מבוא לתורה האלגברית של תבניות ריבועיות

עוזי וישנה

21 באוגוסט 2018

מבוא לתורה האלגברית של תבניות ריבועיות

מהדורה 1.65

הקדמה. לתורה של תבניות ריבועיות יש היבטים אלגבריים, אריתמטיים וגאומטריים. נציג כמה מהמשפטים היפים של התאוריה הזו על קצה המזלג. ידע מוקדם נדרש: בדרך כלל די בהבנה טובה של אלגברה לינארית ובמושגי יסוד מתורת החוגים. לפרקים יש צורך בידע מתקדם יותר מתורת השדות, מאלגברה (למשל מכפלה טנזורית), הכרת חבורות קוהומולוגיה, או יסודות תורת המספרים האלגברית. על הפרקים הדורשים ידע מתקדם אפשר לדלג בדרך כלל ללא פגיעה בנושאים המוצגים מאוחר יותר.

החומר מבוסס ברובו על [19], [12], [15], [7], [4], ובעיקר המבוא המצוין [14].

עוזי וישנה, 8.2014

תוכן עניינים

תוכן עניינים

פרק 1

מרחבים ריבועיים

1.1 תבניות ריבועיות

1.1.1 מרחב ריבועי

יהי F שדה.

הגדרה 1.1.1 **מרחב בילינארי** *מעל F הוא זוג סדור (V,b), שהרכיב הראשון שלו הוא מרחב וקטורי V ממימד סופי מעל F, והשני הוא תבנית בילינארית $b\colon V\times V\to F$. אם $b\colon V\times V\to F$ היא תבנית בילינארית, $q(x)=b(x,x)$ נקראת* ***התבנית הריבועית*** *המושרית על־ידי b, והזוג (V,q) נקרא* ***מרחב ריבועי****.*

במאפיין שונה מ־2, כל תבנית ריבועית מושרית על־ידי תבנית בילינארית **סימטרית** (כלומר $b(x,y)=b(y,x)$). תבנית זו היא יחידה, משום שאפשר לשחזר מ־q באמצעות **הנוסחה הפולרית**

$$b(x,y)=\frac{1}{2}(q(x+y)-q(x)-q(y)).$$

(במאפיין 2 לא כל תבנית ריבועית מושרית על־ידי תבנית סימטרית; לדוגמא, $q(x_1,x_2)=x_1x_2$ אינה מושרית על־ידי תבנית בילינארית סימטרית. יתרה מזו, יתכן ששתי תבניות בילינאריות סימטריות תשרנה את אותה תבנית ריבועית: למשל $b((x_1,x_2),(y_1,y_2))=x_1y_2+x_2y_1$ ותבנית האפס שתיהן משרות את התבנית הריבועית $q(x_1,x_2)=0$. זהו רק היבט אחד שבו התאוריה מסתבכת במאפיין 2.)

המרחבים הריבועיים הם אובייקטים בקטגוריה, שהמורפיזמים שלה הם העתקות לינאריות $\sigma\colon V\to V'$ המקיימות $q'\circ\sigma=q$. מורפיזם כזה הוא **איזומורפיזם** אם σ הפיך (כהעתקה לינארית), ובמקרה זה q ו־q' קובעים זה את זה. האוטומורפיזמים של (V,q) הם ההעתקות הלינאריות ההפיכות $\sigma\colon V\to V$ השומרות על q.

אחת הבעיות הטבעיות של התאוריה היא למיין מרחבים ריבועיים (ותבניות) עד כדי איזומורפיזם. המבנים שנציג בהמשך מאפשרים לארגן את התבניות ולענות על השאלה הזו במידה רבה של פירוט. לשם הקיצור, אם (V,q) הוא מרחב ריבועי, לפעמים נתייחס ל־V או ל־q בתור מרחב ריבועי. בפרט, מגדירים את **הממד** של התבנית q להיות הממד של V.

יש דוגמאות רבות למרחבים ריבועיים. בחקירת פונקציות ממשיות $\mathbb{R}^n\to\mathbb{R}$, התנהגות הפונקציה בנקודה קריטית נקבעת על־ידי התבנית הריבועית שמגדירה הנגזרת השניה. כך גם במשוואות דיפרנציאליות. אם R אלגברה ממימד סופי מעל שדה F אז יש לה שיכון $R\hookrightarrow \mathrm{M}_n(F)$, ופונקציית עקבה $\mathrm{tr}\colon R\to F$ המושרית על־ידי השיכון הזה. לתבנית הריבועית $q(x)=\mathrm{tr}(x^2)$ יש קשר למבנה של האלגברה, ובמקרים מיוחדים היא אפילו קובעת אותו.

1.1.2 הצגה באמצעות מטריצות

יהי V מרחב וקטורי מממד סופי, עם בסיס B. הבסיס מגדיר איזומורפיזם טבעי $V \to F^n$ לפי המעבר לווקטור קואורדינטות, $x \mapsto [x]_B$. ברוח זו, כל תבנית בילינארית $b\colon V \times V \to F$ אפשר לייצג באמצעות מטריצה $A \in \mathrm{M}_n(F)$, לפי הנוסחה $b(x,y) = {[x]_B}^{\mathrm{t}} A [y]_B$. אומרים ש־$A$ היא **המטריצה המייצגת** של b (ושל $q(x) = b(x,x)$) לפי הבסיס B, ומסמנים $A = [b]_B$. התבנית b סימטרית אם ורק אם המטריצה המייצגת אותה היא סימטרית.

כשמציגים וקטור כללי לפי קואורדינטות $x = x_1v_1 + \cdots + x_nv_n$ ו־$y = y_1v_1 + \cdots + y_nv_n$, התבנית היא $b(x,y) = \sum a_{ij}x_iy_j$, ואילו התבנית הריבועית המושרית על־ידי b מקבלת צורה של פולינום ריבועי הומוגני ב־n משתנים, $q(x) = \sum a_{ij}x_ix_j$.

החופש בבחירת הבסיס מאפשר להציג את אותה תבנית בדרכים רבות; המעבר מבסיס לבסיס כמוהו כהפעלת החלפת משתנים לינארית (הפיכה) על המשתנים $x_1, \ldots, x_n$. כיצד משפיעה החלפת הבסיס?

טענה 1.1.2 תהי $M = [I]^B_{B'}$ מטריצת המעבר בין הבסיסים B, B' של V. אז
$$[b]_B = M^{\mathrm{t}}[b]_{B'}M.$$

הוכחה. לכל $x \in V$, $M[x]_B = [x]_{B'}$. כעת, לכל $x \in V$,
$$b(x,y) = {[x]_{B'}}^{\mathrm{t}}[b]_{B'}[y]_{B'} = {[x]_B}^{\mathrm{t}}(M^{\mathrm{t}}[b]_{B'}M)[y]_B = {[x]_B}^{\mathrm{t}}[b]_B[y]_B.$$
□

בעקבות זאת, נאמר ששתי מטריצות $A, A' \in \mathrm{M}_n(F)$ הן **חופפות** אם יש $P \in \mathrm{GL}_n(F)$ כך ש־$A = P^{\mathrm{t}}A'P$. זה כמובן יחס שקילות.

מסקנה 1.1.3 שתי מטריצות מייצגות את אותה תבנית ריבועית, בבסיסים שונים, אם ורק אם הן חופפות.

אם כך, בעיית המיון של תבניות ריבועיות (עד כדי איזומורפיזם) מעל מרחב וקטורי n־ממדי שקולה לבעיה של מיון המטריצות הסימטריות בגודל $n \times n$ עד כדי חפיפה. השאלה האם שתי תבניות הן איזומורפיות כמוה כשאלה האם שתי מטריצות הן חופפות.

1.2 הצורה האלכסונית

משפט 1.2.1 *מעל שדה ממאפיין שונה מ־2, כל מטריצה סימטרית חופפת למטריצה אלכסונית. במלים אחרות, כל תבנית ריבועית אפשר להציג בצורה אלכסונית.*

בעיה 1.2.2 כתוב הוכחה מלאה למשפט ההצגה האלכסונית, משפט 1.2.1.

הגדרה 1.2.3 *את התבנית הריבועית $q(x_1, \ldots, x_n) = \sum \alpha_i x_i^2$, שהמטריצה המייצגת שלה היא המטריצה האלכסונית* $\begin{pmatrix} \alpha_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha_n \end{pmatrix}$*, מסמנים ב־*$\langle \alpha_1, \ldots, \alpha_n \rangle$.

בפרט, $\langle a \rangle$ מציין את התבנית $q(x) = ax^2$ על המרחב החד־ממדי F. הבה נמיין את התבניות מממד 1:

טענה 1.2.4 התבניות $\langle a \rangle$ ו־$\langle a' \rangle$ איזומורפיות אם ורק אם $aF^{\times 2} = a'F^{\times 2}$.

הוכחה. אכן, החלפת בסיס במרחב החד־ממדי פירושה כפל של איבר הבסיס בסקלר שונה מאפס, כלומר מעבר לנציג אחר במחלקה של המנה $F^{\times}/F^{\times 2} \cup \{0\}$. □

תרגיל 1.2.5 תן דוגמא נגדית (מממד 2) למשפט 1.2.1 במאפיין 2.

1.3 אורתוגונליות וסכום אורתוגונלי

תהי b תבנית בילינארית סימטרית. אומרים ששני תת־מרחבים $V_1, V_2 \subseteq V$ הם **אורתוגונליים** זה לזה (ביחס ל־b), אם $b(V_1, V_2) = 0$. אם המרחבים V_1, V_2 אורתוגונליים זה לזה ו־$V = V_1 \oplus V_2$, אז אפשר לחשב את התבנית b מן הצמצום שלה b_1, v_2 ל־V_1, V_2, מכיוון ש־

$$b(v_1 \oplus v_2, v_1' \oplus v_2') = b(v_1, v_1') + b(v_2, v_2') = b_1(v_1, v_1') + b_2(v_2, v_2'); \tag{1.1}$$

במקרה כזה אומרים ש־(V, b) הוא **סכום אורתוגונלי** (או סתם סכום ישר) של $(V_1, b|_{V_1})$ ו־$(V_2, b|_{V_2})$. אם B_1 ו־B_2 הם בסיסים של V_1, V_2 בהתאמה, אז $B_1 \cup B_2$ הוא בסיס של $V = V_1 \oplus V_2$, והמטריצה המייצגת של $b = b_1 \perp b_2$ היא

$$[b]_{B_1 \cup B_2} = [b_1]_{B_1} \oplus [b_2]_{B_2} = \begin{pmatrix} [b_1]_{B_1} & 0 \\ 0 & [b_2]_{B_2} \end{pmatrix}.$$

את הפירוק הפנימי הזה אפשר לחקות גם בדרך של בניה חיצונית. יהיו (V_1, b_1) ו־(V_2, b_2) מרחבים ריבועיים; הסכום האורתוגונלי (החיצוני) שלהם מוגדר על המרחב $V_1 \oplus V_2$ לפי הנוסחה

$$(b_1 \perp b_2)(v_1 \oplus v_2, v_1' \oplus v_2') = b_1(v_1, v_1') + b_2(v_2, v_2').$$

בתוך המרחב החדש, V_1, V_2 הם תת־מרחבים אורתוגונליים. לפעמים כותבים ישירות את הסכום של התבניות הריבועיות המתאימות: $q \perp q'$ היא התבנית הריבועית על המרחב $V \oplus V'$ המוגדרת לפי $(q \perp q')(x, x') = q(x) + q'(x')$. התבנית q נקראת **תת־תבנית** של $q \perp q'$.

תורת ההצגות רומזת שעלינו ללמוד את תת־המרחבים האי־פריקים, כלומר אלו שאי אפשר לפרק אותם לסכום אורתוגונלי של תת־מרחבים. אלא שלפי הסעיף הקודם, גישה זו אינה מוצלחת: במאפיין שונה מ־2, כל תבנית אפשר לפרק לסכום אורתוגונלי של תבניות חד־ממדיות, והפירוק הזה רחוק מלהיות יחיד.

1.4 תבניות רגולריות ולא רגולריות

נניח ש־b תבנית בילינארית סימטרית. לכל תת־מרחב $U \subseteq V$ מסמנים

$$U^\perp = \{x \in V : \ b(x, U) = 0\}.$$

לפי הסימון הזה, V_1, V_2 אורתוגונליים אם ורק אם $V_1 \subseteq V_2^\perp$ (אם ורק אם $V_2 \subseteq V_1^\perp$).

הרדיקל של המרחב V עצמו מוגדר כתת־המרחב $V^\perp = \{x : \ \forall u \in V, b(x, u) = 0\}$. אם $V^\perp = 0$, התבנית נקראת **רגולרית**. כאשר התבנית רגולרית, עובדות יסודיות באלגברה לינארית מראות שלכל תת־מרחב U, $\dim(U) + \dim(U^\perp) = \dim(V)$.

תרגיל 1.4.1 תהי A מטריצה המייצגת את התבנית הסימטרית b. אז b רגולרית אם ורק אם $\det(A) \neq 0$.

תרגיל 1.4.2 נניח ש־$V = V_1 \perp V_2$; אז V רגולרי אם ורק אם V_1, V_2 רגולריים.

הגדרה 1.4.3 *אם יש פירוק $V = U \perp U'$, כותבים $U \leq V$.*

טענה 1.4.4 נניח ש־$U \subseteq V$ הוא תת־מרחב רגולרי של מרחב רגולרי. אז $U \leq V$. ("תת־מרחב רגולרי של מרחב רגולרי הוא מחובר אורתוגונלי".)

הוכחה. החיתוך $U \cap U^\perp$ הוא הרדיקל של U, השווה לאפס לפי ההנחה. לפי הרגולריות של V, נוסחת הממד נותנת $V = U \oplus U^\perp$. אבל המרחבים $U, U^\perp$ אורתוגונליים, ולכן זה סכום אורתוגונלי. □

כעת נחזור על טענה 1.2.4, עבור תבניות רגולריות:

טענה 1.4.5 התבניות הרגולריות החד־ממדיות נמצאות בהתאמה חד־חד־ערכית ועל לחבורה $F^\times/F^{\times 2}$.

מסקנה 1.4.6 מעל $\mathbb{C}$ (או כל שדה סגור־ריבועית אחר), יש רק תבנית רגולרית חד־ממדית אחת, $\langle 1\rangle$. מעל $\mathbb{R}$ (או כל שדה סגור־ממשית אחר), יש רק שתי תבניות רגולריות חד־ממדיות: $\langle 1\rangle$ ו־$\langle -1\rangle$.

בעיה 1.4.7 הראה שבמאפיין 2, כל תבנית רגולרית איזומטרית לסכום של תבניות חד־ממדיות ודו־ממדיות.

בעיה 1.4.8 הגדר וחקור רדיקל שמאלי ורדיקל ימני עבור תבנית בילינארית שאינה בהכרח סימטרית.

1.4.1 מרחבים לא רגולריים

אם התבנית אינה רגולרית אז אפשר להגדיר על מרחב המנה $V/V^\perp$ את התבנית המושרית
$$b(v+V^\perp, v'+V^\perp) = b(v,v');$$
זה מוגדר היטב, ומתקיים
$$(V,b) \cong (V/V^\perp, b) \perp (V^\perp, 0).$$

תרגיל 1.4.9 מרחב המנה $V/V^\perp$ הוא רגולרי.

תרגיל 1.4.10 אם $V = U \perp 0$, כאשר U רגולרי ו־0 מייצג מרחב וקטורי (ממימד כלשהו) שהתבנית הריבועית עליו היא תבנית האפס, אז $V/V^\perp \cong U$.

מסקנה 1.4.11 כל מרחב ריבועי מתפרק באופן יחיד לסכום אורתוגונלי של מרכיב רגולרי ומרכיב אפס.

מסקנה 1.4.12 כל מטריצה סימטרית חופפת למטריצה מהצורה $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ כאשר A הפיכה. אם $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} A' & 0 \\ 0 & 0 \end{pmatrix}$ אז $A \sim A'$.

תרגיל 1.4.13 תהי b תבנית בילינארית על המרחב V, המיוצגת על־ידי המטריצה A. אז ממד המרכיב הרגולרי $V/V^\perp$ שווה לדרגה של A.

1.5 הכללות

(הקורא המתחיל מוזמן לדלג על הסעיף הזה, שאינו מפורט כקודמיו.)

1.5.1 מאפיין 2

עד כאן הנחנו שמאפיין השדה שונה מ־2. כדי לכסות את המקרה הכללי, נתבונן שוב בקשר שבין תבנית בילינארית לתבנית הריבועית שהיא מגדירה. אומרים שתבנית b היא **מתחלפת** אם היא מקיימת $b(x,x)=0$. כל תבנית מתחלפת היא אנטי־סימטרית, ובמאפיין שונה מ־2, המושגים מתלכדים. תבנית משרה את תבנית האפס אם ורק אם היא מתחלפת, ולכן המרחב של התבניות הריבועיות על מרחב נתון הוא מרחב כל התבניות הבילינאריות, מודולו מרחב התבניות המתחלפות.

ביתר פירוט, נתבונן בהתאמה $b \mapsto b^{\mathrm{an}}$ כאשר $b^{\mathrm{an}}(x,y) = b(x,y)-b(y,x)$. הגרעין שלה הוא מרחב התבניות הסימטריות, שממדו $\frac{n(n+1)}{2}$, והתמונה שלה מוכלת באוסף התבניות המתחלפות, שממדו $\frac{n(n-1)}{2}$. לפי השוואת ממדים, הוכחנו שיש סדרה מדוייקת קצרה
$$0 \longrightarrow \mathrm{Sym} \longrightarrow \mathrm{Bil} \longrightarrow \mathrm{Alt} \longrightarrow 0.$$
במאפיין שונה מ־2, הסדרה הזו מתפצלת, ו־$\mathrm{Bil} = \mathrm{Sym} \oplus \mathrm{Alt}$. לעומת זאת במאפיין 2, $\mathrm{Sym} \subseteq \mathrm{Alt}$.

1.5.2 תבניות הרמיטיות מעל אלגברה פשוטה

עד כאן דיברנו על תבניות בילינאריות סימטריות מעל שדה. ההכללה המוכרת היא לתבניות הרמיטיות, מעל הרחבה ריבועית F/F_0 (ובפרט מעל ההרחבה $\mathbb{C}/\mathbb{R}$). באופן כללי עוד יותר, תהי (A,σ) אלגברה פשוטה עם אינוולוציה (ראה סעיפים 3.4.4 ו־3.4.6); כלומר A פשוטה כאלגברה ומוגדרת עליה אינולוציה, או ש־$A \cong B \times B^{\mathrm{op}}$ עם האינוולוציה $(x,y) \mapsto (y,x)$.

מרחב ϵ־הרמיטי מעל (A,σ) הוא זוג (M,h), כאשר M מודול (בהכרח חופשי) מעל A ו־$h\colon M \times M \to A$ היא תבנית ססקוי־לינארית המקיימת $h(y,x) = \epsilon\sigma(h(x,y))$. התבנית נקראת **הרמיטית** אם $\epsilon = 1$, ואנטי־הרמיטית אם $\epsilon = -1$. המקרה של תבנית בילינארית סימטרית מתקבל כאשר $A = F$. כל אלגברה פשוטה עם אינוולוציה היא מהצורה $(\mathrm{End}_D(V), ad_h)$ כאשר ad_h היא האינוולוציה הצמודה ל־h, שהיא תבנית ϵ־הרמיטית על מרחב וקטורי V מעל חוג עם חילוק D.

נניח ש־A חוג עם חילוק. אז משפט 1.2.1 תקף עבור תבניות ϵ־הרמיטיות מעל (A,σ), פרט למקרה $(\sigma,\epsilon) = (\mathrm{id},-1)$. היינו, בכל מקרה אחר, כל תבנית ϵ־הרמיטית אפשר להביא לצורה $h(x,y) = \sum \sigma(x_i)a_iy_i$.

על ההכללה של חוג ויט (שנגדיר מעל שדה בתת־סעיף 2.3.3) עבור תבניות הרמיטיות, ראה הערה 2.3.15.

1.5.3 תבניות לא סימטריות

ראה עבודת הדוקטורט של אוריה פירסט (בעקבות עבודות של Scharlau, Bayer ואחרים).

1.5.4 תבניות מעל חוגים קומוטטיביים

זה נושא עשיר באלגברה ובאריתמטיקה של חוגים. ראה רמזים בכיוון בפרק 8, והערה 8.3.8.

1.5.5 כיוונים נוספים

אתגר 1.5.1 הצע תורת מבנה לתבניות טרילינאריות וכדומה.

אתגר 1.5.2 הצע תורת מבנה לתבניות ממימד אינסופי מעל שדה.

אתגר 1.5.3 הצע תורת מבנה למרחבים בילינאריים שהם מרחבי בנך מעל שדה עם הערכה.

אתגר 1.5.4 הצע תורת מבנה לזוגות של תבניות מעל שדה.
(הוכח שאם לתבניות המיוצגות על־ידי המטריצות A,B יש בסיס שבו שתיהן אלכסוניות, אז AB^{-1} לכסינה במובן הרגיל. האם הכיוון ההפוך נכון?)

פרק 2

המבנה של תבניות ריבועיות

לאור מסקנה 1.4.11, די לנו לעסוק מעתה בתבניות רגולריות.

2.1 תבניות היפרבוליות

תהי b תבנית ריבועית על מרחב V. וקטור $v \in V$ נקרא **איזוטרופי** אם הוא מקיים $b(v,v) = 0$. תת־מרחב $U \subseteq V$ הוא איזוטרופי אם $b(U,U) = 0$. תת־מרחב הוא איזוטרופי אם ורק אם הוא אורתוגונלי לעצמו.

תרגיל 2.1.1 במאפיין שונה מ־2, U איזוטרופי אם ורק אם כל הווקטורים ב־U איזוטרופיים.

אם אין במרחב אף וקטור איזוטרופי, הוא נקרא **מרחב אנאיזוטרופי**.

הגדרה 2.1.2 *המרחב הריבועי הדו־ממדי $\langle 1, -1 \rangle$ נקרא **המישור ההיפרבולי**, ומסמנים אותו ב־$\mathbb{H}$. סכום ישר של עותקים של המישור הזה, כלומר מרחב עם תבנית ריבועית אלכסונית $\langle 1, \ldots, 1, -1, \ldots, -1 \rangle$ עם סימנים מאוזנים, נקרא **מרחב היפרבולי** (ומסמנים אותו ב־$\mathbb{H}^m$, כאשר m הוא חצי הממד).*

תרגיל 2.1.3 הוכח שהתבניות הריבועיות $q(x,y) = x^2 - y^2$ ו־$q'(x,y) = xy$ איזומורפיות זו לזו (מאפיין שונה מ־2).

טענה 2.1.4 יש רק מרחב ריבועי רגולרי איזוטרופי אחד מממד 2, והוא המישור ההיפרבולי.

הוכחה. אחרי המעבר לבסיס אלכסוני, המטריצה המייצגת של התבנית היא מהצורה $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, כאשר $ab \neq 0$ בגלל הרגולריות. לפי ההנחה יש $(0,0) \neq (u,v) \in F^2$ כך ש־$au^2 + bv^2 = 0$. בפרט $u, v \neq 0$. לכן $(u,v), (u,-v)$ מהווה בסיס, שביחס אליו התבנית היא

$$q((u,v)x + (u,-v)y) = au^2(x+y)^2 + bv^2(x-y)^2 = 2(au^2 - bv^2)xy,$$

והתבנית הזו איזומורפית ל־$q'(x,y) = xy$ ולכן ל־$\langle 1, -1 \rangle$. $\square$

טענה 2.1.5 הממד של תת־מרחב איזוטרופי של מרחב רגולרי מממד n הוא לכל היותר $\frac{1}{2}n$.

הוכחה. נניח ש־U מרחב איזוטרופי מממד m. נבחר בסיס של U ונשלים אותו לבסיס של V. בהצגת התבנית לפי הבסיס הזה, למטריצה המייצגת יש בלוק בגודל $m \times m$ שכולו אפס. מכיוון שהדטרמיננטה של התבנית אינה אפס, יש אלכסון מוכלל שלארכו המכפלה אינה אפס; אבל בחישוב אלכסון מוכלל, בכל שורה מ־m השורות הראשונות נבחרת עמודה מבין ה־$n-m$ האחרונות, כלומר $m \leq n-m$. $\square$

טענה 2.1.6 יהי V מרחב ריבועי רגולרי ממימד n עם תת־מרחב איזוטרופי U, ממימד $m = \frac{1}{2}n$. אז V הוא מרחב היפרבולי.

הוכחה. אם $m = 0$ אין מה להוכיח. יהי U תת־מרחב איזוטרופי ממימד m. נבחר $u \in U$, ונתבונן במרחב המנה $u^\perp/Fu$; ממדו $2m-2$, והוא מכיל את תת־המרחב האיזוטרופי U/Fu. לפי הנחת האינדוקציה, U/Fu היפרבולי, ולכן יש לו בסיס $v_1, \dots, v_{2m-2}$ כך ש־$(v_i, v_j) = 0$ ל־$i \neq j$ ו־$(v_i, v_i) = \pm 1$. יהי $w \notin u^\perp$, כך ש־$V = \sum Fv_i \oplus (Fu + Fw)$. ברור ש־$(u, v_i) = 0$ לכל i. נחליף את w ב־$w' = w - \sum \frac{(w,v_j)}{(v_j,v_j)} v_i$, ואז $(w', v_j) = (w, v_j) - \sum_i \frac{(w,v_j)}{(v_j,v_j)}(v_i, v_j) = 0$. כעת $V = (\sum Fv_i) \perp (Fu + Fw')$, שהוא סכום אורתוגונלי של מרחב היפרבולי ממימד $n-2$ והמישור ההיפרבולי $Fu + Fw'$. □

משפט 2.1.7 *יהי V מרחב ריבועי רגולרי ממימד n, עם תת־מרחב איזוטרופי U ממימד m. אז $\mathbb{H}^m \leq V$ (ראה הגדרה **1.4.3**).*

הוכחה. נבחר בסיס של U, נשלים אותו לבסיס של $U^\perp$, ואת זה נשלים לבסיס של V. בבסיס הזה, המטריצה המייצגת של התבנית היא מטריצת בלוקים $[b] = \begin{pmatrix} 0 & 0 & A \\ 0 & B & X \\ A^{\mathrm{t}} & X^{\mathrm{t}} & C \end{pmatrix}$, כאשר הבלוקים מחולקים לפי הפירוק $m + (n-2m) + m = n$. נבחר $\tilde{P} = \begin{pmatrix} 1 & 0 & 0 \\ D & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, ונחשב:

$$\tilde{P}[b]\tilde{P}^{\mathrm{t}} = \begin{pmatrix} 1 & 0 & 0 \\ D & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & A \\ 0 & B & X \\ A^{\mathrm{t}} & X^{\mathrm{t}} & C \end{pmatrix} \begin{pmatrix} 1 & D^{\mathrm{t}} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & A \\ 0 & B & DA + X \\ A^{\mathrm{t}} & A^{\mathrm{t}}D^{\mathrm{t}} + X^{\mathrm{t}} & C \end{pmatrix}.$$

לפי הרגולריות A מוכרחה להיות הפיכה, ואם נבחר $D = -XA^{-1}$ הרי זה כאילו דאגנו ש־$X = 0$. אבל אז המטריצה מתפרקת לסכום ישר $[b] = \begin{pmatrix} 0 & A \\ A^{\mathrm{t}} & C \end{pmatrix} \oplus (B)$, כשהמרכיב הראשון, ממימד $2m$, מכיל תת־מרחב איזוטרופי ממימד m. לפי טענה **2.1.6**, המרכיב הראשון הזה היפרבולי, כלומר איזומורפי ל־$\mathbb{H}^m$. זה מוכיח את הטענה לפי מסקנה **1.1**. □

מסקנה 2.1.8 למרחב רגולרי יש וקטור איזוטרופי אם ורק אם הוא מכיל תת־מרחב היפרבולי.

2.2 המרכיב האנאיזוטרופי

2.2.1 איזומטריות

יהי (V, q) מרחב ריבועי מעל שדה F כלשהו (מאפיין שונה מ־2). חבורת האיזומטריות של המרחב היא

$$O(V, q) = \{T : V \to V : \ q(Tx) = q(x)\},$$

וזו כמובן תת־חבורה של $\mathrm{GL}(V)$. נקבע מטריצה מייצגת A של q; אפשר לזהות את $O(V, q)$ עם חבורת המטריצות $\{T : \ TAT^{\mathrm{t}} = A\} \leq \mathrm{GL}_n(F)$ כאשר $n = \dim(V)$. מן השוויון $TAT^{\mathrm{t}} = A$ יוצא ש־$\det(T) = \pm 1$. מסמנים

$$O^+(V, q) = \{T \in O(V, q) : \ \det(T) = 1\}.$$

למה 2.2.1 יהי (V,q) מרחב ריבועי עם $v \in V$ כך ש־$q(v) \neq 0$. נסמן ב־b את התבנית הבילינארית הסימטרית המתאימה ל־q. אז ההעתקה

$$\tau_v(x) = x - 2\frac{b(x,v)}{b(v,v)}v \tag{2.1}$$

היא איזומטריה מסדר 2, המייצבת את $v^\perp$ ומעבירה v ל־$-v$. העתקה זו נקראת **השיקוף ביחס ל־v**.

הוכחה. ראשית נראה שזו איזומטריה:

$$\begin{aligned} q(\tau(x)) &= q(x - \frac{b(x,v)}{q(v)} \cdot v) \\ &= b(x - 2\frac{b(x,v)}{q(v)} \cdot v, x - 2\frac{b(x,v)}{q(v)} \cdot v) \\ &= b(x,x) - 4\frac{b(x,v)}{q(v)}b(x,v) + 4\frac{b(x,v)^2}{q(v)^2}q(v) = q(x). \end{aligned}$$

ברור שהיא מייצבת כל וקטור המאונך ל־v, ומעבירה את v ל־$-v$; מכאן שהיא מסדר 2. □

למה 2.2.2 נניח ש־$\mathrm{char} F \neq 2$. יהי (V,q) מרחב ריבועי ויהיו $v, v' \in V$ וקטורים אנאיזוטרופיים שווי אורך, היינו $q(v) = q(v') \neq 0$. אז יש איזומטריה המעבירה $v \mapsto v'$; האיזומטריה היא שיקוף או מכפלת שני שיקופים.

הוכחה. נסמן ב־b_q את התבנית הביליניארית המתאימה ל־q. לפי ההנחה $v + v', v - v'$ מאונכים זה לזה כי $b_q(v+v', v-v') = b_q(v,v) - b_q(v',v') = 0$. ראשית נניח ש־$q(v-v') \neq 0$. אז $\tau_{v-v'}(v-v') = v'-v$ ו־$\tau_{v-v'}(v+v') = v+v'$, ולכן

$$\tau_{v-v'}(v) = \frac{1}{2}\tau_{v-v'}((v+v') + (v-v')) = \frac{1}{2}((v+v') - (v-v')) = v'.$$

מאידך אם $q(v-v') = 0$, אז $q(v+v') = 2(q(v)+q(v')) - q(v-v') = 4q(v) \neq 0$ לפי שוויון המקבילית. לפי המקרה הקודם $\tau_{v+v'}(v) = -v'$, ולכן $\tau_{v'}\tau_{v+v'}(v) = v'$. □

משפט 2.2.3 *יהי (V,q) מרחב ריבועי רגולרי. כל איזומטריה $\sigma : V \to V$ היא מכפלה של שיקופים.*

הוכחה. באינדוקציה על הממד. אם $\dim V = 1$ האיזומטריה הלא־טריוויאלית היחידה היא שיקוף. נניח ש־$\dim V = n > 1$, ותהי σ איזומטריה של V. נבחר וקטור אנאיזוטרופי $v \in V$, אז $v, \sigma(v)$ הם וקטורים מאותו אורך, ולפי למה 2.2.2 יש איזומטריה τ, שהיא שיקוף או מכפלת שני שיקופים, כך ש־$\tau(v) = \sigma(v)$; היינו $\tau^{-1}\sigma$ שומר על v, ומכאן ש־$\tau^{-1}\sigma$ היא איזומטריה של $v^\perp$. לפי הנחת האינדוקציה $\tau^{-1}\sigma$ היא מכפלת שיקופים שם, ולכן גם σ כזו. □

(ההוכחה מראה שכל איזומטריה היא מכפלה של לכל היותר $2n-1$ שיקופים, כאשר $n = \dim V$. למעשה כל איזומטריה היא מכפלה של עד n שיקופים; [4, Ex. 2.8].)

2.2.2 משפט הצמצום של ויט

מסקנה 2.1.8 מאפשרת לקלף מהמרחב הריבועי תת־מרחבים היפרבוליים, כל עוד יש לו וקטורים איזוטרופיים. כדי שהגישה הזו תהיה אפקטיבית, עלינו לדעת שכל הדרכים לבצע קילוף כזה מביאות לאותה תוצאה.

משפט 2.2.4 (משפט הצמצום של ויט (Witt)) במאפיין שונה מ־2, אם $V \perp V' \cong V \perp V''$, אז $V' \cong V''$.

הוכחה. מכיוון שאפשר להביא את V לצורה אלכסונית, די להוכיח את הטענה במקרה שבו V הוא מרחב חד־ממדי, עם התבנית $\langle a\rangle$. לפי מסקנה 1.4.11 אפשר להניח ש־$a\neq 0$. נתבונן איפה במרחב (W,q) שיש בו שני וקטורים, v,v', עם $q(v)=q(v')=a$. אפשר לפרק את המרחב בשתי דרכים: $W=Fv\perp v^{\perp}=Fv'\perp v'^{\perp}$, ועלינו להוכיח ש־$v^{\perp}\cong v'^{\perp}$.

לפי למה 2.2.2 יש איזומטריה σ כך ש־$\sigma(v)=v'$, ואז σ מהווה איזומטריה בין המשלימים האורתוגונליים. □

תרגיל 2.2.5 (משפט הצמצום של ויט נכשל במאפיין 2)

נסמן ב־$\mathbb{O}$ את המרחב הדו־ממדי עם התבנית הבילינארית הרגולרית $\begin{pmatrix}0&1\\1&0\end{pmatrix}$. במאפיין 2, $\mathbb{O}\perp\langle 1\rangle\cong\langle 1,1,1\rangle$ למרות ש־$\mathbb{O}\not\cong\langle 1,1\rangle$ (הבחן כי התבנית הריבועית המושרית על $\mathbb{O}$ היא תבנית האפס).

