Tímarit um raunvísindi og stærðfræði
2. árg. 2. hefti 2004 – raust.is/2004/2/16

Ferningsform yfir kroppa með kennitölu 2⋆

Jón Kr. Arason

Raunvísindastofnun Háskólans

Vefútgáfa: 16. desember 2004

Ágrip – Þegar fjallað er um ferningsform yfir kroppa þá er oftast gert ráð fyrir því að kennitala kroppsins sé ekki 2. Í fyrirlestrinum er leitazt við að lýsa því með dæmum að margt verður öðruvísi ef kennitalan er 2. Helzta dæmið eru nýlegir útreikningar fyrirlesarans á Witt-grúpu kropps Laurent raða yfir kropp með kennitölu 2.

1. Inngangur

Við vitum öll hvernig annarrar gráðu jafnan

$$ax^2 + bx + c = 0$$

er leyst. Við tökum a út fyrir sviga og fullkomnum ferninginn. Jafnan verður þá

$$a\left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a} = 0$$

Ef til er ferningsrót d af $b^2 - 4ac$ þá fást lausnirnar

$$x = \frac{-b \pm d}{2a}$$

Hér er gert ráð fyrir að grunnreiknigerðirnar fjórar séu til taks. Það þýðir að við erum að vinna í kroppi K. Við deilum með a svo við verðum að gera ráð fyrir að a sé ekki núll. Það er engin takmörkun því annars væri jafnan ekki annarrar gráðu jafna. En við deilum líka með 2 svo við verðum að gera ráð fyrir að 2 sé ekki núll, þ.e. að kennitala kroppsins K sé ekki 2. Þetta er takmörkun. Ef K er til dæmis kroppurinn með tveim stökum 0 og 1, þar sem $1 + 1 = 0$, þá hefur jafnan $x^2 + x + 1 = 0$ enga lausn í K þótt draga megi ferningsrætur af báðum stökunum í K.

Í fræðunum um ferningsform er annarrar gráðu jafnan gerð einsleit og skrifuð á forminu

$$ax^2 + bxy + cy^2 = 0$$

Það breytir litlu við lausnina. Almennar skoða menn jöfnur af taginu

$$\sum_{1 \le i \le j \le n} a_{ij} x_i x_j = 0$$

Vinstri hliðin hér er ferningsform í n breytum. Ef kennitalan er ekki 2 þá má nota sömu hugmynd og fyrir annarrar gráðu jöfnuna til að koma þessari jöfnu á formið

$$\sum_{1 \le i \le n} b_i y_i^2 = 0$$

með línulegum breytuskiptum. Ferningsformið á vinstri hlið þessarar jöfnu er sagt vera á hornalínuformi.

Til að fá fullkomna yfirsýn yfir leysanleika jafna af taginu

$$\sum_{1 \le i \le j \le n} a_{ij} x_i x_j = 0$$

yfir gefinn kropp K vilja menn flokka öll möguleg ferningsform yfir K þannig að tvö ferningsform séu talin jafngild, þ.e. lendi í sama flokki, ef hægt er að fá hvort þeirra úr hinu með línulegum breytuskiptum. Þá er til þæginda gert ráð fyrir að ferningsformin séu ekki úrkynjuð, en það þýðir nokkurn veginn að ekki sé hægt að fækka breytunum með línulegum breytuskiptum. Fyrir ferningsform á hornalínuformi þýðir þetta (ef kennitalan er ekki 2) að enginn stuðlanna sé 0.

⋆ Grein þessi er efni fyrirlesturs á ráðstefnunni *Stærðfræði á Íslandi 2003* á Akureyri 30.-31. ágúst 2003

Fyrir flesta kroppa K er mjög erfitt að flokka ferningsform á þennan hátt. En auðvelt er að sjá að yfir tvinntölurnar flokkast ferningsformin algerlega eftir fjölda breytanna. Það er heldur ekki er erfitt að sanna að yfir rauntölurnar nægir að skoða fjölda jákvæðra stuðla og fjölda neikvæðra stuðla eftir að búið er að koma ferningsforminu á hornalínuform.

