g = \prod_{t=1}^{r} b_t^{k_t}$, akkor

$$\chi(g) = \chi\left(\prod_{t=1}^{r} b_t^{k_t}\right) = \prod_{t=1}^{r} \left(\chi(b_t)\right)^{k_t} = \prod_{t=1}^{r} \left(\left(\varepsilon_1^{(n_t)}\right)^{m_t}\right)^{k_t}$$
$$= \prod_{t=1}^{r} \left(\chi'(b_t)\right)^{k_t} = \chi'\left(\prod_{t=1}^{r} b_t^{k_t}\right) = \chi'(g),$$

így a χ_i-k generálják $\widehat{\mathcal{G}}$-ot.
Ha $\prod_{t=1}^{r} {\chi_t}^{s_t} = \chi_0$, akkor $1 = \chi_0(b_i) = \prod_{t=1}^{r} {\chi_t}^{s_t}(b_i) = \left({\varepsilon_1}^{(n_i)}\right)^{s_i}$ akkor és csak akkor, ha $n_i \mid s_i$. Ekkor viszont χ_i a B minden elemén 1, de akkor

$$\left(1, k\frac{2\pi}{n}\right) = \left(1, \frac{2\pi}{n}\right)^k = 1 = (1, 0)$$

valamennyi elemén is 1, $\chi_i \equiv 1$, vagyis $\chi_i = \chi_0$. Mivel ez minden $r \geq i \in \mathbb{N}^+$-ra igaz, ezért $\widehat{B}$ valóban bázis. Mivel B és $\widehat{B}$ elemeinek száma azonos, és minden i-re b_i és χ_i rendje azonos, így $\mathcal{G} \cong \widehat{\mathcal{G}}$. $\square$

2.9. Tétel. *Ha a $\mathcal{G}$ (nem feltétlenül véges) kommutatív csoportnak van bázisa, akkor tetszőleges $g \in \mathcal{G}\backslash\{e\}$-hez van olyan χ karakter, hogy $\chi(g) \neq 1$, ahol e a $\mathcal{G}$ egységeleme.*

Bizonyítás. Jelöljük $\mathcal{G}$ bázisát B-vel. A g báziselemek hatványszorzataként való felírásában van legalább egy olyan tényező, amely nem az egységelem, vagyis ha ez $b \in B$ a k kitevővel, akkor $b^k \neq e$. Ha b n-ed rendű, akkor legyen $\alpha = \varepsilon_1^{(n)}$, különben $\alpha = e^{i2\pi c}$ (e a természetes logaritmus alapja, és $k \neq 0$ a feltétel miatt), ahol $k^{-1} \neq c \in \mathbb{R}$.
Definiáljuk χ-t úgy, hogy

a) $\chi(b) = a$,

b) $b' \in B\backslash\{b\}$-re $\chi(b') = 1$, és

c) ha a $\mathcal{G}$ g' eleme $g' = b^{k_b} \cdot \prod_{b' \in \subseteq B\backslash\{b\}} (b')^{k'_b}$ alakú, akkor $\chi(g') = \alpha^{k_b}$.

Ez $\mathcal{G}$ minden eleméhez hozzárendel egy és csak egy nem nulla komplex számot, hiszen a bázisban való felírás egyértelmű. Ha $g_1 = b^{k_1}h_1$, $g_2 = b^{k_2}h_2$, ahol h_1 és h_2 felírásában már nem szerepel a b elem, akkor

$$\chi(g_1g_2) = \alpha^{k_1+k_2} = \alpha^{k_1}\alpha^{k_2} = \chi(g_1)\chi(g_2),$$

így χ karakter $\mathcal{G}$-n. Az α választása miatt $\alpha^k \neq 1$, ezért $\alpha^k = \chi(g) \neq 1$. $\square$

2.10. Következmény. Véges kommutatív csoport minden $g \neq e$ eleméhez van $\mathcal{G}$-nek olyan χ karaktere, amelyre $\chi(g) \neq 1$.

2.11. Tétel. *Legyen χ a $\mathcal{G}$ véges Abel-csoport karaktere. Ekkor*

$$\sum_{g\in\mathcal{G}}\chi(g)=\begin{cases}|\mathcal{G}| & , \text{ ha } \chi=\chi_0\\ 0 & , \text{ ha } \chi\neq\chi_0.\end{cases}$$

2.12. Tétel. *Legyen g a $\mathcal{G}$ véges Abel-csoport rögzített eleme. Ekkor*

$$\sum_{\chi\in\widehat{\mathcal{G}}}\chi(g)=\begin{cases}|\mathcal{G}| & , \text{ ha } g=e\\ 0 & , \text{ ha } g\neq e.\end{cases}$$

2.13. Tétel. (ortogonalitási tételek) *Legyen $\mathcal{G}$ véges Abel-csoport, χ_1 és χ_2, illetve g_1 és g_2 a $\mathcal{G}$ két karaktere és két eleme. Ekkor*

1. $\displaystyle\sum_{g\in\mathcal{G}}\chi_1(g)\overline{\chi}_2(g)=\begin{cases}|\mathcal{G}| & , \text{ ha } \chi_1=\chi_2\\ 0 & , \text{ ha } \chi_1\neq\chi_2.\end{cases}$

2. $\displaystyle\sum_{\chi\in\widehat{\mathcal{G}}}\chi(g_1)\overline{\chi}(g_2)=\begin{cases}|\mathcal{G}| & , \text{ ha } g_1=g_2\\ 0 & , \text{ ha } g_1\neq g_2.\end{cases}$

2.14. Példa. Legyen $\mathcal{G}$ negyedrendű ciklikus csoport γ generátorelemmel. Mivel $\gamma^4=1$, a $\mathcal{G}$ egy χ karakterére $\chi(\gamma)^4=1$, így χ csak négy értéket vehet fel γ-ban, lehet 1, -1, i vagy $-i$. Ha $\chi(\gamma)$ ismert, a χ többi értékét szorzással határozhatjuk meg: $\chi(\gamma^j)=\chi(\gamma)^j$. Így négy karaktert kapunk, melyek értékei az alábbi táblázatban láthatók.

	1	γ	γ^2	γ^3
$1_{\mathcal{G}}$	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	i	-1	$-i$
χ_3	1	$-i$	-1	i

3. Csoportreprezentáció

A fejezet megírásához a [7] irodalmat használtam fel.

A továbbiakban feltesszük, hogy G csoport és K test.

3.1. Definíció. A G *n-dimenziós reprezentációja* K fölött ($n \geq 1$) egy $\Phi\colon G \to GL(V)$ csoporthomomorfizmus, ahol V n-dimenziós vektortér K fölött, és $GL(V)$ jelölje az invertálható $V \to V$ lineáris transzformációk csoportját.