מסקנה 2.2.6 במאפיין שונה מ־2:

1. כל תבנית ריבועית אפשר לפרק באופן יחיד כסכום אורתוגונלי של תבנית האפס, תבנית היפרבולית ותבנית אנאיזוטרופית.
2. כל תבנית ריבועית רגולרית אפשר לפרק באופן יחיד כסכום של תבנית היפרבולית ותבנית אנאיזוטרופית.

הגדרה 2.2.7 *תהי q תבנית ריבועית. נניח שהיא מתפרקת $q=\mathbb{H}^r\perp q_0$, כאשר q_0 אנאיזוטרופית. התבנית q_0 היא **המרכיב האנאיזוטרופי** של q, והערך r נקרא **אינדקס ויט** של q.*

כמובן, לתבניות איזומטריות יש אותו אינדקס ויט.

2.3 חוג ויט

2.3.1 שקילות של תבניות

לאור מסקנה 2.2.6, טבעי ללמוד את אוסף התבניות האנאיזוטרופיות. הבעיה היא שסכום אורתוגונלי של תבניות אנאיזוטרופיות עשוי להיות איזוטרופי. הרעיון היסודי של ויט היה להפוך את $\mathbb{H}$ למרכיב טריוויאלי, ולזהות את כל התבניות מהצורה $q\perp\mathbb{H}^m$ זו עם זו. ביתר דיוק:

הגדרה 2.3.1 *שתי תבניות רגולריות הן **שקולות** במובן של ויט, אם יש להן אותו מרכיב אנאיזוטרופי.*

במלים אחרות, אם q_0 תבנית אנאיזוטרופית, מחלקת השקילות שלה כוללת את כל התבניות $q_0\perp\mathbb{H}^m$. בתוך מחלקת שקילות ידועה, הממד קובע את אינדקס ויט ולהיפך.

מסקנה 2.3.2 תבנית ריבועית רגולרית נקבעת על־ידי המרכיב האנאיזוטרופי שלה (או מחלקת השקילות) והממד (או אינדקס ויט).

את המחלקה של התבנית q מסמנים ב־$[q]$. במחלקה $[0]$ נמצאות התבניות ההיפרבוליות, ורק הן.

2.3.2 פעולות בין תבניות

יש שתי פעולות טבעיות שאפשר להגדיר בין תבניות ריבועיות.

הסכום של מרחבים ריבועיים הוגדר בסעיף 1.4. אפשר לחשב אותו כסכום ישר של המטריצות המייצגות, $A\oplus B=\begin{pmatrix}A&0\\0&B\end{pmatrix}$, וגם לפי הנוסחה:

תרגיל 2.3.3 $\langle a_1,\dots,a_n\rangle\perp\langle b_1,\dots,b_m\rangle=\langle a_1,\dots,a_n,b_1,\dots,b_m\rangle$.

המכפלה הטנזורית של תבניות בילינאריות מוגדרת בדרך דומה:

$$(V,b)\otimes(V',b') = (V\otimes V', b\otimes b'),$$

כאשר $(b\otimes b')(x\otimes x', y\otimes y') = b(x,y)b'(x',y')$. בפרט, עבור תבניות ריבועיות חד־ממדיות, $\langle a\rangle\langle a'\rangle = \langle aa'\rangle$, ומזה אפשר להוציא את הנוסחה הכללית:

תרגיל 2.3.4 $\langle a_1,\dots,a_n\rangle\otimes\langle b_1,\dots,b_m\rangle = \langle a_1b_1\rangle \perp \cdots \perp \langle a_nb_m\rangle$.

תרגיל 2.3.5 נניח ש־A, A' הן מטריצות מייצגות של התבניות q, q'. אז $A\otimes A'$ היא מטריצה מייצגת של התבנית $q\otimes q'$.

2.3.3 חוג ויט

הגדרה 2.3.6 ***חיבור וכפל של מחלקות:*** $[q]+[q'] = [q\perp q']$; $[q]\cdot[q'] = [q\otimes q']$.

תרגיל 2.3.7 לכל תבנית q, התבנית $\mathbb{H}\otimes q$ היא היפרבולית. **הדרכה.** לכל $a\in F^\times$, $\langle 1,-1\rangle\otimes\langle a\rangle \cong \langle a,-a\rangle \cong \langle 1,-1\rangle$.

תרגיל 2.3.8 פעולות החיבור והכפל של מחלקות מוגדרות היטב.

לפעמים נשמיט את סימן המחלקה, ונחבר תבניות ישירות, כלומר נכתוב $q+q'$ במקום $q\perp q'$. בדומה לזה נכתוב לפעמים $q\cdot q'$ במקום $q\otimes q'$. בפרט, עבור תבניות חד־ממדיות, $\langle a\rangle\langle b\rangle = \langle ab\rangle$.

תרגיל 2.3.9
1. פעולות החיבור והכפל הן קומוטטיביות ואסוציאטיביות;
2. הכפל דיסטריבוטיבי ביחס לחיבור;
3. התבנית 0 (על המרחב האפס ממדי) היא איבר אפס ביחס לחיבור;
4. $[-q]$ הוא הנגדי של $[q]$, כאשר $(-q)(x) = -q(x)$ (משום ש־$\mathbb{H}\cong\langle a,-a\rangle$ לכל a);
5. התבנית $\langle 1\rangle$ (על המרחב החד־ממדי) היא איבר יחידה ביחס לכפל.

כעת אפשר להגדיר את אחד האובייקטים המרכזיים של התאוריה:

הגדרה 2.3.10 ***חוג ויט הוא החוג של מחלקות השקילות של תבניות ריבועיות (ממימד סופי) מעל השדה F, עם פעולות החיבור והכפל שהוגדרו לעיל. מסמנים אותו ב־$W(F)$.***

נחשב כמה דוגמאות. ראשית, כפי שראינו בסעיף 1.2 (במאפיין שונה מ־2), כל תבנית אפשר להציג כסכום אורתוגונלי של תבניות ממימד 1.

מסקנה 2.3.11 כחבורה אדיטיבית, $W(F)$ נוצר על־ידי התבניות מהצורה $\langle a\rangle$, $a\neq 0$.

יתרה מזו, התבניות הרגולריות $\langle a\rangle$ ו־$\langle a'\rangle$ איזומורפיות אם ורק אם הן מייצגות אותה מחלקה ב־$F^\times/F^{\times 2}$ (טענה 1.4.5).

דוגמא 2.3.12 לפי מסקנה 1.4.6, יש רק מחלקה אחת ממימד אחד מעל $\mathbb{C}$, והיא $\langle 1\rangle$. מכיוון ש־$\mathbb{H} = \langle 1,-1\rangle \cong \langle 1,1\rangle = \langle 1\rangle\perp\langle 1\rangle$, נובע ש־$W(\mathbb{C})\cong\mathbb{Z}/2\mathbb{Z}$.

תרגיל 2.3.13 מעל הממשיים יש שתי תבניות חד־ממדיות, $\langle 1\rangle$ ו־$\langle -1\rangle$, כלומר $1,-1$ של חוג ויט. התבניות $\langle 1,\dots,1\rangle$ אינן איזוטרופיות, ולכן כל אחת מהן מהווה מחלקה לעצמה, ו־$W(\mathbb{R})\cong\mathbb{Z}$. הערך של התבנית $\langle 1,\dots,1,-1,\dots,-1\rangle$ בחוג ויט הוא סכום הסימנים; העובדה שהוא אינו תלוי בהצגת התבנית היא **משפט הסימנים של סילווסטר** (שנובע, משום כך, ממשפט הצמצום של ויט).

דוגמא 2.3.14 לגבי חוג ויט של שדה המספרים ה־p־אדיים $\mathbb{Q}_p$, ראה תת־סעיף 8.2.5.

הכללות

הערה 2.3.15 הערה זו ממשיכה את תת־סעיף 1.5.2. משפט הצמצום של ויט עובד מעל כל (A,σ), וכך אפשר להגדיר את חוג ויט $W_\epsilon(A,\sigma)$ של המחלקות של תבניות ϵ־הרמיטיות; אם $\epsilon = 1$, כותבים סתם $W(A,\sigma)$.

ידוע שאם $(A,\sigma) = (\mathrm{M}_n(F), \mathrm{t})$, אז $W(A,\sigma) \cong W(F)$ ו־$W_{-1}(A,\sigma) = 0$. אם σ אינוולוציה מסוג ראשון ו־A ממימד זוגי, אז $W_{-1}(A,\sigma) \cong W(A,\tau)$ כאשר τ מהטיפוס המנוגד ל־σ. אם σ מסוג שני אז $W_{-1}(A,\sigma) \cong W(A,\sigma)$ *[1]*.

לדוגמא, אם R שדה סגור ממשית, אז $W(R) \cong \mathbb{Z}$; אם $C = R[\sqrt{-1}]$ ו־$H = (-1,-1)_R$, אז גם $W(C,-) \cong W(H,-) \cong \mathbb{Z}$.

2.3.4 האידיאל היסודי

מכיוון שאיבר היחידה של חוג ויט הוא $\langle 1 \rangle$, מסמנים לפעמים את התבנית הזו ב־1. כמובן, האיבר $\langle 1,1 \rangle = \langle 1 \rangle \perp \langle 1 \rangle = 1+1 = 2$, בעוד שהתבנית $\langle 2 \rangle$ מייצגת איבר אחר לגמרי. **האידיאל היסודי** (the basic ideal) של חוג ויט הוא האידיאל $I(F)$ של התבניות ממימד זוגי.

טענה 2.3.16 כחבורה אדיטיבית, $I(F)$ נוצר על־ידי התבניות מהצורה $\langle\langle a \rangle\rangle = \langle 1, -a \rangle$.

הוכחה. מספיק לכתוב $\langle a,b \rangle \sim \langle 1,a \rangle + \langle -1,b \rangle \sim \langle 1,a \rangle - \langle 1,-b \rangle = \langle\langle -a \rangle\rangle - \langle\langle b \rangle\rangle$. □

הסימון $I^n(F) = (I(F))^n$ מתייחס לחזקה ה־n־ית של $I(F)$, לפי ההגדרה המקובלת בתורת החוגים. לשרשרת האידיאלים

$$W(F) \supset I(F) \supset I^2(F) \supset I^3(F) \supset \cdots$$

חשיבות גדולה בתורת התבניות הריבועיות. משפטים משנות השמונים והתשעים יודעים לקשר את המנות $I^n(F)/I^{n+1}(F)$ לחבורות קוהומולוגיה ולחבורות־K, שהן אובייקטים חשובים ביותר באריתמטיקה של שדות (ראו פרק 4).

הגדרה 2.3.17 *התבניות ממימד 2^n מהצורה*

$$\begin{aligned} \langle\langle a_1,\dots,a_n \rangle\rangle &= \langle\langle a_1 \rangle\rangle \otimes \cdots \otimes \langle\langle a_n \rangle\rangle \\ &= \langle 1,\, -a_1,\dots,-a_n,\, a_1a_2,\dots,a_{n-1}a_n,\,\dots,(-1)^n a_1\cdots a_n \rangle \end{aligned}$$

*נקראות **תבניות פיסטר** (Pfister) מסדר n.*

לתבניות פיסטר יש תכונות יפות שנפגוש בהמשך החוברת (בעיקר בפרק 6).

מסקנה 2.3.18 כחבורה אדיטיבית, $I^n(F)$ נוצר על־ידי תבניות פיסטר מסדר n.

2.4 תבניות תחת הרחבת שדות

2.4.1 העתקת הצמצום

יהי $F \hookrightarrow K$ שיכון של שדות. אפשר לראות כל תבנית q מעל F כאילו היא תבנית מעל K, שאותה מסמנים ב־q_K. ביתר דיוק, **הצמצום** (restriction) של המרחב הריבועי (V,q) מ־F ל־K מוגדר כ־

$$\mathrm{res}_{K/F}(V,q) = (K \otimes V, q_K),$$

כאשר התבנית הבילינארית המתאימה ל־q_K מוגדרת לפי $b_K(a \otimes v, a' \otimes v') = aa'b(v,v')$. בפרט,

$$\dim(q_K) = \dim(q).$$

הפונקציה $[q] \mapsto [q_K]$ היא הומומורפיזם של חוגים $\mathrm{res}_{K/F}\colon W(F)\to W(K)$. באופן הזה $F \mapsto W(F)$ הוא פונקטור (קונטרה־וריאנטי) מקטגוריית השדות לקטגוריית החוגים הקומוטטיביים.
הנה דוגמא שתשמש אותנו בפרק 7.

טענה 2.4.1 נניח ש־K/F הרחבה טרנסצנדנטית טהורה. אם q אנאיזוטרופית מעל F אז גם q_K אנאיזוטרופית.
בפרט, הצמצום $\mathrm{res}_{K/F}\colon W(F)\to W(K)$ הוא חד־חד־ערכי.

הוכחה. נניח ש־q_K איזוטרופית.
נבחר קבוצת יוצרים טרנסצנדנטית להרחבה K/F. אפשר להחליף את K בשדה K' הנוצר על־ידי כל היוצרים המשתתפים בנקודה המאפסת את q, כך ש־$\mathrm{trdeg}(K'/F)$ סופי, ולפעול באינדוקציה על מספר המשתנים. מספיק, אם כך, להניח ש־$K = F(\lambda)$. אם $q(f_1(\lambda), \dots, f_n(\lambda)) = 0$, אפשר להניח על־ידי כפל במכנה משותף ש־$f_1, \dots, f_n \in F[\lambda]$ ושהם זרים במשותף. לכן אפשר להציב $\lambda \mapsto 0$ ולקבל נקודה מעל F המאפסת את q, כך ש־q איזוטרופית. $\square$

לאור טענה 2.4.1, ומכיוון שבכל הרחבה של שדות יש הרחבת ביניים טרנסצנדנטית שהמרכיב מעליה אלגברי, עיקר העניין בהעתקת הצמצום הוא כאשר ההרחבה אלגברית.

2.4.2 הרחבות ריבועיות

בסעיף הזה ננתח את העתקת הצמצום במקרה שבו K/F הרחבה ריבועית. נכתוב $K = F[\delta]$, כאשר $\delta^2 = \Delta$. הסוגיה העיקרית במעבר לשדה הרחבה היא לתאר אלו תבניות אנאיזוטרופיות נעשות איזוטרופיות או אפילו היפרבוליות. במקרה של הרחבה ריבועית יש לשאלה הזו תשובה מלאה.

דוגמא 2.4.2 תהי $K = F[\delta]/F$ הרחבה ממימד 2 במאפיין שונה מ־2. הנורמה בהרחבה הזו היא $\mathrm{N}(x + y\delta) = x^2 - \Delta y^2$. כלומר, בבסיס $\{1, \delta\}$ של $F[\delta]$, **תבנית הנורמה** של ההרחבה היא תבנית אלכסונית עם ההצגה $\langle\langle \Delta \rangle\rangle = \langle 1, -\Delta \rangle$.

מכיוון ש־K הוא שדה לפי ההנחה, Δ אינו ריבוע ב־F, ולכן תבנית הנורמה $\langle\langle \Delta \rangle\rangle$ מוכרחה להיות אנאיזוטרופית מעל F. מאידך התבנית נעשית איזוטרופית מעל K, שהרי $\delta^2 - \Delta = 0$, ולכן התבנית $\langle\langle \Delta \rangle\rangle_K$ היפרבולית (טענה 2.1.4). כלומר, $\langle\langle \Delta \rangle\rangle \in \mathrm{Ker}(\mathrm{res}_{K/F})$.

משפט 2.4.3 *תהי K/F הרחבה ריבועית כלעיל, ותהי q תבנית אנאיזוטרופית מעל F.*

1. *q_K איזוטרופית אם ורק אם יש ל־q תת־תבנית שהיא כפולה סקלרית של $\langle\langle \Delta \rangle\rangle$.*

2. *q_K היא היפרבולית אם ורק אם $q \in \langle\langle \Delta \rangle\rangle W(F)$, כלומר q ניתנת לפירוק בצורה $q \cong \langle\langle \Delta \rangle\rangle q''$.*

הוכחה. בשני המקרים כיוון אחד טריוויאלי, משום ש־$\langle\langle \Delta \rangle\rangle_K \cong \mathbb{H}_K$.

1. נכתוב $q = \langle a_1, \dots, a_n \rangle$, ונניח ש־$q_K$ איזוטרופית. לכן יש $x_i + y_i\delta \in K$, לא כולם אפס, כך ש־$0 = \sum a_i(x_i + \delta y_i)^2 = (\sum a_i x_i^2 + \Delta \sum a_i y_i^2) + 2\sum a_i x_i y_i \delta$. נסמן ב־$b_q$ את התבנית הבילינארית המתאימה ל־q, ונכתוב $x = (x_1, \dots, x_n)$ ו־$y = (y_1, \dots, y_n)$. לפי השוואת המקדמים, $b_q(x, y) = 0$ ו־$q(x) + \Delta q(y) = 0$. מהשוויון האחרון נובע ש־$q(x), q(y) \neq 0$, שהרי q אנאיזוטרופית. נתבונן בתת־המרחב $Fx + Fy$ של F^n: צמצום q לתת־המרחב הזה נותן את התבנית הדו־ממדית $\langle q(x), q(y) \rangle \cong \langle q(y) \rangle \cdot \langle -\Delta, 1 \rangle$, ולפי טענה 1.4.4 נובע מזה ש־$\langle q(y) \rangle \langle\langle \Delta \rangle\rangle$ היא תת־תבנית של q.

2. נניח ש־q_K היפרבולית. הפעלה חוזרת של הסעיף הראשון מראה שאפשר לפרק את q לסכום ישר של תבנית מהצורה $\langle c_i \rangle \langle\langle \Delta \rangle\rangle$, ולכן $q = \langle c_1, \dots, c_t \rangle \langle\langle \Delta \rangle\rangle$.

□

ניסוח אחר לסעיף 2 של משפט 2.4.3: הגרעין של העתקת הצמצום שווה לחשוד המיידי:

$$\mathrm{Ker}(\mathrm{res}_{K/F}) = \langle\langle \Delta \rangle\rangle \cdot W(F);$$

כלומר, יש סדרה מדוייקת

$$W(F) \xrightarrow{-\cdot\langle\langle\Delta\rangle\rangle} W(F) \xrightarrow{\mathrm{res}_{K/F}} W(K) \tag{2.2}$$

2.4.3 הטרנספר

שוב תהי K/F הרחבה. הצמצום מפרש תבנית מעל F כאילו היא מוגדרת מעל K. איך אפשר לפעול בכיוון ההפוך ולהעביר תבנית ריבועית מעל K לתבנית מעל F?

הגדרה 2.4.4 *יהיו $F \subseteq K$ שדות כלשהם, ותהי $s : K \to F$ העתקה F־לינארית (שאינה אפס). יהי V מרחב וקטורי מעל K, ותהי $q : V \to K$ תבנית ריבועית.* ***הטרנספר*** *של המרחב הריבועי (V, q) הוא המרחב הריבועי (V, s_*q), מעל F, כאשר $(s_*q)(x) = s(q(x))$.*

התבנית מוגדרת על אותו מרחב וקטורי V, ולכן $\dim(s_*q) = [K : F] \cdot \dim(q)$.

דוגמא 2.4.5 אם $\mathrm{tr} : K \to F$ היא העקבה, אז $q = tr_*\langle 1 \rangle$, שהיא התבנית $x \mapsto \mathrm{tr}(x^2)$, נקראת **תבנית העקבה** של ההרחבה.

דוגמא 2.4.6 נחזור לדוגמא 2.4.2, שם ראינו שתבנית הנורמה של ההרחבה $K = F[\delta \mid \delta^2 = \Delta]/F$ היא $\langle\langle \Delta \rangle\rangle$. העקבה מוגדרת לפי $\mathrm{tr}(x + y\delta) = 2x$, ולכן תבנית העקבה היא

$$\mathrm{tr}((x + y\delta)^2) = \mathrm{tr}(x^2 + \Delta y^2 + 2xy\delta) = 2(x^2 + \Delta y^2),$$

היינו $\langle\langle -\Delta \rangle\rangle$.

הערה 2.4.7 תבנית העקבה מוגדרת עבור כל אלגברה מעל F שיש לה פונקציית עקבה. הדוגמאות המוכרות הן כמובן מטריצות מכל ממד, ודרכן כל אלגברה פשוטה מעל F. אלגברה שמוגדרת עליה תבנית בילינארית המקיימת את האקסיומה $(ab, c) = (a, bc)$ נקראת "אלגברת פרובניוס".

תרגיל 2.4.8 $s_*(q \perp q') = s_*q \perp s_*q'$.

תרגיל 2.4.9 אם $q \cong q'$ מעל K אז $s_*q \cong s_*q'$ מעל F.

טענה 2.4.10 (תכונת ההיפוך של פרובניוס) תהיינה q תבנית ריבועית מעל K ו־φ תבנית ריבועית מעל F. אז $s_*(q \otimes_K \varphi_K) \cong s_*(q) \otimes_F \varphi$.

$$\begin{array}{ccc} q & \otimes & \varphi_K \\ \big\downarrow{\scriptstyle s_*} & \big\downarrow{\scriptstyle s_*} & \big\uparrow \\ s_*q & \otimes & \varphi \end{array}$$

הוכחה. נתונים המרחבים הריבועיים (V,q) ו־(W,φ). המרחבים שעליהם מוגדרות התבניות הם $(V\otimes_K(K\otimes W), s_*(q\otimes_K\varphi_K))$ ו־$(V\otimes_F W, s_*(q)\otimes_F\varphi)$. כדי להראות שההתאמה $v\otimes(a\otimes w) \mapsto av\otimes w$ היא איזומטריה, נסמן ב־b_q ו־β_φ את התבניות הבילינאריות המתאימות. כעת נחשב:

$$\begin{aligned}(s_*(b_q\otimes_K\beta_{\varphi_K}))(v\otimes(a\otimes w), v'\otimes(a'\otimes w')) &= s((b_q\otimes_K\beta_{\varphi_K})(v\otimes(a\otimes w), v'\otimes(a'\otimes w'))) \\ &= s(b_q(v,v')\beta_\varphi(a\otimes w, a'\otimes w')) \\ &= s(b_q(v,v')aa'\beta_\varphi(w,w')) \\ &= s(aa'b_q(v,v'))\beta_\varphi(w,w') \\ &= s(b_q(av,a'v'))\beta_\varphi(w,w') \\ &= (s_*(b_q)\otimes_F\beta_\varphi)(av\otimes w, a'v'\otimes w')\end{aligned}$$

□

טענה 2.4.11 אם q תבנית היפרבולית מעל K, אז s_*q היפרבולית מעל F.

הוכחה. לפי האדיטיביות, מספיק לחשב את: $s_*(\mathbb{H}_K) = s_*(\langle 1\rangle\otimes\mathbb{H}_K) = s_*(\langle 1\rangle)\otimes\mathbb{H}$ (השתמשנו בהיפוך), וזו תבנית היפרבולית (מממד $2[K:F]$) לפי תרגיל 2.3.7. □

מסקנה 2.4.12 תהי $s: K\to F$ העתקה F־לינארית. אז $s_*: W(K)\to W(F)$ מוגדרת היטב לפי הנוסחה $s_*[q] = [s_*q]$.

תכונת ההיפוך של פרובניוס נותנת כעת לכל $a\in W(K)$ ו־$\alpha\in W(F)$,

$$s_*(a\cdot \mathrm{res}_{K/F}\alpha) = s_*(a)\cdot\alpha \tag{2.3}$$

אפשר לראות ב־$W(K)$ מודול (ימני) מעל $W(F)$ באמצעות הפעולה $(a,\alpha)\mapsto a\cdot\mathrm{res}_{K/F}(\alpha)$.

מסקנה 2.4.13 $s_*: W(K)\to W(F)$ היא הומומורפיזם של מודולים מעל $W(F)$.

כעת נוכל להמשיך את הסדרה המדוייקת (2.2).

משפט 2.4.14 *תהי $K = F[\sqrt{\Delta}]$ הרחבה ריבועית ספרבילית של F. תהי $s: K\to F$ העתקה לינארית המקיימת $s(1) = 0$ (יש אחת כזו, עד כפל בסקלר). אז*

$$W(F)\xrightarrow{-\cdot\langle\langle\Delta\rangle\rangle} W(F)\xrightarrow{\mathrm{res}_{K/F}} W(K)\xrightarrow{s_*} W(F) \tag{2.4}$$

היא סדרה מדוייקת מדוייקת של מודולים מעל $W(F)$.

הוכחה. בתת־סעיף 2.4.2 הוכחנו שהסדרה מדוייקת ב־$W(F)$. תהי $\langle a\rangle$ תבנית מעל F, אז $\mathrm{res}_{K/F}(\langle a\rangle)$ היא התבנית החד־ממדית מעל K, ו־$q = s_*(\langle a\rangle)$ היא התבנית על K המוגדרת לפי

$$q(x+y\sqrt{\Delta}) = s(a(x+y\sqrt{\Delta})^2) = as(x^2+\Delta y^2+2xy\Delta) = 2as(\Delta)xy,$$

וזו תבנית היפרבולית. לכן $s_*\circ\mathrm{res}_{K/F} = 0$.

נוכיח שכל תבנית אנאיזוטרופית מעל K אפשר לפרק לחלק שהטרנספר שלו אנאיזוטרופי וחלק המושרה מ־F. כלומר, כל מרחב ריבועי אנאיזוטרופי (V,φ) מעל K אפשר לפרק $\varphi = q_K\perp\varphi'$, כאשר q היא תבנית מעל F, ו־$s_*\varphi'$ אנאיזוטרופית. אכן, אם $s_*\varphi$ אנאיזוטרופית, סיימנו. אחרת יש $0\neq v\in V$ כך ש־$s(\varphi(v)) = 0$, כלומר $\varphi(v)\in F$ $0\neq b=$. אם כך Kv הוא תת־מרחב רגולרי של V, ואפשר לפרק $\varphi = \langle b\rangle_K\perp\varphi'$; לפי הנחת האינדוקציה את φ' אפשר לפרק לחלק המושרה מ־F וחלק שהטרנספר שלו אנאיזוטרופי, וכך מתקבל פירוק דומה של φ.

כעת נניח ש־φ תבנית אנאיזוטרופית מעל K, ו־$s_*\varphi$ היפרבולית. לפי הסעיף הראשון אפשר לפרק $\varphi = q_K\perp\varphi'$ כאשר $s_*\varphi'$ אנאיזוטרופי, אבל זו תת־תבנית של התבנית ההיפרבולית $s_*\varphi$, כלומר $\varphi' = 0$ ו־$\varphi = q_K\in\mathrm{res}_{K/F}W(K)$. □

המשפט השימושי הזה מתאר את התמונה של הצמצום $\mathrm{res}\colon W(F)\to W(K)$; תבנית $[q] \in W(K)$ מהווה צמצום של תבנית המוגדרת מעל F, אם ורק אם s_*q היפרבולית. כלומר, אם נכתוב $q(x) = q_1(x) + q_2(x)\delta$, אז q מוגדרת מעל F אם ורק אם q_2 היפרבולית.

2.4.4 הרחבות ממימד אי־זוגי

שימוש נוסף בטרנספר מוכיח תוצאה יפה על הרחבות ממימד אי־זוגי.

טענה 2.4.15 לכל הרחבת שדות סופית K/F ולכל העתקת טרנספר $0 \neq s\colon K\to F$, ההרכבה

$$s_* \circ \mathrm{res}_{K/F}\colon W(F)\to W(F)$$

שווה לכפל ב־$s_*(\langle 1\rangle)$.

הוכחה. תהי q תבנית ריבועית מעל F. אז $(s_* \circ \mathrm{res}_{K/F})(q) = s_*(q_K) = s_*(q_K\otimes\langle 1\rangle) = q\otimes s_*(\langle 1\rangle)$ לפי תכונת ההיפוך. $\square$

טענה 2.4.16 תהי K/F הרחבה ממימד איזוגי. אז הצמצום $W(F)\to W(K)$ הוא חד־חד־ערכי.

הוכחה. אפשר להניח ש־$K = F[\theta]$ (אם ההרחבה אינה ספרבילית, באינדוקציה על הממד). נסמן $2m+1 = [K:F]$. נגדיר את העתקת הטרנספר $s\colon K\to F$ לפי $s(1) = 1$ ו־$s(x^i) = 0$ לכל $i = 1,\dots,2m$. נראה ש־$s_*(\langle 1\rangle) \sim \langle 1\rangle$. אכן, ביחס לתבנית $s_*(\langle 1\rangle)\colon a \mapsto s(a^2)$, אפשר לפרק לסכום אורתוגונלי $K = F \perp (Fx+\dots+Fx^{2m})$, ותת־המרחב $Fx+\dots+Fx^m$ הוא איזוטרופי ממימד מחצית הממד של $F^\perp$. לכן $F^\perp$ היפרבולי, ו־$(K, s_*(\langle 1\rangle)) \sim (F,\langle 1\rangle)$. מזה נובע ש־$s_*\circ\mathrm{res}_{K/F}$ הוא כפל ב־$\langle 1\rangle \sim s_*(\langle 1\rangle)$, כלומר העתקת הזהות. זה מוכיח ש־$\mathrm{res}_{K/F}$ חד־חד־ערכי ואילו $s_*\colon W(K)\to W(F)$ על. $\square$

טענה 2.4.16 אומרת שבהרחבה K/F ממימד איזוגי, אם תבנית נעשית היפרבולית מעל K, אז היא היפרבולית מלכתחילה. בהמשך (משפט 2.4.18) נוכיח תוצאה חזקה בהרבה.

2.4.5 משפט שפרינגר

טענה 2.4.17 (טיעון המונום העליון) תהי q תבנית אנאיזוטרופית מעל F. נניח ש־$q(f_1,\dots,f_t) = g$ כאשר $f_1,\dots,f_t, g \in F[\lambda]$. אז $\deg(g) = 2\max\{\deg(f_1),\dots,\deg(f_t)\}$.

הוכחה. נסמן $m = \max\{\deg(f_i)\}$ ו־$n = \deg(g)$. ברור ש־$n \leq 2m$. נסמן ב־$a_1,\dots,a_t$ את המקדם של λ^m ב־$f_1,\dots,f_n$, וב־b את המקדם של λ^{2m} ב־g. אז $q(a_1,\dots,a_t) = b$, ואם $n < 2m$ אז $b = 0$ ובהכרח גם $a_1 = \dots = a_t = 0$. $\square$

משפט 2.4.18 (משפט שפרינגר (Springer)) *תהי K/F הרחבה ממימד אי־זוגי. לכל תבנית אנאיזוטרופית q מעל F, גם התבנית q_K אנאיזוטרופית.*

הוכחה (בהנחה ש־$\mathrm{char}F \neq 2$). נכתוב $q = \langle a_1,\dots,a_t\rangle$. ההוכחה היא באינדוקציה על הממד $m = [K:F]$. באינדוקציה על מספר היוצרים, די להניח שההרחבה פשוטה. נכתוב $K = F[\theta]$, ויהי $p(\lambda) \in F[\lambda]$ הפולינום המינימלי של θ מעל F. בפרט $\deg(p) = m$. נניח, בשלילה, שהתבנית q_K איזוטרופית. אז יש אברים $\beta_1,\dots,\beta_t \in K$ כך ש־$a_1\beta_1^2+\dots+a_t\beta_t^2 = 0$. כל $\beta_i \in K$ אפשר להציג בצורה $\beta_i = f_i(\theta)$ כאשר $f_1,\dots,f_t \in F[\lambda]$ הם פולינומים ממעלה $\deg(f_i) < m$. את השוויון הקודם אפשר להציג בצורה

$$a_1 f_1(\lambda)^2 + \dots + a_t f_t(\lambda)^2 \equiv 0 \pmod{p(\lambda)}. \tag{2.5}$$

אם לפולינומים $f_1(\lambda),\dots,f_t(\lambda)$ יש גורם משותף מעל F, אפשר לחלק בו והשוויון נשמר. לכן אפשר להניח שהם זרים (במשותף). לפי השוויון (2.5) אפשר לפרק את אגף שמאל,

$$a_1 f_1(\lambda)^2 + \dots + a_t f_t(\lambda)^2 = p(\lambda)h(\lambda), \tag{2.6}$$

כאשר $h(\lambda) \in F[\lambda]$ פולינום מדרגה $\deg(h) \leq m-2$. מכיוון ש־p ממעלה אי־זוגית לפי ההנחה, והמעלה של אגף שמאל זוגית לפי טיעון המונום העליון, גם המעלה של h אי־זוגית. נבחר גורם אי־פריק p' ממעלה אי־זוגית של h. נתבונן בשדה $K' = F[\lambda]/\langle p'(\lambda) \rangle$, שממדו מעל F הוא $\deg(p') < m$. נסמן ב־$\theta' = \lambda + p'(\lambda)$ את השורש $p'(\lambda)$, היוצר את ההרחבה K'/F. מכיוון שה־f_i זרים, לא יתכן שכולם מתחלקים ב־p', ולכן הוקטור $(f_1(\theta'), \dots, f_t(\theta'))$ אינו אפס. נציב $\lambda = \theta'$ בשוויון (2.6) ונקבל

$$a_1 f_1(\theta')^2 + \cdots + a_t f_t(\theta')^2 = 0,$$

כלומר, התבנית q איזוטרופית מעל K' שממדו אי־זוגי וקטן מ־m, בסתירה להנחת האינדוקציה, אלא אם $f_i(\theta') = 0$ לכל i; אבל גם זה בלתי אפשרי כי אז כל הפולינומים $f_i(\lambda)$ מתחלקים ב־p'. □

תרגיל 2.4.19 טענה 2.4.16 נובעת ממשפט 2.4.18. **הדרכה**. אם $0 \neq [q] \in W(F)$ אז q שקולה לתבנית אנאיזוטרופית, שנשארת כזו מעל K.

תרגיל 2.4.20 בדוק שהוכחת משפט 2.4.18 תקפה גם בלי להניח ש־q אלכסונית, ולכן היא נכונה גם במאפיין 2.