2. Witt-grúpa

Nú á dögum nota menn í þessum fræðum heldur rúmfræðilegri talsmáta. Ferningsform yfir K er skilgreint sem vörpun $\varphi : V \to K$, þar sem V er endanlega vítt vigurrúm yfir K, þannig að ef valinn er einhver grunnur fyrir V þá verði $\varphi(\underline{x})$ gefið með formúlu af taginu

$$\varphi(\underline{x}) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$$

þar sem $x_1, \ldots, x_n$ tákna hnit vigursins $\underline{x}$ miðað við þennan grunn. Það má líka orða þetta þannig að $\varphi(a\underline{x}) = a^2\varphi(\underline{x})$ fyrir öll a í K og öll $\underline{x}$ í V og að vörpunin $\beta : V \times V \to K$, $(\underline{x}, \underline{y}) \mapsto \varphi(\underline{x} + \underline{y}) - \varphi(\underline{x}) - \varphi(\underline{y})$, sé tvílínuleg. Það að ferningsformið sé ekki úrkynjað þýðir að þetta tvílínulega form β sé ekki úrkynjað, þ.e. að $\beta(\underline{x}, \underline{y}) = 0$ fyrir öll $\underline{y} \in V$ gildi ekki nema $\underline{x} = 0$. Við munum yfirleitt gera ráð fyrir að svo sé án þess að taka það sérstaklega fram. Í stað breytuskipta má núna skoða mismunandi grunna fyrir tilheyrandi vigurrúm. Með því að nota þennan talsmáta verða tvö ferningform jafngild ef þau eru einsmóta, þ.e. ef til er andhverfanleg línuleg vörpun á milli tilheyrandi vigurrúma sem breytir öðru ferningsforminu yfir í hitt.

Með því að nota beinar summur vigurrúma má nú skilgreina beinar summur ferningsforma. Ef φ er skilgreint á V og χ á W þá er $\varphi \oplus \chi$ skilgreint á $V \oplus W$ með $(\varphi \oplus \chi)(\underline{x}, \underline{y}) = \varphi(\underline{x}) + \chi(\underline{y})$. Mengi allra jafngildisflokka ferningsforma verður þá samlagningarhálfgrúpa (sér í lagi víxlin). Það var E. Witt [6] sem innleiddi þennan hugsunarhátt á fjórða áratug 20. aldar. Ein af undirstöðusetningum hans er að styttireglan gildir í þessari hálfgrúpu.

Ferningform φ er sagt vera ísótróp ef jafnan $\varphi(\underline{x}) = 0$ hefur aðra lausn en þá augljósu $\underline{x} = 0$. Annars er φ sagt vera anísótróp. Ferningsformið $\eta : K^2 \to K$, $(x, y) \mapsto xy$, er kallað breiðgera planið. Ljóst er að η er ísótróp. Önnur af undirstöðusetningum Witts er að sérhvert ísótróp ferningsform er einsmóta beinni summu tveggja ferningsforma þar sem annað er breiðgera planið. Athugum að samkvæmt fyrr nefndri undirstöðusetningu Witts er jafngildisflokkur hins hlutans ótvírætt ákvarðaður. Með því að nota þetta aftur og aftur sést að sérhvert ferningsform φ er einsmóta beinni summu af anísótróp ferningsformi φ_0 og k eintökum af breiðgera planinu þar sem $k \ge 0$. Auk þess er jafngildisflokkur φ_0, sem kallað er anísótróp kjarni φ, ótvírætt ákvarðaður. Það má því skilgreina nýja flokkun ferningsforma með því að segja að tvö ferningsform séu Witt-jafngild ef þau hafa einsmóta anísótróp kjarna. Þessi flokkun er grófari en sú fyrri, en munurinn liggur eingöngu í breiðgerum plönum sem eru einföld viðfangs. Stóri kosturinn er nú að Witt-jafngildisflokkarnir mynda ekki aðeins samlagningarhálfgrúpu, heldur samlagningargrúpu. (Ástæðan er að bein summa ferningsforms φ og ferningsformsins $-\varphi$ er einsmóta beinni summu breiðgerra plana. Til dæmis er $ax^2 - ay^2 = uv$ þar sem $u = ax + ay$ og $v = x - y$.) Þessi grúpa er nú kölluð Witt-grúpa kroppsins K og er táknuð $W_q(K)$. Stærð $W_q(K)$ er mælikvarði á hve erfitt er að leysa jöfnur af taginu $\varphi(\underline{x}) = 0$ þar sem φ er ótiltekið ferningsform yfir K. Sem dæmi má nefna að Witt-grúpa tvinntalnanna hefur aðeins tvö stök og að Witt-grúpa rauntalnanna er einsmóta samlagningargrúpu heilu talnanna. (Þetta eru einfaldar afleiðingar af áður lýstri flokkun ferningsforma yfir þessa kroppa.)