3.2. Megjegyzés. Speciálisan: az egydimenziós reprezentációk a karakterek.

Más szavakkal a reprezentáció egy szabály arra, hogyan rendeljünk hozzá egy lineáris transzformációt G minden eleméhez úgy, hogy összeegyeztethető legyen a csoport műveletekkel. Ezzel a szabállyal G hat a V vektortéren. A $\Phi(g)(v)$ jelölés helyett gyakran használnak $g \cdot v$-t, gv-t, vagy v^g-t $g \in G$-re és $v \in V$-re.

3.3. Példa. 1. Legyen G tetszőleges csoport, K tetszőleges test, a

$$\Phi\colon G \to GL_1(K) = K^\times,\ g \mapsto 1\ \forall g \in G$$

leképezés reprezentáció. Ezt G *triviális reprezentációjának* nevezzük K fölött.

2. Legyen $G = C_2 = \{1, g\}$ a másodrendű ciklikus csoport. Tetszőleges K test fölött

$$\Phi\colon G \to GL_1(K) = K^\times,\ g \mapsto -1$$

egy reprezentáció.

3. A $D_{2n} = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ diédercsoport természetesen hat a szabályos n-szögön, és ez egy hatást indukál $\mathbb{R}^2$-en vagy $\mathbb{C}^2$-en úgy, hogy

$$\sigma \mapsto \begin{bmatrix} \cos 2\pi/n & \sin 2\pi/n \\ -\sin 2\pi/n & \cos 2\pi/n \end{bmatrix},\ \tau \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

ami D_{2n}-nek egy 2-dimenziós reprezentációját definiálja.

4. Legyen $Q_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$ a kvaterniócsoport. Az

$$x \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \; y \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

egy reprezentációja Q_8-nak.

5. Legyen G véges csoport és legyen $X = \{x_1, \ldots, x_n\}$ véges halmaz, amin G hat. Tetszőleges K test felett tekintsünk egy n-dimenziós V vektorteret egy bázissal, melynek elemeit X elemeivel indexeljük: $v_{x_1}, \ldots, v_{x_n}$. A G csoport hatása V-n a következő: $g(v_x) = v_{g(x)}$ $\forall x \in X$ és $g \in G$. Ekkor G permutálja a bázis elemeit. Ezt *permutáció reprezentációnak* nevezzük K felett rögzített X mellett, és $K[X]$-el jelöljük.

   Ennek egy speciális esete, amikor H a G csoport részcsoportja, és X a G/H mellékosztályok halmaza. G az X-en a balról szorzás hatással hat: $g(kH) = (gk)H$. Ekkor a permutáció reprezentációt kapjuk rögzített $H \leq G$ mellett.

   Megjegyezzük, hogy ha $H = G$, akkor a triviális reprezentációt kapjuk. Ha $H = \{e\}$, azaz $X = G$, melyen G hat a balról szorzással, akkor az így kapott $K[G]$ permutáció reprezentációt *reguláris reprezentációnak* hívjuk.

3.4. Definíció. A $\Phi\colon G \to GL(V)$ és $\Psi\colon G \to GL(W)$ *reprezentációk közötti homomorfizmus* egy $f\colon V \to W$ lineáris leképezés, ami megőrzi a G hatását: $f(\Phi(g)(v)) = \Psi(g)(f(v))$.

A reprezentációk *izomorfizmusa* olyan homomorfizmus, ami a vektortereknek egy izomorfizmusa. Ha létezik egy izomorfizmus V és W között, akkor azt mondjuk, hogy V és W izomorf, amit $V \cong W$-vel jelölünk.

Legyen $\Phi\colon G \to GL(V)$ egy reprezentáció. Válasszunk egy V-beli bázist. Minden $V \to V$ lineáris leképezést ki tudunk fejezni egy K-beli együtthatós, $n \times n$-es mátrixként. Így egy olyan $G \to GL_n(K)$ leképezést kapunk, ahol $GL_n(K)$ a K-beli együtthatós, $n \times n$-es invertálható mátrixok csoportja. A

$$G \to GL_n(K),\ g \mapsto X_g$$
$$G \to GL_m(K),\ g \mapsto Y_g$$

homomorfizmusok egy $n \times m$-es A mátrixot adnak a következő tulajdonsággal:

$$AX_g = Y_g A \quad \forall g \in G$$

Ez izomorfizmus lesz egy olyan A-val megadva, ami négyzetes és invertálható. Ha választunk egy másik bázist V-n, akkor az X_g mátrixokat konjugáljuk egy invertálható mátrixszal. Így a reprezentációt a $\Phi\colon G \to GL_n(K)$ csoporthomomorfizmus egy konjugált osztályaként adjuk meg.

Tehát $\Phi\colon G \to GL_n(K)$ és $\Psi\colon G \to GL_n(K)$ azonosíthatók, ha létezik $A \in GL_n(K)$ úgy, hogy $\Phi(g) = A\Psi(g)A^{-1}$ $\forall g \in G$.

3.1. Mascke-tétel

3.5. Definíció. A $\Phi\colon G \to GL(V)$ reprezentáció egy *részreprezentációja* a V vektortér egy U altere, amin G invariánsan hat : $\Phi(g)(U) \leq U$ $\forall g \in G$.

3.6. Definíció. Egy reprezentáció *irreducibilis*, ha nem nulla és nincs nem nulla részreprezentációja.

3.7. Definíció. Vegyünk egy V reprezentációt és egy U részreprezentációt. Ekkor a V/U faktortér is reprezentáció a $g(v+U) = gv + U$ hatással. Ezt *faktor reprezentációnak* nevezzük.

3.8. Példa. Legyen G véges csoport, $K[G]$ pedig legyen a K test fölötti reguláris reprezentáció. A $K[G]$ vektortér egy bázisának elemei legyenek $v_g\colon g \in G$. Például: $v = \sum_{g \in G} v_g$ egy vektor $K[G]$-ben. Ez a vektor G hatása alatt állandó, ugyanis bármely $h \in G$-vel

$$h\left(\sum_{g \in G} v_g\right) = \sum_{g \in G} h(v_g) =^{g'=hg} \sum_{g' \in G} v_{g'} = v.$$

Tehát v lineáris burka $K[G]$-nek egy-dimenziós reprezentációja, ami izomorf a triviális reprezentációval.

Speciálisan, a reguláris reprezentáció sosem irreducibilis, kivéve, ha $|G| = 1$.

3.9. Definíció. Legyen V és W két reprezentációja G-nek. *V és W direkt összege* a $V \oplus W$-n adott reprezentáció, melyen $g(v, w) = (gv, gw)$, azaz G komponensenként hat $V \oplus W$ -n.