תרגיל 2.4.21 תהי q תבנית אנאיזוטרופית מעל שדה F. יהי $g(\lambda)$ ערך של התבנית מעל חוג הפולינומים $F[\lambda]$. הראה שהמעלה של כל גורם ראשוני של $g(\lambda)$ היא זוגית.

הדרכה. נניח ש־$g(\lambda) = q(f_1(\lambda), \dots, f_n(\lambda))$, ויהי $p(\lambda)$ גורם אי־פריק של $g(\lambda)$. נסמן ב־α שורש של p בשדה ההרחבה $K = F[\lambda]/\langle p(\lambda) \rangle$. אז $q(f_1(\alpha), \dots, f_n(\alpha)) = g(\alpha) = 0$, ולכן q_K איזוטרופית. משפט שפרינגר אינו מאפשר זאת אם $\deg(p(\lambda)) = [K:F]$ אי־זוגי.

אתגר 2.4.22 האם יתכן שהעתקת הצמצום $W(F) \to W(K)$ היא חד־חד־ערכית, ובכל זאת קיימת תבנית אנאיזוטרופית q מעל F כך ש־q_K איזוטרופית?

2.5 גורמי דמיון

חבורת המחלקות $F^\times/F^{\times 2}$ פועלת על התבניות הריבועיות לפי כפל בסקלר, $\alpha F^{\times 2} : q \mapsto \langle \alpha \rangle \otimes q$. תהי q תבנית מעל שדה F. נגדיר את **חבורת גורמי הדמיון** של q לפי

$$G(q) = \left\{ t \in F^\times/F^{\times 2} :\ \langle t \rangle \otimes q \cong q \right\} \subseteq F^\times/F^{\times 2}.$$

כמייצב של q במרחב התבניות, זו בוודאי חבורה.

הערה 2.5.1 מכיוון שכפל בתבנית חד־ממדית שומר על הממד, יכולנו לכתוב גם בשפה של חוג ויט, $G([q]) = \{t \in F^\times :\ \langle t \rangle \cdot [q] = [q]\}$.

הערה 2.5.2 תהי q תבנית ריבועית. אז $G(q) = \{b \in F^\times :\ \langle\langle b \rangle\rangle \otimes q \sim 0\}$.

הוכחה. $0 \sim q \perp -bq$ **אם ורק אם** $\langle\langle b \rangle\rangle \otimes q \cong q$ **אם ורק אם** $\langle b \rangle \cdot q \cong q$. □

דוגמא 2.5.3 לכל תבנית חד־ממדית, $G(\langle a \rangle) = F^{\times 2}$, משום ש־$t \in G(\langle a \rangle)$ אם ורק אם $\langle ta \rangle \cong \langle a \rangle$.

הערה 2.5.4 לכל שתי תבניות q, q', $G(q) \subseteq G(q \otimes q')$ (משום שאם $\langle t \rangle \otimes q \cong q$ אז בוודאי $\langle t \rangle \otimes q \otimes q' \cong q \otimes q'$).

תרגיל 2.5.5 לתבנית פיסטר מסדר ראשון, $G(\langle\langle a \rangle\rangle) = \left\{x^2 - ay^2 :\ x, y \in F\right\}$, כלומר גורמי הדמיון הם הערכים של $\langle\langle a \rangle\rangle$. דוגמא זו תקבל הכללות מרחיקות לכת בפרק 6.

טענה 2.5.6 תהי $K = F[\sqrt{\Delta}]$ הרחבה ריבועית ספרבילית של F, ותהי q תבנית אנאיזוטרופית מעל F. אם q_K היפרבולית אז $-\Delta \in G(q)$.

הוכחה. **לפי משפט 2.4.3, אפשר לפרק** $q = \langle\langle\Delta\rangle\rangle q''$. **לכן** $-\Delta \in G(\langle\langle\Delta\rangle\rangle) \subseteq G(q)$; **נעזרנו כאן בהערה 2.5.4.** $\square$

(בטענה 2.5.6 נשתמש כדי להוכיח את משפט 5.5.8, שהוא אחד המשפטים העיקריים על תבניות בשדות הניתנים לסידור).

פרק 3

השמורות הראשונות

3.1 זוגיות הממד

פונקציית הממד אינה מוגדרת היטב על חוג ויט, משום שתבניות היפרבוליות שקולות לאפס. עם זאת, הממד כן מוגדר מודולו 2, וזה מאפשר להגדיר סדרה קצרה מדוייקת

$$0 \longrightarrow I(F) \hookrightarrow W(F) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

כלומר איזומורפיזם

$$W(F)/I(F) \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z}.$$

3.2 הדטרמיננטה

לאחר שחישבנו את המנה $W/I \cong \mathbb{Z}/2\mathbb{Z}$, הצעד הבא הוא לחשב את המנה I/I^2. לשם כך עלינו למצוא הומומורפיזם מ־$I(F)$, שהגרעין שלו הוא $I^2(F)$. נזכר שכל תבנית ריבועית מוצגת על־ידי מטריצה A; ואז היא מוצגת גם על־ידי כל מטריצה מהצורה PAP^{t}. עובדה זו מציעה שנגדיר על תבנית את ה**דטרמיננטה** שלה,

$$\det(q) = \det(A)F^{\times 2} \in F^{\times}/F^{\times 2},$$

כאשר A היא מטריצה כלשהי המייצגת את q. מכיוון ש־

$$\det(PAP^{\mathrm{t}}) = \det(A)\det(P)^2 \sim \det(A)$$

בחבורת המחלקות הריבועיות $F^{\times}/F^{\times 2}$, הדטרמיננטה של תבנית מוגדרת היטב (מודולו ריבועים). יתרון נוסף נובע מהתכונות של מטריצות בלוקים:

$$\det(q \perp q') = \det(q)\det(q').$$

עם זאת, $\det(\mathbb{H}) = \det(\langle 1, -1\rangle) = -1$, ולכן הדטרמיננטה של מחלקה בחוג ויט אינה מוגדרת היטב, אלא עד כדי ריבועים וסימן.

תרגיל 3.2.1 המישור הרגולרי היחיד (V, q) בעל $\det(q) = -1$ הוא המישור ההיפרבולי (השווה לטענה 2.1.4). **הדרכה.** הבא את התבנית לצורה אלכסונית.

תרגיל 3.2.2 אם $\langle a, b, c\rangle$ איזוטרופית, אז $\langle a, b, c\rangle \sim \langle -abc\rangle$.

3.3 הדיסקרימיננטה

כפי שראינו הדטרמיננטה אינה מוגדרת היטב על מחלקות בחוג ויט. הדיסקרימיננטה פותרת את הבעיה הזו. נגדיר את ה**דיסקרימיננטה** של תבנית q מממד $n = \dim(q)$ לפי

$$\mathrm{disc}(q) = (-1)^{n(n-1)/2} \det(q);$$

ובאופן יותר מפורש,

$$\mathrm{disc}(\langle a_1, \dots, a_n\rangle) = (-1)^{n(n-1)/2} a_1 \cdots a_n.$$

מתקיים

$$\mathrm{disc}(q \perp \mathbb{H}) = (-1)^{(n+2)(n+1)/2} \det(q \perp \mathbb{H}) = -(-1)^{n(n-1)/2+1} \det(q) = \mathrm{disc}(q),$$

ולכן הדיסקרימיננטה מוגדרת היטב על מחלקות.

תרגיל 3.3.1 גם הפונקציה $d'(q) = (-1)^n \det(q)$ מוגדרת היטב על מחלקות בחוג ויט; ויחד עם $\mathrm{disc}(q)$, אלו כל הפונקציות מהצורה $q \mapsto c_{\dim q} \det(q)$ המוגדרות היטב על מחלקות.

נחשב כמה מקרים מיוחדים:

$$\mathrm{disc}(\langle a\rangle) = a;$$

$$\mathrm{disc}(\langle\langle a\rangle\rangle) = \mathrm{disc}(\langle 1, -a\rangle) = a;$$

$$\mathrm{disc}(\langle\langle a, b\rangle\rangle) = \mathrm{disc}(\langle 1, -a, -b, ab\rangle) = (-1)^{\frac{3\cdot 4}{2}} a^2b^2 \sim 1.$$

טענה 3.3.2 הדיסקרימיננטה משרה הומומורפיזם של חבורות אבליות,

$$d : I/I^2 \to F^\times/F^{\times 2},$$

לפי $d(q + I^2) = \mathrm{disc}(q)F^{\times 2}$.

הוכחה. חישוב ישיר מראה שלכל שתי תבניות q, q' מתקיים $\mathrm{disc}([q]+[q']) = (-1)^{nn'}\mathrm{disc}([q])\mathrm{disc}([q'])$, כאשר $n = \dim(q)$ ו־$n' = \dim(q')$. אם אחת התבניות מממד זוגי אז

$$\mathrm{disc}([q] + [q']) = \mathrm{disc}([q])\mathrm{disc}([q]');$$

בפרט, $d : I(F) \to F^\times/F^{\times 2}$ הוא הומומורפיזם של חבורות. לפי מסקנה 2.3.18, I^2 נוצר על־ידי תבניות פיסטר מסדר 2 וראינו ש־$\mathrm{disc}(\langle\langle a, b\rangle\rangle) = 1$. מכאן ש־$d$ מוגדר היטב על חבורת המנה I/I^2. □

למה 3.3.3 (כמעט אדיטיביות של תבניות פיסטר)

$$\langle\langle a\rangle\rangle \perp \langle\langle b\rangle\rangle \sim \langle\langle ab\rangle\rangle \perp \langle\langle a, b\rangle\rangle.$$

הוכחה. מכיוון ש־$\mathbb{H} \cong \langle ab, -ab\rangle$,

$$\begin{aligned}\langle\langle a\rangle\rangle \perp \langle\langle b\rangle\rangle &\cong \langle 1, -a, 1, -b\rangle \\ &\sim \langle 1, -a, 1, -b, ab, -ab\rangle \\ &\cong \langle 1, -a, -b, ab\rangle \perp \langle 1, -ab\rangle = \langle\langle a, b\rangle\rangle \perp \langle\langle ab\rangle\rangle.\end{aligned}$$

□

משפט 3.3.4 *הדיסקרימיננטה משרה איזומורפיזם*

$$d\colon I/I^2 \to F^\times/F^{\times 2}.$$

הוכחה. הפונקציה $d(q + I^2) = \mathrm{disc}(q)F^{\times 2}$ מוגדרת היטב לפי טענה 3.3.2, והיא על מפני שלכל a, $\mathrm{disc}(\langle\langle a\rangle\rangle + I^2) = aF^{\times 2}$. בכיוון ההפוך הפונקציה

$$f_1\colon F^\times/F^{\times 2} \to I/I^2$$

השולחת $f_1 : aF^{\times 2} \mapsto \langle\langle a\rangle\rangle + I^2$ מוגדרת היטב; והיא הומומורפיזם משום שלפי הכמעט־אדיטיביות (למה 3.3.3),

$$\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle \sim \langle\langle ab\rangle\rangle \perp \langle\langle a, b\rangle\rangle \equiv \langle\langle ab\rangle\rangle \pmod{I^2}.$$

התוצאה נובעת מכך ששתי ההעתקות הופכות זו את זו. □

בעיה 3.3.5 הראה שלכל תבנית q מממד איזוגי, $q \perp \langle\mathrm{disc}(q)\rangle \in I^2(F)$. מצא הצגה של $\langle a_1, \dots, a_n, (-1)^{n(n-1)/2}a_1\cdots a_n\rangle$ בתור סכום של תבניות פיסטר מסדר 2. **הדרכה.** נסמן $n = \dim q$. אם $n = 1$ אז $q \perp \langle\mathrm{disc}(q)\rangle \sim \mathbb{H}$. אם $n = 3$,

$$\langle a_1, a_2, a_3, -a_1a_2a_3\rangle \sim \langle\langle -a_1, -a_2\rangle\rangle - \langle\langle -a_1a_2, a_3\rangle\rangle$$

ואם $n > 3$, אז עבור $b = (-1)^{n(n-1)/2}a_1\cdots a_n$ מתקיים

$$\langle a_1, \dots, a_n, b\rangle \sim \langle\langle -a_1, -a_2\rangle\rangle - \langle\langle -a_1a_2, a_3\rangle\rangle + \langle -a_1a_2a_3, a_4, \dots, a_n, b\rangle.$$

הגדרה 3.3.6 *תהי φ תבנית פיסטר. מסמנים ב־φ' את* ***תת־התבנית הטהורה****, שהיא התבנית מממד $\dim(\varphi) - 1$ שעבורה $\varphi \cong \langle 1\rangle \perp \varphi'$.*

תרגיל 3.3.7 לתבנית ריבועית מממד 4 יש דיסקרימיננטה 1 אם ורק אם היא תבנית פיסטר.

נסמן ב־Quad_n את אוסף התבניות הלא־מנוונות מממד n מעל השדה, וב־P_n את אוסף תבניות פיסטר מממד 2^n.

תרגיל 3.3.8 מצא התאמה חד־חד־ערכית ועל $\Delta\colon \mathrm{Quad}_3 \longleftrightarrow \mathrm{Quad}_1 \times P_2$. **הדרכה.** התאם $\Delta\langle a, b, c\rangle = (\langle abc\rangle, \langle\langle -ab, -ac\rangle\rangle)$ ו־$\Delta^{-1}(\langle\delta\rangle, \pi) = \langle\delta\rangle\pi'$. הראה שתחת התאמה זו, מרכיב פיסטר של $\Delta(\varphi)$ הוא היפרבולי אם ורק אם φ איזוטרופי.

3.3.1 תבניות בינאריות

תבנית על מרחב דו־ממדי נקראת גם **תבנית בינארית**. נעזר בדיסקרימיננטה כדי למיין את התבניות האלה:

טענה 3.3.9 את התבנית הבינארית q אפשר להציג בצורה $\langle a,b\rangle$ אם ורק אם a הוא ערך של התבנית, ו־$ab = -\operatorname{disc}(q)$.

הוכחה. **אם $q = \langle a,b\rangle$ אז $a = q(1,0)$ הוא ערך של התבנית ו־$\operatorname{disc}(q) = -ab$. בכיוון ההפוך נניח ש־$q$ נתונה, a הוא ערך שלה ו־$-ab = \operatorname{disc}(q)$. אז יש $x \in F^2$ עם $\operatorname{disc}(x) = a$; אפשר להשלים את $\{x\}$ לבסיס אורתוגונלי, ולכתוב $q \cong \langle a,c\rangle$ עבור איזשהו $c \in F^\times$. אבל אז $-ab = \operatorname{disc}(q) = \operatorname{disc}(\langle a,c\rangle) = -ac$ ו־$c \equiv b \pmod{F^{\times 2}}$.** □

מסקנה 3.3.10 את התבנית הבינארית q אפשר להציג בצורה $\langle a,*\rangle$ אם ורק אם a הוא ערך של התבנית.

מסקנה 3.3.11 (הצגות של תבנית בינארית) $\langle a,b\rangle \cong \langle c,d\rangle$ אם ורק אם c הוא ערך של התבנית, כלומר מהצורה ax^2+by^2, ו־$cd \equiv ab \pmod{F^{\times 2}}$.

תרגיל 3.3.12 נניח ש־$\operatorname{char}F = 2$, ונסמן $\mathcal{P}(F) = \{u^2+u\colon u \in F\}$; זוהי תת־חבורה חיבורית של $(F,+)$. כל תבנית בינארית אפשר לייצג כמטריצה (לאו דווקא סימטרית) בדרכים שונות; הראה שהדטרמיננטה של המטריצה המייצגת מוגדרת היטב בחבורת המנה $F/\mathcal{P}(F)$.

תרגיל 3.3.13 הראה שבמאפיין 2, כל תבנית רגולרית דו־ממדית שאינה סכום של תבניות חד־ממדיות, אפשר להציג בצורה $ax^2+xy+by^2$ (שאותה מסמנים $[a,b]$).

בעיה 3.3.14 $\operatorname{char}F = 2$. הראה ש־$[a,b] \cong [c,d]$ אם ורק אם c הוא ערך של התבנית $ax^2+xy+by^2$, ו־$ab \equiv cd \pmod{\mathcal{P}(F)}$ (זוהי השמורה של ארף (Arf), המחליפה את הדיסקרימיננטה במאפיין 2).

3.3.2 יוצרים ויחסים לחוג ויט

כדי להגדיר הומומורפיזמים מחוג ויט, טוב שתהיה לנו הצגה שלו באמצעות יוצרים ויחסים. הדרך להצגה כזו עוברת בתכונה חשובה ושימושית שהוכיח ויט.

משפט 3.3.15 (משפט השרשרת של ויט) *כל איזומורפיזם $\langle b_1,\dots,b_n\rangle \xrightarrow{\cong} \langle a_1,\dots,a_n\rangle$ של תבניות ריבועיות אפשר להציג כשרשרת של איזומורפיזמים כך שבכל צעד משתנים רק שני רכיבים סמוכים; כלומר, כל צעד הוא מהצורה $\langle c_1,\dots,c_i',c_{i+1}',\dots,c_n\rangle \xrightarrow{\cong} \langle c_1,\dots,c_i,c_{i+1},\dots,c_n\rangle$.*

הוכחה. **את האיזומורפיזם אפשר לתאר כמעבר ממטריצה מייצגת A למטריצה מייצגת $B = PAP^{\mathrm{t}}$, כאשר P הפיכה. כידוע, כל מטריצה הפיכה אפשר להציג כמכפלה של מטריצות אלמנטריות, וכל אחת מאלה פועלת רק על שני רכיבים. כדי לדאוג שהרכיבים יהיו סמוכים, די לבצע סדרה של החלפות, והרי $\langle a,b\rangle = \langle b,a\rangle$.** □

בעיה 3.3.16 כתוב הוכחה שלמה של משפט השרשרת.

נגדיר חבורה W' הנוצרת על־ידי היוצרים $[a]$ (לכל $a \in F^\times$) בכפוף ליחסים

* $[ac^2] = [a]$,
* $[1]+[-1] = 0$,
* $[a]+[b] = [a+b]+[ab(a+b)]$.

למה 3.3.17 אם $\langle a,b\rangle \cong \langle c,d\rangle$ אז $[a]+[b]=[c]+[d]$.

הוכחה. לפי מסקנה **3.3.11**, יש $x,y,z \in F$ כך ש־$c=ax^2+by^2$ ו־$d=abcz^2$. לכן

$$[a]+[b]=[ax^2]+[by^2]=[ax^2+by^2]+[abx^2y^2(ax^2+by^2)]=[c]+[abc]=[c]+[d].$$

□

משפט 3.3.18 *כחבורה אבלית,* $W(F)$ *נוצר על־ידי התבניות* $\langle a\rangle$ ($a \in F^\times$)*, בכפוף ליחסים הבאים (בלבד):*

1. $\langle ac^2\rangle = \langle a\rangle$ *לכל* $c \in F^\times$;
2. $\langle 1\rangle + \langle -1\rangle = 0$;
3. $\langle a\rangle + \langle b\rangle = \langle a+b\rangle + \langle ab(a+b)\rangle$ *לכל* $a,b\in F^\times$ *כך ש־*$a+b\neq 0$.

הוכחה. עלינו להראות שההעתקה $W' {\rightarrow} W(F)$ המוגדרת לפי $\langle a\rangle \mapsto [a]$ היא איזומורפיזם. ההעתקה מוגדרת היטב משום ש־$\mathbb{H} = \langle 1,-1\rangle$ ו־$\langle a,b\rangle \cong \langle a+b, ab(a+b)\rangle$. היא על משום שלכל תבנית ב־$W(F)$ יש הצגה אלכסונית (במאפיין 2 הגרסה הנכונה היא שלכל תבנית q, $\langle 1\rangle \perp q$ אלכסונית, וכמובן די בזה). נשאר להוכיח שההעתקה חד־חד־ערכית. נניח ש־$\sum[a_i] - \sum[a_i'] \mapsto 0$. אפשר להוסיף מרכיב היפרבולי לאחד האגפים, ולהסיק ש־$\langle a_1,\dots,a_n\rangle \cong \langle a_1',\dots,a_n'\rangle$. לפי משפט השרשרת אפשר להניח שרק שני רכיבים סמוכים משתנים במעבר הזה, ולפי משפט הצמצום פירושו של דבר ש־$\langle a_i,a_{i+1}\rangle \cong \langle a_i',a_{i+1}'\rangle$. מזה נובע $[a_i]+[a_{i+1}]=[a_i']+[a_{i+1}']$ לפי למה **3.3.17**. □

מסקנה 3.3.19 כחוג, $W(F)$ נוצר על־ידי התבניות $\langle a\rangle$ בכפוף ליחסים שנמנו לעיל, בתוספת

4. $\langle a\rangle\langle b\rangle = \langle ab\rangle$.

את מסקנה 3.3.19 הוכיח האריסון (Harrison) ב־1970. בעקבות זאת אפשר להגדיר לכל חוג קומוטטיבי את חוג ויט־הריסון המופשט שלו [5], בתור החוג הנוצר על־ידי יוצרים פורמליים $\langle a\rangle$ לכל $0 \neq a\in R$, ובכפוף לאותם יחסים (ביחס $\langle ac^2\rangle=\langle a\rangle$ נדרש ש־c הפיך, וביחס $\langle a\rangle+\langle b\rangle = \langle a+b\rangle+\langle ab(a+b)\rangle$ נדרש רק שכל המקדמים שונים מאפס).

דוגמא 3.3.20 ההומומורפיזם של הממד מודולו 2 מוגדר לפי $\langle a\rangle \mapsto 1$. אפשר לבדוק שהוא מוגדר היטב גם דרך היחסים.

מכיוון ש־$I(F)$ היא תת־חבורה מאינדקס סופי של $W(F)$, תהליך רדמייסטר־שרייר (Reidmeister-Schreier) יודע לחשב מן ההצגה של $W(F)$ הצגה של $I(F)$:

טענה 3.3.21 כחבורה אבלית, $I(F)$ נוצר על־ידי התבניות $\langle\langle a\rangle\rangle$ ($a\in F^\times$), בכפוף ליחסים הבאים:

א. $\langle\langle ac^2\rangle\rangle = \langle\langle a\rangle\rangle$;

ב. $\langle\langle 1\rangle\rangle = 0$;

ג. $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = \langle\langle a+b\rangle\rangle + \langle\langle ab(a+b)\rangle\rangle$ ($a\neq -b$).

תרגיל 3.3.22 לפי הכמעט־אדיטיביות (למה 3.3.3), $I^2(F)$ נוצר על־ידי ההפרשים $\langle\langle a\rangle\rangle+\langle\langle b\rangle\rangle - \langle\langle ab\rangle\rangle$. חבר עובדה זו לטענה 3.3.21 כדי לקבל הצגה של $I(F)/I^2(F)$. הסק מכאן את טענה 3.3.4.

במשפט 4.3.8 אנו מביאים הצגה של $I^n(F)$ לכל F. הצגות של המנות I^n/I^{n+1} נובעות מהשערת מילנור, ראו בהמשך (סעיפים 4.3 ו 4.4).

3.4 אלגברות קליפורד

השמורה האפס של תבנית הוא מספר, זוגיות הממד. השמורה הראשונה, הדיסקרימיננטה, הוא סקלר בשדה, מודולו ריבועים. השמורה שנבנה בסעיף הזה הוא אובייקט קונקרטי - אלגברה מממד סופי, המוגדרת לכל תבנית q. אם מצטמצמים ל־I^2 (שם הדיסקרימיננטה טריוויאלית), מתקבל הומומורפיזם אל חבורת בראוור (Brauer) של האלגברות הפשוטות המרכזיות.

3.4.1 אלגברת קליפורד של תבנית

יהי V מרחב וקטורי. **אלגברת הטנזורים** של V היא האלגברה

$$T(V) = F \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots,$$

עם הפעולה $(v_1 \otimes \cdots \otimes v_n) \cdot (w_1 \otimes \cdots \otimes w_m) = v_1 \otimes \cdots \otimes v_n \otimes w_1 \otimes \cdots \otimes w_m$. האלגברה **מדורגת** לפי אורך הטנזורים. אם בוחרים בסיס $V = \operatorname{span}\{x_i\}$, זו אינה אלא **האלגברה החופשית** עם היוצרים x_i. ההצגה במונחי V נוחה יותר, למשל משום שכאשר נגדיר בעזרתה מושגים שונים, לא יהיה צורך להוכיח שההוכחה אינה תלויה בבסיס.

הגדרה 3.4.1 ***אלגברת קליפורד*** *של מרחב ריבועי (V, q) היא האלגברה*

$$C(V, q) = T(V) / \langle v \otimes v - q(v) \rangle,$$

כאשר האידיאל נוצר על־ידי כל האברים מהצורה $v \otimes v - q(v)$, $v \in V$. (במאפיין 2 יש להוסיף את היחסים $u \otimes v \otimes v \otimes w = q(v) u \otimes w$. במאפיין שונה מ־2 אין בהם צורך משום שהם נובעים מן היחס $v \otimes v = q(v)$.)

אם כך, אלגברת קליפורד היא האלגברה הכללית ביותר הנוצרת על־ידי המרחב V והמקיימת את היחס $v^2 = q(v)$ לכל $v \in V$.

דוגמא 3.4.2 אלגברת קליפורד של מרחב חד־ממדי $V = Fx$, עם התבנית הריבועית $\langle a \rangle$, היא $C(\langle a \rangle) = F[x : \ x^2 = a] = F[\sqrt{a}]$.

טענה 3.4.3 יהי $v_1, \dots, v_n$ בסיס של V. אז אוסף המכפלות המסודרות מכל האורכים,

$$1, v_1, \dots, v_n, v_1 v_2, \dots, v_{n-1} v_n, \dots, v_1 \cdots v_n,$$

מהווה בסיס ל־$C(V, q)$.

מסקנה 3.4.4 נניח ש־$\dim(V) = n$, אז $\dim C(V, q) = 2^n$.

נסמן ב־$b_q : V \times V \to F$ את התבנית הבילינארית המתאימה ל־q. אז באלגברה $C(V)$, לכל $u, v \in V$ מתקיים $uv + vu = (u+v)^2 - u^2 - v^2 = 2b_q(u, v)$, כלומר

$$vu = 2b_q(u, v) - uv.$$

בפרט, אם u, v מאונכים, אז u, v אנטי־מתחלפים.

מסקנה 3.4.5 נניח שהתבנית $q = \langle a_1, \dots, a_n \rangle$ אלכסונית ביחס לבסיס $\{v_1, \dots, v_n\}$, אז

$$C(V, q) \cong F[v_1, \dots, v_n \mid v_i^2 = a_i, \qquad v_j v_i = -v_i v_j \quad (i \neq j)]. \tag{3.1}$$

איזומורפיזמים ואוטומורפיזמים

תרגיל 3.4.6 התוצאה הבאה טריוויאלית מתוך ההגדרה: אם $q \cong q'$ אז $C(q) \cong C(q')$. הוכח את הטענה ישירות מן ההצגה (3.1).

תרגיל 3.4.7 הוכח שכל איזומורפיזם $C(V,q) \to C(V',q')$ המעביר את V ל־V' הוא איזומטריה. כלומר, אם יש איזומורפיזם $C(V,q) \to C(V',q')$ המעביר את V ל־V', אז $q \cong q'$. נסה להוכיח שאם $C(q) \cong C(q')$ אז $q \cong q'$. הסבר מהו הקושי המהותי בכיוון הזה. ראה בעיה 3.4.46.

תרגיל 3.4.8 בדומה לתרגיל 3.4.7, כל אוטומורפיזם של $C(V,q)$ השומר על V משרה על V איזומטריה.

המרכז של אלגברת קליפורד

נסמן ב־v_I, כאשר $I = \{i_1,\dots,i_t\} \subseteq N = \{1,\dots,n\}$, את המכפלה הסדורה $v_I = v_{i_1}\cdots v_{i_t}$. קל להוכיח ש־

$$v_I v_J = (-1)^{|I||J|-|I\cap J|} v_J v_I. \tag{3.2}$$

כמו־כן,

$$v_I^2 = (-1)^{\binom{|I|}{2}} \prod_{i\in I} a_i. \tag{3.3}$$

טענה 3.4.9 המרכז של $C(q)$ הוא $\mathrm{Z}(C(q)) = \begin{cases} F & n \equiv 0 \pmod 2 \\ F[v_N] & n \equiv 1 \pmod 2 \end{cases}$.

הוכחה. **כפל ב־v_i, מימין או משמאל, מהווה תמורה של אברי הבסיס v_I. לכן, אם $z = \sum \alpha_I v_I$ מתחלף עם יוצר v_i, היוצר מוכרח להתחלף עם כל מחובר $\alpha_I v_I$. אבל v_I מתחלף עם v_i אם ורק אם $|I| \equiv \delta_{i\in I} \pmod 2$, כאשר $\delta_{i\in I} = \begin{cases} 1 & i\in I \\ 0 & i\notin I \end{cases}$. אם $\emptyset \subset I \subset N$, אז הערך של $\delta_{i\in I}$ אינו קבוע, ולכן יש יוצרים שאינם מתחלפים עם v_I, ומכאן שהמקדם של v_I הוא אפס. האיבר v_N מתחלף עם כל היוצרים אם ורק אם n אי־זוגי, וזה משלים את החישוב.** $\square$

תרגיל 3.4.10 המכפלה $v_1\cdots v_n$ אינה תלויה בבסיס (כל עוד q אלכסונית ביחס אליו), אלא עד־כדי כפל בסקלר.

טכניקה דומה לחישוב המרכז מאפשרת להוכיח את התכונה החשובה הבאה:

טענה 3.4.11 אלגברת קליפורד היא אלגברה פשוטה.

כידוע, המרכז של כל חוג פשוט הוא שדה (ואז החוג מהווה אלגברה מעל אותו שדה). אלגברה מעל שדה F נקראת **מרכזית** אם המרכז שלה שווה ל־F. לפי טענה 3.4.9, המרכז של $C(V,q)$ הוא F כאשר V מממד זוגי.

מסקנה 3.4.12 אם $\dim(V)$ זוגי, אלגברת קליפורד של (V,q) היא פשוטה מרכזית מעל F.

3.4.2 קווטרניונים

הגדרה 3.4.13 *יהי F שדה. אלגברה פשוטה מרכזית מעל F, שהממד שלה הוא 4, נקראת **אלגברת קווטרניונים** מעל F.*

תרגיל 3.4.14 כל אלגברת קווטרניונים פרט ל־$\mathrm{M}_2(F)$ היא אלגברת חילוק.

הגדרה 3.4.15 *יהי F שדה ממאפיין שונה מ־2. יהיו $a, b \in F^\times$. האלגברה $(a,b) = (a,b)_{2,F}$ היא האלגברה עם יוצרים x, y ויחסים*

$$x^2 = a, \qquad y^2 = b, \qquad yx = -xy;$$

זו אלגברה ממד 4, עם בסיס $1, x, y, xy$.

טענה 3.4.16 יהי F שדה ממאפיין שונה מ־2. כל אלגברת קווטרניונים אפשר להציג בצורה (a,b) (בדרכים רבות), וכל אלגברה מהצורה הזו היא אלגברת קווטרניונים.

תרגיל 3.4.17 הראה ש־$(1,b)_{2,F} \cong \mathrm{M}_2(F)$ לכל $b \in F^\times$.

תרגיל 3.4.18 מצא זוג יוצרים סטנדרטיים של $(1,b) \cong \mathrm{M}_2(F)$.

דוגמא 3.4.19 אלגברת קליפורד של מרחב דו־ממדי $V = Fx + Fy$, עם התבנית הריבועית $\langle a, b\rangle$, היא אלגברת קווטרניונים $C(\langle a,b\rangle) \cong (a,b)_{2,F}$. בפרט $C(\langle\langle a\rangle\rangle) \cong \mathrm{M}_2(F) \sim F$.

טענה 3.4.20 (חוקי המשחק בקווטרניונים) לכל $a, b, a', b' \in F^\times$,

1. $(a,b)\otimes(a,b') \sim (a,bb')$;
2. $(a,b)\otimes(a',b) \sim (aa',b)$;
3. אם $a+b=1$ אז $(a,b) \sim F$.
4. $(a,-a) \sim F$.
5. $(a,b) \cong (b,a)$.

הוכחה. **קבוצת יוצרים סטנדרטית של $(a_1,b_1)\otimes(a_2,b_2)$ היא רביעיה x_1, y_1, x_2, y_2 כך ש־$x_i^2 = a_i$, $y_i^2 = b_i$, $y_ix_i = -x_iy_i$, ו־x_1, y_1 מתחלפים עם x_2, y_2.**

1. **נבחר קבוצת יוצרים סטנדרטית x, y, x', y' של אגף שמאל. אז xx'^{-1}, y, x', yy' היא קבוצת יוצרים סטנדרטית של $(1,b)\otimes(a,bb')$ הדומה ל־(a,bb') לפי תרגיל 3.4.17.**
2. **תרגיל.**
3. **יהי x, y זוג יוצרים סטנדרטי של (a,b), כלומר $x^2 = a$, $y^2 = b$ ו־$yx = -xy$. אז $(x+y)^2 = x^2 + xy + yx + y^2 = 1$, ולכן $(x+y+1)(x+y-1) = 0$. באלגברת חילוק אין מחלקי אפס, ומכאן ש־$(a,b) \cong \mathrm{M}_2(F)$ (תרגיל 3.4.14).**
4. **כמו בסעיף 3, $(x+y)^2 = a - a = 0$.**
5. **החלף את x, y ב־y, x.**

□

תרגיל 3.4.21 העזר בתרגיל 3.4.19 (ובטענה 3.4.20) כדי להראות ש־$C(\langle a\rangle \cdot \mathbb{H}) \cong \mathrm{M}_2(F)$ לכל $a \in F^\times$.

3.4.3 חישוב אלגברת קליפורד

נראה שאלגברת קליפורד של תבנית ממימד זוגי היא מכפלה טנזורית של אלגברות קווטרניונים.