Witt gerði reyndar ráð fyrir að kennitala kroppsins væri ekki 2 en fáum árum síðar sannaði C. Arf [4] undirstöðusetningarnar tvær, sem áður er getið, fyrir kroppa með kennitölu 2.

3. Kennitala ekki 2

Gerum ráð fyrir að kennitala kroppsins K sé ekki 2. Þá má, eins og áður kom fram, koma sérhverju ferningsformi á hornalínuform. Það þýðir að ferningsformið er einsmóta beinni summu einvíðra ferningsforma. Af þessu leiðir að Witt-grúpa K er spönnuð af flokkum einvíðu ferningsformanna. Witt sýndi einnig fram á hvernig lýsa mætti venzlunum milli þessara spönnuða.

Einvíða ferningsformið $K \to K$, $x \mapsto ax^2$, er táknað $\langle a \rangle$ og flokkur þess í $W_q(K)$ er táknaður $\langle a \rangle^\sim$. Hér er a í K, $a \neq 0$. Þá er Witt-grúpa K sem sagt spönnuð af þessum $\langle a \rangle^\sim$ sem samlagningargrúpa. Witt sýndi að venzlin milli þeirra ákvarðist af:

$$\langle a \rangle^\sim = \langle ar^2 \rangle^\sim$$
$$\langle a \rangle^\sim + \langle b \rangle^\sim = \langle a + b \rangle^\sim + \langle (a + b)ab \rangle^\sim \text{ ef } a + b \neq 0$$
$$\langle a \rangle^\sim + \langle -a \rangle^\sim = 0$$

(Reglan í miðjunni fæst af því að $ax^2 + by^2 = (a + b)u^2 + (a + b)abv^2$ ef við skrifum $x = u - bv$ og $y = u + av$.)

Látum $L = K((S))$ vera kropp allra Laurent raða í breytunni S yfir K, þ.e. allra formlegra raða af taginu $f(S) = \sum_{i=n}^{\infty} a_i S^i$ þar sem n er heil tala og stuðlarnir a_i eru í K. Ef $a_n \neq 0$ þá er ekki erfitt að sýna að skrifa má $f(S)$ á forminu $a_n g(S)^2$ ef n er slétt tala en á forminu $a_n S g(S)^2$ ef n er oddatala. Svo $\langle f(S)\rangle^{\sim} = \langle a_n\rangle^{\sim}$ eða $\langle f(S)\rangle^{\sim} = \langle a_n S\rangle^{\sim}$ í $W_q(L)$. Með því að nota framsetninguna að ofan á Witt-grúpum með spönnuðum og venzlum þá er hægt að sýna að þetta gefur okkur einsmótun grúpna $W_q(L) \cong W_q(K) \oplus W_q(K)$. Þetta sannaði T.A. Springer [5] fyrstur en á annan hátt.

4. Kennitala 2

Gerum nú ráð fyrir að kennitala K sé 2. Þá er ekki lengur hægt að koma ferningsformum yfir K á hornalínuform. Það sáum við þegar við fjölluðum um annarrar gráðu jöfnuna. Hinsvegar er sérhvert ferningsform yfir K einsmóta beinni summu tvívíðra ferningsforma. (Ástæðan er sú að vegna þess að kennitalan er 2 þá er tvílínulega formið, sem tilheyrir ferningsforminu, mishverft (symplektískt) og er því bein summa tvívíðra forma.) Hvert hinna tvívíðu ferningsforma er einsmóta formi af taginu $[a, b]$ þar sem a og b eru í K. Hér er ferningsformið $[a, b]$ skilgreint á K^2 með $(x, y) \mapsto ax^2 + xy + by^2$. Sér í lagi er $[0, 0]$ breiðgera planið. Ef við táknum flokk $[a, b]$ í $W_q(K)$ með $[a, b]^{\sim}$ þá leiðir af þessu að Witt-grúpa K er spönnuð af þessum $[a, b]^{\sim}$ sem samlagningargrúpa. Fyrirlesarinn [2] hefur sýnt fram á að venzlin milli þessara spönnuða ákvarðist af:

$$
\begin{aligned}
&[a_1 + a_2, b]^{\sim} = [a_1, b]^{\sim} + [a_2, b]^{\sim}\\
&[a, b_1 + b_2]^{\sim} = [a, b_1]^{\sim} + [a, b_2]^{\sim}\\
&[a, ar^2 + r]^{\sim} = 0\\
&[a, br^2]^{\sim} = [ar^2, b]^{\sim}
\end{aligned}
$$