3.10. Definíció. A reprezentáció *felbonthatatlan*, ha nem nem-triviális részreprezentációk direkt összege.

Egy irreducibilis reprezentáció természetesen felbonthatatlan, de ez visszafelé nem mindig igaz. Ahhoz, hogy megértsünk minden véges dimenziós K test feletti csoportreprezentációt, elég, ha megértünk minden felbonthatatlant, mivel minden reprezentáció előáll felbonthatatlan reprezentációk direkt összegeként. Az irreducibilitás egy extrém korlátozó tényező, de gyakran egyszerűbb az irreducibilis reprezentációk osztályozása. De ez nem elég minden reprezentáció megértéséhez. Szerencsére ez a két tulajdonság (az irreducibilitás és a felbonthatatlanság) sok esetben megegyezik. Más szavakkal, minden véges dimenziós reprezentáció felírható irreducibilisek direkt összegeként.

3.11. Tétel. (Maschke-tétel) *Legyen G véges csoport és K test, melynek karakterisztikája relatív prím $|G|$-hez. Legyen V véges dimenziós reprezentációja G-nek K fölött és legyen U egy részreprezentáció. Ekkor létezik egy $W \leq V$ részreprezentáció úgy, hogy $V \cong U \oplus W$. Itt W -t az U komplementerének nevezzük V-ben.*

Bizonyítás. Legyen W' egy tetszőleges komplementere U-nak a V vektortérben. Nyilván W'-nek nem szükséges részreprezentációnak lennie. Konstruálunk egy W *komplementer részreprezentációt* U-hoz V-ben: legyen $\pi' \colon V \to U$ a W' menti vetítés: Mivel $V = U \oplus W'$ vektortér, minden $v \in V$-t felírhatunk $v = u + w'$ formában, ahol $u \in U$, $w' \in W'$, és legyen $\pi'(v) = u$. Megjegyezzük, hogy π' a vektorterek homomorfizmusa, és nem a reprezentációké. Továbbá π az identikus leképezés, melyet így definiálunk:

$$\pi(v) = \frac{1}{G} \sum_{g \in G} g^{-1} \pi(gv).$$

Azt állítom, hogy $W = \ker \pi$ az a komplementer, amit keresünk. Mivel U egy részreprezentáció, $\pi(gu) = gu \ \forall u \in U, \ g \in G$, ezért $\pi' \mid_U$ is az identikus leképezés. Ebből következik, hogy $W \cap U = \{0\}$. Ebből az is látszik, hogy π U-ba képez, ugyanis $\dim(\ker(\pi)) + \dim(im(\pi)) = \dim(V)$ (dimenziótétel lineáris leképezésekre), ahol $V \cong U \oplus W$. Azt kell még megmutatni, hogy W egy részreprezentáció.

Ehhez megmutatjuk, hogy π a reprezentációk homomorfizmusa. Vegyünk tetszőleges $v \in V$-t és $h \in G$-t. Ekkor

$$\begin{aligned}\pi(hv) &= \frac{1}{G}\sum_{g\in G} g^{-1}\pi(ghv) \\ &=^{g'=gh} \frac{1}{G}\sum_{g\in G} g^{-1}\pi(ghv) \\ &= h\pi(v).\end{aligned}$$

Vagyis π a reprezentációk homomorfizmusa, és ekkor W egy részreprezentáció. $\square$

3.12. Következmény. Ha G véges csoport és K test, melynek karakterisztikája $|G|$-hez relatív prím, akkor G-nek K fölött minden véges dimenziós reprezentációja irreducibilis reprezentációk direkt összege.

4. Véges test feletti vektorterek reprezentációi

4.1. Mátrixreprezentáció

A mátrixreprezentációk leírásához a [8] irodalmat használtam fel.
A legtöbb absztrakt algebrával foglalkozó egyetemi jegyzet azt mutatja meg, hogyan reprezentáljuk az $\mathbb{F}_q$ véges testet a prímteste, $\mathbb{F}_p$ fölött, azáltal, hogy világosan meghatározzák az additív struktúráját vektortérként vagy egy $\mathbb{F}_p$ fölötti hányadosgyűrűként, míg a multiplikatív struktúrát nehéz meghatározni; vagy részletesen jellemzik a multiplikatív csoport ciklikus struktúráját, anélkül, hogy az jól láthatóan kapcsolódna az additív struktúrához. A *mátrixreprezentáció* természetesen és egyszerűen adja meg az $\mathbb{F}_p$ prímtest feletti $\mathbb{F}_q$ test additív és multiplikatív struktúráit, ahol $q = p^d$. Bár ez a reprezentáció ismert, nem terjedt el széles körben az absztrakt algebrai irodalomban.

4.1.1. Először tekintsük a 8 elemű $\mathbb{F}_8$ testet a prímteste, $\mathbb{F}_2$ fölött. $\mathbb{F}_8$ additív struktúrája egy $\mathbb{F}_2$ fölötti 3-dimenziós vektortér:

$$V = \{ \begin{pmatrix}0 & 0 & 0\end{pmatrix}, \begin{pmatrix}1 & 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0 & 1\end{pmatrix}, \\ \begin{pmatrix}1 & 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1 & 1\end{pmatrix}\}$$

Azonban nem teljesen nyilvánvaló, hogyan definiáljuk ezeknek a vektoroknak a szorzatát, hogy $\mathbb{F}_8$ multiplikatív struktúráját kapjuk.

Bizonyítható, hogy ha megadjuk a V-beli $B = \{\begin{pmatrix}1 & 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0 & 1\end{pmatrix}\}$ bázis szorzástábláját,

			$\begin{pmatrix}1 & 0 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$
$\begin{pmatrix}1 & 0 & 0\end{pmatrix}$			$\begin{pmatrix}1 & 0 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$
$\begin{pmatrix}0 & 1 & 0\end{pmatrix}$			$\begin{pmatrix}0 & 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1 & 0\end{pmatrix}$
$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$			$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1 & 1\end{pmatrix}$

ebből megkapható $\mathbb{F}_8$ multiplikatív struktúrája.

Egy megszokottabb és hasznosabb eljárás, hogy $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x + 1)$ -et az $\mathbb{F}_2$ feletti összes polinom gyűrűjeként reprezentáljuk modulo a harmadfokú, irreducibilis $x^3 + x + 1$ polinom. Jelölje $a \in \mathbb{F}_8$ az x maradékosztályát modulo $x^3 + x + 1$, ekkor $a^3 + a + 1 = 0$. Mivel a karakterisztika 2, egyszerűen látszik,

hogy $a^3 = a + 1$, $a^4 = a^2 + a$, $a^5 = a^2 + a + 1$, $a^6 = a^2 + 1$, és $a^7 = 1$. Így

$$\begin{aligned}\mathbb{F}_8 &= \{0, 1, a, a^2, a^3, a^4, a^5, a^6\} \\ &= \{0, 1, a, a^2, a + 1, a^2 + a, a^2 + a + 1, a^2 + 1\}.\end{aligned}$$

Ebből következik, hogy $\mathbb{F}_8$ multiplikatív csoportja az $\mathbb{F}_8^* = \langle a \rangle$ hetedrendű ciklikus csoport, melyet a generál. $\mathbb{F}_8$ additív struktúrája már egyszerűen látszik a formula második feléből, bár a multiplikatív struktúrája még egy kicsit homályos. Az $\mathbb{F}_8$-beli elemek szorzásához használhatjuk a rövidített szorzástáblát a disztributivitással együtt.