משפט 3.4.22 *נניח ש־$q = \langle a_1, \dots, a_n \rangle$ כאשר $n = 2m$ זוגי. אז $C(q)$ היא מכפלה טנזורית של m אלגברות קווטרניונים,*

$$C(q) \cong \bigotimes_{i=1}^{m} ((-1)^{i-1} a_1 \dots a_{2i-2} a_{2i-1}, (-1)^{i-1} a_1 \dots a_{2i-2} a_{2i})_2$$

הוכחה. עבור $i = 1, \dots, m$, נסמן $p_i = v_1 v_2 \cdots v_{2i-3} v_{2i-2}$ (כך ש־$p_1 = 1$). נתבונן בתת־האלגברה $Q_i = F[p_i v_{2i-1}, p_i v_{2i}]$. נוסחת ההעלאה בריבוע (3.3) מראה ש־

$$Q_i \cong ((-1)^{\binom{2i-1}{2}} a_1 \dots a_{2i-2} a_{2i-1}, (-1)^{\binom{2i-1}{2}} a_1 \dots a_{2i-2} a_{2i})$$

הן אלגברות קווטרניונים, ובדיקה מראה שהן מתחלפות זו עם זו. לכן

$$C(q) \cong Q_1 \otimes Q_2 \otimes \cdots \otimes Q_m.$$

הנוסחה שבטענה נובעת מכך ש־$\binom{2i-1}{2} \equiv i - 1 \pmod 2$. □

כלומר,

$$C(\langle a_1, a_2, \dots, a_{2m} \rangle) = (a_1, a_2) \otimes (-a_1 a_2 a_3, -a_1 a_2 a_4) \otimes (a_1 a_2 a_3 a_4 a_5, a_1 a_2 a_3 a_4 a_6) \otimes \cdots .$$

אלגברת קליפורד הזוגית

בעיה 3.4.23 פירוק של אלגברה לסכום ישר $A = A_0 \oplus A_1$ נקרא **דירוג** (לפי $\mathbb{Z}/2\mathbb{Z}$) אם $A_i A_j \subseteq A_{i+j \pmod 2}$. הראה ש־$T(V)$ אלגברה מדורגת לפי הפירוק $T(V \otimes V) \oplus (V \otimes T(V \otimes V))$, ושדירוג זה משרה דירוג של אלגברת קליפורד עם המרכיבים

$$C(V, q) = C_0(V, q) \oplus C_1(V, q),$$

המוגדרים (בהמשך לטענה 3.4.3) כך ש־$C_0(q)$ נפרש על־ידי הווקטורים v_I עם $|I|$ זוגי, ו־$C_1(q)$ נפרש על־ידי הווקטורים v_I עם $|I|$ אי־זוגי. **הדרכה**. אכן, היחסים המגדירים את $C(V, q)$ שייכים כולם לחלק הזוגי $T(V \otimes V)$.

תרגיל 3.4.24 חשב את $\mathrm{Z}(C_0(q))$.

תרגיל 3.4.25 הראה ש־$\mathrm{C}_{C(V,q)}(C_0(V, q)) = F$. הסק: אם $w \in C_0(V, q)$ מתחלף עם כל $v \in V$, אז $w \in F$. הראה באותו אופן שאם $w \in C(V, q)$ אנטי־מתחלף עם כל $v \in V$, אז $w = 0$.

3.4.4 אלגברות פשוטות מרכזיות

נסקור בקצרה ובלי הוכחות את יסודות התאוריה של אלגברות פשוטות מרכזיות מעל שדה.

לפי **משפט ודרברן**, כל אלגברה פשוטה A מממד סופי מעל המרכז שלה, איזומורפית לאלגברת מטריצות $\mathrm{M}_r(D)$ כאשר D חוג עם חילוק. לפי התכונות הידועות של מטריצות, לשתי האלגברות יש אותו מרְכָּז $\mathrm{Z}(A) = \mathrm{Z}(D)$. נתבונן באלגברות הפשוטות שהמרכז שלהן שווה לשדה נתון F. אלגברה שהמרכז שלה שווה ל־F נקראת **אלגברה מרכזית** מעל F (ואם השדה ברור מההקשר, סתם אלגברה מרכזית).

הגדרה 3.4.26 *אומרים ששתי אלגברות מרכזיות A, B הן **שקולות במובן של בראואר**, ומסמנים $A \sim B$, אם שתיהן אלגברות מטריצות מעל אותו חוג עם חילוק. תכונה זו שקולה לכך שקיימים r, s כך ש־$\mathrm{M}_r(A) \cong \mathrm{M}_s(B)$. את מחלקת השקילות של A מסמנים ב־$[A]$.*

תרגיל 3.4.27 אם $A \sim B$ ו־$\dim(A) = \dim(B)$ אז $A \cong B$.

טענה 3.4.28 תהיינה A, B אלגברות פשוטות מרכזיות, אז גם $A \otimes_F B$ היא אלגברה פשוטה מרכזית.

הגדרה 3.4.29 *המכפלה של מחלקות (ראה הגדרה 3.4.26) מוגדרת לפי $[A] \cdot [B] = [A \otimes_F B]$.*

טענה 3.4.30 $A \otimes A^{\mathrm{op}} \cong \mathrm{End}_F(A) \cong \mathrm{M}_{\dim(A)} F \sim F$.

מסקנה 3.4.31 אוסף המחלקות של אלגברות פשוטות מרכזיות מעל F, עם פעולת הכפל של מחלקות לפי מכפלת טנזורית של נציגים, מהווה חבורה (הנקראת **חבורת בראואר של** F; מסמנים אותה ב־$\mathrm{Br}(F)$).

המשפט הבא מאפשר לזהות מכפלות טנזוריות:

טענה 3.4.32 תהי A אלגברה פשוטה מרכזית. לכל תת־אלגברה $B \subseteq A$ שהיא בעצמה פשוטה ומרכזית, גם $B' = \mathrm{C}_A(B)$ פשוטה מרכזית, ו־$A \cong B \otimes_F B'$.

העתקת הצמצום

טענה 3.4.33 אם A אלגברה פשוטה מרכזית מעל F, ו־K/F הרחבת שדות, אז $K \otimes_F A$ היא אלגברה פשוטה מרכזית מעל K, והממדים שווים: $[K \otimes_F A : K] = [A : F]$.

טענה 3.4.34 מעל שדה סגור אלגברית אין אלגברת חילוק מממד סופי פרט לשדה עצמו.

מסקנה 3.4.35 הממד של אלגברה פשוטה מרכזית A מעל המרכז שלה הוא תמיד ריבוע של מספר שלם. שורש הממד נקרא **הדרגה** של האלגברה, ומסמנים אותו $\deg(A)$.

כעת מתברר שאלגברות קווטרניונים, בעלות דרגה 2, הן האלגברות הפשוטות המרכזיות בעלות הממד הקטן ביותר האפשרי (פרט לשדה הבסיס כמובן).

טענה 3.4.36 $K \otimes_F (A \otimes_F B) \cong (K \otimes_F A) \otimes_K (K \otimes_F B)$, ולכן $[A] \mapsto [K \otimes_F A]$ מגדיר הומומורפיזם של חבורות

$$\mathrm{res}_{K/F} : \mathrm{Br}(F) \to \mathrm{Br}(K).$$

הסדר של $[A] \in \mathrm{Br}(F)$ נקרא **האקספוננט** של A, ומסמנים אותו ב־$\exp(A)$.

טענה 3.4.37 לכל אלגברה פשוטה מרכזית A, $\exp(A) \mid \deg(A)$. בפרט, הסדר תמיד סופי.

3.4.5 אלגברת קליפורד כאינווריאנט של תבניות

אלגברת קליפורד של q משמרת את הממד של q, ולכן אינה יכולה להיות מוגדרת היטב על מחלקות דמיון בחוג ויט. מאידך, אם נתבונן באלגברה עד כדי דמיון בחבורת בראוור, נאבד את הממד ונוכל להביא בחשבון את השקילות בחוג ויט. למשל, לפי תרגילים 3.4.19 ו־3.4.17, $C(\mathbb{H}) \cong \mathrm{M}_2(F) \sim F$.

חישוב ישיר בעזרת משפט 3.4.22, יחד עם העובדה שאם $n = 2m$ אז $\binom{n}{2} \equiv m \pmod 2$, מביא למסקנה הבאה:

מסקנה 3.4.38 תהיינה q, q' תבניות ריבועיות ממימד זוגי מעל F. אז

$$C(q \perp q') \cong C(q) \otimes C(\langle \mathrm{disc}(q) \rangle \cdot q'),$$

כאשר $\mathrm{disc}(q)$ היא הדיסקרימיננטה.

הערה 3.4.39 אפשר להגדיר *twisted tensor product* של אלגברות מדורגות על־ידי $\mathbb{Z}/2\mathbb{Z}$, ואז

$$C(q \perp q') \cong C(q) \hat{\otimes} C(q').$$

ובפרט (אם נבחר במסקנה 3.4.38 $q' = \langle 1, -1 \rangle$),

מסקנה 3.4.40 תהי q תבנית ריבועית ממימד זוגי מעל F. אז $C(\mathbb{H} \perp q) \sim C(q)$.

מסקנה 3.4.41 התאמת אלגברת קליפורד לתבנית היא העתקה מוגדרת היטב $\gamma : I(F) \to \mathrm{Br}(F)$, לפי $\gamma([q]) = [C(q)]$. זהו **שמורת הסה־ויט** (Hasse-Witt) של q.

מסקנה 3.4.42 הצמצום ל־I^2 הוא הומומורפיזם $\gamma : I^2(F) \to \mathrm{Br}(F)$.

הוכחה. לפי טענה 3.3.2, $\mathrm{disc}(q) = 1$ לכל $q \in I^2$. נציב זאת במסקנה 3.4.38, ונקבל שאם אחת מבין q, q' שייכת ל־I^2, אז $C(q \perp q') \cong C(q) \otimes C(q')$. בפרט $[C(q \perp q')] = [C(q)] + [C(q')]$. $\square$

טענה 3.4.43 יהיו $a, b, c \in F^\times$.

א. $C(\langle c \rangle \langle\langle a, b \rangle\rangle) \sim (a, b)_2$.

ב. $C(\langle\langle a, b, c \rangle\rangle) \sim F$.

הוכחה. 1. לפי משפט 3.4.22 וטענה 3.4.20,

$$\begin{aligned} C(\langle c \rangle \langle\langle a, b \rangle\rangle) &= C(\langle c, -ac, -bc, abc \rangle) \\ &\cong (c, -ac)_2 \otimes (-abc, bc)_2 \\ &\sim (c, a)_2 \otimes (a, bc)_2 \sim (a, b)_2. \end{aligned}$$

2. לפי מסקנה 3.4.38 והסעיף הקודם,

$$\begin{aligned} C(\langle\langle a, b, c \rangle\rangle) &= C(\langle\langle a, b \rangle\rangle \perp \langle -c \rangle \langle\langle a, b \rangle\rangle) \\ &\cong C(\langle 1 \rangle \langle\langle a, b \rangle\rangle) \otimes C(\langle -c \rangle \langle\langle a, b \rangle\rangle) \\ &\sim (a, b)_2 \otimes (a, b)_2 \sim F. \end{aligned}$$

$\square$

מכך ש־$\gamma(\langle\langle a,b,c\rangle\rangle) = 0$ נובע ש־$I^3 \subseteq \mathrm{Ker}(\gamma)$, ובנינו ככלות הכל את השמורה השניה:

מסקנה 3.4.44 יש הומומורפיזם

$$\gamma : I^2(F)/I^3(F) \to \mathrm{Br}(F)$$

המוגדר לפי $\gamma([q]+I^3) = [C(q)]$.

בעיה 3.4.45 הראה שלכל תבנית q ממימד זוגי ולכל $a \in F^\times$, $C_0(\langle a\rangle q) \cong C_0(q)$.

בעיה 3.4.46 מצא תבניות $q, q' \in I^2(F)$ שאינן איזומורפיות, כך ש־$C(q) \cong C(q')$. (אבל ראה תרגיל 3.4.27.)

בעיה 3.4.47 הראה שלכל תבנית q ממימד זוגי, $C(\langle\langle -\mathrm{disc}(q)\rangle\rangle q) \sim F$. הוכח גם ש־$\langle\langle -\mathrm{disc}(q)\rangle\rangle q \in I^3(F)$.

3.4.6 אינוולוציות

תהי R אלגברה מעל שדה F. **אינוולוציה** של R היא אנטי־אוטומורפיזם מסדר 2, כלומר פונקציה $\sigma : R \to R$ המקיימת

$$\begin{aligned}\sigma(t+t') &= \sigma(t)+\sigma(t')\\ \sigma(tt') &= \sigma(t')\sigma(t)\\ \sigma(\sigma(t)) &= t\end{aligned}$$

אינוולוציה היא **מסוג ראשון** אם הצמצום של σ למרכז F הוא הזהות, **ומסוג שני** אם הצמצום הוא אוטומורפיזם לא טריוויאלי.

משפט 3.4.48 *לאלגברה פשוטה מרכזית A יש אינוולוציה מסוג ראשון אם ורק אם* $2 \mid \exp(A)$.

הגדרה 3.4.49 *מסמנים ב־$_2\mathrm{Br}(F)$ את תת־החבורה של $\mathrm{Br}(F)$ הנוצרת על־ידי המחלקות מסדר. לדוגמא, (המחלקה של) כל אלגברת קווטרניונים שייכת ל־$_2\mathrm{Br}(F)$.*

לפי המשפט, לאלגברה פשוטה מרכזית יש אינוולוציה מסוד ראשון אם ורק אם המחלקה שלה שייכת ל־$_p\mathrm{Br}(F)$. לכן כל המחלקות של אלגברות קליפורד $C(V,q)$ עם $\dim V$ זוגי שייכות ל־$_2\mathrm{Br}(F)$, ואפשר לתקן את מסקנה 3.4.44: השמורה γ היא הומומורפיזם

$$\gamma : I^2(F)/I^3(F) \to {}_2\mathrm{Br}(F).$$

(זהו איזומורפיזם; ראה הערה 4.3.5.)

הגדרה 3.4.50 *על אלגברת הקווטרניונים (a,b) מוגדרת **האינוולוציה הסימפלקטית** לפי $x^* = -x$, $y^* = -y$ (ואז $(xy)^* = -xy$).*

תרגיל 3.4.51 האינוולוציה הסימפלקטית היא האינוולוציה היחידה של $Q = (a,b)$ שממד מרחב האברים הסימטריים תחתיה הוא 1. מצא אינוולוציה של Q שאינה סימפלקטית, והראה שממד מרחב האברים הסימטריים עבורה הוא 3.

האינוולוציה הסימפלקטית מגדירה את **הנורמה** $\mathrm{N} : Q \to F$ לפי $\mathrm{N}(w) = ww^*$.

תרגיל 3.4.52 $\mathrm{N}(t_0+t_1x+t_2y+t_3xy) = (t_0+t_1x+t_2y+t_3xy)(t_0-t_1x-t_2y-t_3xy) = t_0^2 - at_1^2 - bt_2^2 + abt_3^2$, כלומר תבנית הנורמה של (a,b) איזומורפית ל־$\langle\langle a,b\rangle\rangle$.

תרגיל 3.4.53 העקבה $\mathrm{tr}: Q \to F$ מוגדרת לפי $tr(w) = w + w^*$. הראה שלכל $w \in Q$ מתקיימת הזהות $w^2 - \mathrm{tr}(w)w + \mathrm{N}(w) = 0$. חשב את תבנית העקבה (הריבועית) של Q, המוגדרת לפי $x \mapsto \mathrm{tr}(x^2)$. השווה לדוגמא 2.4.6.

תרגיל 3.4.54 נניח ש־σ_1, σ_2 הן אינוולוציות של האלגברות הפשוטות המרכזיות A_1, A_2. הראה ש־$\sigma_1 \otimes \sigma_2$ היא אינוולוציה של $A_1 \otimes A_2$, כאשר המכפלה הטנזורית של אינוולוציות מוגדרת לפי $(\sigma_1 \otimes \sigma_2)(a_1 \otimes a_2) = \sigma_1(a_1) \otimes \sigma_2(a_2)$.

על אלגברת קליפורד $C(V,q)$ מוגדרת אינוולוציה לפי $v^* = -v$ לכל $v \in V$. במונחי הבסיס של טענה 3.4.3, האינוולוציה מוגדרת לפי $v_i^* = -v_i$, ולכן $(v_{i_1} \cdots v_{i_t})^* = (-1)^t v_{i_t} \cdots v_{i_1} = (-1)^{\binom{t+1}{2}} v_{i_1} \cdots v_{i_t}$.

דוגמא 3.4.55 תהי $q = \langle a, b \rangle$ תבנית דו־ממדית. כפי שראינו בדוגמא 3.4.19,

$$C(q) = F[x, y \mid x^2 = a,\, y^2 = b,\, yx = -xy]$$

היא אלגברת קווטרניונים. האינוולוציה שהוגדרה כאן מתלכדת עם האינוולוציה הסימפלקטית מהגדרה 3.4.50.

3.4.7 חבורת הספין והנורמה הספינורית

(החומר שבתת־סעיף זה יהיה נחוץ רק בסעיף 8.4 של פרק 8.)

הדטרמיננטה אינה מספקת מידע משמעותי על החבורה $O = O(V,q)$, משום שלכל שיקוף יש דטרמיננטה 1 או -1. מטרתנו היא להגדיר "נורמה ספינורית" $O^+ \to F^\times / F^{\times 2}$, ואת "חבורת הספין", שהיא הרמה מאינדקס 2 של הגרעין של הנורמה הספינורית. נזכיר את משפט 2.2.3:

טענה 3.4.56 $O(V,q)$ נוצרת על־ידי השיקופים τ_u, $u \in V$.

על־ידי בחירת בסיס מתאים, ברור שכל שיקוף צמוד למטריצה האלכסונית $\mathrm{diag}(1, \dots, 1, -1)$, ולכן $\det(\tau_v) = -1$. מכאן שבכל ההצגות של איזומטריה כמכפלת שיקופים, הזוגיות של מספר השיקופים נשמרת.

מסקנה 3.4.57 $O^+(V,q)$ נוצר על־ידי המכפלות של שני שיקופים.

נתבונן באלגברת קליפורד של q. יהי $u \in V$ וקטור אנאיזוטרופי. מכיוון ש־$u^2 = q(u) \neq 0$, u הפיך ו־$u^{-1} = \frac{1}{q(u)} u$. בתרגיל 3.4.8 ראינו שכל אוטומורפיזם של אלגברת קליפורד, השומר על V, משרה איזומטריה. מתברר שהצמדה באיבר של V היא מינוס שיקוף.

טענה 3.4.58 ההצמדה ב־$u \in V$ היא אוטומורפיזם של $C(V,q)$ המשרה את האיזומטריה $-\tau_u$ על V, כאשר τ_u הוא השיקוף המוגדר ב־(2.1).

הוכחה. לכל $v \in V$, $uvu^{-1} = (2b_q(u,v) - vu)u^{-1} = 2\frac{b_q(u,v)}{q(u)} u - v = -\tau_u(v)$. □

נתבונן בחבורת האברים של $C_0(V,q)$ הפועלים על V, כלומר החבורה

$$M^+ = \left\{ y \in C_0(V,q)^\times :\ yV = Vy \right\}. \tag{3.4}$$

לכל $u \in M^+$, נסמן ב־$\gamma_u \in \mathrm{GL}(V)$ את הפעולה המושרית על־ידי ההצמדה, $\gamma_u(x) = uxu^{-1}$.

משפט 3.4.59 *יש סדרה מדוייקת קצרה*

$$1 \longrightarrow F^{\times} \hookrightarrow M^{+} \xrightarrow{T:u\mapsto\gamma_u} O^{+}(V,q) \longrightarrow 1$$

הוכחה. ברור שהפונקציה $T:u \mapsto \gamma_u$ היא הומומורפיזם $M^{+} \to O(V,q)$. הגרעין שלה כולל את האברים ההפיכים ב־$C_0(V,q)$ המתחלפים עם כל אברי V, ואלו הם הסקלרים בלבד לפי תרגיל 3.4.25. לפי מסקנה 3.4.57, כל $\sigma \in O^{+}$ הוא מכפלה של מספר זוגי של שיקופים. נכתוב $\sigma = \tau_{y_1}\cdots\tau_{y_{2m}}$, $y_1,\dots,y_{2m} \in V$, כאשר בהכרח $q(y_i) \neq 0$ לכל i. האיבר $t = y_1\cdots y_{2m} \in C_0(V)$ הוא הפיך, כי $tt^* = q(y_1)\cdots q(y_{2m})$, ולפי טענה 3.4.58, ההצמדה ב־$y_1\dots y_{2m}$ משרה על V את הפעולה $\tau_{y_1}\cdots\tau_{y_{2m}} = (-\tau_{y_1})\cdots(-\tau_{y_{2m}})$. כלומר, $y_1\cdots y_{2m} \in M^{+}$, ו־$T(y_1\cdots y_{2m}) = \sigma$.

נשאר להוכיח שהתמונה של T מוכלת ב־O^{+}. אחרת, יש $t \in M^{+}$ כך ש־$T(t) = \tau_{y_1}\cdots y_{\tau_{2m+1}}$, עבור $y_1,\dots,y_{2m+1} \in V$ אנאיזוטרופיים. נתבונן ב־$w = y_1\cdots y_{2m+1} \in C_1(V)$. לפי הנימוק הקודם הצמדה ב־w משרה את המכפלה $-\tau_{y_1}\cdots y_{2m+1} = -T(t)\gamma_t$ על V, כלומר הצמדה ב־$t^{-1}w \in C_1(V)$ משרה את ההעתקה $x \mapsto -x$ על V. בתרגיל 3.4.25 הראינו שזה בלתי אפשרי. $\square$

מן הפסקה הראשונה בהוכחה נובע:

מסקנה 3.4.60 כל איבר ב־M^{+} הוא מהצורה $\alpha y_1\cdots y_{2m}$ עבור $y_1,\dots,y_{2m} \in V$ אנאיזוטרופיים ו־$\alpha \in F^{\times}$.

מסקנה 3.4.61 לכל $t \in M^{+}$, $N(t) = tt^* \in F^{\times}$. לכן $t \mapsto tt^*$ הוא הומומורפיזם $M^{+} \to F^{\times}$.

הוכחה. אכן $N(y_1\cdots y_{2m}) = y_1\cdots y_{2m}y_{2m}\cdots y_1 = q(y_1)\cdots q(y_{2m})$, וזה הומומורפיזם כי $N(ts) = tss^*t^* = tt^*(ss^*) = N(t)N(s)$. $\square$

הגדרה 3.4.62 *הגרעין של ההומומורפיזם $M^{+} \to F^{\times}$ המוגדר לפי $t \mapsto tt^*$ הוא **חבורת הספין** של (V,q),*

$$\mathrm{Spin}(V,q) = \{y \in C_0(V,q) :\ yy^* = 1, yV = Vy\}.$$

מכיוון שכל $\sigma \in O^{+}$ אפשר להציג בצורה γ_t עבור $t \in M^{+}$ יחיד עד כפל בסקלר, אפשר להגדיר את **הנורמה הספינורית**

$$\theta : O^{+} \to F^{\times}/F^{\times 2}$$

לפי $\theta(\gamma_t) = tt^*F^{\times 2}$; על היוצרים, ההומומורפיזם הזה מוגדר לפי $\theta(\tau_y\tau_{y'}) = q(y)q(y')F^{\times 2}$.

הגדרה 3.4.63 *בדומה להגדרה הקודמת, נסמן*

$$\Theta(V,q) = \mathrm{Ker}(\theta : O^{+} \to F^{\times}/F^{\times 2}) = \left\{\sigma \in O^{+} :\ \theta(\sigma) \equiv 1 \pmod{F^{\times 2}}\right\} \subseteq O^{+}(V,q).$$

הערה 3.4.64 אפשר לסכם את ההגדרה גם כך: $\Theta(V,q)$ כוללת את מכפלות השיקופים $\tau_{y_1}\cdots\tau_{y_{2m}}$ שעבורן $q(y_1)\cdots q(y_{2m}) \in F^{\times 2}$.

נתבונן בדיאגרמה הקומוטטיבית הבאה, המרחיבה את הסדרה המדוייקת של המשפט.

$$\begin{tikzcd}
 & \{\pm1\} \arrow[r, hook] \arrow[d, hook] & \mathrm{Spin}(V,q) \arrow[r] \arrow[d, hook] & \Theta(V,q) \arrow[d, hook] & \\
1 \arrow[r] & F^\times \arrow[r, hook] \arrow[d, "\square^2"] & M^+ \arrow[r, "T:u\mapsto\gamma_u"] \arrow[d, "u\mapsto uu^*"] & O^+(V,q) \arrow[r] \arrow[d, "\theta"] & 1 \\
1 \arrow[r] & F^{\times 2} \arrow[r, hook] & F^\times \arrow[r] & F^\times/F^{\times 2} \arrow[r] & 1
\end{tikzcd}$$

מן הדיאגרמה קל לראות ש־Θ שווה לתמונת T המצומצמת אל חבורת הספין $\mathrm{Spin}(V,q)$, כלומר $\Theta = \{\gamma_u :\ u \in \mathrm{Spin}\}$. קל גם לראות ש־$\mathrm{Ker}(T) \cap \mathrm{Spin} = \{\pm1\}$.

מסקנה 3.4.65 $\Theta \cong \mathrm{Spin}(V,q)/\{\pm1\}$.

כדי להבין את Θ טוב יותר, נשווה אותה לחבורת הקומוטטורים $[O(q),O(q)]$.

הערה 3.4.66 לכל $\sigma \in O(V,q)$, $\sigma\tau_u\sigma^{-1} = \tau_{\sigma u}$. אכן

$$\sigma\tau_u\sigma^{-1}(x) = \sigma(\sigma^{-1}(x) - 2\frac{b(\sigma^{-1}x,v)}{b(v,v)}v) = x - 2\frac{b(x,\sigma v)}{b(\sigma v,\sigma v)}\sigma(v).$$

טענה 3.4.67 החבורת $[O(V,q),O(V,q)]$ נוצרת על־ידי המכפלות $\tau_u\tau_{u'}$ עם $q(u)=q(u')$.

הוכחה. אוסף השיקופים סגור להצמדה, ולכן חבורת הקומוטטורים נוצרת על־ידי הקומוטטורים של יוצרים, $[\tau_u,\tau_v] = \tau_u\tau_v\tau_u\tau_v = \tau_u\tau_{\tau_v(u)}$, והרי $q(\tau_v(u)) = q(u)$. מאידך, לכל u,u' מאותו אורך יש שיקוף σ כך ש־$\pm u' = \sigma(u)$ (למה 2.2.2), ואז $\tau_u\tau_{u'} = [\tau_u,\sigma]$. □

מסקנה 3.4.68 $[O(V,q),O(V,q)] \subseteq \Theta(V,q) \subseteq O^+(V,q) \subset O(V,q)$, ובקיצור

$$[O,O] \subseteq \Theta \subseteq O^+ \subseteq O.$$

אכן, נתבונן ביוצר טיפוסי של חבורת הקומוטטורים, על־פי טענה 3.4.67. יהיו $u,u' \in V$ וקטורים כך ש־$q(u)=q(u')$. אז $\theta(\tau_u\tau_{u'}) = q(u')q(u)F^{\times 2} = F^{\times 2}$, כלומר $\tau_u\tau_{u'} \in \Theta$ (הטענה החלשה יותר $\Theta \subseteq [O^+,O^+]$ היא טריוויאלית, שהרי $O^+/\Theta \subseteq F^\times/F^{\times 2}$ היא חבורה אבלית).

בעיה 3.4.69 חשב את $O(V,q)/[O(V,q),O(V,q)]$. האם זו חבורה מאקספוננט 2?

דוגמא 3.4.70 נחשב את כל החבורות שהוזכרו בסעיף זה עבור התבנית הבינארית $q = \langle a,b\rangle$. אלגברת קליפורד היא $F[x,y]$ עם $x^2=a$, $y^2=b$ ו־$yx=-xy$. החלק הזוגי הוא $K = F[xy] \cong F[\sqrt{-ab}]$. מתברר ש־$M = K^\times$, והריבוע הימני־עליון של הדיאגרמה כולל את החבורות

$$\begin{tikzcd}
\mathrm{Spin} \arrow[r, equal] & K^1 \arrow[r] \arrow[d, hook] & K^\times/\{\pm1\} \arrow[r, "\cong"] & F^\times K^1/F^\times \arrow[r, equal] \arrow[d, hook] & \Theta \\
M \arrow[r, equal] & K^\times \arrow[rr] & & K^\times/F^\times \arrow[r, equal] & O^+
\end{tikzcd}$$

בעיה 3.4.71 אם $\dim V \geq 3$ אז $[O, O] = [O^+, O^+]$ (ראה [15, 43:7]).

תרגיל 3.4.72 אם q תבנית איזוטרופית, אז $[O, O] = \Theta$ ([4, Thm. 10.3.2]).

תרגיל 3.4.73 במשפט 3.4.59 ראינו ש־$O^+ \cong M^+/F^\times$. כהכללה להגדרה של M^+ ב־(3.4), נגדיר $M = \{y \in C(V,q)^\times :\ yV = Vy\}$. הראה שאם $\dim V$ זוגי אז $O \cong M/F^\times$; ואם $\dim V$ אי־זוגי אז $O^+ \cong M^+/F^\times \cong M/F[v_N]^\times$ (v_N הוגדר בתת־סעיף 3.4.3).

פרק 4

השמורות הגבוהות

4.1 תורת־K של חוגים

לכל חוג R אפשר להגדיר חבורה אבלית $\mathrm{K}_n(R)$; כל K_n הוא פונקטור מהקטגוריה של חוגים לקטגוריה של חבורות אבליות, ויש סדרות מדוייקות הקושרות את הפונקטורים זה לזה. את החבורות K_i אפשר להגדיר בכמה דרכים, המתלכדות למרבה המזל עבור $i \leq 2$.

4.1.1 מודולים פרוייקטיביים ו־K_0

אם F הוא מודול חופשי, אז לכל אפימורפיזם $\phi : N \to M$, אפשר למשוך כל הומומורפיזם $f : F \to M$ להומומורפיזם $f' : F \to N$ כך ש־$f = \phi \circ f'$. כל מודול F המקיים תכונה זו נקרא **מודול פרוייקטיבי**. מתברר שמודול הוא פרוייקטיבי אם ורק אם הוא מחובר ישר במודול חופשי.

תרגיל 4.1.1 תן דוגמא לתת־מודול של מודול חופשי, שאינו פרוייקטיבי. (שים לב שמעל תחום ראשי כל מודול חסר פיתול הוא פרוייקטיבי).

החבורה $\mathrm{K}_0(R)$ מקודדת את תורת המודולים הפרוייקטיביים הנוצרים סופית מעל R, באופן הבא. נסמן ב־$\mathrm{Proj}(R)$ את החבורה למחצה של מודולים פרוייקטיביים נוצרים סופית מעל R, עם פעולת הסכום הישר.

תהי S חבורה למחצה קומוטטיבית. נגדיר יחס על הזוגות $(a, a') \in S \times S$ לפי $(a, a') \sim (b, b')$ אם יש $s \in S$ כך ש־$a + b' + s = a' + b + s$. **חבורת גרותנדיק** (Grothendieck) של S היא, לפי ההגדרה, חבורת המחלקות, עם הפעולה $[(a, a')] + [(b, b')] = [(a + b, a' + b')]$. האסוציאטיביות טריוויאלית, וזו אכן חבורה מכיוון ש־$[(a, a')] + [(a', a)] = [(a + a', a + a')] = [(0, 0)]$. אפשר לפרש את המחלקה $[(a, b)]$ כאילו היא ההפרש $a - b$. את הבניה הזו פגשנו קודם לכן: החבורה החיבורית של חוג ויט אינה אלא חבורת גרותנדיק של התבניות הריבועיות, מודולו המרחבים ההיפרבוליים; וחבורת בראוור אינה אלא חבורת גרותנדיק של האלגברות הפשוטות המרכזיות, מודולו המטריצות.

כעת יהי R חוג כלשהו. החבורה $\mathrm{K}_0(R)$ מוגדרת כחבורת גרותנדיק של החבורה למחצה $\mathrm{Proj}(R)$. את $\mathrm{K}_0(R)$ אפשר לפרש גם במונחי מטריצות אידמפוטנטיות מעל R.

דוגמא 4.1.2 מהו $\mathrm{K}_0(F)$ כאשר F שדה? המודולים הפרוייקטיביים הנוצרים סופית הם כמובן המרחבים הוקטוריים הסופיים F^n, ופעולת הסכום הישר מתאימה לחיבור ממדים. לכן $\mathrm{K}_0(F) \cong \mathbb{Z}$.

הערה. ההומומורפיזם $\mathbb{Z} \to \mathrm{K}_0(R)$ המוגדר לפי $1 \mapsto [R]$ הוא שיכון אם ורק אם R מקיים את התכונה IBN (Invariant Base Number). זהו איזומורפיזם אם ורק אם כל מודול פרוייקטיבי הוא חופשי מדרגה מוגדרת היטב.

4.1.2 מטריצות לא אלמנטריות ו־K_1

החבורה $\mathrm{K}_1(R)$ היא המנה של חבורת המטריצות ההפיכות $\mathrm{GL}(R)$ (מכל סדר סופי) מודולו תת־החבורה הנוצרת על־ידי המטריצות האלמנטריות.

יהי R חוג כלשהו. אנחנו מסמנים $\mathrm{GL}(R) = \bigcup_{n\geq 1}\mathrm{GL}_n(R)$. המטריצות $e_{ij}(r) = 1 + re_{ij}$ נקראות **מטריצות אלמנטריות**. מסמנים ב־$E_n(R)$ את חבורת המטריצות הנוצרת על־ידי המטריצות האלמנטריות מסדר n; וכן $E(R) = \bigcup E_n(R)$.

תרגיל 4.1.3 הראה שחבורת המטריצות המשולשיות־עליונות, עם 1 באלכסון, מוכלת ב־$E_n(R)$.

למה 4.1.4 (הלמה של ויטהד (Whitehead)) לכל חוג R, $\mathrm{GL}(R)' = E(R)' = E(R)$.

זה מאפשר להגדיר

$$\mathrm{K}_1(R) = \mathrm{GL}(R)/E(R);$$

לפי הלמה, זוהי האבליאניזציה של $\mathrm{GL}(R)$, שהיא בפרט חבורה אבלית. מכיוון ש־$\mathrm{GL}_d(R)$ ו־$\mathcal{E}(R)$ מוגדרים באופן טבעי, K_1 מהווה פונקטור. הוא מכבד את שקילות מוריטה (Morita) (בפרט $\mathrm{K}_1(\mathrm{M}_n(R)) = \mathrm{K}_1(R)$), ויש לו תכונות שימושיות נוספות.