Með því að nota meðal annars þessa framsetningu á Witt-grúpum með spönnuðum og venzlum þá hefur fyrirlesarinn [3] einnig reiknað út Witt-grúpu $L = K((S))$ þegar kennitalan er 2. Í ljós kemur að $W_q(L)$ er almennt miklu stærri en $W_q(K) \oplus W_q(K)$, en eins og að framan greinir þá eru þessar grúpur einsmóta ef kennitalan er ekki 2. Þessi niðurstaða hefur í för með sér að ýmsar hugmyndir sem notaðar eru við útreikninga á Witt-grúpum kroppa virka ekki og geta ekki virkað ef kennitalan er 2.

Niðurstaða útreikninganna á $W_q(L)$ er nánar tiltekið eftirfarandi:

- Til er eðlileg vaxandi runa $(W_q(L)_m)_{m\geq 0}$ af hlutgrúpum $W_q(L)_m$ í $W_q(L)$ þannig að sammengi þeirra sé öll grúpan $W_q(L)$.
- Til er einsmótun $W_q(L)_0 \cong W_q(K) \oplus W_q(K)$, eins og þegar kennitalan er ekki 2.
- Ef $m > 0$ er slétt tala þá er deildagrúpan $W_q(L)_m/W_q(L)_{m-1}$ einsmóta beinni summu tveggja eintaka af ytra margfeldinu $K \wedge_{K_0} K$.
- Ef $m > 0$ er oddatala þá er deildagrúpan $W_q(L)_m/W_q(L)_{m-1}$ einsmóta þinfeldinu $K \otimes_{K_0} K$.

Hér er $K_0 = \{\, r^2 \mid r \in K \,\}$. Þar sem kennitala K er 2 þá er K_0 hlutkroppur í K. Sér í lagi má skoða K sem vigurrúm yfir K_0.

Athugum að grúpan $K \otimes_{K_0} K$ er aldrei fánýt (þ.e. jöfn $\{\, 0 \,\}$). Sér í lagi er $W_q(L)$ aldrei jafnt $W_q(L)_0$. Grúpan $K \wedge_{K_0} K$ er fánýt þá og því aðeins að $K = K_0$, þ.e.a.s. þá og því aðeins að sérhvert stak í K sé ferningsstak.

5. Um sannanir

Til að sýna að framsetningin á $W_q(K)$ með spönnuðum og venzlum þegar kennitalan er 2 sé rétt látum við M vera grúpuna með spönnuðum $\lfloor a, b\rfloor$, $a, b \in K$, og venzlum eins og lýst var. Auðvelt er að sjá að venzlin gilda í $W_q(K)$. (Með því að skrifa $y_1 = v + y_2$ og $x_2 = x_1 + u$ fæst til dæmis að $a_1x_1^2 + x_1y_1 + by_1^2 + a_2x_2^2 + x_2y_2 + by_2^2$ er jafnt $(a_1 + a_2)x_1^2 + x_1v + bv^2 + a_2u^2 + uy_2$. Þetta sýnir að $[a_1, b] \oplus [a_2, b]$ er einsmóta $[a_1 + a_2, b] \oplus [a_2, 0]$. En $[a_2, 0]$ er einsmóta breiðgera planinu svo af þessu leiðir að $[a_1, b] \oplus [a_2, b]$ er Witt-jafngilt $[a_1 + a_2, b]$.) Við höfum því augljósa grúpumótun $M \to W_q(K)$ og hún er átæk. Til að sanna að hún sé einsmótun þá þarf að sanna að ef beina summan $\bigoplus_i [a_i, b_i]$ er einsmóta beinni summu breiðgerra plana þá sé summan $\sum_i \lfloor a_i, b_i\rfloor$ jöfn 0 í M. Þetta er gert með þrepun yfir fjölda liða í summunni.

Fyrsta skrefið er að sýna að ef $[a, b]$ er einsmóta $[c, d]$ þá séu $\lfloor a, b\rfloor$ og $\lfloor c, d\rfloor$ jöfn í M. Þetta er ekki svo erfitt því forsendunni má lýsa með jöfnum sem tengja a, b, c og d. Þá er, sér í lagi, þrepunarbyrjunin komin.