	1	a	a^2
1	1	a	a^2
a	a	a^2	$a+1$
a^2	a^2	$a+1$	a^2+1

A $\{0, 1, a, a^2, a+1, a^2+a, a^2+a+1, a^2+1\}$-beli elemek szorzására használhatjuk az $a^3+a+1 = 0$ egyenlőséget. Ez a véges testek *standard reprezentációja*. Azonban az összeadás és a szorzás közötti átmenet még mindig nem egészen világos.

Tekintsük $\mathbb{F}_8$ egy tetszőleges b elemét, ekkor a b-vel való balról szorzás egy L_b lineáris transzformáció az $\mathbb{F}_2$ fölötti $V = \mathbb{F}_8$ vektortéren. Ha kiválasztjuk a $V = \mathbb{F}_8$ egy tetszőleges B' bázisát $\mathbb{F}_2$ felett, megkaphatjuk az L_b B'-re vonatkozó mátrixát: $[L_b] = [L_b]_{B'}$. Ha rögzítjük a B' bázist, és $\mathbb{F}_8$ minden eleméhez találunk ezzel a módszerrel egy mátrixot, azt kapjuk, hogy a mátrixok egy $\mathbb{F}_8$-cal izomorf testet alkotnak. Így minden egyes bázis választással, $\mathbb{F}_8$ egy, az eddigiektől eltérő mátrixreprezentációját kapjuk.

Első ránézésre úgy látszik, hogy mielőtt megkaphatnánk a mátrixreprezentációt, szükségünk van a test egy szorzástáblájára, de van egy módszer ennek elkerülésére. Legyen

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

az $f(x) = x^3 + x + 1$ harmadfokú irreducibilis polinom kísérő mátrixa az $\mathbb{F}_2$ test felett. Ekkor $f(A) = 0$, tehát A hatványai kielégítik a fent említett a által

kielégített egyenlőséget. Speciálisan, az A mátrix generálja az $\langle A\rangle$ hetedrendű ciklikus csoportot, amely $\mathbb{F}_8^*$-gal izomorf, és az

$$\mathbb{F}_2[A] = \{0, I, A, A^2, A^3, A^4, A^5, A^6\}$$

mátrixok gyűrűje izomorf az $\mathbb{F}_8$ testtel.

4.1.2. Vizsgáljuk a háromelemű $\mathbb{F}_3$ test fölötti $g(x) = x^2 + 1$ irreducibilis polinomot. Ennek B kísérőmátrixának a multiplikatív rendje 4 :

$$B = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, B^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, B^3 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Ez $\mathbb{F}_9$ elemeihez nem lesz elég. Szerencsére a megoldás egyszerű. Adjuk a 0, $I+B$, $I+B^3$, $B+B^2$, B^2+B^3 mátrixokat B hatványainak halmazához, hogy megkapjuk a a B által generált mátrixok gyűrűjét, $\mathbb{F}_3[B]$-t. Az $\mathbb{F}_3[B]$ gyűrű izomorf az $\mathbb{F}_9$ testtel, mivel $g(B) = B^2 + I = 0$. Ebből következik, hogy B megadja a 9 elemű test egy mátrixreprezentációját, $\mathbb{F}_3[B]$-t. Ilyenkor azt mondjuk, hogy B az $\mathbb{F}_9$ test egy generátora. Mi viszont, $\mathbb{F}_9$ egy *ciklikus generátorát* szeretnénk megkapni, ami egy olyan M mátrix, amire az $\mathbb{F}_9$ multiplikatív csoportja, $\mathbb{F}_9^*$ izomorf az M által generált $\langle M\rangle$ ciklikus csoporttal. Egy 8 elemű ciklikus csoportnak pontosan $\varphi(8) = 4$ generátora van, melyek közül egyik sem negyedrendű elem hatványa. Ezért az $\mathbb{F}_3[B]^* \cong \mathbb{F}_9^*$ multiplikatív csoport ciklikusan generálható 4 nemnulla mátrix bármelyikével $\mathbb{F}_3[B]$-ből, amik nem B hatványai. Belátható, hogy $M = I + B = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$ az $\mathbb{F}_9$ egy ciklikus generátora. Megjegyezzük, hogy az $\mathbb{F}_3[B]$ csoport $\mathbb{F}_3$ felett az I és B, valamint az I és M mátrixok által generált. Tehát $\mathbb{F}_3[B] = L(I, B) = L(I, M)$. Ha a B és M által alkotott bázisok (I, B) és (I, M),

akkor

$$\begin{aligned}
L_B\colon I \mapsto B = 0*I+1*B \qquad & \text{így } [L_B]_B = \begin{bmatrix}0 & 2\\ 1 & 0\end{bmatrix} = B,\\
B \mapsto B^2 = 2*I+0*B & \\
L_M\colon I \mapsto M = 1*I+1*B \qquad & \text{így } [L_M]_B = \begin{bmatrix}1 & 2\\ 1 & 1\end{bmatrix} = M, \text{ és}\\
B \mapsto MB = 2*I+1*B & \\
L_M\colon I \mapsto M = 0*I+1*M \qquad & \text{így } [L_M]_M = \begin{bmatrix}0 & 1\\ 1 & 2\end{bmatrix} = A\\
M \mapsto M^2 = 1*I+2*M &
\end{aligned}$$

Mivel A hasonló M-hez, A egy másik ciklikus generátora $\mathbb{F}_9$-nek. Ezenfelül A az $f_A(x) = x^2+x+2$ karakterisztikus polinom kísérőmátrixa. Ekkor A-t $\mathbb{F}_9$ kanonikus ciklikus generátorának nevezzük, és az $\mathbb{F}_3[A] = \{0, I, A, A^2, A^3, A^4, A^5, A^6, A^7\}$ reprezentációt $\mathbb{F}_9$ *kanonikus ciklikus reprezentációjának* nevezzük.

4.2. Weil-reprezentáció

A fejezethez a [9] és a [10] irodalmakat használtam fel.
Legyen V véges dimenziós vektortér az $\mathbb{F}_q$ véges test felett, melynek rendje q. Definiáljuk a $GL(V)$ π *természetes reprezentációját* a $\mathbb{C}[V]$ térben, amely az összes komplexértékű V-n értelmezett függvény tere. A π foka a V vektortér dimenziója. A π-t a következőképpen adjuk meg:

$$(\pi(g)f)(x) = f(g^{-1}x),$$

ahol $g \in G$, $f \in \mathbb{C}[V]$ és $x \in V$. A π reprezentáció karakterét a $g \mapsto q^{N(V;g)}$ hozzárendelés határozza meg, ahol $N(V;g) = \dim\ker(g^{-1})$.