עבור חוג קומוטטיבי, אפשר להתקדם עוד צעד. מוגדרת העתקת הדטרמיננטה $\mathrm{GL}(R) {\to} R^\times$, שאת הגרעין שלה מסמנים ב־$\mathrm{SL}(R)$. ברור ש־$E(R) \subseteq \mathrm{SL}(R)$. לכן אפשר להגדיר את המנה $\mathrm{SK}_1(R) = \mathrm{SL}(R)/E(R)$, ומתקבלת סדרה מדוייקת

$$1 \longrightarrow \mathrm{SK}_1(R) \longrightarrow \mathrm{K}_1(R) \longrightarrow R^\times \longrightarrow 1.$$

אם $R = F$ הוא שדה, תהליך האלמינציה של גאוס אומר ש־$\mathrm{SK}_1(F) = 0$, ולכן $\mathrm{K}_1(F) = F^\times$. תכונה זו נכונה למעשה לכל חוג מקומי (לאו דווקא קומוטטיבי), בזכות **דטרמיננטת דודונה** (Dieudonné) $\mathrm{GL}_d(R) {\to} R^\times/[R^\times, R^\times]$.

הערה 4.1.5 הערה זו מסבירה את הקשר בין K_0 ו־K_1.

יהי R חוג. נסמן ב־$\mathcal{P}(R)$ את הקטגוריה של מודולים פרוייקטיביים נוצרים סופית מעל R. תהי $\mathcal{M}$ תת־קטגוריה אדמיסיבילית של קטגוריה אבלית (איננו מגדירים מושגים אלה כאן, אבל $\mathcal{P}(R)$, כתת־קטגוריה של $\mathbf{Mod}(R)$, היא דוגמא טובה). **חבורת גרותנדיק** של $\mathcal{M}$ היא החבורה האבלית $\mathrm{K}_0(\mathcal{M})$ הנוצרת על־ידי מחלקות האיזומורפיזמים של אובייקטים ב־$\mathcal{M}$, מודולו היחס $[M] = [M'] + [M'']$ לכל סדרה קצרה מדוייקת $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$.

1. הראה ש־$[M] = [N]$ אם ורק אם יש X, Y עם סדרות מדוייקות $0 \longrightarrow A \longrightarrow X \longrightarrow B \longrightarrow 0$ ו־$0 \longrightarrow A \longrightarrow Y \longrightarrow B \longrightarrow 0$ כך ש־$M \oplus X \cong N \oplus Y$.

2. אם $0 \longrightarrow M_t \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0$ היא סדרה ארוכה מדוייקת אז $\sum(-1)^i[M_i] = 0$.

3. $\mathrm{K}_0(\mathcal{P}(R)) = \mathrm{K}_0(R)$.

נסמן ב־$\mathcal{M}^{\mathbb{Z}}$ את הקטגוריה של הזוגות (M, α), כאשר α אוטומורפיזם של M, והמורפיזמים הם מורפיזמים של $\mathcal{M}$ היוצרים דיאגרמות מתחלפות עם האוטומורפיזמים. **חבורת וייטהד** $\mathrm{K}_1(\mathcal{M})$ של $\mathcal{M}$ היא חבורת המנה של $\mathrm{K}_0(\mathcal{M})$ מודולו היחסים $[M, \alpha\alpha'] = [M, \alpha] + [M, \alpha']$.

4. $\mathrm{K}_1(\mathcal{P}(R)) = \mathrm{K}_1(R)$ על־ידי הזיהוי של $[\alpha] \in \mathrm{K}_1(R)$, כלומר הקוסט של $\alpha \in \mathrm{GL}_n(R)$ בחבורת המנה $\mathrm{GL}(R)/E(R)$, עם האיבר $[R^n, \alpha]$.

4.1.3 יחסים אלמנטריים ו־K_2

החבורה $\mathrm{K}_2(R)$ מתארת את היחסים שמקיימות המטריצות האלמנטריות מעל R, מודולו היחסים הטריוויאליים (המתקיימים בכל חוג). ההגדרה נעזרת במושג בעל חשיבות עצמאית בתורת החבורות.

הרחבת חבורות
$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$
נקראת **הרחבה מרכזית** של G ב־A, אם $A \subseteq \mathrm{Z}(E)$.

הערה 4.1.6 נקבע חבורה אבלית A. שתי הרחבות $1\to A\to E_1\to G\to 1$ ו־$1\to A\to E_2\to G\to 1$ של G על־ידי A הן **שקולות** אם יש דיאגרמה מתחלפת

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, equal] & E_1 \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \arrow[r] & E_2 \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

(במקרה כזה $E_1 \cong E_2$).

לכל חבורה אבלית A, אוסף ההרחבות המרכזיות, עד כדי שקילות, מהווה חבורה אבלית שמסמנים $\mathrm{Ext}(G,A)$; היא איזומורפית ל־$\mathrm{H}^2(G,A)$.

הרחבה מרכזית $E \twoheadrightarrow G$ היא **אוניברסלית** אם לכל הרחבה מרכזית $E_1 \twoheadrightarrow G$, יש הומומורפיזם יחיד מ־E אל E_1, המתחלף עם הזהות על G.

תרגיל 4.1.7 הראה שאם E_1, E_2 הן הרחבות מרכזיות אוניברסליות של החבורה G, אז $E_1 \cong E_2$.

הערה 4.1.8 נניח ש־G חבורה מושלמת, המוצגת כמנה $G = F/R$, כאשר F חופשית. ההרחבה המרכזית האוניברסלית טמונה בסדרה

$$1 \longrightarrow (R \cap [F,F])/[F,R] \longrightarrow [F,F]/[F,R] \longrightarrow F/R \longrightarrow 1,$$

שבה ההעתקה $[F,F]/[F,R] \longrightarrow F/R$ מוגדרת לפי השוויון $[F,F]R/R = F/R$. הגרעין הוא **כופל שור** של G, והוא אינו תלוי בהצגה.

הרחבה **טריוויאלית** היא הרחבה מהצורה $1\to A \overset{a\mapsto(1,a)}{\longrightarrow} G\oplus A \overset{(g,a)\mapsto g}{\longrightarrow} G\to 1$, כאשר A אבלית.

משפט 4.1.9 *לחבורה G יש הרחבה מרכזית אוניברסלית אם ורק אם G היא חבורה מושלמת (כלומר $[G,G]=G$). במקרה זה, ההרחבה האוניברסלית E היא בעצמה מושלמת, וכל הרחבה מרכזית של E היא טריוויאלית.*

אחרי שהגדרנו את החבורה $\mathrm{K}_1(R)$, המודדת עד כמה המטריצות האלמנטריות רחוקות מליצור את כל $\mathrm{GL}(R)$, עלינו להבין את החבורה $E(R)$ עצמה.

הערה 4.1.10 המטריצות האלמנטריות מקיימות את היחסים

$$\begin{array}{rcll}
e_{ij}(a)e_{ij}(b) & = & e_{ij}(a+b); & \\
[e_{ij}(a), e_{kl}(b)] & = & 1 & j \neq k,\ i \neq l; \\
[e_{ij}(a), e_{jk}(b)] & = & e_{ik}(ab) & i,j,k \text{ distinct}; \\
[e_{ij}(a), e_{ki}(b)] & = & e_{kj}(-ab) & i,j,k \text{ distinct}.
\end{array}$$

לאור היחסים האלה, נגדיר את החבורה $\mathrm{St}(R)$ לפי היוצרים $x_{ij}(a)$ (לכל $i \neq j$ ולכל $a \in R$), עם היחסים של הערה 4.1.10, כלומר $x_{ij}(a)x_{ij}(b) = x_{ij}(a+b)$ וכו'. זוהי **חבורת סטיינברג** (Steinberg) של R. לפי ההגדרה יש הטלה $\mathrm{St}(R) \to E(R)$, ואנו יכולים להגדיר $\mathrm{K}_2(R) = \mathrm{Ker}(\mathrm{St}(R) \to E(R))$, כך שיש סדרה קצרה מדוייקת

$$1 \longrightarrow \mathrm{K}_2(R) \longrightarrow \mathrm{St}(R) \longrightarrow E(R) \longrightarrow 1.$$

משפט 4.1.11 *לכל חוג R, $\mathrm{K}_2(R)$ הוא המרכז של $\mathrm{St}(R)$. יתרה מזו,*

$$0 \longrightarrow \mathrm{K}_2(R) \longrightarrow \mathrm{St}(R) \longrightarrow E(R) \longrightarrow 0$$

היא הרחבה מרכזית אוניברסלית של $E(R)$.

באופן כללי קשה מאד לחשב את החבורות $\mathrm{K}_2(R)$. במקרה הקומוטטיבי באים לעזרתנו כמה חישובים פלאיים. עבור $u, v \in R^{\times}$, נסמן

$$w_{ij}(u) = x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u),$$

$$h_{ij}(u) = w_{ij}(u)w_{ij}(-1),$$

ו־

$$\{u, v\} = [h_{12}(u), h_{13}(v)].$$

תרגיל 4.1.12 בדוק ש־$\{u, v\} \in \mathrm{K}_2(R)$, על־ידי חישוב התמונה ב־$E(R)$.

4.2 חבורות K של מילנור

כעת נגדיר את החבורות $\mathrm{K}_n(F)$ של מילנור (Milnor), לכל $n \geq 0$. ההגדרה פורמלית ונראית אפילו מלאכותית, אבל היא מזקקת תובנות עמוקות על האריתמטיקה של השדה.

הגדרה 4.2.1 *יהי F שדה. החבורה $\mathrm{K}_n(F)$ (**נקראת חבורת K ה־n־ית של מילנור**) היא החבורה האבלית החופשית הנוצרת על־ידי הסמלים $\{a_1, \ldots, a_n\}$, $a_1, \ldots, a_n \in F^{\times}$, בכפוף ליחסים הבאים:*

1. *הסמל הוא מולטיאדיטיבי בכל רכיב, כלומר*

$$\{a_1, \ldots, a_i a_i', \ldots, a_n\} = \{a_1, \ldots, a_i, \ldots, a_n\} + \{a_1, \ldots, a_i', \ldots, a_n\};$$

2. *אם $a_i + a_j = 1$ אז $\{a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n\} = 0$.*

הכתיב לפעולה בחבורות $\mathrm{K}_n(F)$ הוא חיבורי. אם מגדירים פעולת כפל

$$\{a_1, \ldots, a_i\} \cdot \{b_1, \ldots, b_j\} = \{a_1, \ldots, a_i, b_1, \ldots, b_j\},$$

הסכום הישר $\mathrm{K}_*(F) = \bigoplus_{n \geq 0} \mathrm{K}_n(F)$ הופך לחוג מדורג (מעל $\mathbb{N}$).

לכל שיכון של שדות $\iota : F \hookrightarrow E$ מוגדרת העתקת **הצמצום**, $\mathrm{res}_{E/F} : \mathrm{K}_*(F) \to \mathrm{K}_*(E)$ לפי התאמת הסמל $\{a_1, \dots, a_n\} \in \mathrm{K}_n(F)$ עבור $a_i \in F^\times$ לסמל $\{\iota(a_1), \dots, \iota(a_n)\} \in \mathrm{K}_n(E)$. זהו הומומורפיזם של חוגים, וכך הופכת ההתאמה

$$F \mapsto \mathrm{K}_*(F)$$

לפונקטור מהקטגוריה של שדות לקטגוריה של חוגים קומוטטיביים מדורגים.

נחשב את חבורות־K הראשונות לפי ההגדרה החדשה. פורמלית, $\mathrm{K}_0(F)$ נוצרת על־ידי הסמל הריק $\{\}$, ולכן $\mathrm{K}_0(F) = \mathbb{Z}$. כמו־כן, $\mathrm{K}_1(F)$ נוצר על־ידי הסמלים $\{a\}$, עם היחסים $\{ab\} = \{a\} + \{b\}$. לפיכך, $\mathrm{K}_1(F) = F^{\times 2}$. הגדרות אלו מתלכדות עם ההגדרות הכלליות יותר מהסעיפים הקודמים.

העובדה שחבורת K_2 של שדה כפי שהגדיר אותה מילנור זהה להגדרה של סעיף 4.1.3 היא משפט לא קל של Matsumoto. נתעד כמה זהויות ב־$\mathrm{K}_2(F)$, לשימוש עתידי.

הערה 4.2.2 (איך משחקים ב־$\mathrm{K}_2(F)$) בחבורה $\mathrm{K}_2(F)$ מתקיים לכל $a, b \in F^\times$:

1. $\{a, 1\} = \{1, a\} = 0$.
2. $\{a, -a\} = 0$.
3. $\{a, b\} = -\{b, a\}$.
4. $\{a, b\} = \left\{-\frac{a}{b}, a + b\right\}$.

הוכחה. (1) ברור. עבור (2), חשב את $0 = \left\{a^{-1}, 1 - a^{-1}\right\} = -\left\{a, \frac{1-a}{-a}\right\} = \{a, 1 - a\} - \{a, -a\}$. עבור (3), חשב $\{a, b\} + \{b, a\} = \{a, -a\} + \{a, b\} + \{b, a\} + \{b, -b\} = \{ab, -ab\} = 0$. לבסוף עבור (4), מתקיים $\left\{-\frac{a}{b}, a + b\right\} - \{a, b\} = \left\{\frac{-a}{b}, \frac{a+b}{b}\right\} = \left\{-\frac{a}{b}, 1 + \frac{a}{b}\right\} = 0$. $\square$

(יחסים אלה מראים שהסמלים של $K_2(F)/2K_2(F)$ מתנהגים, במובן מסויים, כמו תבניות ריבועיות: ראו למה 4.4.2.)

4.2.1 העתקת השארית

(תת־סעיף זה אינו נחוץ בהמשך.)

נניח ש־F שדה עם הערכה דיסקרטית $\nu : F \to \mathbb{Z}$. נסמן ב־$\bar{F}$ את שדה השאריות. פונקציית ההערכה מתאימה לכל $\{a\} \in \mathrm{K}_1(F)$ את הערך $\nu(a) \in \mathbb{Z} = \mathrm{K}_0(F)$, ומגדירה הומומורפיזם $\mathrm{K}_1(F) \to \mathrm{K}_0(\bar{F})$. באופן יותר כללי, יש הומומורפיזם יחיד $\partial_\nu : \mathrm{K}_{n+1}(F) \to \mathrm{K}_n(\bar{F})$ המקיים

$$\partial_\nu(\{a_0, a_1, \dots, a_n\}) = \nu(a_0) \cdot \{\bar{a_1}, \dots, \bar{a_n}\}$$

לכל $a_1, \dots, a_n \in F^\times$ עם $\nu(a_1) = \dots = \nu(a_n) = 0$, כאשר $\bar{a} \in \bar{F}$ מציין את השארית של a. ההומומורפיזם הזה נקרא **העתקת השארית**.

העתקת השארית מתחלפת עם העתקת הצמצום, במובן הבא. תהי F'/F הרחבה של שדות, עם הערכות דיסקרטיות $\nu : F \to \mathbb{Z}$ והרחבה $\nu' : F' \to \frac{1}{e}\mathbb{Z}$, ועם שדות שאריות $\bar{F} \subseteq \bar{F}'$. במקרה כזה, הדיאגרמה הבאה מתחלפת:

$$\begin{tikzcd}
\mathrm{K}_{n+1}(F') \arrow[r, "\partial_{\nu'}"'] & \mathrm{K}_n(\bar{F}') \\
\mathrm{K}_{n+1}(F) \arrow[u, "\mathrm{res}_{F'/F}"] \arrow[r, "e \cdot \partial_\nu"'] & \mathrm{K}_n(\bar{F}) \arrow[u, "\mathrm{res}_{\bar{F}'/\bar{F}}"']
\end{tikzcd}$$

הקשר בין חבורות $\mathrm{K}_{*+1}(F)$ לבין $\mathrm{K}_*(\bar{F})$ מתחזק עוד יותר על־ידי המשפט הבא של מילנור. כידוע, ההערכות הדיסקרטיות של $F(t)$ מתאימות לפולינומים האי־פריקים ב־$F[t]$, בתוספת ההערכה $\deg$ – המתאימה לנקודה באינסוף.

משפט 4.2.3 *לכל שדה F, הסדרה*

$$0 \longrightarrow \mathrm{K}_{n+1}(F) \xrightarrow{\mathrm{res}_{F(t)/F}} \mathrm{K}_{n+1}(F(t)) \xrightarrow{(\partial_x)} \bigoplus_{x\in\mathbb{A}^1_{(0)}} \mathrm{K}_n(F(x)) \longrightarrow 0$$

היא סדרה מדוייקת מפוצלת; כאן $F(x)$ הוא שדה השאריות ביחס להערכה x.

4.3 השערת מילנור

בסעיף הזה נסקור את השערת מילנור, המתארת את כל המנות $I^n(F)/I^{n+1}(F)$ על־ידי יוצרים ויחסים. מגדירים $\mathrm{k}_n(F) = \mathrm{K}_n(F)/2\mathrm{K}_n(F)$.

כפי שראינו לעיל, $\mathrm{K}_0(F) = \mathbb{Z}$ ו־$\mathrm{K}_1(F) = F^\times$, ומכאן ש־$\mathrm{k}_0(F) = \mathbb{Z}/2\mathbb{Z}$ ו־$\mathrm{k}_1(F) = F^\times/F^{\times 2}$. את החבורות האלה כבר פגשנו:

$$\mathrm{k}_0(F) \cong W(F)/I(F) \cong \mathbb{Z}/2\mathbb{Z};$$

$$\mathrm{k}_1(F) \cong I(F)/I^2(F) \cong F^\times/F^{\times 2}.$$

אין זה פלא, אם כך, שננסה להגדיר הומומורפיזם

$$f_n : \mathrm{k}_n(F) \longrightarrow I^n/I^{n+1};$$

אכן, נגדיר את ההומומורפיזם לפי הפעולה על היוצרים,

$$f_n : \{a_1,\dots,a_n\} \mapsto \langle\langle a_1,\dots,a_n\rangle\rangle. \tag{4.1}$$

כדי להוכיח ש־f_n מוגדר היטב, נצטרך שני יחסים על תבניות פיסטר מסדר 2:

טענה 4.3.1 1. לכל $a,b\in F^\times$, $\langle\langle a\rangle\rangle \perp \langle\langle b\rangle\rangle \equiv \langle\langle ab\rangle\rangle \pmod{I^2}$.

2. אם $a+b=1$ אז $\langle\langle a,b\rangle\rangle \equiv 0$.

הוכחה. הכמעט־אדיטיביות של תבניות פיסטר (למה 3.3.3) קובעת ש־

$$\langle\langle a\rangle\rangle \perp \langle\langle b\rangle\rangle \sim \langle\langle ab\rangle\rangle \perp \langle\langle a,b\rangle\rangle \sim \langle\langle ab\rangle\rangle \pmod{I^2}.$$

בנוסף לזה אם $a+b=1$ אז

$$\begin{aligned}\langle\langle a,b\rangle\rangle &= \langle 1,ab\rangle + \langle -1\rangle\langle a,b\rangle \\ &\cong \langle 1,ab\rangle + \langle -1\rangle\langle 1,ab\rangle = \langle 1,-1\rangle\langle 1,ab\rangle = \mathbb{H}\otimes\langle 1,ab\rangle \sim 0.\end{aligned}$$

□

טענה 4.3.2 הנוסחה (4.1) מגדירה הומומורפיזם $f_n : \mathrm{k}_n(F) \to I^n/I^{n+1}$.

הוכחה. כדי להראות זאת עלינו להוכיח שההעתקה שומרת על היחסים המגדירים את $\mathrm{k}_n(F)$. ראשית, לכל $q \in I^n$ מתקיים $2q = \langle\langle -1\rangle\rangle q \in I^{n+1}$ ולכן $2q \equiv 0$. לכן נותר לאשר את היחסים המגדירים את $\mathrm{K}_n(F)$. מכיוון שב־$\mathrm{k}_n(F)$ הסמל הוא סימטרי (הערה 4.2.2), אפשר להניח שהיחס חל על הרכיבים הראשונים. כעת,

$$\begin{aligned} f_n(\{a_1,a_2,\dots,a_n\}+\{a'_1,a_2,\dots,a_n\}) &= \langle\langle a_1,a_2,\dots,a_n\rangle\rangle \perp \langle\langle a'_1,a_2,\dots,a_n\rangle\rangle \\ &= (\langle\langle a_1\rangle\rangle \perp \langle\langle a'_1\rangle\rangle)\langle\langle a_2,a_3,\dots,a_n\rangle\rangle \\ &\sim \langle\langle a_1a'_1\rangle\rangle\langle\langle a_2,a_3,\dots,a_n\rangle\rangle \\ &= f(\{a_1a'_1,a_2,\dots,a_n\}) \end{aligned}$$

מודולו $I^{2+(n-1)} = I^{n+1}$; ובדומה לזה אם $a_1+a_2=1$ אז

$$\begin{aligned} f_n(\{a_1,a_2,\dots,a_n\}) &= \langle\langle a_1,a_2,\dots,a_n\rangle\rangle \\ &= \langle\langle a_1,a_2\rangle\rangle\otimes\langle\langle a_3,\dots,a_n\rangle\rangle \\ &\sim \langle\langle 1,1\rangle\rangle\otimes\langle\langle a_3,\dots,a_n\rangle\rangle \sim 0. \end{aligned}$$

□

הערה 4.3.3 0. $f_0\colon \mathrm{k}_0(F)\to W(F)/I(F)$ מוגדר לפי $\{\} \mapsto \langle\langle\rangle\rangle = \langle 1\rangle$, וזה האיזומורפיזם מסעיף 3.1.

1. $f_1\colon \mathrm{k}_1(F)\to I(F)/I^2(F)$ מוגדר לפי $\{a\} \mapsto \langle\langle a\rangle\rangle$, ומתלכד עם האיזומורפיזם באותו שם ממשפט 3.3.4.

הטענה ש־$f_n\colon \mathrm{k}_n(F)\to I^n/I^{n+1}$ הוא איזומורפיזם היא **השערת מילנור**. על מנת להציג אותה בהקשר כללי יותר, נתאר אובייקט חשוב אחר.

הגדרה 4.3.4 *1. תהי G חבורה ויהי M מודול מעל חוג החבורה $\mathbb{Z}[G]$. מסמנים ב־$\mathrm{H}^n(G,M)$ את חבורת הקוהומולוגיה ה־n־ית עם מקדמים ב־M. המכפלה $a\otimes b \mapsto a\cup b$, המוגדרת לפי*

$$(a\cup b)_{g_0,\dots,g_{i-1},g_i,\dots,g_{i+j-1}} = a_{g_0,\dots,g_{i-1}}\otimes b_{g_i,\dots,g_{i+j-1}},$$

*היא הומומורפיזם $\mathrm{H}^i(G,M)\otimes\mathrm{H}^j(G,N)\to\mathrm{H}^{i+j}(G,M\otimes N)$, הנקרא **מכפלת ה־$\cup$** (cup product). זו "פעולה קומוטטיבית" של חוגים מדורגים, כלומר $b\cup a = (-1)^{\deg(a)\deg(b)}a\cup b$.*

*2. יהי F שדה ויהי ℓ מספר טבעי זר למאפיין של F. מסמנים ב־$\mathrm{H}^n(F,M)$ את **קוהומולוגיית גלואה**, שהיא חבורת הקוהומולוגיה של חבורת גלואה האבסולוטית $\Gamma = \mathrm{Gal}(F_\mathrm{s}/F)$ עם מקדמים ב־M. כאשר ℓ זר למאפיין של F, Γ פועלת באופן טבעי על חבורת שורשי היחידה $\mu_\ell \subseteq F_\mathrm{s}$, ו־$\mu_\ell^{\otimes n}$ מציין את החבורה (הציקלית מסדר ℓ) עם הפעולה המעוותת $\sigma(\rho\otimes\cdots\otimes\rho) = \sigma(\rho)\otimes\cdots\otimes\sigma(\rho)$.*

*3. יש הומומורפיזם $F^\times\to\mathrm{H}^1(F,\mu_\ell)$ המוגדר לפי $a\mapsto(a)$, כאשר $(a)\colon\sigma\mapsto\frac{\sigma(a^{1/\ell})}{a^{1/\ell}}$; הגרעין של הוא $F^{\times\ell}$, ולמעשה יש כאן איזומורפיזם $F^\times/F^{\times\ell}\to\mathrm{H}^1(F,\mu_\ell)$. מכפלת ה־$\cup$ ממשיכה את ההומומורפיזם הזה **להעתקת שארית הנורמה** (norm residue map), שגילה John Tate:*

$$\varphi_{n,\ell}\colon \mathrm{K}_n(F)/\ell \longrightarrow \mathrm{H}^n(F,\mu_\ell^{\otimes n}).$$

*4. יש איזומורפיזם קלאסי ${}_\ell\mathrm{Br}(F) \xrightarrow{\cong} \mathrm{H}^2(F,\mu_\ell)$ הקשור בבניה של **מכפלות משולבות** (שימו לב שכאן מדובר בחבורת הקוהומולוגיה השניה). בדרך כלל החבורות $\mathrm{H}^2(F,\mu_\ell)$ ו־$\mathrm{H}^2(F,\mu_\ell^{\otimes 2})$ שונות זו מזו, אבל אם השדה F מכיל את שורשי היחידה מסדר ℓ אז פעולת Γ על μ_ℓ ממילא טריוויאלית, והחבורות מתלכדות. זה קורה, בפרט, כאשר $\ell = 2$.*

הערה 4.3.5 השערת בלוך-קטו (*Bloch-Kato*) קובעת ש־$\varphi_{n,\ell}$ הוא איזומורפיזם. בהערה זו נתאר כמה מקרים פרטיים.

1. $n=\ell=2$: האובייקטים שפגשנו מסודרים בדיאגרמה

$$\begin{tikzcd} \mathrm{K}_2(F)/2 \arrow[r, "\varphi_{2,2}"] \arrow[d, "f_2"'] & \mathrm{H}^2(F,\mathbb{Z}/2) \arrow[d, "\cong"] \\ I^2/I^3 \arrow[r, "\gamma"] & {}_2\mathrm{Br}(F) \end{tikzcd}$$

כאשר γ הוא ההומומורפיזם של תת־סעיף 3.4.5. את השערת בלוך-קטו למקרה הזה (היינו האיזומורפיזם $\mathrm{K}_2(F)/2 \to \mathrm{H}^2(F,\mathbb{Z}/2)$) הוכיח מרקורייב (*Merkurjev*) ב־*1980*.

2. באופן כללי יותר, עדיין עם $n=2$ אבל לכל ℓ, האידיאל היסודי נעשה לא רלוונטי, ומתקבלת הדיאגרמה הבאה, שבה הקו המרוסק נכון רק כאשר $\mu_\ell \subseteq F$:

$$\begin{tikzcd} \mathrm{K}_2(F)/\ell \arrow[r, "\varphi_{2,\ell}"] & \mathrm{H}^2(F,\mu_\ell^{\otimes 2}) \arrow[d, equal, dashed] \\ & \mathrm{H}^2(F,\mu_\ell) \arrow[r, "\cong"] & {}_\ell\mathrm{Br}(F) \end{tikzcd}$$

את העובדה ש־$\varphi_{2,\ell}$ הוא איזומורפיזם הוכיחו מרקורייב-סוסלין (*Suslin*) ב־*1981*.

3. בכיוון אחר, עם $\ell=2$ ולכל n, מתקבלת הדיאגרמה

$$\begin{tikzcd} \mathrm{K}_n(F)/2 \arrow[r, "\varphi_{n,2}"] \arrow[d, "f_n"] & \mathrm{H}^n(F,\mathbb{Z}/2) \\ I^n/I^{n+1} \end{tikzcd}$$

את השערת מילנור (הקובעת כאמור ש־f_n הוא איזומורפיזם) הוכיחו מילנור עבור $n=2$, רוסט (*Rost*) ומרקורייב-סוסלין עבור $n=3$, ורוסט עבור $n=4$. לבסוף הוכיחו את ההשערה *Orlov-Vishik-Voevodsky* בכל דרגה (מאפיין אפס) *[17, Sec. 4.1]*.

4. את השערת בלוך-קטו במקרה הכללי (לכל n ולכל ℓ) הוכיחו *Voevodsky* ו־*Rost* בתחילת שנות ה־*2000* (המאמר המסכם הופיע ב־*2009*). על עבודתו בנושא זה זכה *Voevodsky* במדליית פילדס לשנת *2002*. מן המשפט הזה נובע שחוג הקוהומולוגיה $\mathrm{H}^*(F,\mu_\ell)$ נוצר על־ידי אברים מדרגה 1, ומוגדר על־ידי יחסים מדרגה 2.

תרגיל 4.3.6 נגדיר $\mathrm{k}_*(F) = \bigoplus \mathrm{k}_n(F)$ עם פעולת הכפל המושרית מ־$\mathrm{K}_*(F)$. מצא הצגה של החוג באמצעות יוצרים ויחסים.

נסמן ב־$GW_*(F) = \bigoplus_n I^n(F)/I^{n+1}(F)$ את **חוג ויט המדורג**. הראה שזה חוג ממאפיין 2 (**הדרכה**. $2I^n = \langle 1,1\rangle I^n \subseteq I^{n+1}$). הראה שההומומורפיזמים $f_n\colon \mathrm{k}_n(F) \to I^n/I^{n+1}$ שהוגדרו לעיל משתלבים להומומורפיזם של חוגים $\mathrm{k}_*(F) \to GW_*(F)$.

המשפט הבא, שההוכחה שלו משתמשת בהשערת מילנור, מספק הצגה של I^n (זוהי כמובן הכללה של משפט 3.3.21). לפני כן נזדקק לחישוב קל:

למה 4.3.7 לכל a,b,c מתקיים

$$\langle\langle a,b\rangle\rangle \perp \langle\langle ab,c\rangle\rangle \cong \langle\langle b,c\rangle\rangle \perp \langle\langle a,bc\rangle\rangle.$$

הוכחה. שני האגפים דומים ל־$\langle 1,1,-a,-b,-c,abc\rangle \sim \langle\langle a,b\rangle\rangle + \langle\langle b,c\rangle\rangle + \langle b\rangle\langle\langle a,c\rangle\rangle$. □

משפט 4.3.8 **([7, משפט 42.4])** *כחבורה אבלית, I^n נוצרת על־ידי תבניות פיסטר מסדר n, עם היחסים הבאים:*

$$\langle\langle 1,1,\dots,1\rangle\rangle = 0;$$

לכל תבנית פיסטר ϕ מסדר $n-2$ ולכל $a,b,c\in F^\times$,

$$\langle\langle a,b\rangle\rangle\otimes\phi + \langle\langle ab,c\rangle\rangle\otimes\phi = \langle\langle b,c\rangle\rangle\otimes\phi + \langle\langle a,bc\rangle\rangle\otimes\phi.$$

המשפט מעלה את השאלה איך אפשר לזהות שוויון בין תבניות פיסטר. לפי מסקנה 7.4.5, תבניות פיסטר מסדר n הן איזומטריות אם ורק אם הן שוות בחבורות המנה I^n/I^{n+1}.

4.4 השערת מילנור ל־$n=2$

בסעיף הקודם בנינו הומומורפיזם $f_n\colon \mathrm{k}_n(F)\to I^n(F)/I^{n+1}(F)$, והבחנו שעבור $n=0$ ו־$n=1$ הוא משחזר את זוגיות הממד ואת הדיסקרימיננטה. כעת נוכיח ש־f_n הוא איזומורפיזם עבור $n=2$. לשם כך נגדיר העתקה הפוכה, $I^2(F)/I^3(F)\to \mathrm{k}_2(F)$.

למעשה נעשה מעט יותר מזה. כשהגדרנו את $\gamma\colon I^2/I^3\to {}_2\mathrm{Br}(F)$ בתת־סעיף 3.4.5, התאמנו ערך (אלגברת קליפורד) לכל תבנית (אפילו מממד אי־זוגי); עבור תבניות מממד זוגי עברנו למחלקות בחבורת בראואר, כך שהפונקציה מוגדרת על מחלקות ויט; ואז ראינו כאשר שמצמצמים אותו ל־I^2, זהו הומומורפיזם. נחזור כאן על אותם שלבים, ונגדיר שמורה לכל תבנית.

הגדרה 4.4.1 *תהי q תבנית ריבועית מעל F. נכתוב $q\cong\langle a_1,\dots,a_n\rangle$, ונגדיר $w(q)\in \mathrm{k}_2(F)$ לפי*

$$w(q) = \sum_{i<j}\{a_i,a_j\}.$$

למה 4.4.2 אם $\langle a,b\rangle\cong\langle c,d\rangle$ אז $\{a,b\}\equiv\{c,d\}$ מודולו $2\mathrm{K}_2(F)$.

הוכחה. הדרך הכללית ביותר להציג את $\langle a,b\rangle$ היא בצורה $\langle c,d\rangle$ כאשר $c=ax^2+by^2$ ו־$d=abcz^2$ עבור $x,y,z\in F$, $z\neq 0$ (מסקנה 3.3.11). אם $x=0$ אז $\{c,d\}=\{by^2,a(byz)^2\}\equiv\{a,b\}$; כך גם אם $y=0$. ואם $x,y\neq 0$ אז $\{c,d\}=\{c,-cd\}=\{c,-ab\}\equiv\{c,-by^2/ax^2\}=\{ax^2,by^2\}=\{a,b\}$ לפי הערה 4.2.2. □

טענה 4.4.3 הערך $w(q)$ מוגדר היטב.