Í þrepunarskrefinu nægir að sýna að ef beina summan $\bigoplus_{i=1}^{n} [a_i, b_i]$ er ísótróp þá séu til $c_1, \ldots, c_{n-1}, d_1, \ldots, d_{n-1}$ í K þannig að

$\sum_{i=1}^{n}\lfloor a_i, b_i\rfloor = \sum_{i=1}^{n-1}\lfloor c_i, d_i\rfloor$ í M. Með því að nota fyrsta skrefið á hvern lið má sýna að við megum gera ráð fyrir að $a_1 + \cdots + a_n = 0$. Með því að nota að $\lfloor a_{n-1}, b_{n-1}\rfloor + \lfloor a_n, b_n\rfloor = \lfloor a_{n-1} + a_n, b_{n-1}\rfloor + \lfloor a_n, b_{n-1} + b_n\rfloor$ má svo fækka liðunum um einn.

Í eldri grein fyrirlesarans [1] var reyndar gefin önnur framsetning á $W_q(K)$ með spönnuðum og venzlum. En þar var verið að líta á Witt-grúpuna sem módúl yfir Witt-bauginn, en honum lýsum við ekki hér.

Fyrsta skrefið í útreikningunum á $W_q(L)$, þar sem $L = K((S))$, er að sýna að flokkur $[f(S), g(S)]$ sé 0 ef $f(S)g(S)$ er af taginu $\sum_{i=1}^{\infty} a_i S^i$. Það fæst með því að nota lemma Hensels. Þá er hægt að sýna að ef $f(S) = \sum_i a_i S^i$ og $g(S) = \sum_j b_j S^j$ þá sé

$$[f(S), g(S)]^{\sim} = \sum_{i,j;i+j\leq 0} [a_i S^i, b_j S^j]^{\sim}$$

og að það sé vit í þessari jöfnu. (Athugið að til eru heilar tölur m og n þannig að $a_i = 0$ ef $i < m$ og $b_j = 0$ ef $j < n$.) Svo grúpan $W_q(L)$ er spönnuð af flokkum ferningsformanna $[aS^i, bS^j]$ þar sem a og b eru í K og $i + j \leq 0$.

Næst þarf að finna út hvernig lýsa megi venzlunum milli þessara nýju spönnuða. En það er auðvelt því að við höfum hér að ofan ákveðna formúlu til að lýsa upphaflegu spönnuðunum út frá þeim nýju.

Hlutgrúpan $W_q(L)_m$ er nú skilgreind sem hlutgrúpan sem spönnuð er af öllum þessum $[aS^i, bS^j]$ með $i+j \geq -m$. Talsverða tæknilega útreikninga þarf til að sýna að venzlin á milli þessara spönnuða fyrir grúpuna $W_q(L)_m$ séu ekki fleiri en við mátti búast út frá lýsingu á venzlunum milli þeirra sem spönnuða fyrir $W_q(L)$. En þegar það er komið þá er auðvelt að fá framsetningar á $W_q(L)_0$ og deildagrúpunum $W_q(L)_m/W_q(L)_{m-1}$ fyrir $m > 0$ með spönnuðum og venzlum. Að lokum þarf að sýna að grúpurnar, sem lýst er með þessum framsetningum, séu einsmóta þeim sem gefnar eru í lýsingunni hér að framan á niðurstöðunni.

Summary

In the algebraic theory of quadratic forms over fields it is usually assumed that the characteristic of the field is not equal 2. The talk is an attemp to describe by examples how the theory is different in characteristic equal 2. The main example is the computation of the Witt group of the field of Laurent series over a field of characteristic 2. This computation was made recently by the author.

Heimildir

[1] J.K. Arason: Wittring and Galoiscohomologie bei Charakteristik 2. *J. Reine Angew. Math.* **307/308**, 247–256 (1979).

[2] J.K. Arason: Generators and relations for $W_q(K)$. Handrit.

[3] J.K. Arason: Generators and relations for $W_q(K((S)))$. Handrit.

[4] C. Arf: Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I). *J. Reine Angew. Math.* **183**, 148–167 (1941).

[5] T.A. Springer: Quadratic forms over a field with a discrete valuation. *Indag. math.* 17, 352–362 (1955)

[6] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern. *J. Reine Angew. Math.* **176**, 31–44 (1937)

Um höfundinn: Jón Kr. Arason er prófessor í stærðfræði við Háskóla Íslands.

Raunvísindastofnun Háskólans
Dunhaga 3
IS-107 Reykjavík
jka@hi.is

Móttekin: 1. júlí 2004