4.2.1. Az általános lineáris csoport Weil-reprezentációja

Legyen V véges dimenziós vektortér az $\mathbb{F}_q$ véges test felett, és legyen V^* a V duális tere (a $V \to \mathbb{F}_q$ leképezések vektortere). Jelölje $< y, x >$ az $y \in V^*$ hatását $x \in V$-n és V^{**}-ot azonosítsuk V-vel $< x, y >= - < y, x >$ mellett.

4.1. Definíció. Legyen H csoport. Az a, $b \in H$ elemek *kommutátora*: $[a, b] = a^{-1}b^{-1}ab$.

4.2. Definíció. Jelölje $H(V)$ a $V \times V^* \times \mathbb{F}_q$ csoportot az alábbi szorzás művelettel: Minden egyes $(x, y, z) \in H(V)$-t azonosítunk a következő mátrixszal :

$$\begin{bmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}.$$

A $H(V)$ csoportot a *V-re vonatkozó Heisenberg csoportnak* nevezzük.

A szorzásszabály a következő:

$$(x, y, z) \cdot (x', y', z') = (x + x', y + y', z + z' + < y, x' >)$$

Ez azt mutatja, hogy a V, V^* és $\mathbb{F}_q$ csoportokat részcsoportként beágyaztuk a $H(V)$ csoportba. A $H(V)$ csoporton egy bilineáris formát indukálunk a $V \times V^*$-on definiált kommutátor segítségével:

$$[(x, y, z), (x', y', z')] = (0, 0, < y, x' > - < y', x >).$$

Ez a bilineáris forma alternáló, de egyben nem-elfajuló is, mert ha $((x, y), (x', y')) \mapsto 0$ minden x', y'-re, akkor $< y, x' >=< y', x >$. Legyen $y' = 0$, akkor $< y, x' >= 0$ minden x'-re és ekkor $y = 0$, és hasonlóképpen, ha $x' = 0$, akkor $< y', x >= 0$ minden y'-re és ekkor $x = 0$.

A bilineáris formának a nem-elfajultságából következik, hogy $H(V)$ centruma $\mathbb{F}_q$: ugyanis, legyen Z a centrum és $h = (x, y, z) \in Z$. A szorzásszabályból látható, hogy

$$< y, x' >=< y', x >$$

minden x', y'-re, azaz $< y, x' > - < y', x >= 0$. Ebből következik, hogy $x = y = 0$, tehát $h \in \mathbb{F}_q$. Az $\mathbb{F}_q \subseteq Z$ tartalmazás közvetlenül következik a szorzásszabályból. A nem-elfajultságból az is következik, hogy $V \times \mathbb{F}_q$ és $V^* \times \mathbb{F}_q$ is a $H(V)$ maximális kommutatív részcsoportja.

A továbblépéshez még szükségünk van a most következő, reprezentációkra vonatkozó általános állításra.

4.3. Állítás. *Legyen H véges csoport Z centrummal. Tegyük fel, hogy Z-nek van olyan ζ karaktere, amire minden $h \in H \backslash Z$-hez létezik $h' \in H$ úgy, hogy $[h', h] \in Z$ és $\zeta([h', h]) \neq 1$. Ekkor H bármely η reprezentációja megadható ζ-val Z-n :*

1. *η karakterének tartója Z-ben van, azaz $\mathrm{Tr}_\eta(h) = 0$ minden $h \in H \backslash Z$,*
2. *η akkor és csak akkor irreducibilis, ha a foka $d(\eta) = \sqrt{|H : Z|}$.*
3. *Egyetlen ilyen irreducibilis η van.*

Bizonyítás. Legyen η a Z-n ζ-val meghatározott reprezentáció.
Bármely $h \in H \backslash Z$-hez válasszuk h'-t olyannak, mint az állítás feltételében.

1. Ekkor
$$\begin{aligned} \mathrm{Tr}\,\eta(h) = \mathrm{Tr}\,\eta(h'hh'^{-1}) = \mathrm{Tr}\,\eta([h', h]h) = \\ = \mathrm{Tr}\,(\zeta([h', h])\eta(h)) = \zeta([h', h])\mathrm{Tr}\,(\eta(h)) \end{aligned}$$
Innen következik, hogy $\mathrm{Tr}\,\eta(h) = 0$.

2. η akkor és csak akkor irreducibilis, ha a véges csoportokra vonatkozó dimenziós tétel szerint a csoport elemszáma az η irreducibilis reprezentációk csoportkaraktereinek négyzetösszege (lásd [13]), azaz
$$\sum_{h \in H} |\mathrm{Tr}\,(\eta(h))|^2 = |H|.$$
Most
$$\sum_{h \in H} |\mathrm{Tr}\,(\eta(h))|^2 = \sum_{z \in Z} |\zeta(z)|^2 d(\eta)^2 = d(\eta)^2 \sum_{z \in Z} |\zeta(z)|^2 = d(\eta)^2 |H|,$$
amiből következik az állítás.

3. Legyen π a ζ által meghatározott reprezentáció H-n. Ekkor bármely $z \in Z$-re és a π képterében lévő f-re,
$$\pi(z)(f)(h) = f(hz) = f(zh) = \zeta(z)f(h).$$
Ez azt jelenti, hogy $\pi(z) = \zeta(z) \cdot 1$, ezért π minden irreducibilis komponense megadható ζ-val Z-n, ebből következik a létezés.

Az egyértelműséghez tegyük fel, hogy η és η' is teljesítik a feltételeket. Ekkor

$$< \chi_\eta, \chi_{\eta'} > = |H|^{-1} \sum_{h \in H} \overline{Tr(\eta(h))} Tr(\eta'(h)) =$$
$$= |H|^{-1} d(\eta) d(\eta') \sum_{z \in Z} \overline{\zeta(z)} \zeta(z) = 1,$$

tehát $\eta = \eta'$.

Ezzel az állítás mindhárom részét igazoltuk. □

4.4. Állítás. *Legyen ζ a $H(V)$ csoport Z centrumának nem-triviális karaktere. Ekkor egyértelműen létezik $H(V)$-nek olyan η_ζ irreducibilis reprezentációja, amit ζ határoz meg Z-n. Ennek a foka $|V|$, és karakterének tartója Z.*

Bizonyítás. Mivel $H(V)$ centruma $\mathbb{F}_q$, ζ-t tekinthetjük egy $\mathbb{F}_q$-n értelmezett karakterként. Mivel ζ nemtriviális, és a bilineáris forma $V \times V^*$-on nem-elfajuló, így bármely $(x, y) \in V \times V^*$-ra tudunk találni olyan (x', y')-t, amire

$$\zeta(< y, x' > + < x, y' >) \neq 1.$$

Ez azt jelenti, hogy bármelyik $h \in H \backslash Z$-hez létezik olyan h', amivel $\zeta([h', h]) \neq 1$ és nyilván $[h', h]$ a Z centrumban van.