הוכחה. ראשית, החלפה של רכיבים סמוכים בהצגה האלכסונית של q משנה בתמונה רק מחובר אחד, מ־$\{a_i,a_{i+1}\}$ ל־$\{a_{i+1},a_i\}$, אבל שני אלו שווים ב־$\mathrm{k}_2(F)$. נניח שנתונות שתי הצגות אלכסוניות של q. לפי משפט השרשרת 3.3.15, אפשר להניח ששתי ההצגות שונות רק בשני רכיבים, ובעזרת החלפה אפשר להניח שמדובר ברכיבים שבמקומות הראשונים. כלומר, ההצגות הן

$$\langle a_1,a_2,a_3,\dots,a_n\rangle,\qquad \langle b_1,b_2,a_3,\dots,a_n\rangle,$$

כאשר $\langle a_1,a_2\rangle\cong\langle b_1,b_2\rangle$. עלינו להראות ש־

$$\{a_1,a_2\}+\sum_{i=3}^n\{a_1,a_i\}+\sum_{i=3}^n\{a_2,a_i\}+\sum_{3\le i<j\le n}\{a_i,a_j\}$$

שווה ל־

$$\{b_1,b_2\}+\sum_{i=3}^{n}\{b_1,a_i\}+\sum_{i=3}^{n}\{b_2,a_i\}+\sum_{3\leq i<j\leq n}\{a_i,a_j\}.$$

מכיוון ש־$\{a_1,a_2\}=\{b_1,b_2\}$ לפי למה 4.4.2, ההפרש בין שני הסכומים הוא

$$\left\{\frac{a_1a_2}{b_1b_2},a_3\cdots a_n\right\}=\{1,a_3\cdots a_n\}=0$$

כי הרי $a_1a_2=\operatorname{disc}(\langle a_1,a_2\rangle)=\operatorname{disc}(\langle b_1,b_2\rangle)=b_1b_2$ ב־${F^\times/F^\times}^2$. □

מן ההגדרה (והאדיטיביות של הסמל) קל לחשב ש־

$$w(q_1\perp q_2)=w(q_1)+w(q_2)+\{\det(q_1),\det(q_2)\}. \tag{4.2}$$

מכיוון ש־

$$w(\mathbb{H})=w(\langle 1,-1\rangle)=\{1,-1\}=0,$$

הערך של w אינו מוגדר היטב על מחלקות ויט באופן כללי:

$$w(q\perp\mathbb{H})=w(q)+\{\det(q),-1\}. \tag{4.3}$$

יש, אם כך, שתי בעיות: w אינו אדיטיבי על תבניות, וגם אינו מוגדר היטב על מחלקות ויט. הדיסקרימיננטה של כל תבנית ב־$I^2(F)$ היא 1, וזה מאפשר לשלוט בדטרמיננטה ולפתור את שתי הבעיות יחד. נעזר בכך שאם $q\in I^2(F)$ תבנית ממימד (זוגי בהכרח) $n=\dim(q)$, אז

$$\det(q)=(-1)^{n/2}\operatorname{disc}(q)=(-1)^{n/2}$$

כי $\binom{n}{2}\equiv\frac{n}{2}\pmod 2$ לכל n זוגי. כלומר, אם $q,q'\in I^2(F)$, אז

$$w(q\perp q')=w(q)+w(q')+\frac{\dim(q)\dim(q')}{4}\{-1,-1\}, \tag{4.4}$$

התיקון נעשה באופן הבא. נגדיר $\hat{w}:I^2\to\mathrm{K}_2(F)/2\mathrm{K}_2(F)$ לפי

$$\hat{w}(q)=w(q)+\left[\frac{\dim(q)}{4}\right]\{-1,-1\}. \tag{4.5}$$

תרגיל 4.4.4 1. לכל n זוגי, $\left[\frac{n+2}{4}\right]-\left[\frac{n}{4}\right]\equiv\frac{n}{2}$.

2. לכל n,n' זוגיים, $\left[\frac{n+n'}{4}\right]-\left[\frac{n}{4}\right]-\left[\frac{n'}{4}\right]\equiv\frac{nn'}{4}\pmod 2$.

(בפרט, הפונקציה $\frac{nn'}{4}\mapsto(n,n')$ שייכת לתמונה של $\delta^1:C^1(2\mathbb{Z},\mathbb{Z}/2\mathbb{Z})\to C^2(2\mathbb{Z},\mathbb{Z}/2\mathbb{Z})$.)

טענה 4.4.5 $\hat{w}$ מוגדר היטב על I^2, והוא הומומורפיזם $\hat{w}:I^2\to\mathrm{K}_2(F)/2\mathrm{K}_2(F)$.

הוכחה. עבור $q \in I^2$ נסמן $n = \dim(q)$, אז

$$\begin{aligned}
\hat{w}(q \perp \mathbb{H}) &= w(q \perp \mathbb{H}) + \left[\frac{n+2}{4}\right]\{-1,-1\} \\
&= w(q) + \left\{(-1)^{n/2}, -1\right\} + \left[\frac{n+2}{4}\right]\{-1,-1\} \\
&= w(q) + \left(\left[\frac{n+2}{4}\right] - \frac{n}{2}\right)\{-1,-1\} \\
&= w(q) + \left[\frac{n}{4}\right]\{-1,-1\} \\
&= \hat{w}(q)
\end{aligned}$$

לפי (4.5) ותרגיל 4.4.4.(1). האדיטיביות של $\hat{w}$ נובעת כעת מ־(4.4) בעזרת תרגיל 4.4.4.(2). □

תרגיל 4.4.6 תהי q תבנית ממימד n. לכל $c \in F^\times$,

$$w(\langle c\rangle \cdot q) = w(q) + \left\{c,\, (-1)^{\binom{n}{2}}\det(q)^{n-1}\right\}.$$

בפרט אם n זוגי אז

$$w(\langle c\rangle \cdot q) = w(q) + \{c, \mathrm{disc}(q)\}.$$

בפרט אם $q \in I^2(F)$, אז

$$w(\langle c\rangle \cdot q) = w(q).$$

למה 4.4.7 1. לכל $a,b \in F^\times$, $\hat{w}(\langle\langle a,b\rangle\rangle) = \{a,b\}$.

2. לכל $a,b \in F^\times$, $\hat{w}(\langle\langle a,b,c\rangle\rangle) = 0$.

הוכחה. לפי ההגדרה,

$$\begin{aligned}
\hat{w}(\langle\langle a,b\rangle\rangle) &= \hat{w}(\langle 1,-a,-b,ab\rangle) \\
&= \{-a,-b\} + \{-a,ab\} + \{-b,ab\} + \{-1,-1\} \\
&= \{a,-1\} + \{a,-b\} = \{a,b\}.
\end{aligned}$$

לפי תרגיל 4.4.6, $\hat{w}(\langle c\rangle q) = \hat{w}(q)$ עבור $q = \langle\langle a,b\rangle\rangle$, ולכן

$$\hat{w}(\langle\langle a,b,c\rangle\rangle) = \hat{w}(\langle\langle a,b\rangle\rangle) + \hat{w}(\langle c\rangle\langle\langle a,b\rangle\rangle) = 2\{a,b\} = 0.$$

□

משפט 4.4.8 *$\hat{w} : I^2/I^3 \to \mathrm{K}_2(F)/2\mathrm{K}_2(F)$ הוא איזומורפיזם.*

הוכחה. ראינו שזה הומומורפיזם מוגדר היטב, והוא הפכי ל־f_2. □

בעיה 4.4.9 כהכללה ל־$s_2 = w$ מהגדרה 4.4.1, נגדיר את **סמל שטיפל־ויטני** (Stiefel-Whitney) **מסדר** d,

$$s_d : W(F) \to \mathrm{k}_d(F),$$

לפי הנוסחה

$$s_d(\langle a_1,\ldots,a_n\rangle) = \sum_{i_1<\cdots<i_d} \{a_{i_1},\ldots,a_{i_d}\}.$$

הראה ש־s_d מוגדר היטב על תבניות ריבועיות. מצא תיקון של s_d (בדומה לתיקון $\hat{w}$ של w) שיהיה מוגדר היטב על מחלקות בחוג ויט. בנה בעזרת זה הומומורפיזם $I^d(F)/I^{d+1}(F) \to \mathrm{k}_d(F)$. (ראה [7].)

פרק 5

סדר ותבניות

5.1 שדות סדורים

שדה סדור הוא שדה שעליו מוגדר יחס סדר לינארי, כך שאם $a < b$ אז $a + c < b + c$ לכל c, ו־$ac < bc$ לכל $c > 0$.

גישה אחרת לשדות סדורים מתבוננת באוסף האברים החיוביים: קבוצה $P \subseteq F$ נקראת **קבוצת חיוביים** אם P סגור לחיבור ולכפל, ו־$F^{\times} = P \cup -P$. שדה סדור הוא שדה שנתונה בו קבוצת חיוביים.

תרגיל 5.1.1 שני התאורים לעיל של שדה סדור הם שקולים: בהנתן סדר $<$, $P = \{x\colon\ x > 0\}$ היא קבוצת חיוביים; ובהנתן קבוצת חיוביים P, הקביעה ש־$a < b$ אם ורק אם $b - a \in P$ מגדירה את $<$ כסדר על השדה.

הערה 5.1.2 בשדה סדור כל סכום של ריבועים הוא חיובי. בפרט, המאפיין של שדה סדור הוא אפס.

הגדרה 5.1.3 *שדה סדור הוא* ***אוקלידי*** *אם כל איבר חיובי הוא ריבוע.*

הגדרה 5.1.4 *שדה E הוא* ***סגור ממשית*** *אם הוא מקיים את אחת התכונות השקולות הבאות:*

1. *E סדור, ואין לו הרחבות אלגבריות אמיתיות שהן סדורות;*
2. *-1 אינו ריבוע ב־E ו־$E[\sqrt{-1}]$ סגור אלגברית;*
3. *E אוקלידי ולכל פולינום ממעלה אי־זוגית יש בו שורש.*

הדוגמא הקלאסית לשדה סגור ממשית היא כמובן שדה הממשיים, $\mathbb{R}$. לכל שדה סדור F יש **סָגוֹר ממשי** יחיד (עד כדי איזומורפיזם של שדות סדורים), שהוא, בהגדרה, הרחבה אלגברית סגורה ממשית של F. לכל שדה סדור יש גם **סגור אוקלידי**, שהוא השדה האוקלידי הקטן ביותר המכיל את השדה הנתון.

5.1.1 שדות ניתנים לסידור

שדה נקרא **ממשי** (**פורמלית**) אם -1 אינו סכום של ריבועים, **ולא ממשי** אחרת. מתברר ששדה הוא ממשי פורמלית אם ורק אם אפשר להגדיר עליו סדר. בנוסף לזה, לכל $a \in F$ שאינו סכום של ריבועים, קיים סידור של השדה שבו a שלילי (ארטין־שרייר (Artin-Schreier)).

הערה 5.1.5 התכונות הבאות שקולות עבור שדה F:

א. $F^{\times}$ הוא איחוד זר של ${F^{\times}}^2$ ו־$-{F^{\times}}^2$.

2. $F^\times/F^{\times 2} = \left\{F^{\times 2}, -F^{\times 2}\right\}$, חבורה מסדר 2.

3. -1 אינו ריבוע, ו־$F[\sqrt{-1}]$ היא ההרחבה הריבועית היחידה של F.

נקרא לסידור α של שדה **סידור אוקלידי** אם ביחס ל־α, השדה אוקלידי; כלומר, כל איבר חיובי ביחס ל־α הוא ריבוע. לשדה יש לכל היותר סידור אוקלידי אחד, משום שבסידור אוקלידי קבוצת החיוביים שווה לקבוצת הריבועים.

טענה 5.1.6 עבור שדה ניתן לסידור, התכונות הבאות שקולות:

1. $F^\times = F^{\times 2} \cup -F^{\times 2}$.
2. $F[\sqrt{-1}]$ היא ההרחבה הריבועית היחידה של F (-1 אינו ריבוע ולכן אלו התכונות של הערה 5.1.5).
3. כל סידור של השדה הוא אוקלידי.
4. לשדה יש סידור אוקלידי.

הוכחה. $(1) \Leftarrow (2)$: **-1 אינו ריבוע כי השדה ניתן לסידור, וההנחה מראה שיש לכל היותר הרחבה ריבועית אחת.**
$(2) \Leftarrow (3)$: **נקבע סידור של השדה, ויהי a איבר חיובי ביחס אליו. אם a אינו ריבוע הרי ש־$-a$ ריבוע, ואז a שלילי, בסתירה להנחה.**
$(3) \Leftarrow (4)$: **ההנחה הראשית היא ש־F ניתן לסידור, ובסידור זה כל איבר חיובי הוא ריבוע לפי (3).**
$(4) \Leftarrow (1)$: **בסידור אוקלידי, לכל $a \neq 0$, $a > 0$ או $-a > 0$, ו־a הוא ריבוע או מינוס ריבוע בהתאמה.** $\square$

הערה 5.1.7 טענה 5.1.6 מראה ששדה ניתן לסידור המקיים $F^\times = F^{\times 2} \cup -F^{\times 2}$, ניתן לסידור אוקלידי. התכונה $F^\times = F^{\times 2} \dot\cup - F^{\times 2}$ (עם חלקים לא ריקים) אינה מספיקה בפני עצמה, כפי שמראה כל שדה סופי מסדר $\equiv -1 \pmod 4$.

בעיה 5.1.8 יהי K **שדה מספרים** (כלומר הרחבה ממימד סופי של $\mathbb{Q}$). הראה ש־$\mathbb{R}\otimes_{\mathbb{Q}}K \cong \mathbb{R}^r \times \mathbb{C}^s$ כאשר $r + 2s = [K:F]$. הוכח שיש בדיוק r דרכים לשכן $K \to \mathbb{R}$, ושיש r דרכים לסדר את K.

תרגיל 5.1.9 יהי E שדה סדור המכיל את $\mathbb{R}$. נאמר ש־$\epsilon \in E$ הוא **אינפיניטיסימל** אם $0 < \epsilon < a$ לכל $a \in \mathbb{R}$ חיובי. הראה שבכל סידור אפשרי של $\mathbb{R}(x)$ מעל $\mathbb{R}$, יש יוצר של ההרחבה שהוא אינפיניטיסימל; לכן, כשדה סדור, $\mathbb{R}(x) \cong \mathbb{R}(\epsilon)$.

בעיה 5.1.10 נסמן ב־$A(\mathbb{R})$ את תת־השדה של $\mathbb{R}((x))$ הכולל את הטורים $\sum a_i x^i$ שעבורם $\limsup \sqrt[n]{|a_n|} < \infty$ ("טורים אנליטיים בסביבה של אפס"). מהו חוג ויט של $A(\mathbb{R})$?

5.2 סימן סילבסטר

תהי $q = \langle a_1, \dots, a_n\rangle$ תבנית ריבועית מעל שדה סדור F. **סימן סילבסטר** של q, $\operatorname{sign}(q)$, הוא מספר המקדמים החיוביים פחות מספר המקדמים השליליים בהצגה. אם יש צורך לציין זאת, נכתוב $\operatorname{sign}_\alpha(q)$ כאשר α הוא הסידור שביחס אליו מחושבים הסימנים.

תרגיל 5.2.1 $\operatorname{sign}(q)$ מוגדר היטב, כלומר אינו תלוי בהצגה של q. **הדרכה.** מעל $\mathbb{R}$ זהו משפט הסימנים של סילבסטר (ראה גם תרגיל 2.3.13), שההוכחה שלו תקפה לכל שדה סדור; אפשר להוכיח את הטענה גם ישירות ממשפט השרשרת של ויט עם מסקנה 3.3.11 על הצגת תבניות ממימד 2.

טענה 5.2.2 סימן סילבסטר הוא אפימורפיזם של חוגים, $\operatorname{sign}_\alpha(\cdot) : W(F) \to \mathbb{Z}$.

הוכחה. הסימן מוגדר היטב על אברי $W(F)$ מכיוון שהסימן של $\langle 1,-1\rangle$ הוא אפס. קל לראות שהסימן שומר על חיבור וכפל. הפונקציה על משום שהסימן של $\langle 1\rangle$ הוא 1. $\square$

הערה 5.2.3 הסימן של q הוא אפס אם ורק אם q היפרבולית מעל הסגור הממשי של F.

תרגיל 5.2.4 אם E שדה אוקלידי (ובפרט: שדה סגור ממשית), אז $W(E)\cong\mathbb{Z}$.

תרגיל 5.2.5 נסמן ב־$\widehat{F}$ את הסגור הממשי של F. אז האפימורפיזם של טענה 5.2.2 הוא העתקת הצמצום $W(F)\to W(\widehat{F})=\mathbb{Z}$.

הערה 5.2.6 כל מנה ראשונית של $W(F)$ היא גם מנה של החוג $\mathbb{Z}$. אכן, יהי $P\lhd W(F)$ אידיאל ראשוני. לכל $a\in F^\times$ מתקיים $\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle=\langle\langle a,-a\rangle\rangle=0$, ולכן $\langle\langle a\rangle\rangle\in P$ או $\langle\langle -a\rangle\rangle\in P$; כלומר, $\langle a\rangle\equiv\pm\langle 1\rangle \pmod P$. לכן חוג המנה נוצר על־ידי התבנית $\langle 1\rangle$.

למה 5.2.7 (Harrison ו־Lorenz-Leicht, 1970) יש התאמה חד־חד־ערכית ועל בין הסידורים של F לבין אידיאלים ראשוניים $P\lhd W(F)$ כך ש־$2\notin P$.

הוכחה. יהי P אידיאל ראשוני כך ש־$2\notin P$. לפי ההוכחה של הערה 5.2.6, $\langle\langle a\rangle\rangle\in P$ או $\langle\langle -a\rangle\rangle\in P$ לכל $a\in F^\times$. נגדיר קבוצת חיוביים $Q\subseteq F$, לפי $Q=\{a\colon \langle\langle a\rangle\rangle\in P\}$, אז $Q\cup -Q=F^\times$. עלינו להוכיח שהקבוצה סגורה לכפל ולחיבור. נניח ש־$a,b\in Q$.

1. $\langle\langle ab\rangle\rangle=\langle\langle a\rangle\rangle+\langle a\rangle\langle\langle b\rangle\rangle\in P$ ולכן $ab\in Q$.

2. נסמן $c=a+b$. $\langle\langle a+b\rangle\rangle=\langle\langle abc\rangle\rangle+\langle -c\rangle\langle\langle ab\rangle\rangle$ ולכן

$$2\langle\langle c\rangle\rangle=\langle\langle c\rangle\rangle+\langle\langle abc\rangle\rangle+\langle -c\rangle\langle\langle ab\rangle\rangle=\langle\langle a,b\rangle\rangle+\langle -c\rangle\langle\langle ab\rangle\rangle\in P;$$

אבל $2\notin P$, ומכאן ש־$\langle\langle c\rangle\rangle\in P$ ולכן $a+b=c\in Q$, כפי שרצינו.

בכיוון ההפוך, תהי Q קבוצת חיוביים ב־F. יהי P האידיאל הנוצר על־ידי כל התבניות $\langle\langle a\rangle\rangle$ עבור $a\in Q$. לפי ההגדרה P מוכל בגרעין של סימן סילבסטר $\mathrm{sign}_Q(\cdot)\colon W(F)\to\mathbb{Z}$ ומצד שני אם $\langle a_1,\dots,a_n\rangle$ בעלת סימן אפס, אפשר להציג אותה כסכום של תבניות מהצורה $\langle a,b\rangle=\langle a\rangle\langle\langle -ab\rangle\rangle$ עם $a\in Q$ ו־$-b\in Q$, השייכות ל־P, ולכן P שווה לגרעין. מכיוון שחוג המנה $\mathbb{Z}$ הוא תחום שלמות, P ראשוני. בנוסף $2=\langle 1,1\rangle\notin P$ כי $\mathrm{sign}(\langle 1,1\rangle)=2$.

$\square$

בעיה 5.2.8 השלם את הוכחת למה 5.2.7: הראה שההתאמות בין אידיאלים ראשוניים וסידורים של השדה הופכות זו את זו.

5.3 שדות פיתגוריים

שדה (ממאפיין שונה מ־2) F הוא **פיתגורי** אם כל סכום של ריבועים הוא ריבוע, כלומר $F^2+F^2\subseteq F^2$. מיד נובע ששדה פיתגורי F הוא ממשי פורמלית (כלומר ניתן לסידור) אם ורק אם $\sqrt{-1}\notin F$. אומרים ששדה **סגור לריבועים** אם ורק אם כל איבר בו הוא ריבוע (במאפיין שונה מ־2 פירושו של דבר שאין לו הרחבות ריבועיות).

יש שני סוגים של שדות פיתגוריים: כאלו הניתנים לסידור, וכאלו שאינם ניתנים לסידור.

הערה 5.3.1 שדה פיתגורי שאינו ניתן לסידור הוא סגור ריבועית. שכן אם השדה אינו ניתן לסידור, -1 הוא סכום של ריבועים, ולכן ריבוע, ואז כל איבר הוא סכום של ריבועים (משום שהוא הפרש של ריבועים).

אפשר לסכם זאת בשתי היררכיות של שדות, סדורים ולא ניתנים לסידור:

פיתגורי ממשי פורמלית $\Longleftarrow$ אוקלידי $\Longleftarrow$ סגור ממשית

פיתגורי לא ממשי $\Longleftarrow$ סגור ריבועית $\Longleftarrow$ סגור אלגברית

משפט 5.3.2 (משפט Diller-Dress, [13, Thm. 5.14]) אם F אינו פיתגורי אז שום הרחבה סופית של F אינה פיתגורית.

הוכחה. השדה K פיתגורי. נניח ש־$F \subseteq K$ אינו פיתגורי. לכן יש $a \in F$ כך ש־$t = 1 + a^2$ אינו ריבוע ב־F, אבל זהו כן ריבוע ב־K, ולכן $F \subset E = F[\sqrt{t}] \subseteq K$. באינדוקציה אפשר להניח ש־E כן פיתגורי. נתבונן ב־$u = 1 + (a + \sqrt{t})^2 = 2(t + a\sqrt{t})$, שהוא ריבוע ב־$E$ לפי ההנחה, ולכן הנורמה שלו $\mathrm{N}_{E/F}(u) = 4(t^2 - ta^2) = 4t$ היא ריבוע ב־F, בסתירה להנחה. $\square$

קל לראות שחיתוך של משפחת תת־שדות פיתגוריים הוא תת־שדה פיתגורי. לכל שדה יש הרחבה אלגברית פיתגורית, ולכן החיתוך של כל השדות הפיתגוריים המכילים את F מהווה **סגור פיתגורי**, $F \subseteq F_{\mathrm{pyth}}$. אם F סדור, גם הסגור הפיתגורי סדור.
מתברר שפיתגוריות אפשר לאבחן באופן מלא בעזרת חוג ויט.

טענה 5.3.3 התכונות הבאות שקולות עבור שדה F ממאפיין שונה מ־2:

1. F הוא פיתגורי לא ממשי;
2. F סגור לריבועים;
3. $W(F) \cong \mathbb{Z}/2\mathbb{Z}$.

הוכחה. $(1)\Leftarrow(2)$: **לפי ההנחה כל איבר, לרבות -1, הוא ריבוע.**
$(2)\Leftarrow(1)$: **יהי $a \in F$, אז $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$ הוא סכום של ריבועים כי $\sqrt{-1} \in F$, ולכן ריבוע.**
$(3)\Leftarrow(2)$: **מכיוון שכל איבר הוא ריבוע יש רק תבנית חד־ממדית אחת, הלוא היא $\langle 1 \rangle$. בנוסף, מכיוון ש־-1 ריבוע, $0 = \langle 1, -1 \rangle = \langle 1, 1 \rangle = 2$ בחוג ויט.**
$(2)\Leftarrow(3)$: **לפי ההנחה $[\langle 1 \rangle] = [\langle a \rangle]$ לכל $a \in F^{\times}$, ולכן $\langle 1 \rangle \cong \langle a \rangle$ ו־a הוא ריבוע.** $\square$

טענה 5.3.4 התכונות הבאות שקולות עבור שדה F ממאפיין שונה מ־2:

1. F הוא פיתגורי ממשי;
2. $W(F)$ חסר פיתול.
3. אם $2[q] = 0$ ב־$W(F)$ אז $[q] = 0$.

הוכחה. $(2)\Leftarrow(1)$: **נראה שבשדה פיתגורי ממשי, אם q תבנית איזוטרופית אז גם $k \cdot q$ איזוטרופית לכל $k \geq 1$. בפרט נובע ש־$k \cdot [q] \neq 0$. נכתוב $q = \langle a_1, \dots, a_n \rangle$. נניח ש־$k \cdot q$ איזוטרופית, אז יש ערכים $x_{ij} \in F$ כך ש־$0 = \sum_j (\sum_i a_i x_{ij}^2) = \sum_i a_i (\sum_j x_{ij}^2)$. לפי ההנחה אפשר לכתוב $y_i^2 = \sum_j x_{ij}^2$, וקיבלנו $\sum_i a_i y_i^2 = 0$, אלא שהאיזוטרופיות של q גוררת ש־$y_i = 0$ לכל i. אבל אם $\sum_i x_{ij}^2 = 0$, בהכרח $x_{ij} = 0$ לכל i, j.**
$(3)\Leftarrow(2)$: **טריוויאלי.**
$(1)\Leftarrow(3)$: **כעת נניח ש־$W(F)$ חסר פיתול. יהיו $a, b \in F$, ונסמן $c = a^2 + b^2$. אז $\langle c, c \rangle \cong \langle 1, 1 \rangle$ לפי מסקנה 3.3.11, ומכאן ש־$2(\langle c \rangle - \langle 1 \rangle) = 0$. מכיוון שאין 2־פיתול, $\langle c \rangle = \langle 1 \rangle$ ו־$c \in F^{\times 2}$. לכן F פיתגורי. אם F לא היה ממשי, אז $W(F)$ היה 2־מפותל לפי טענה 5.3.3, לכן F לא ממשי.** $\square$

5.4 מרחב הסידורים של שדה

בסעיף הקודם טיפלנו בסימן מעל לשדה סדור. כעת נניח ש־F סגור ממשית, כלומר ניתן לסידור, מן הסתם בדרכים שונות. נסמן ב־O_F את אוסף הדרכים לסדר את השדה F.

תרגיל 5.4.1 יש התאמה בין סידורים של השדה F לבין שיכונים של F בשדה סגור ממשית.

דוגמא 5.4.2 מרחב הסידורים של שדה מספרים הוא סופי. ביתר פירוט, יהי K שדה מספרים, כלומר הרחבה סופית של $\mathbb{Q}$. אז $\mathbb{R}\otimes_{\mathbb{Q}}K$ הוא חוג (קומוטטיבי) ראשוני למחצה, ולכן מכפלה סופית של תחומי שלמות. מכיוון שזו גם אלגברה ממימד סופי מעל $\mathbb{R}$, יש שלמים r,s כך ש־$r+2s=[K\!:\!\mathbb{Q}]$, ו־$\mathbb{R}\otimes_{\mathbb{Q}}K\cong\mathbb{R}^r\times\mathbb{C}^s$. יש r דרכים לסדר את K, בהתאמה לשיכונים של K ב־$\mathbb{R}$.

נגדיר על O_F טופולוגיה. כל סדר $\alpha\in O_F$ משרה פונקציית סימן טבעית $F^\times\to\{\pm1\}$, המגדירה את הסדר. זה נותן שיכון $O_F\hookrightarrow \mathrm{Maps}(F^\times\to\{\pm1\})$. על המרחב

$$\mathrm{Maps}(F^\times\to\{\pm1\})=\{\pm1\}^{F^\times}$$

יש טופולוגיה טבעית, הלוא היא טופולוגיית המכפלה, המוגדרת לפי תת־בסיס הכולל את הקבוצות $H_a=\{f:F^\times\to\{\pm1\}:\ f(a)=1\}$ והמשלימות שלהן. נזכיר ש**מרחב בוליאני** הוא מרחב קומפקטי, האוסדורף, שהוא בלתי קשיר לחלוטין (=מחלקות הקשירות הן נקודונים). לפי משפט המכפלה של טיכונוף, $\mathrm{Maps}(F^\times\to\{\pm1\})$ קומפקטי. לפי מבנה הבסיס, המרחב הזה גם האוסדורף ובלתי קשיר לחלוטין, ולכן הוא בוליאני.

טענה 5.4.3 O_F הוא מרחב בוליאני.

הוכחה. כל תת־מרחב סגור של מרחב בוליאני הוא בוליאני בעצמו. לכן די להראות שהתמונה של O_F סגורה ב־$\mathrm{Maps}(F^\times\to\{\pm1\})$. תהי $f\in\mathrm{Maps}(F^\times\to\{\pm1\})$ פונקציה שאינה מגדירה סידור של F, אז יש $a,b,c\in F^\times$ כך ש־$f(a)=f(b)=1$ ו־$f(c)=-1$, למרות ש־$c\in\{a+b,ab\}$. אבל אז $f\in H_a\cap H_b\cap H_c^c$, שהיא קבוצה פתוחה שאינה נחתכת עם O_F. □

חיתוך קבוצות תת־הבסיס של $\{\pm1\}^{F^\times}$ עם O_F מספק תת־בסיס למרחב O_F: אוסף הקבוצות מהצורה $H(a)=\{\alpha\in O_F:\ a>_\alpha 0\}$.

בעיה 5.4.4 נניח ש־$P_1,\dots,P_t$ הם סידורים של F; אז $F^{\times 2}\subseteq T\subseteq F^\times$, עם $[F^\times\!:\!T]=2^m$ עבור $m\le t$ מתאים. טבעי לשאול מה יכול להיות הקשר בין m ו־t. נראה שתי דוגמאות קיצוניות.

1. נניח ש־F שדה מספרים ממשי לחלוטין, ממימד m. לפי **עקרון הקירוב החלש** (Platonov-Rapinchuk, Theorem 1.4), השיכון $F\hookrightarrow\mathbb{R}\otimes_{\mathbb{Q}}F=\mathbb{R}^m$ הוא צפוף. נסמן ב־T את קבוצת המספרים החיוביים לחלוטין ב־F. הראה ש־$[F^\times\!:\!T]=2^m$ (עם m סידורים).
2. אם k שדה סדור, $x\in k((x))$ הוא **אינפיניטיסימל** אם $0<x<a$ לכל $0<a\in k$, או $0<-x<a$ לכל $0<a\in k$. נסמן ב־T את קבוצת האברים של $F=\mathbb{R}((x_1))\cdots((x_{m-1}))$ שהם חיוביים ביחס לכל הסידורים שעבורם כל x_i הוא אינפיניטיסימל ביחס ל־$\mathbb{R}((x_1))\cdots((x_{i-1}))$. הראה ש־$[F^\times\!:\!T]=2^{m}$ (עם 2^{m-1} סידורים).
3. לכל שלושה סידורים P_1,P_2,P_3, $[F^\times\!:\!P_1\cap P_2\cap P_3]=2^3$ (ולכן אם $t=1,2,3$ אז $m=t$).

5.5 הסימן הגלובלי

הסימן מגדיר עבור כל $[q] \in W(F)$ את פונקציית הסימן $\hat{q}: O_F \to \mathbb{Z}$, לפי $\alpha \mapsto \mathrm{sign}_\alpha(q)$. ההתאמה $q \mapsto \hat{q}$ מגדירה את **הסימן הגלובלי**, שהוא פונקציה מ־$W(F)$ לחוג החזקה $\mathrm{Maps}(O_F \to \mathbb{Z})$.

טענה 5.5.1 הסימן הגלובלי הוא הומומורפיזם של חוגים.

הוכחה. צריך להראות שלכל סדר α, $\mathrm{sign}_\alpha(q' \perp q'') = \mathrm{sign}_\alpha(q') + \mathrm{sign}_\alpha(q'')$ ו־$\mathrm{sign}_\alpha(q' \otimes q'') = \mathrm{sign}_\alpha(q')\mathrm{sign}_\alpha(q'')$; זה נובע מההגדרה של $\mathrm{sign}_\alpha(\cdot)$. $\square$

טענה 5.5.2 לכל $q \in W(F)$, הפונקציה $\hat{q}: O_F \to \mathbb{Z}$ רציפה (ביחס לטופולוגיה הדיסקרטית של $\mathbb{Z}$).

הוכחה. מספיק להוכיח את הטענה עבור הפונקציות $q = \langle a \rangle$, משום שסכום של פונקציות רציפות לחבורה הטופולוגית $\mathbb{Z}$ הוא פונקציה רציפה. אבל $\hat{q}^{-1}(1) = H(a)$, $\hat{q}^{-1}(-1) = H(-a)$, ואלו קבוצות פתוחות. $\square$

אם כך, הסימן הגלובלי $q \mapsto \hat{q}$ מהווה הומומורפיזם

$$c: W(F) \to C(O_F, \mathbb{Z}),$$

כאשר $C(O_F, \mathbb{Z})$ הוא חוג הפונקציות הרציפות מ־O_F ל־$\mathbb{Z}$.

5.5.1 חוג ויט של שדה לא־ממשי

תרגיל 5.5.3 יהי $t \in R$ איבר לא נילפוטנטי בחוג קומוטטיבי. אז יש אידיאל ראשוני שאינו מכיל את t. **הדרכה**. לפי הלמה של צורן יש אידיאל מקסימלי שאינו מכיל אף חזקה של t. הראה שהוא ראשוני.

טענה 5.5.4 אם F שדה לא ממשי (כלומר אינו ניתן לסידור), אז יש r כך ש־$0 = \langle 1,1 \rangle^r = 2^r$.

הוכחה. אנו מוכיחים ש־2 נילפוטנטי בחוג ויט. נניח שלא, אז לפי דוגמא 5.5.3 יש אידיאל ראשוני P כך ש־$2 \notin P$, ולפי למה 5.2.7 האידיאל הזה משרה סדר של F, בסתירה להנחה ש־F אינו ניתן לסידור. $\square$

נזכיר שחבורה G היא בעלת **פיתול־**p אם הסדר של כל איבר $g \in G$ הוא חזקה של p.

מסקנה 5.5.5 אם F שדה לא־ממשי, אז $W(F)$ הוא בעל פיתול־2.

5.5.2 חוג ויט של שדה אוקלידי

טענה 5.5.6 אם F אוקלידי אז c הוא איזומורפיזם.

הוכחה. יש סדר יחיד, ולכן $C(O_F, \mathbb{Z}) = \mathbb{Z}$. אבל במקרה זה $c: W(F) \to \mathbb{Z}$ הוא איזומורפיזם (תרגיל 5.2.4). $\square$

5.5.3 הגרעין של הסימן הגלובלי

בעזרת המקרים שטופלו בשני תת־הסעיפים הקודמים, נוכל כעת להוכיח שני משפטים מרכזיים על הקשר בין תבניות לסידורים של השדה.

הערה 5.5.7 תת־חבורת הפיתול של $W(F)$ מוכלת ב־$\mathrm{Ker}(c)$.

הוכחה. אם $[q] \in W(F)$ מפותל, אז $c(q)$ איבר מפותל של החבורה $C(O_F, \mathbb{Z})$ שכמו $\mathbb{Z}$ היא חסרת פיתול, ולכן $c(q) = 0$. $\square$

משפט 5.5.8 $\mathrm{Ker}(c)$ *הוא בעל פיתול־*2.

הוכחה. תהי q תבנית שאינה 2־מפותלת; נבנה סידור α של F כך ש־$\mathrm{sign}_\alpha(q) \neq 0$, וזה יוכיח ש־$q \notin \mathrm{Ker}(c)$. לפי הלמה של צורן, יש הרחבה אלגברית מקסימלית K של F ביחס לתכונה ש־q_K לא 2־מפותלת.

נוכיח ש־K אוקלידי. ראשית, K ניתן לסידור משום שאחרת כל תבנית מעל K היא 2־מפותלת (מסקנה 5.5.5). כעת יהי $a \in K^\times$. לפי טענה 5.1.6 מספיק להוכיח ש־a או $-a$ ריבועים. נניח שלא, אז $K[\sqrt{a}]$ ו־$K[\sqrt{-a}]$ הרחבות של K, ולפי המקסימליות של K, q_K נעשית 2־מפותלת מעל שתיהן. כלומר יש t כך ש־$Q = 2^t q$ היפרבולית מעל שני השדות $K[\sqrt{\pm a}]$. לפי טענה 2.5.6 נובע ש־$\pm a \in G(Q_K)$, ולכן $-1 \in G(Q_K)$, כלומר $2^{t+1}q_K = 2Q_K \sim 0$, בסתירה לבחירת K.

כעת יהי α הסידור האוקלידי של K. לפי סידור זה $\mathrm{sign}(q) \neq 0$ כי q_K אינה 2־מפותלת (ראה טענה 5.5.6), מש"ל. □

הערה 5.5.9 לפי מסקנה 6.6.5, אידיאל הפיתול של $W(F)$ נוצר על־ידי תבניות פיסטר דו־ממדיות.

מסקנה 5.5.10 התנאים הבאים שקולים עבור תבנית q מעל F:

1. $[q] \in W(F)$ איבר מפותל בחבורה החיבורית של חוג ויט.
2. יש n כך ש־$n \cdot q$ היפרבולית.
3. יש תבנית פיסטר $\varphi = \langle\langle -1, \dots, -1 \rangle\rangle$ כך ש־$\varphi \otimes q$ היפרבולית.
4. $c(q) = 0$.
5. לכל סידור α של F, $\mathrm{sign}_\alpha(q) = 0$.
6. לכל סגור ממשי E של F, q_E היפרבולית.

הוכחה. $(1) \Leftrightarrow (2)$: זו ההגדרה של פיתול. $(2) \Leftarrow (4)$: הערה 5.5.7. $(4) \Leftarrow (3)$: משפט 5.5.8. $(4) \Leftrightarrow (6)$: הערה 5.2.3. $(4) \Leftrightarrow (5)$: ההגדרה של c. $(3) \Leftarrow (1)$: לפי ההנחה $2^m q$ היפרבולית ל־m מתאים. □

אם הופכים את תנאים 1 ו־5 במסקנה, מקבלים:

מסקנה 5.5.11 הסדר של $q \in W(F)$ הוא אינסוף אם ורק אם יש סידור של F כך ש־$\mathrm{sign}_\alpha(q) \neq 0$.

מסקנה 5.5.12 נניח ש־F שדה פיתגורי ממשי. לפי טענה 5.3.4, $W(F)$ חסר פיתול, ולכן $c\colon W(F) \to C(O_F, \mathbb{Z})$ הוא שיכון. כלומר, מעל שדה פיתגורי, איבר בחוג ויט מאופיין באופן מלא על־ידי הסימן הגלובלי שלו.

דוגמא 5.5.13 את $\mathbb{Q}$ יש רק דרך אחת לסדר (כל מספר טבעי הוא סכום של ריבועים: $n = 1 + \dots + 1$). לכן האפימורפיזם של סימן סילבסטר הוא $W(\mathbb{Q}) \to W(\mathbb{R}) = \mathbb{Z}$. הגרעין של $W(\mathbb{Q}) \to W(\mathbb{R})$ נוצר (כחבורה) על־ידי התבניות $\langle a \rangle \cdot \langle\langle b \rangle\rangle$ עבור $b > 0$, ואכן $4\langle\langle b \rangle\rangle = \langle\langle -1, -1, b \rangle\rangle \sim 0$ לכל $b > 0$ לפי משפט ארבעת הריבועים של לגרנז'.

תרגיל 5.5.14 נניח שלשדה F יש בדיוק שני סידורים. הראה שאידיאל הפיתול של $W(F)$ נוצר (כאידיאל) על־ידי התבניות $\langle\langle b \rangle\rangle$ כאשר b חיובי לחלוטין.

תרגיל 5.5.15 נניח שלשדה F יש בדיוק שלושה סידורים. הראה שאידיאל הפיתול של $W(F)$ נוצר (כאידיאל) על־ידי התבניות $\langle\langle b \rangle\rangle$ כאשר b חיובי לחלוטין, ו־$\langle\langle b, b' \rangle\rangle$ כאשר $c(b) = (+,+,-)$ ו־$c(b') = (+,-,+)$.

בעיה 5.5.16 התבניות $\langle\langle a_1, \dots, a_t \rangle\rangle$, עם $\bigcup H(a_i) = O_F$, כולן מפותלות. האם הן יוצרות את אידיאל הפיתול?

המשפט הבא, שנביא ללא הוכחה, מתאר את הגרעין של העתקת סימן חלקית. יהי $0 \neq T$ קדם־סדר. נסמן ב־$O_F(T)$ את תת־המרחב של O_F הכולל רק את הסדרים המכילים את T. נסמן ב־$c_T: W(F) \to C(O_F(T), \mathbb{Z})$ את העתקת הסימן המוגבלת לסדרים המכילים את T.

משפט 5.5.17 **([13, Thm. 1.16])** *$\mathrm{Ker}(c_T)$ שווה לסכום המאפסים של התבניות $\langle t_1, \ldots, t_n\rangle$ עבור $t_1, \ldots, t_n \in T$; וגם לסכום כל המאפסים של התבניות $\langle\langle -t_1, \ldots, -t_n\rangle\rangle$ עבור $t_1, \ldots, t_n \in T$.*

מסקנה 5.5.18 $\mathrm{Ker}(c_T)$ נוצר על־ידי תבניות פיסטר $\langle\langle b\rangle\rangle$, כאשר $b \in T$.

הוכחה. ראה משפט 6.6.3 לגבי המאפסים של תבניות פיסטר ותרגיל 6.6.6. □

5.5.4 הקו־גרעין של הסימן הגלובלי

נסמן ב־χ_B את הפונקציה המציינת של תת־קבוצה $B \subseteq O_F$. כזכור, הקבוצות $H(a) = \{\alpha \in O_F : a >_\alpha 0\}$ מהוות תת־בסיס למרחב הטופולוגי O_F, ולכן הקבוצות $H(a_1, \ldots, a_n) = H(a_1) \cap \cdots \cap H(a_n)$ מהוות לו בסיס.

טענה 5.5.19 תהי $B \subseteq O_F$ קבוצה פתוחה וסגורה. אז יש $n \geq 0$ ותבנית $q \in I^n(F)$ כך ש־$2^n \chi_B = \hat{q}$.

הוכחה. נסמן ב־$\mathcal{F}$ את אוסף תת־הקבוצות הפתוחות־וסגורות של O_F שעבורן הטענה נכונה.

ראשית נראה שקבוצות הבסיס שייכות ל־$\mathcal{F}$. יהיו $a_1, \ldots, a_n \in F^\times$. נסמן $q = \langle\langle -a_1, \ldots, -a_n\rangle\rangle$, אז
$$\hat{q}(\alpha) = \begin{cases} 2^n & a_1, \ldots, a_n >_\alpha 0 \\ 0 & \text{אחרת} \end{cases}$$
כלומר $\hat{q} = 2^n \chi_{H(a_1,\ldots,a_n)}$. מכאן ש־$H(a_1, \ldots, a_n) \in \mathcal{F}$.

שנית, נראה ש־$\mathcal{F}$ סגור לאיחוד. אכן, נניח ש־$B_1, B_2 \in \mathcal{F}$. אז יש מספר טבעי m ותבניות $q_1, q_2 \in I^m(F)$ כך ש־$\hat{q}_i = 2^m \chi_{B_i}$. נסמן $[q] = 2^m[q_1] + 2^m[q_2] - [q_1][q_2] \in I^{2m}(F)$, ונחשב ש־
$$\begin{aligned} 2^{2m}\chi_{B_1 \cup B_2} &= 2^{2m}(\chi_{B_1} + \chi_{B_2} - \chi_{B_1}\chi_{B_2}) \\ &= 2^m \hat{q}_1 + 2^m \hat{q}_2 - \hat{q}_1\hat{q}_2 = \hat{q}. \end{aligned}$$

לבסוף, תהי B קבוצה פתוחה וסגורה כלשהי. כתת־קבוצה סגורה של O_F, B קומפקטית. לכן היא איחוד סופי של קבוצות בסיס, ומכאן ש־$B \in \mathcal{F}$. □

הערה 5.5.20 לכל סדר של F ולכל $q \in I^n(F)$, $2^n \mid \mathrm{sign}(q)$. זאת מפני ש־$q$ היא סכום של תבניות פיסטר מסדר n (מסקנה 2.3.18), והסימן של תבנית פיסטר, כפי שראינו בהוכחת המשפט, הוא או אפס או 2^n.

מסקנה 5.5.21 לכל $B \subseteq O_F$ פתוחה וסגורה, $\chi_B \in C(O_F, \mathbb{Z})/\mathrm{Im}(c)$ היא 2־מפותלת (לפי טענה 5.5.19).

משפט 5.5.22 *המנה $\mathrm{coKer}(c) = C(O_F, \mathbb{Z})/\mathrm{Im}(c)$ היא 2־מפותלת.*

הוכחה. עלינו להראות שלכל פונקציה רציפה $f: O_F \to \mathbb{Z}$ יש r ותבנית $q \in W(F)$ כך ש־$2^r f = \hat{q}$. מכיוון ש־O_F קומפקטי, f חסומה, ולכן היא צירוף לינארי סופי של פונקציות מציינות על הקבוצות $B_i = f^{-1}(\{i\})$. לכן די להוכיח את הטענה עבור פונקציות מהצורה $f = \chi_B$, כאשר B קבוצה פתוחה וסגורה ב־O_F, וזו מסקנה 5.5.21. □

שילוב משפטים 5.5.8 ו־5.5.22 מספק את התאור הבא לחבורה האדיטיבית של $W(F)$:

מסקנה 5.5.23 **([14, cor. 5.8])** $W(F) \cong W_t(F) \oplus P$ כאשר $W_t(F)$ היא תת־החבורה של האברים המפותלים, ו־P היא חבורה אבלית חופשית שדרגתה $\mathrm{rank} P = \mathrm{rank}\, C(O_F, Z)$.

פרק 6

תבניות פיסטר

בהגדרה 2.3.17 הגדרנו את תבניות פיסטר מסדר n, $\langle\langle a_1,\dots,a_n\rangle\rangle = \langle\langle a_1\rangle\rangle\otimes\cdots\otimes\langle\langle a_n\rangle\rangle$, כאשר $\langle\langle a\rangle\rangle = \langle 1,-a\rangle$. ראינו ש־$I^n(F)$ נוצר, כחבורה חיבורית, על־ידי התבניות מסדר n. פרק זה מוקדש לתכונות יוצאות הדופן של תבניות פיסטר.

6.1 נוסחאות מכפלה

הדוגמא המוכרת ביותר לתבנית פיסטר היא התבנית $\langle\langle -1,\dots,-1\rangle\rangle$, שהיא סכום של 2^n ריבועים. בסעיף הראשון נדון בכפליות של קבוצת הערכים של תבניות כאלה.

אוילר הראה שראשוני p ניתן להצגה כסכום של שני ריבועים אם ורק אם $p=2$ או $p\equiv 1 \pmod 4$. בעזרת נוסחת המכפלה

$$(x_1^2+x_2^2)(y_1^2+y_2^2) = (x_1y_1+x_2y_2)^2+(x_1y_2-x_2y_1)^2$$

הוא יכול היה לקבוע בדיוק אלו מספרים ניתנים להצגה כסכום של שני ריבועים. הזהות הזו שקולה לכך שהנורמה $\mathrm{N}:\mathbb{Q}[\sqrt{-1}]\to\mathbb{Q}$ היא כפלית.

פרמה שער שכל מספר טבעי הוא סכום של ארבעה ריבועים. אוילר, שניסה להוכיח את ההשערה, גילה ב־1743 נוסחת כפל עבור סכום של ארבעה משתנים. לגרנז' נעזר בנוסחה זו ב־1770 כשהשלים את הוכחת משפט ארבעת הריבועים, הנקרא היום על שמו. כשהמילטון גילה ב־1843 את הקווטרניונים, הוא חשף דרך חדשה לפרש את נוסחת הכפל של ארבעה ריבועים: ככפליות של תבנית הנורמה באלגברות קווטרניונים. גרייבס (Graves) וקיילי (Cayley) גילו את אלגברות האוקטוניונים זמן קצר אחר־כך (הראשון כתב על כך להמילטון כבר בסוף 1843, אך פרסם את התגלית רק ב־1848, וכך יוחסה הבכורה לקיילי שפרסם את האוקטוניונים ב־1845). אחד מפירות המבנה האלגברי החדש היה נוסחאות כפל לסכומים של שמונה ריבועים.

לנוסחאות הכפל האלו אין אנלוג לסכום של שלושה ריבועים. והראיה, 3 ו־5 הם סכומים של שלושה ריבועים, אבל המכפלה 15 איננה כזו. נסיונות להכליל את הנוסחאות האלה לסכום של 16 ריבועים וכדומה, נכשלו. משפט Hurwitz מסביר מדוע: אין פולינומים $z_1,\dots,z_n\in F[x_1,\dots,x_n][y_1,\dots,y_n]$ כך ש־$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2)=z_1^2+\cdots+z_n^2$, אלא אם $n=1,2,4,8$.

משפט 6.1.1 (משפט Hurwitz, 1898) יהי F שדה ממאפיין $\neq 2$. נניח שיש תבניות בילינאריות $z_1,\dots,z_n:(Fx_1+\cdots+Fx_n)\times(Fy_1+\cdots+Fy_n)\to F$ כך ש־

$$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2)=z_1^2+\cdots+z_n^2. \tag{6.1}$$

אז $n=1,2,4,8$.

הוכחה. נכתוב $AY = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = Z$, כאשר המקדמים a_{ij} הם צירופים לינאריים של ה־x_k. את סכום הריבועים אפשר להציג כמכפלה סקלרית, ולקבל

$$\begin{aligned}(x_1^2+\cdots+x_n^2)(y_1,\ldots,y_n)^{\mathrm{t}}(y_1,\ldots,y_n) &= (z_1,\ldots,z_n)^{\mathrm{t}}(z_1,\ldots,z_n) \\ &= (y_1,\ldots,y_n)^{\mathrm{t}}A^{\mathrm{t}}A(y_1,\ldots,y_n).\end{aligned}$$

מהשוואת התבניות הריבועיות ב־$y_1,\ldots,y_n$, נובע השוויון

$$A^{\mathrm{t}}A = (x_1^2+\cdots+x_n^2)I_n.$$

מכיוון שכל רכיב של A הוא צירוף ליניארי של $x_1,\ldots,x_n$, אפשר לפרק $A = A_1x_1+\cdots+A_nx_n$, כאשר $A_1,\ldots,A_n \in \mathrm{M}_n(F)$. השוויון שלנו הופך להיות $\sum {A_i}^{\mathrm{t}}A_jx_ix_j = \sum x_k^2$, כלומר

$$\begin{aligned}{A_i}^{\mathrm{t}}A_i &= I_n; && (6.2)\\ {A_i}^{\mathrm{t}}A_j + {A_j}^{\mathrm{t}}A_i &= 0 \qquad (i\neq j) && (6.3)\end{aligned}$$

אם $n=1$ אין מה להוכיח (אפשר לבחור $A_1 = (1)$). נניח אם כך ש־$n \geq 2$. נתבונן ב־$n-1$ המטריצות $B_i = {A_n}^{\mathrm{t}}A_i$, $i=1,\ldots,n-1$; הן מקיימות

$$\begin{aligned}{B_i}^{\mathrm{t}} &= -B_i; && (6.4)\\ B_i^2 &= -I_n; && (6.5)\\ B_iB_j &= -B_jB_i \qquad (i\neq j). && (6.6)\end{aligned}$$

מכך ש־B_i הן אנטי־סימטריות והפיכות, נובע שהממד n הוא זוגי.

תהי $G = \{I_n, B_1,\ldots,B_{n-1}, B_1B_2,\ldots,B_{n-2}B_{n-1},\ldots\}$ קבוצת כל המכפלות המסודרות של מטריצות מהרשימה $B_1,\ldots,B_{n-1}$; ב־G יש 2^{n-1} מטריצות, ו־$G \cup -G$ היא חבורה (השווה לטענה 3.4.3 על הבסיס של אלגברות קליפורד). אברי G הם מטריצות סימטריות או אנטי־סימטריות, בהתאם לאורך: מכפלות באורך $\equiv 0,3 \pmod 4$ הן סימטריות, ומכפלות באורך $\equiv 1,2 \pmod 4$ הן אנטי־סימטריות. מכיוון שכפל ביוצר יכול להאריך או לקצר מכפלה (תלוי אם הוא משתתף בה או שאינו משתתף), לכל $g \in G$ פרט ל־I ולמכפלה המלאה $B_1\cdots B_{n-1}$ יש יוצר B_i כך ש־B_ig מאותו טיפוס סימטריה כמו g.

נאמר שיחס ליניארי בין אברים של G הוא *מינימלי* אם אין יחס קצר יותר בין האברים המשתתפים בו. כפולה של יחס מינימלי באיבר של G נותנת יחס שגם הוא מינימלי. מחיבור היחס עם היחס המתקבל משחלוף שלו, נובע שהמטריצות המשתתפות ביחס מינימלי הן או כולן סימטריות או כולן אנטיסימטריות. נתבונן ביחס מינימלי בין אברי G. נכפיל את היחס באחת המטריצות המשתתפות בו, ונקבל יחס שמשתתפת בו מטריצת היחידה, ולכן כל אבריו סימטריים. אם נכפיל את היחס הזה באחד ה־B_i, נקבל יחס שיש לו רכיב אנטי־סימטרי, ולכן כל רכיביו אנטי־סימטריים; אבל לכל רכיב g פרט ל־I ולמכפלה המלאה יש יוצר B_i כך ש־B_ig סימטרי, ומכאן שאיבר כזה אינו יכול להופיע ביחס. מכאן שיחס מינימלי, עד כדי כפל באיבר של G, הוא מהצורה $I = \alpha B_1\cdots B_{n-1}$.

היחס $I = \alpha B_1\cdots B_{n-1}$ וכפולותיו מאפשרים להחליף כל מכפלה של יותר מ־$\frac{n-1}{2}$ מטריצות במכפלה של פחות מ־$\frac{n-1}{2}$ מטריצות, וכפי שראינו, בין המטריצות הקצרות לא קיים יחס לינארי. כלומר, הן בלתי תלויות, ומכאן שמספרן 2^{n-2} חסום על־ידי ממד מרחב המטריצות שהוא n^2. אי־השוויון $2^{n-2} \leq n^2$ מתקיים רק כאשר $n \leq 8$. כבר ראינו ש־n זוגי, ולכן נשאר לפסול רק את המקרה $n=6$.

אכן, אם $n=6$ אז המכפלה המלאה $B_1\cdots B_5$ היא אנטי־סימטרית, ולכן לא קיים יחס מינימלי, כלומר כל 2^5 המטריצות בלתי־תלויות. יש $16 = 1 + 10 + 5$ מכפלות באורך $1,2,5$, שהן אנטי־סימטריות, יותר מממד מרחב המטריצות האנטי־סימטריות ב־$\mathrm{M}_6(F)$ שהוא רק $15 = \frac{6(6-1)}{2}$. לכן ההנחה שהמטריצות $B_1,\ldots,B_5$ קיימות מביאה במקרה זה לסתירה. □

תרגיל 6.1.2 באשר לנוסחאות הכפל עבור סכומים של $n = 2, 4, 8$ איברים, נקבע מרחב וקטורי V בגודל n. לכל $i \in V$ נגדיר $z_i = \sum_{j\in V} \epsilon_{ij}x_jy_{i+j}$. נניח שהנוסחה (6.1) מתקיימת. הראה שכל $\epsilon_{ij} = \pm 1$. הראה שיש בדיוק 2^3 נוסחאות אפשריות עבור $n = 2$, 2^8 נוסחאות כאלו עבור $n = 4$, ו־2^{19} עבור $n = 8$.

בעיה 6.1.3 לסכום של כמה ריבועים יש נוסחאות מכפלה כאשר $\mathrm{char}F = 2$?

6.2 ערכים של תבנית

בהמשך נראה שעבור תבנית פיסטר, בניגוד למקרה הכלל, הקשר בין הערכים לגורמי הדמיון הוא חזק במיוחד. בסעיף הזה נאסוף כמה תכונות פשוטות של קבוצת הערכים.

הגדרה 6.2.1 $D(q) = \{q(u) : q(u) \neq 0\}$ *קבוצת הערכים של* q.

החבורה $G(q) \subseteq F^\times/F^{\times 2}$ הוגדרה בסעיף 2.5.

הערה 6.2.2
1. $G(q)$ פועלת על $D(q)$: אם $g \in G(q)$ ו־$c \in D(q)$ אז $gc \in D(\langle g\rangle q) = D(q)$ ולכן $gc \in D(q)$.
2. בפרט אם $1 \in D(q)$ אז $G(q) \subseteq D(q)$.

דוגמא 6.2.3 עבור תבנית פיסטר מסדר ראשון $q = \langle\langle a\rangle\rangle$, $D(q) = G(q)$. אכן, $G(q) \subseteq D(q)$ כי 1 הוא ערך של התבנית, ומצד שני לכל ערך $c \in D(\langle\langle a\rangle\rangle)$ מתקיים $\langle\langle a\rangle\rangle \cong \langle 1, -a\rangle \cong \langle c, -ac\rangle \cong \langle c\rangle\langle\langle a\rangle\rangle$ לפי מסקנה 3.3.11.

במסקנה 3.3.11 ראינו שעבור תבנית ממימד 2, כל ערך יכול להופיע כמקדם בהצגה אלכסונית של התבנית. תכונה זו נכונה באופן כללי: כל הערכים של תבנית מופיעים בהצגות האלכסוניות שלה.

טענה 6.2.4 תהי q תבנית מעל F, ויהי $a \in F^\times$. אז $a \in D(q)$ אם ורק אם יש ל־q הצגה אלכסונית $q = \langle a, b_2, \dots, b_n\rangle$.

הוכחה. **אם $q = \langle a, b_2, \dots, b_n\rangle$, ברור ש־$a \in D(q)$. בכיוון ההפוך אם $a = q(u)$ אז אפשר לפרק $V = Fu \perp u^\perp$, ולהציג את הצמצום של q ל־$u^\perp$ בצורה אלכסונית $\langle b_2, \dots, b_n\rangle$.** □

6.3 הצגות של תבניות פיסטר

למה 6.3.1 הצגות של תבנית פיסטר מסדר 2:
1. אם $c \in D(\langle\langle a\rangle\rangle)$ אז $\langle\langle a, b\rangle\rangle \cong \langle\langle a, bc\rangle\rangle$.
2. אם $d \in D(\langle a, b\rangle)$ אז $\langle\langle a, b\rangle\rangle \cong \langle\langle d, abd\rangle\rangle$.

הוכחה. **1. לפי מסקנה 6.2.3 $\langle\langle a\rangle\rangle \cong \langle c\rangle\langle\langle a\rangle\rangle$, כלומר $0 \sim \langle\langle c\rangle\rangle\langle\langle a\rangle\rangle$. לפי הכמעט־אדיטיביות (למה 3.3.3) $\langle\langle b, c\rangle\rangle \perp \langle\langle bc\rangle\rangle \sim \langle\langle c\rangle\rangle \perp \langle\langle b\rangle\rangle$, וכשנכפיל ב־$\langle\langle a\rangle\rangle$ נקבל**

$$\langle\langle a, c\rangle\rangle \sim \langle\langle a, b\rangle\rangle \perp \langle\langle a, c\rangle\rangle \sim \langle\langle a, bc\rangle\rangle \perp \langle\langle a, b, c\rangle\rangle \sim \langle\langle a, bc\rangle\rangle;$$

אבל התבניות מאותו ממד.

2. שוב בעזרת מסקנה 6.2.3,

$$\begin{aligned}\langle\langle a,b\rangle\rangle &\cong \langle 1,-a,-b,ab\rangle\\ &\cong \langle 1\rangle \perp \langle -1\rangle\langle a,b\rangle \perp \langle ab\rangle\\ &\cong \langle 1\rangle \perp \langle -1\rangle\langle d,abd\rangle \perp \langle abd^2\rangle\\ &\cong \langle\langle d,abd\rangle\rangle.\end{aligned}$$

□

אם $\varphi \cong \varphi_1 \otimes \varphi_2$ הן תבניות פיסטר, נאמר ש־φ_1 **מחלק** את φ. ראינו (טענה 6.2.4) שתבנית ריבועית q אפשר להציג בצורה $\langle a,\dots\rangle$ אם ורק אם a הוא ערך של q. אם נתונה תבנית פיסטר, מהם הערכים a שעבורם אפשר להציג את φ בצורה $\langle\langle a,\dots\rangle\rangle$? על שאלה זו עונה המשפט הבא (ראה הגדרה 3.3.6).

משפט 6.3.2 (משפט תת־התבנית הטהורה) *תהי φ תבנית פיסטר מסדר n, ויהי $a \in F^\times$. אז $\langle\langle a\rangle\rangle$ מחלק את φ אם ורק אם $-a \in D(\varphi')$.*

הוכחה. אם $\varphi \cong \langle\langle a,b_2,\dots,b_n\rangle\rangle$ אז ברור ש־$-a$ הוא ערך של $\varphi' \cong \langle -a,-b_2,\dots\rangle$. נוכיח את הכיוון ההפוך, באינדוקציה על n. אם $n=1$, אז $\varphi = \langle\langle a_1\rangle\rangle = \langle 1,-a_1\rangle$ ו־$\varphi' = \langle -a_1\rangle$. ההנחה $-a \in D(\langle -a_1\rangle)$ פירושה ש־$\langle -a_1\rangle = \langle -a\rangle$ ואז $\varphi = \langle\langle a\rangle\rangle$.

נניח שהטענה נכונה עבור $n-1$, ונוכיח אותה לתבנית מסדר n. כל תבנית פיסטר היא מכפלת תבניות פיסטר מסדר 1, ולכן יש תבנית פיסטר t מסדר $n-1$, וסקלר $\pi \in F^\times$, כך ש־$\varphi = t\otimes\langle\langle \pi\rangle\rangle = t \perp \langle -\pi\rangle t$. מכאן נובע ש־$\varphi' = t' \perp \langle -\pi\rangle t$. לפי ההנחה, $-a$ הוא ערך של התבנית φ', כלומר אפשר לכתוב

$$-a = -\alpha' + \pi\beta,$$

כאשר $-\alpha'$ הוא ערך של t' ו־$-\beta$ הוא ערך של t; כלומר $\beta = -c^2 + \beta'$ כאשר $-\beta'$ הוא ערך של t'. אם $\beta = 0$ אז $-a = -\alpha'$ הוא ערך של t', ולפי הנחת האינדוקציה t מתחלק ב־$\langle\langle a\rangle\rangle$; לכן אפשר להניח $\beta \neq 0$.

נראה ש־$\varphi \cong t\otimes\langle\langle -\beta\pi\rangle\rangle$. אם $\beta' = 0$ אז $\beta = -c^2$ ו־$\langle\langle \pi\rangle\rangle \cong \langle\langle -\beta\pi\rangle\rangle$, כך שהטענה הזו ברורה. לכן נניח $\beta' \neq 0$.

מכיוון ש־$-\beta'$ הוא ערך של t', אפשר לפי הנחת האינדוקציה לכתוב $t \cong s\otimes\langle\langle \beta'\rangle\rangle$ (כאשר s תבנית פיסטר מסדר $n-2$). בנוסף, $-\beta = c^2 - \beta'$ הוא ערך של התבנית $\langle\langle \beta'\rangle\rangle$, ולפי למה 6.3.1.(1)

$$\varphi = t\otimes\langle\langle \pi\rangle\rangle = s\otimes\big\langle\big\langle \beta',\pi\big\rangle\big\rangle \cong s\otimes\big\langle\big\langle \beta',-\beta\pi\big\rangle\big\rangle = t\otimes\langle\langle -\pi\beta\rangle\rangle.$$

אם $\alpha' = 0$, גמרנו כי $a = -\pi\beta$. לכן נניח $\alpha' \neq 0$. לפי הנחת האינדוקציה, מכיוון ש־$-\alpha'$ הוא ערך של t', $\langle\langle \alpha'\rangle\rangle$ מחלק את t, ולכן $\langle\langle \alpha',-\pi\beta\rangle\rangle$ מחלק את φ. אבל $a = \alpha' - \pi\beta$ הוא ערך של התבנית $\langle \alpha',-\pi\beta\rangle$, ומלמה 6.3.1.(2) מקבלים ש־φ מתחלק ב־

$$\big\langle\big\langle \alpha',-\pi\beta\big\rangle\big\rangle \cong \big\langle\big\langle a,-\pi\alpha'\beta\big\rangle\big\rangle,$$

כך ש־$\langle\langle a\rangle\rangle$ מחלק את φ. □

6.4 המשפטים המרכזיים

כעת אפשר להוכיח את המשפט המרכזי על תבניות פיסטר.

משפט 6.4.1 *תהי φ תבנית פיסטר. אם φ איזוטרופית, היא היפרבולית.*

הוכחה. נניח ש־φ איזוטרופית. אז יש לה תת־תבנית היפרבולית, כלומר $\langle 1,-1\rangle \perp \cdots = \varphi = \langle 1\rangle \perp \varphi'$. לכן $\langle -1\rangle$ היא תת־תבנית של φ', ו־-1 הוא ערך של φ'. לפי משפט 6.3.2, $\langle\langle 1\rangle\rangle$ מחלק את φ, ומיד נובע ש־$\varphi = \langle 1,-1\rangle\otimes t = t \perp -t$ היפרבולית. □

משפט 6.4.2 *תהי φ תבנית פיסטר. אז $D(\varphi) = G(\varphi)$.*

הוכחה. לאור הערה 6.2.2 די להוכיח שכל ערך $c \in D(\varphi)$ הוא גורם דמיון. נכתוב $c = \varphi(u)$, אז $\langle\langle c\rangle\rangle\otimes\varphi = \varphi \perp -c\varphi$ היא איזוטרופית כי $\varphi(u) - c\varphi(1,0,\dots,0) = 0$, ולפי משפט 6.4.1 התבנית $\langle\langle c\rangle\rangle\varphi$ היפרבולית. היינו, $\varphi \perp -c\varphi \sim 0$ בחוג ויט, ולכן $\varphi \cong c\varphi$. □

אבל $G(\varphi)$ היא חבורה, ולכן:

מסקנה 6.4.3 לכל תבנית פיסטר φ, אם $a,b \in D(\varphi)$ אז גם $ab \in D(\varphi)$.

בסעיף 7.2 נוכיח את הכיוון ההפוך: אם יש ב־$D(q)$ נוסחת כפל לערכים, אז q מוכרחה להיות תבנית פיסטר.

משפט 6.4.4 ([7, משפט 6.10]) *אם $\langle\langle a_1,\dots,a_n\rangle\rangle \cong \langle\langle b_1,\dots,b_n\rangle\rangle$ תבניות לא איזוטרופיות אז יש שרשרת של צעדים מהתבנית הראשונה לשניה, כך שבכל צעד מחליפים $\langle\langle a_i,a_j\rangle\rangle \cong \left\langle\left\langle a_i',a_j'\right\rangle\right\rangle$.*

6.5 רמה של שדה

נציג את אחת המסקנות היפות של תכונת הכפליות של תבניות פיסטר (מסקנה 6.4.3). **האורך** של מספר $a \in F$ הוא m המינימלי כך ש־a שווה לסכום של m ריבועים, או ∞ אם אין כזו הצגה. **הרמה** של השדה F היא האורך של -1. מסמנים את הרמה של F ב־$s(F)$. הרמה היא סופית אם ורק אם השדה אינו ניתן לסידור.

משפט 6.5.1 (פיסטר) *הרמה של שדה היא אינסוף (כשהשדה ממשי) או חזקה של 2.*

הוכחה. נניח ש־-1 הוא סכום של פחות מ־2^{s+1} ריבועים. אז אפשר לכתוב $-1 = a + b$ כאשר a סכום של 2^s ריבועים ו־b סכום של $2^s - 1$ ריבועים. ברור ש־$b + 1$ הוא סכום של 2^s ריבועים, ולכן גם המכפלה $a(b+1) = -a^2 \sim -1$ היא סכום של 2^s ריבועים. □

דוגמא 6.5.2 הנה כמה דוגמאות לרמה של שדות.