Mivel $\sqrt{|H(V) \colon Z|} = \sqrt{|V \times V^*|} = |V|$, így az állítás következik az előzőből. □

Vegyünk $\mathbb{F}_q$-n egy nem-triviális ζ karaktert. Legyen $1 \cdot \zeta$ az a karakter $V^* \cdot \mathbb{F}_q$-n (a tenzorszorzat jelet elhagyjuk), amit $1 \cdot \zeta(yz) = \zeta(z)$ határoz meg. Legyen π az $1 \cdot \zeta$ által meghatározott reprezentáció $H(V)$-n.

$\mathbb{C}[V]$-t beágyazhatjuk π standard terébe, mert minden $h \in H(V)$ Heisenberg-csoportbeli elem egyértelműen felírható $k \times x$ szorzatként, ahol $k \in V^* \cdot \mathbb{F}_q$, $x \in V$. Mivel
$(x, y, z) = (0, y, z) \cdot (x, 0, 0)$, így bármely $f \in \mathbb{C}[V]$-t tekinthetjük $\mathbb{C}[H(V)]$-belinek, az $f(h) = \zeta(h) f(x)$ azonosítással. Mivel $\mathbb{C}[V]$ invariáns altér a π leképezésre, így a π leszűkítésével kapunk egy η reprezentációt a $\mathbb{C}[V]$ térben. Mivel

$$(x, 0, 0) \cdot (x_0, y_0, z_0) = (0, y_0, z_0 - < y_0, x + x_0 >) \cdot (x + x_0, 0, 0),$$

η a következőképpen fejezhető ki:

$$(\eta(x_0, y_0, z_0)f)(x) = \zeta(z_0)\zeta(< x + x_0, y_0 >)f(x + x_0).$$

Legyen $x_0 = y_0 = 0$, akkor η-t ζ definiálja Z-n, és mivel ennek a foka $\dim(\mathbb{C}[V]) = |V|$, ebből következik, hogy $\eta = \eta_\zeta$.

Legyen $G(V)$ a $G(V \times V^*)$ azon részcsoportja, ami a $H(V)$ által a $V \times V^*$-on indukált bilineáris formára invariáns. Tetszőleges $g \in GL(V)$-hez találhatunk olyan $g^* \in GL(V^*)$ elemet, amire $< g^*y, gx >=< y, x >$ minden x, y esetén (ugyanis $g^*y = yg^{-1}$). Ekkor $G(V) = \{(g, g^*) \mid g \in GL(V)\}$ és mivel $(gg')^* = g^*g'^*$, azt kapjuk, hogy $G(V) \cong GL(V)$. Ez azt jelenti, hogy $G(V)$ egy reprezentációja egyben $GL(V)$ reprezentációja is. $G(V)$ a következőképpen hat $H(V)$-n:

$$g \cdot (x, y, z) \mapsto (gx, g^*y, z).$$

Végül, legyen $GH(V)$ a $G(V)$ és $H(V)$ terek féldirekt szorzata.

4.5. Definíció. A G_2 és G_1 csoportok *féldirekt szorzata* az (x, y) számpárok halmaza, ahol $x \in G_2$, $y \in G_1$ és egy adott $\alpha\colon G_2 \to \mathrm{Aut}(G_1)$, $x \mapsto \alpha_x$ homomorfizmussal: $(\alpha_{xy} = \alpha_x \circ \alpha_y)$, ahol a csoportművelet

$$(x_1, x_2)(y_1, y_2) = (x_1\alpha_{x_2}(y_1), x_2y_2).$$

Triviális α-ra a direkt szorzatot kapjuk. Jele: $G_2 \ltimes G_1$.

4.6. Tétel. (Weil-reprezentáció) *A $G(V)$ csoporton egyértelműen létezik egy W reprezentáció, amit $G(V)$ Weil-reprezentációnak nevezünk, úgy, hogy*

1. *$H(V)$ tetszőleges olyan η irreducibilis reprezentációjára, ami nem-triviális $H(V)$ Z centrumán, van $GH(V)$-nek egy olyan ρ reprezentációja az η terében, hogy ρ megegyezik η-val $H(V)$-n és ρ leszűkítése a $G(V)$-re W.*

2. *W karaktere pozitív értékeket vesz fel.*

Bizonyítás. Az egyértelműség 1.-ből és 2.-ből rögtön következik.

A létezéshez, legyen Z-n adott egy ζ karakter. Tekintsük $G(V) \times V^* \times \mathbb{F}_q$ karakterét, $1 \cdot 1 \cdot \zeta$-t és az általa indukált reprezentációt $GH(V)$-n. Ezt a reprezentációt az előbbi módon meg tudjuk szorítani a ρ reprezentációra a $\mathbb{C}[V]$ térben:

$$(\rho(g_0, x_0, y_0, z_0)f)(x) = \zeta(z_0)\zeta(< g_0^{-1}(x + x_0), y_0 >)f(g_0^{-1}(x + x_0)).$$

Megszorítjuk $H(V)$-re, azaz ha $g_0 = 1$, akkor $\rho = \eta_\zeta$, és leszűkítjük $G(V)$-re, azaz ha $x_0 = y_0 = z_0 = 0$, akkor ρ hatása $(\rho(g)f)(x) = f(g^{-1}x)$ független ζ-tól. Ez azt jelenti, hogy vehetjük W-t, ami a ρ-nak $G(V)$-re való megszorítása.

Most legyen $\{e_v \in \mathbb{C}[V] \mid v \in V\}$, ahol e_v az a függvény, ami v-t az 1-be képezi ($v \mapsto 1$), minden mást pedig a 0-ba. Ezek $\mathbb{C}[V]$ egy bázisát alkotják.

$$(W(g)e_v)(x) = e_v(g^{-1}x) = e_{gv}(x), \ \textit{azaz}\ W(g)e_v = e_{gv}.$$

Következésképpen, ebben a bázisban, $W(g)$ az egységmátrix egy permutációja, ezért a nyoma pozitív.
Ezzel a tételt beláttuk. □

4.7. Következmény. A W Weil-reprezentációra és bármely $g \in G(V)$-re,

$$\operatorname{Tr} W(g) = q^{N(V;g)},$$

ahol $N(V; g) = \frac{1}{2} \dim \ker (g - 1)$.

Bizonyítás. A tétel bizonyításából látjuk, hogy $W(g)$ nyoma azon $v \in V$-k számával egyenlő, amikre $e_{gv} = e_v$, vagyis egyenlő a $g - 1$ elemnek, mint $GL(V)$-beli elem magjának a rendjével. Ennek a dimenziója egy $GL(V \times V^*)$-beli $g - 1$ elem magterének a fele. Az állítás abból következik, hogy ez a mag vektortér az $\mathbb{F}_q$ véges test felett. □

4.3. A Heisenberg csoport egydimenziós reprezentációi véges test felett

A fejezet megírásához a [11] irodalmat használtam fel.
Legyen F véges test, melynek $q = p^m$ eleme van, ahol p prím és m pozitív egész. Legyen W véges dimenziós vektortér F fölött és legyen $< , >$ nem-elfajuló szimplektikus bilineáris forma W-n, azaz $< , >$ egy $W \times W \to F$ leképezés a következő tulajdonságokkal:

1. $< , >$ mindkét változóban lineáris;

2. $< , >$ *nem-elfajuló*, azaz bármely $w \in W$, $w \neq 0$-hoz van $w' \in W$ úgy, hogy $< w, w' > \neq 0$;

3. $< , >$ *szimplektikus*, azaz minden w, $w' \in W$-re $< w, w' > = - < w', w >$.

4.8. Definíció. A $H = H(W)$ a W*-hez rendelt Heisenberg csoport*, amelynek alaphalmaza $W \times F$, és a szorzásművelet a következő:

$$(w, a)(w', a') = (w + w', a + a' + < w, w' >)$$

minden w, $w' \in W$-re és a, $a' \in F$-re.

Megmutatjuk, hogy $H(W)$-nek q^{2n} egydimenziós reprezentációja van.
Legyen $\dim W = 2n$, valamilyen pozitív n egészre. Ekkor $|H| = q^{2n+1}$.
Ha $p = 2$, akkor a csoport Abel-csoport és minden reprezentációja egydimenziós, azaz karakter.
Most feltesszük, hogy p páratlan prím.

4.9. Lemma. *Legyen $w \in W$, $w \neq 0$. Definiáljuk a $\varphi_w \colon W \to F$ leképezést a következő módon: $\varphi_w(w') = < w, w' >$. Ekkor φ_w ráképezés.*

Bizonyítás. Legyen $b \in F$. Ha $b = 0$, akkor legyen $w' = 0$. Vegyük $b \neq 0$-t. Mivel $<, >$ nem-elfajuló, van olyan $w' \in W$, amire $< w, w' > = 1$. Ebből következik, hogy $\varphi_w(bw') = < w, bw' > = b < w, w' > = b$. □

4.10. Lemma. *H-nak $q^{2n} + q - 1$ konjugált osztálya van.*

Bizonyítás. Legyen $(w, 0) \in H$ és $w \neq 0$. Ekkor az a konjugált osztály, ami tartalmazza ezt az elemet:

$$(w', a')(w, 0)(-w', -a') = (w, 2 < w', w >).$$

Ebből és a 4.9-ból az következik, hogy $(w, 0)$ konjugált osztálya $\{(w, a) \in H \mid w \neq 0\}$. Ezért $q^{2n} - 1$ ilyen osztály van és minden osztályban q elem van.

Legyen most $w = 0$ és tekintsük $(0, a)$ konjugált osztályait, ahol $a \in F$. Ekkor az előbbihez hasonló számolással meg tudjuk mutatni, hogy q különböző ilyen konjugált osztály van és minden osztályban egy elem van. □

4.11. Következmény. $H(W)$-ben a konjugált osztályoknak 2 típusa van: a $(w,0)$, $w \neq 0$ és $(0,a)$, $w \in W$, $a \in F$ reprezentáns elemekkel.

4.12. Következmény. A $H(W)$ Heisenberg-csoportnak $q^{2n}+q-1$ irreducibilis reprezentációja van.

4.13. Lemma. *H centruma, $Z(H)$, izomorf F^+-szal.*

Bizonyítás. Legyen $(w,a) \in Z(H)$, ekkor

$$(w,a)(w',a') = (w',a')(w,a)$$

minden $(w',a') \in H$ esetén. Ezért

$$(w'+w, a'+a+ < w', w >) = (w+w', a+a'+ < w, w' >).$$

Itt $< w,w' >=< w',w >$ vagy $< w,w' >= 0$. Mivel $<,>$ nem-elfajuló, $w = 0$. Ezért

$$Z(H) = \{(0,a) \in H \mid a \in F\}.$$

Definiáljuk $f\colon Z(H) \to F^+$ -t úgy, hogy $f(0,a) = a$. Könnyű belátni, hogy f izomorfizmus. $\square$

4.14. Lemma. *H kommutátorcsoportja, $[H,H]$, megegyezik H centrumával, $Z(H)$-val.*

Bizonyítás. Legyen (w,a), $(w',a') \in H$. Ekkor

$$(w,a)(w',a')(-w,-a)(-w',-a') = (0, < w,w' >).$$

Az 4.9-at alkalmazva azt kapjuk, hogy $[H,H] = Z(H)$. $\square$

4.15. Következmény. A $H/Z(H)$ faktorcsoport kommutatív, és elemszáma $|H/Z(H)| = \frac{q^{2n+1}}{q} = q^{2n}$.

4.16. Lemma. *H bármely ρ karaktere (egydimenziós reprezentációja) indukálja a $H/Z(H)$ egy karakterét, és megfordítva is, $H/Z(H)$ bármely karaktere indukálja H egy karakterét.*

Bizonyítás. Legyen (w,a), $(w',a') \in H$. Ekkor

$$\begin{aligned}\rho((w,a)(w',a')(-w,-a)(-w',-a')) &= \rho((w,a)\rho(w',a')\rho(-w,-a)\rho(-w',-a')) \\ &= \rho((w,a)\rho(w',a')(\rho((w,a))^{-1}(\rho(w',a'))^{-1} \\ &= 1 \\ &= \rho(0,<w,w'>).\end{aligned}$$

Tehát ρ triviális $[H,H] = Z(H)$-n. Legyen $\widetilde{(w,a)}$ a $H/Z(H)$ faktorcsoport egy eleme, amit (w,a) reprezentál. Könnyen ellenőrizhető, hogy $\tilde{\rho}$: $H/Z(H) \to \mathbb{C}^\times$, $\tilde{\rho}\left(\widetilde{(w,a)}\right) = \rho(w,a)$ $H/Z(H)$-nak egy jól definiált karaktere. Megfordítva, $H/Z(H)$ tetszőleges $\tilde{\rho}$ karaktere meghatározza H egy karakterét a következőképpen: $\rho(w,a) = \tilde{\rho}\left(\widetilde{(w,a)}\right)$.
□

4.17. Lemma. *A $H/Z(H)$ csoport izomorf a W additív csoportjával.*

Bizonyítás. Legyen φ: $H \to W$ a következőképpen definiálva: $\varphi(w,a) = w$. Ekkor φ ráképező homomorfizmus és magja $Z(H)$. □

4.18. Következmény. A $H/Z(H)$ csoport bármely karakterét meghatározza a W-n felvett értéke a következőképpen: A $Z(H)$ halmaz összes reprezentáló elemének halmaza $H/Z(H)$-ban a $W \times \{0\} = \{(w,0) \mid w \in W\}$.

Bizonyítás. Legyen $\widetilde{(w,a)} \in H/Z(H)$. Ekkor $\widetilde{(w,a)} = \widetilde{(w,0)}$, mivel $(w,a) - (w,0) = (0,a) \in Z(H)$. □

A H Heisenberg-csoport minden karakterét jellemzi az alábbi állítás.

4.19. Állítás. *Legyen χ az F^+ csoport nem-triviális karaktere.*
Bármely $(w,0) \in W \times \{0\}$-ra definiáljuk $\widetilde{\psi_{(w,\chi)}}$-t a következőképpen:
$\widetilde{\psi_{(w,\chi)}}$: $H/Z(H) \to \mathbb{C}^\times$, $\widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w',0)}\right) = \chi(<w,w'>)$ *minden* $\widetilde{(w',0)} \in H/Z(H)$ *elemre. Ekkor* $\widetilde{\psi_{(w,\chi)}}$ *a* $H/Z(H)$ *egy karaktere.*

Bizonyítás. Először azt mutatjuk meg, hogy $\widetilde{\psi_{(w,\chi)}}$ jól definiált:
Legyen $\widetilde{(w_1,0)} = \widetilde{(w_2,0)} \in H/Z(H)$, innen következik, hogy $(w_1,0) - (w_2,0) \in$

$Z(H)$. Ekkor $(w_1 - w_2, 0 + 0+ < w_1, w_2 >) \in Z(H)$, így $w_1 - w_2 = 0$. Vagyis $w_1 = w_2 = w'$, azaz

$$\widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_1,0)}\right) = \widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_2,0)}\right) = \chi(< w, w' >).$$

Másrészt

$$\begin{aligned}
\widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_1,0)}\widetilde{(w_2,0)}\right) &= \widetilde{\psi_{(w,\chi)}}\left((w_1 + w_2, 0 \widetilde{+ 0+} < w_1, w_2 >)\right) \\
&= \widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_1 + w_2}, 0)\right) \\
&= \chi(< w, w_1 + w_2 >) \\
&= \chi(< w, w_1 > + < w, w_2 >) \\
&= \chi(< w, w_1 >)\chi(< w, w_2 >) \\
&= \widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_1,0)}\right)\widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w_2,0)}\right)
\end{aligned}$$

□

4.20. Lemma. *Bármely $a \in F^\times$-re a $\widetilde{\psi_{(aw,\chi)}} = \widetilde{\psi_{(w,\chi_a)}}$ leképezés, ahol $\chi_a(x) = \chi(ax)$ minden $x \in F$-re, az F^+ csoport karaktere.*

Bizonyítás. Tetszőleges $\widetilde{(w',0)} \in H/Z(H)$ esetén

$$\begin{aligned}
\widetilde{\psi_{(aw,\chi)}}\left(\widetilde{(w',0)}\right) &= \chi(< aw, w' >) \\
&= \chi(a < w, w' >) \\
&= \chi_a(< w, w' >) \\
&= \widetilde{\psi_{(w,\chi_a)}}\left(\widetilde{(w',0)}\right).
\end{aligned}$$

□

4.21. Lemma. *Legyen χ az F^+ csoport egy karaktere. Ha $\widetilde{\psi_{(w,\chi)}} = \widetilde{\psi_{(w',\chi)}}$, akkor $w = w'$.*

Bizonyítás. Legyen $\widetilde{\psi_{(w,\chi)}} = \widetilde{\psi_{(w',\chi)}}$. Ekkor bármely $\widetilde{(w'',0)} \in H/Z(H)$ esetén

$$\begin{aligned}
\widetilde{\psi_{(w,\chi)}}\left(\widetilde{(w'',0)}\right) &= \chi(< w, w'' >) \\
&= \widetilde{\psi_{(w',\chi)}}\left(\widetilde{(w'',0)}\right) \\
&= \chi(< w', w'' >).
\end{aligned}$$

Ebből azt kapjuk, hogy

$$\chi(< w - w', w'' >) = 1.$$

Mivel $<,>$ nem-elfajuló, így $w - w' = 0$, akkor $w = w'$. $\square$

4.22. Tétel. *A $H = H(W)$ Heisenberg-csoportnak q^{2n} karaktere van.*

Bizonyítás. Mivel $|W \times \{0\}| = |\{(w, 0) \mid w \in W\}| = q^{2n}$, 4.20-ból és 4.21-ből következik, hogy $H/Z(H)$-nak q^{2n} karaktere van. 4.16-ból pedig következik a tétel. $\square$

4.23. Megjegyzés. A $H(W)$ Heisenberg-csoportnak van további $q - 1$ irreducibilis reprezentációja. Ezeknek a dimenziója egynél nagyobb, és leírásuk bonyolultabb. Ezeket a szakdolgozatomban nem részletezem.

5. Irodalomjegyzék

Hivatkozások

[1] G. Mullen, D. Panario - Handbook of Finite Fields, CRC Press (2013), 1-43

[2] Horváth Gábor - Véges testek és alkalmazásaik, Debreceni Egyetem (2016), 1-107

[3] Gonda János - Véges testek, ELTE Informatikai Kar Jegyzet (2012), 1-195

[4] Keith Conrad - Finite Fields, University of Connecticut, Handout, 1-13

[5] Keith Conrad - Characters of finite Abelian groups, University of Connecticut, Handout, 1-26

[6] Andrei Marcus - Algebra, Kolozsvári Egyetemi Kiadó (2008), 225-227

[7] Alex Bartel - Introduction to representation theory of finite groups, Lecture notes (2017), 2-6

[8] William P. Wardlaw - Matrix Representation of Finite Fields, Mathematical Association of America vol.67 (1944), 289-291

[9] Tim Tzaneteas - Weil Representations of Finite Fields, Lecture notes (2005), 1-7

[10] Paul Gérardin - Weil Representations Associated to Finite Fields, Journal of Algebra 46 (1977), 54-101

[11] Manouchehr Misaghian - The Representations of the Heisenberg Group over a Finite Field, Armenian Journal of Mathematics vol.3 (2010), 162-173

[12] Menezes, Blake, Gao, Mullin, Vanstone, Yanghoobian - Applications of Finite Fields, Springer (1993)

[13] Eric W. Weisstein - Dimensionality Theorem (1996), http://mathworld.wolfram.com/DimensionalityTheorem.html