1. הרמה של שדה הניתן לסידור היא ∞.
2. הרמה של שדה סופי מסדר $q \equiv 1 \pmod 4$ היא 1, משום ש־-1 הוא ריבוע.
3. הרמה של שדה סופי מסדר $q \equiv -1 \pmod 4$ היא 2, משום שכל איבר שונה מאפס הוא סכום של שני ריבועים (טענה 8.1.1).
4. נתבונן בשדה $F = \mathbb{Q}[\sqrt{-d}]$ כאשר d מספר טבעי שהוא סכום של שלושה ריבועים שלמים, $d = x_1^2+x_2^2+x_3^2$ (כלומר אינו מהצורה $4^k(8n+7)$). אז $-1 = \sum(x_i\frac{\sqrt{-d}}{d})^2$, ולכן $s(F) \leq 3$. ממשפט 6.5.1 יוצא ש־$s(F) \leq 2$. (תרגיל: מצא פתרון מפורש למשוואה $-1 = x^2 + y^2$ בשדה כזה).
5. נתבונן בשדה $F = Q[\sqrt{-d}]$ כאשר d מספר טבעי שאינו סכום של שלושה ריבועים. לפי משפט לגרנז' האורך של d הוא 4, ולפי אותו נימוק $s(F) \leq 4$. נראה שיש כאן שוויון, כלומר, -1 אינו סכום של שני ריבועים. אחרת, $\langle 1,1,1\rangle_{\mathbb{Q}}$ איזוטרופית מעל F, ולפי משפט 2.4.3.(1) פירושו של דבר ש־$\langle 1,1,1\rangle \cong \langle a\rangle\langle 1,d\rangle \perp \langle d\rangle$ מעל $\mathbb{Q}$, כאשר הרכיב השלישי בפירוק מתקבל מן הדטרמיננטה. כלומר, d הוא סכום של שלושה ריבועים מעל הרציונליים, ומתוצאה בתורת המספרים נובע ש־d סכום של שלושה ריבועים מעל השלמים, בסתירה להנחה.

6. משפט זיגל (Siegel): בשדה גלובלי, האורך של כל סכום של ריבועים הוא לכל היותר 4. בפרט, הרמה של שדה גלובלי הוא $1, 2, 4$ או אינסוף.

7. לכל שדה F, $s(F(\lambda)) = s(F)$ ו־$s(F((\lambda))) = s(F)$.

6.6 בוני פיתול

יהי a סכום של ריבועים ב־F. אז $-a$ **שלילי לחלוטין**, כלומר שלילי בכל סידור של F. לכן הסימן של $\langle\langle a\rangle\rangle$ הוא אפס בכל סידור, והוא שייך לגרעין של ההעתקה $c\colon W(F){\rightarrow}C(O_F,\mathbb{Z})$. במשפט 5.5.8 ראינו שבמקרה כזה, $\langle\langle a\rangle\rangle$ מוכרח להיות מפותל, וקיים n כך ש־$2^n\langle\langle a\rangle\rangle = \langle\langle -1,\dots,-1,a\rangle\rangle = 0$.

טענה 6.6.1 הסדר של $\langle\langle a\rangle\rangle$ בחבורה האדיטיבית של $W(F)$ שווה ל־2^n המינימלי כך ש־$2^n \geq \mathrm{len}(a)$.

הוכחה. נסמן $t = \langle\langle -1,\dots,-1\rangle\rangle$, סכום ריבועים באורך 2^n. אז $t\otimes\langle\langle a\rangle\rangle = 0$ בחוג ויט אם ורק אם $w \in G(t) = D(t)$ לפי משפט 6.4.2, אם ורק אם w הוא סכום של 2^n ריבועים. □

מסקנה 6.6.2 יהי F שדה לא־ממשי מרמה 2^r. חוג ויט $W(F)$ הוא בעל מאפיין 2^{r+1}.

הוכחה. לפי טענה 6.6.1, הסדר של $2 = \langle 1,1\rangle = \langle\langle -1\rangle\rangle$ הוא האורך של -1, כלומר הרמה של השדה. □

(השווה בין טענה 8.1.1 לבין דוגמא 6.5.2 לאור המסקנה הזו.)
בהערה 2.5.2 ראינו ש־$\langle\langle b\rangle\rangle\otimes q \sim 0$ אם ורק אם $b \in G(q)$. היינו, המאפס

$$\mathrm{Ann}(q) = \{t\colon\ t\otimes q \sim 0\}$$

בחוג ויט כולל את כל התבניות $\langle\langle b\rangle\rangle$ עבור $b \in G(q)$. מתברר שהן יוצרות אותו.

משפט 6.6.3 (משפט המאפס של ויט־פיסטר) *תהי q תבנית לא היפרבולית המקיימת $D(q) = G(q)$. אז המאפס $\mathrm{Ann}(q)$ נוצר, כאידיאל, על־ידי תבניות פיסטר מסדר ראשון.*

הוכחה. ראשית נניח ש־q איזוטרופית. אז היא מכילה תת־תבנית היפרבולית ולכן $D(q) = F^\times$; מכאן שגם $G(q) = F^\times$, ואז $\langle\langle a\rangle\rangle\otimes q \sim 0$ לכל $a \in F^\times$, כלומר $\mathrm{Ann}(q) = I(F)$ והתוצאה מתקבלת מהערה 2.3.16.

נשאר לטפל במקרה האנאיזוטרופי. תהי q תבנית לא היפרבולית המקיימת $D(q) = G(q)$, ונניח ש־$\varphi\otimes q \sim 0$. נכתוב $\varphi = \langle a_1,\dots,a_n\rangle$, ונתקדם באינדוקציה על n. במקרה $n = 1$ אין מה להוכיח כי $\langle a_1\rangle\otimes q \not\sim 0$. נניח אם כך ש־$n \geq 2$. לפי ההנחה, התבנית $a_1q \perp \cdots \perp a_nq$ איזוטרופית, ולכן יש $c_1,\dots,c_n \in D(q)$ כך ש־$a_1c_1 + \cdots + a_nc_n = 0$. לכל i, $\langle a_i\rangle\langle\langle c_i\rangle\rangle\otimes q \sim 0$ ולכן $\langle a_1c_1,\dots,a_nc_n\rangle \sim \varphi - \sum\langle a_i,-a_ic_i\rangle$ שייכת למאפס. אבל זו תבנית איזוטרופית כי סכום המקדמים שלה הוא אפס, ולכן היא שקולה לתבנית ממימד קטן מ־n, שהיא סכום של תבניות פיסטר מאפסות לפי הנחת האינדוקציה. □

המסקנה הבאה מתקבלת מהפעלת המשפט לתבנית $q = \langle\langle -1,\dots,-1\rangle\rangle$ מסדר t.

מסקנה 6.6.4 נניח ש־$2^t \neq 0$ בחוג ויט. אז $\mathrm{Ann}(2^t)$ נוצר על־ידי תבניות פיסטר $\langle\langle a\rangle\rangle$ שעבורן a הוא סכום של 2^t ריבועים.

מסקנה 6.6.5 בהמשך למשפט 5.5.8, חבורת הפיתול של $W(F)$ נוצרת (כאידיאל) על־ידי התבניות $\langle\langle a\rangle\rangle$ שעבורן a הוא סכום של ריבועים.

תרגיל 6.6.6 אידיאל של $W(F)$ הוא **קשיר** אם הוא נוצר על־ידי תבניות פיסטר מסדר ראשון השייכות לו. הראה שסכום (כלשהו) של אידיאלים קשירים הוא קשיר.

פרק 7

שיטות גנריות

באלגברה קל להוכיח שדברים שווים זה לזה: במקרים רבים מספיק לתת נוסחה מפורשת. למשל, כדי להראות שאיבר של שדה הוא סכום של ארבעה ריבועים, אפשר פשוט להציג אותו כסכום כזה. לעומת זאת, הרבה יותר קשה להוכיח שאיבר אינו ניתן להצגה כסכום של ארבעה ריבועים. סדר שבו האיבר הוא שלילי יפתור את הבעיה, אבל איך אפשר למצוא איבר שהוא סכום של חמישה ריבועים לפחות? זו עשויה להיות בעיה קשה. גישה אפשרית היא לבחון "איבר גנרי", כזה שאם אפשר להציג אותו כערך של התבנית $\langle 1,1,1,1\rangle$, אז אפשר יהיה להציג כל איבר אחר. המועמד הטבעי לתכונה כזו הוא איבר נטול תכונות, המקיים מה שהנחנו ולא יותר. למשל, האיבר $\lambda_1^2+\cdots+\lambda_5^2$ של השדה $F(\lambda_1,\dots,\lambda_5)$. גישה זו מנחה את הפרק הנוכחי.

7.1 ערכים פולינומיים של תבנית

במהלך הפרק נטפס מהשדה הנתון F לשדות הרחבה טרנסצנדנטיים מעליו. דרוש לנו עקרון שיאפשר לבצע את צעד האינדוקציה של הוספת משתנה אחד.

7.1.1 פרמטריזציה

באופן טיפוסי, אם למשוואה ריבועית (בנעלם אחד) יש שורש, אז יש לה שני שורשים. כדי להכליל הבחנה פשוטה זו, נוח לחשוב פרוייקטיבית: וקטור $u\in V$ מתאים לנקודה הפקוייקטיבית Fu, וזוג וקטורים u,t מתאים לישר הפרוייקטיבי $Fu+Ft$. מושג האיזוטרופיות עובר למרחב הפרוייקטיבי, משום שהתבניות הריבועיות שלנו הן תמיד הומוגנית.

טענה 7.1.1 (פרמטריזציה של תבנית ריבועית) תהי q תבנית ריבועית F, ויהי u וקטור איזוטרופי. אז לכל כיוון t שאינו מאונך ל־u, יש על הישר הפרוייקטיבי $Fu+Ft$ נקודה איזוטרופית נוספת יחידה פרט ל־Fu.

הוכחה. תהי b_q התבנית הבילינארית המתאימה ל־q. לפי ההנחה $q(u)=0$ ו־$b_q(u,t)\neq 0$, ולכן

$$q(\alpha u+\beta t)=q(u)\alpha^2+2\alpha\beta b_q(u,t)+\beta^2 q(t)=\beta(2b_q(u,t)\alpha+q(t)\beta),$$

ומכיוון ש־$b_q(u,t)\neq 0$ לפי ההנחה, הנקודה הפרוייקטיבית היחידה פרט ל־Fu המאפסת את התבנית היא $F(2b_q(t,u)t-q(t)u)$.

(אם $b_q(t,u)=0$ יש שתי אפשרויות: אם $q(t)=0$ אז $Fu+Ft$ כולו איזוטרופי, ואם $q(t)\neq 0$ אז $Fu+Ft$ משיק ליריעה $q=0$ בנקודה Fu, ואין עליו נקודות אפס נוספות.) $\square$

תרגיל 7.1.2 (פרמטריזציה מפורשת) תהי q תבנית ריבועית $n+1$־ממדית מעל F, שיש לה נקודה רציונלית $(\gamma_0,\gamma_1,\dots,\gamma_n)=(\gamma_0,\vec{\gamma})$ (היינו $q(\gamma_0,\vec{\gamma})=0$). תהי b התבנית הבילינארית

המתאימה ל־q. אז הפתרון הכללי למשוואה

$$q(y_0, y_1, \ldots, y_n) = 0, \qquad y_0 \neq \gamma_0$$

הוא

$$y_0 = \gamma_0 + x_0, \qquad (y_1, \ldots, y_n) = \vec{y} = \vec{\gamma} + x_0\vec{t}$$

כאשר $\vec{t} = (t_1, \ldots, t_n) \in F^n$ מקיים $b((\gamma_0, \vec{\gamma}), (1, t)) \neq 0$, ו־$x_0 = -2\frac{b((\gamma_0,\vec{\gamma}),(1,\vec{t}))}{q(1,\vec{t})}$.
(האילוץ $y_0 \neq \gamma_0$ אינו מגבלה אמיתית, משום שחוץ מהאפס הנתון $(\gamma_0, \gamma_1, \ldots, \gamma_n)$, כל נקודת אפס אחרת נמצאת מחוץ לעל מישור מהצורה $y_i = \gamma_i$. הנוסחאות מגדירות איזומורפיזם בין יריעת האפסים למרחב הפרוייקטיבי $\mathbb{P}^n F$, בהתאם לטענה 7.3.4 (להלן).)
הוכחה. נכתוב $q = \langle a_0 \rangle \perp q'$. נסמן ב־$b'$ את התבנית הבילינארית המתאימה ל־q'. נציב $y_0 = \gamma + x_0$, כך שמותר להניח $x_0 \neq 0$, ו־$\vec{y} = \vec{\gamma} + x_0\vec{t}$, כאשר $\vec{t} = (t_1, \ldots, t_n) \in F^n$ הוא וקטור כלשהו. נחשב:

$$\begin{aligned}
q(x_0 + \gamma_0, x_0\vec{t} + \vec{\gamma}) &= a_0(x_0^2 + 2\gamma_0 x_0 + \gamma_0^2) + b'(x_0\vec{t} + \vec{\gamma}, x_0\vec{t} + \vec{\gamma}) \\
&= a_0(x_0^2 + 2\gamma_0 x_0 + \gamma_0^2) + b'(x_0\vec{t}, x_0\vec{t}) + 2b'(x_0\vec{t}, \vec{\gamma}) + b'(\vec{\gamma}, \vec{\gamma}) \\
&= (a_0 + b'(\vec{t}, \vec{t}))x_0^2 + 2(a_0\gamma_0 + b'(\vec{t}, \vec{\gamma}))x_0 \\
&= q(1, \vec{t})x_0^2 + 2b((\gamma_0, \vec{\gamma}), (1, \vec{t}))x_0.
\end{aligned}$$

על־מנת שלמשוואה יהיה פתרון $x_0 \neq 0$, בהכרח נדרש $b((\gamma_0, \vec{\gamma}), (1, \vec{t})) \neq 0$; ואם מניחים שזה כך, אז מקיומו של פתרון מתחייב גם ש־$q(1, \vec{t}) \neq 0$, ואז $x_0 = -2\frac{b((1,\vec{t}),(\gamma_0,\vec{\gamma}))}{q(1,\vec{t})}$.

7.1.2 ערכים פולינומיים

משפט 7.1.3 (משפט קסלס־פיסטר Cassels-Pfister) *תהי q תבנית ריבועית מעל השדה F. אם התבנית מציגה פולינום $g \in F[\lambda]$ מעל $F(\lambda)$, אז היא מציגה אותו כבר מעל $F[\lambda]$.*

הוכחה. **אם התבנית איזוטרופית, אין מה להוכיח משום שכל $g \in F[\lambda]$ אפשר להציג כערך של התבנית ההיפרבולית, $g = (\frac{1}{2}(g-1))^2 - (\frac{1}{2}(g+1))^2$. נניח אם כך שהתבנית אנאיזוטרופית, ונכתוב אותה בצורה אלכסונית $q \cong \langle a_1, \ldots, a_n \rangle$. יהי $g(\lambda) \in F[\lambda]$ פולינום שהוא ערך של התבנית מעל $F(\lambda)$. על־ידי כפל במכנה משותף, ההנחה היא שיש $f_0, f_1, \ldots, f_n \in F[\lambda]$ כך ש־**

$$a_1 f_1(\lambda)^2 + \cdots + a_n f_n(\lambda)^2 = g(\lambda) f_0^2(\lambda),$$

כאשר $f_0 \neq 0$.
נתבונן בתבנית $Q = \langle -g, a_1, \ldots, a_n \rangle$ מעל $F(\lambda)$, וביריעת האפסים שלה $Z(Q) \subseteq F(\lambda)^{n+1}$. לפי ההנחה, $\vec{f} = (f_0, f_1, \ldots, f_n) \in Z(Q)$. אם המעלה $m = \deg(f_0)$ היא אפס, סיימנו. נניח אם כך ש־$m > 0$.
נחלק כל f_i, עם שארית, ב־f_0: יש פולינומים $g_1, \ldots, g_n,\ r_1, \ldots, r_n \in F[\lambda]$, כך ש־$f_i = f_0 g_i + r_i$ ו־$\deg(r_i) < m$ לכל $i = 0, \ldots, n$. בפרט $r_0 = 0$ ו־$g_0 = 1$. באופן מקוצר אפשר לכתוב $\vec{f} = f_0\vec{g} + \vec{r}$. אפשר להניח שהפולינומים $f_1, \ldots, f_n$ זרים במשותף, משום שאחרת אפשר לצמצם ולקבל וקטור שלרכיב האפס שלו מעלה קטנה יותר. בפרט, $\vec{r} \neq 0$.
כעת נבנה נקודה נוספת, $\vec{f'} = (f'_0, f'_1, \ldots, f'_n) \in Z(Q)$, עם $m' = \deg(f'_0) < m$. באינדוקציה, יוצא מזה שקיימת נקודה שעבורה הרכיב האפס הוא סקלר, וזה נותן הצגה שלמה של g.
נבחר $\vec{f'} = B(\vec{g}, \vec{g}) \cdot \vec{f} - 2B(\vec{g}, \vec{f}) \cdot \vec{g}$, שהיא על־פי החישוב בטענה 7.1.1 נקודה המקיימת $Q(\vec{f'}) = 0$. כדי לקבל את מעלת רכיב האפס של הנקודה החדשה, נחשב ש־

$$\begin{aligned}
f_0 f'_0 &= f_0^2 B(\vec{g}, \vec{g}) - 2f_0 B(\vec{g}, \vec{f}) \\
&= B(f_0\vec{g},\ f_0\vec{g} - 2\vec{f}) \\
&= B(f_0\vec{g},\ -\vec{f} - \vec{r}) \\
&= B(\vec{f} - \vec{r},\ -\vec{f} - \vec{r}) \\
&= B(\vec{r}, \vec{r}) \ = \ \sum a_i r_i(\lambda)^2.
\end{aligned}$$

מכיוון ש־q אנאיזוטרופית ולא כל ה־r_i הם אפס, קיבלנו ש־$f_0 f_0' \neq 0$. לכן

$$\deg(f_0) + \deg(f_0') = \deg(\sum a_i r_i^2) \leq 2 \max \deg(r_i) < 2 \deg(f_0),$$

כלומר $\deg(f_0') < \deg(f_0)$. □

בעיה 7.1.4 נסה לנסח ולהוכיח תוצאה דומה למשפט פיסטר־קסלס 7.1.3 עבור תבנית q מעל $\mathbb{Z}$, המציגה ערך שלם מעל $\mathbb{Q}$. מה משתבש בהוכחה, ומה אפשר להציל ממנה? איך אפשר להכליל את התוצאה בכל זאת לתחומי שלמות (אוקלידיים) אחרים?

דוגמא 7.1.5 תהי $q = q(x_1, x_2)$ תבנית אנאיזוטרופית בינארית מעל F. אז $A\lambda^2 + 2B\lambda + C \in D_{F(\lambda)}(q)$ אם ורק אם $A \in D_F(q)$ ו־$AC - B^2 = \det(q)$.

הוכחה. נניח ש־$p(\lambda) = A\lambda^2 + 2B\lambda + C$ הוא פולינום ריבועי. אם p הוא ערך של התבנית מעל $F(\lambda)$, אז לפי משפט קסלס־פיסטר p הוא ערך מעל $F[\lambda]$. לפי טיעון המונוס העליון 2.4.17, $p(\lambda) = q(a\lambda + b, c\lambda + d)$. חישוב ישיר מראה שבמקרה זה $(A, B, C) = (q(a, c), 2b_q((a, c), (b, d)), q(b, d))$. במלים אחרות, מקדמי הפולינום הם מקדמי התבנית ביחס לבסיס החדש. לכן $A\lambda^2 + 2B\lambda + C$ הוא ערך של q אם ורק אם $q \cong Ax_1^2 + 2Bx_1x_2 + Cx_2^2$. לפי טענה 3.3.9, זה קורה אם ורק אם $A \in D_F(q)$ ו־$AC - B^2 = \det(q)$.

תרגיל 7.1.6 ידוע אלו ערכים רציונליים אפשר להביע כסכום של שני ריבועים (רציונליים). השתמש בדוגמא 7.1.5 כדי לתאר אלו פולינומים ממעלה שניה אפשר להביע כסכום של שני ריבועים מעל $\mathbb{Q}(\lambda)$.

בעיה 7.1.7 התבנית $q = \langle 1, 1, 1 \rangle$ יודעת להציג את הפולינום

$$8\lambda^2 + 4\lambda + 9 = 2^2 + \left(\frac{2(\lambda^3 - \lambda^2 - 1)}{\lambda^2 + 1}\right)^2 + \left(\frac{2\lambda^3 + 3\lambda^2 + 2\lambda + 1}{\lambda^2 + 1}\right)^2$$

מעל $\mathbb{Q}(\lambda)$. מצא הצגה של אותו פולינום כסכום של שלושה ריבועים גם מעל $\mathbb{Q}[\lambda]$, כפי שהמשפט מבטיח שאפשר לעשות. הוכח (בעזרת תרגיל 7.1.5) שאי אפשר להציג את $8\lambda^2 + 4\lambda + 9$ כסכום של שני ריבועים.

בעיה 7.1.8 יהי $g(\lambda) \in F[\lambda]$ ערך מעל $F(\lambda)$ של תבנית איזוטרופית q מעל F. אז המעלה של כל גורם אי־פריק של g היא זוגית. **הדרכה.** תרגיל 2.4.21.

בעיה 7.1.9 מצא תבנית ריבועית מעל F עם ערך פולינומי מעל $F(x, y)$ שאינו ערך מעל $F[x, y]$. **פתרון**. ראה [18, p. 9] לפתרון מפורש (המיוחס למוצקין (Motzkin), 1967):

$$p(x, y) = 1 - 3x^2y^2 + x^4y^2 + x^2y^4 = \left(\frac{1 + x^2 - 2x^2y^2}{1 + x^2}\right)^2 + \left(1 + x^2 + y^2\right) x^2y^2 \left(\frac{1 - x^2}{1 + x^2}\right)$$

הוא סכום של ארבעה ריבועים מעל $\mathbb{Q}(x)[y]$, אבל לא מעל $\mathbb{Q}[x, y]$. (ראה [14, Equation 9.6] ופרק 3 ב־[19]).

מסקנה 7.1.10 (עקרון ההצבה) תהי q תבנית מעל F, ויהי $g(\lambda_1, \ldots, \lambda_m) \in F[\lambda_1, \ldots, \lambda_m]$ פולינום שהוא ערך של q מעל $F(\lambda_1, \ldots, \lambda_m)$. אז לכל $\alpha_1, \ldots, \alpha_m \in F$, גם $g(\alpha_1, \ldots, \alpha_m)$ הוא ערך של התבנית מעל F.

(התוצאה אינה מיידית: נניח שאפשר להציג $g(\vec{\lambda}) = q(u_1(\vec{\lambda}), \ldots, u_n(\vec{\lambda}))$, עם $u_i(\vec{\lambda}) \in F(\vec{\lambda})$; לא ברור שאפשר להציב $\lambda_i \mapsto \alpha_i$, שמא ההצבה מאפסת את המכנה של אחד ה־u_i.)

הוכחה. לפי משפט קסלס־פיסטר, אפשר להציג את q מעל החוג $F(\lambda_1, \ldots, \lambda_{m-1})[\lambda_m]$; כעת אפשר להציב $\lambda_m \mapsto \alpha_m$, ובאינדוקציה מתקבלת הצגה של הערך $p(\alpha_1, \ldots, \alpha_m)$. □

7.1.3 סכום הריבועים הגנרי

משפט 7.1.11 (צמצום משתנה) *נניח ש־$q \perp \langle d\rangle$ תבנית אנאיזוטרופית מעל F, ויהי $a \in F^\times$. אז $a \in D_F(q)$ אם ורק אם $a + d\lambda^2 \in D_{F(\lambda)}(q \perp \langle d\rangle)$.*

הוכחה. כיוון אחד טריוויאלי: אם $a = q(c_1, \dots, c_n)$, אז $a + d\lambda^2 = q(c_1, \dots, c_n) + d\lambda^2$ הוא ערך של התבנית $q \perp \langle a\rangle$. כעת נניח שאפשר להציג את $a + d\lambda^2$ מעל $F(\lambda)$. לפי משפט קסלס־פיסטר אפשר להציג את $a + d\lambda^2$ גם מעל $F[\lambda]$, כלומר קיימים פולינומים $f_1, \dots, f_n, g$ כך ש־$q(f_1, \dots, f_n) + dg^2 = a + d\lambda^2$. לפי טיעון המונום העליון 2.4.17, g לינארית. נבחר $\alpha \in F$ הפותר את אחת המשוואות $g(\lambda) = \pm\lambda$. כך $g(\alpha) = \pm\alpha$, וכשנציב $\alpha \mapsto \lambda$ נקבל $q(f_1(\alpha), \dots, f_n(\alpha)) = a$. □

תרגיל 7.1.12 בדוק מה קורה במשפט אם התבנית $q \perp \langle a\rangle$ איזוטרופית.

תרגיל 7.1.13 בדוק מה קורה במשפט אם $\mathrm{char} F = 2$ (למשל, יתכן ש־$g(\lambda) = \lambda + 1$).

תרגיל 7.1.14 הסק את המשפט מן המקרה הפרטי $d = 1$.

טענה 7.1.15 יהי F שדה ממשי. לכל $a \in F^\times$, $\mathrm{len}_{F(\lambda)}(a + \lambda^2) = 1 + \mathrm{len}_F(a)$.

הוכחה. נסמן $n = \mathrm{len}_F(a)$. ברור ש־$\mathrm{len}_{F(\lambda)}(a + \lambda^2) \le 1 + n$. בכיוון ההפוך, נניח שאפשר להציג את $a + \lambda^2$ כסכום של n ריבועים מעל $F(\lambda)$. התבנית $n \cdot \langle 1\rangle$ אנאיזוטרופית מעל F לפי ההנחה, ולכן אפשר להפעיל את משפט 7.1.11 על $q = (n-1)\cdot\langle 1\rangle$ ולקבל הצגה של a כסכום של $n-1$ ריבועים, בסתירה להנחה. □

בעיה 7.1.16 תן דוגמא לשדה שאינו ניתן לסידור, עם $a \in F^\times$ כך ש־$\mathrm{len}_{F(\lambda)}(a+\lambda^2) = \mathrm{len}_F(a)$.
פתרון. נניח ש־$i = \sqrt{-1} \in F$ אבל $\sqrt{2} \notin F$. אז $2 + \lambda^2 = (1 + \frac{1+i}{4}\lambda^2)^2 + (1 + \frac{1-i}{4}\lambda^2)^2$ ולכן $\mathrm{len}(2 + \lambda^2) = \mathrm{len}(2) = 2$.

מסקנה 7.1.17 יהי F שדה ממשי. אז האורך של $\lambda_1^2 + \dots + \lambda_n^2$ בשדה $F(\lambda_1, \dots, \lambda_n)$ הוא n.

כלומר, יש סכומים של n ריבועים שאי אפשר להציג כסכום של פחות מ־n ריבועים.

7.2 ערכים גנריים

נסמן $\Lambda = (\lambda_1, \dots, \lambda_n)$, כאשר $\lambda_1, \dots, \lambda_n$ הם משתנים טרנסצנדנטיים מעל F. בדרך כלל n יהיה ברור מההקשר. כך למשל $F(\Lambda) = F(\lambda_1, \dots, \lambda_n)$ הוא ההרחבה הטרנסצנדטית הטהורה מדרגה n של F. אם $q = \langle a_1, \dots, a_n\rangle$ תבנית מממד n מעל F, אז $q(\Lambda)$ מציין את **הערך הגנרי** $a_1\lambda_1^2 + \dots + a_n\lambda_n^2$. בפרט, $q(\Lambda) \in D_{F(\Lambda)}(q)$.

המשפט הבא מתאר את כל תת־התבניות של תבנית אנאיזוטרופית ρ, במונחי הערכים ש־ρ יכולה להציג באופן גנרי.

משפט 7.2.1 (משפט תת־התבנית) *תהיינה ρ, σ תבניות ריבועיות מעל F, ונניח ש־ρ אנאיזוטרופית. התנאים הבאים שקולים:*

1. *σ היא תת־תבנית של ρ.*
2. *$D_K(\sigma) \subseteq D_K(\rho)$ לכל הרחבת שדות K/F ("כל ערך של σ הוא ערך של ρ").*

$2'$. *$D_K(\sigma) \subseteq D_K(\rho)$ לכל הרחבת שדות טרנסצנדנטית טהורה K/F.*

3. *$\sigma(\Lambda) \in D_{F(\Lambda)}(\rho)$ ("הערך הגנרי של σ הוא ערך של ρ").*

הוכחה. ברור ש־$(3)\Leftarrow(2')\Leftarrow(2)\Leftarrow(1)$, כך שעלינו להוכיח ש־$(1)\Leftarrow(3)$. נניח ש־ $\sigma(\Lambda) \in D_{F(\Lambda)}(\rho)$, ונוכיח ש־$\sigma$ היא תת־תבנית של ρ. נכתוב $\sigma = \langle a_1, \dots, a_s \rangle$, ונתקדם באינדוקציה על הממד של ρ. אם $\rho = 0$ אין ל־ρ ערכים ובהכרח גם $\sigma = 0$. נניח ש־$a_1\lambda_1^2 + \cdots + a_s\lambda_s^2 \in D_{F(\lambda_1,\dots,\lambda_s)}(\rho)$. לפי עקרון ההצבה (מסקנה **7.1.10**), $a_1 \in D_F(\rho)$ ולכן אפשר לפרק $\rho = \langle a_1 \rangle \perp \rho'$ כאשר ρ' תבנית אנאיזוטרופית מממד נמוך משל ρ. נכתוב גם $\sigma = \langle a_1 \rangle \perp \sigma'$ ונסמן $\Lambda' = (\lambda_2, \dots, \lambda_s)$. לפי ההנחה

$$a_1\lambda_1^2 + \sigma'(\Lambda') = \sigma(\Lambda) \in D_{F(\Lambda)}(\rho) = D_{F(\Lambda')(\lambda_1)}(\langle a_1 \rangle \perp \rho'),$$

ולפי עקרון הצמצום (משפט **7.1.11**), $\sigma'(\Lambda') \in D_{F(\Lambda')}(\rho')$. זה מאפשר להפעיל את הנחת האינדוקציה, ולהסיק ש־σ' היא תת־תבנית של ρ'. לכן $\sigma = \langle a_1 \rangle \perp \sigma'$ היא תת־תבנית של $\rho = \langle a_1 \rangle \perp \rho'$. □

משפט תת־התבנית מאפשר להוכיח שתכונת הכפליות של קבוצת הערכים, שאותה הוכחנו לתבניות פיסטר (משפט 6.4.2), נכונה רק עבורן.

משפט 7.2.2 *תהי q תבנית אנאיזוטרופית מעל F ($n = \dim(q)$). אז התנאים הבאים שקולים:*

1. *q היא תבנית פיסטר.*

2. *$D_K(q)$ היא חבורה לכל שדה הרחבה K/F.*

2′. *$D_K(q)$ היא חבורה לכל הרחבה טרנסצנדנטית טהורה K/F.*

3. *$q(\lambda_1, \dots, \lambda_n) \cdot q(\lambda_1', \dots, \lambda_n') \in D_{F(\lambda_1,\dots,\lambda_n,\lambda_1',\dots\lambda_n')}(q)$.*

4. *$q(\lambda_1, \dots, \lambda_n) \in G_{F(\lambda_1,\dots,\lambda_n)}(q)$ ("הערך הגנרי הוא גורם דמיון של התבנית").*

הוכחה. $(4)\Leftarrow(1)$: מכיוון ש־q תבנית פיסטר, $q(\Lambda) \in D_{F(\Lambda)}(q) = G_{F(\lambda)}(q)$.
$(3)\Leftarrow(4)$: ברור ש־$q(\Lambda') \in D_{F(\Lambda')}(q) \subseteq D_{F(\Lambda,\Lambda')}(q) = D_{F(\Lambda,\Lambda')}(q(\Lambda) \cdot q)$ ואפשר להכפיל ולקבל $q(\Lambda)q(\Lambda') \in D_{F(\Lambda,\Lambda')}(q)$.
$(2)\Leftarrow(3)$: תהי K הרחבת שדות, ויהיו $q(u), q(v)$ ערכים של q מעל K. לפי ההנחה התבנית q מציגה את $q(\Lambda)q(\Lambda')$ מעל $F(\Lambda, \Lambda')$ ולכן גם מעל $K(\Lambda, \Lambda')$. לפי עקרון ההצבה, $q(u)q(v)$ הוא ערך של q מעל K.
$(2')\Leftarrow(2)$: ברור.
$(1)\Leftarrow(2')$: מכיוון ש־$D_F(q)$ היא חבורה, $\langle 1 \rangle$ תת־תבנית של q. תהי ρ תת־תבנית פיסטר של q בעלת ממד מקסימלי, 2^r. נניח בשלילה ש־$n > 2^r$, ונכתוב $q = \rho \perp q_0$. יהי $c \in D_F(q_0)$. נראה ש־$\rho \perp \langle c \rangle\rho = \langle\langle -c \rangle\rangle\rho$ היא תת־תבנית של q; זו סתירה למקסימליות של ρ, והוכחה לכך ש־$\dim(q) = \dim(\rho) = 2^r$, כך ש־$q \cong \rho$ היא תבנית פיסטר. כדי להוכיח ש־$\rho \perp \langle c \rangle\rho$ היא תת־תבנית של q בעזרת משפט תת־התבנית, עלינו להראות שהערך הגנרי $\rho(\Lambda) + c\rho(\Lambda')$ היא ערך של q מעל $E = F(\Lambda, \Lambda')$. ברור ש־$\rho(\Lambda), \rho(\Lambda') \in D_E(\rho)$, ומכיוון ש־$\rho$ תבנית פיסטר, גם המנה $\frac{\rho(\Lambda)}{\rho(\Lambda')} \in D_E(\rho) \subseteq D_E(q)$. מאידך $\rho(\Lambda) + c \in D_E(\rho \perp \langle c \rangle) \subseteq D_E(\rho \perp q_0) = D_E(q)$. לפי ההנחה, גם מכפלת הערכים היא ערך $\rho(\Lambda) + c\rho(\Lambda') = \frac{\rho(\Lambda)}{\rho(\Lambda')}(\rho(\Lambda) + c) \in D_E(q)$, כפי שרצינו. □

7.3 שדה הפונקציות של תבנית

יריעת האפסים של תבנית ריבועית $q = \langle a_1, \dots, a_n \rangle$ מעל F היא קבוצת הוקטורים $Z(q) = \left\{(x_1, \dots, x_n) \in F^n :\ a_1x_1^2 + \cdots + a_nx_n^2 = 0\right\}$. זו יריעה אלגברית, וקל להוכיח שהיא אי־פריקה וחלקה. לשדה הפונקציות של היריעה קוראים **שדה הפונקציות של** q; זהו שדה השברים של תחום השלמות

$$F(q) = F[\lambda_1, \dots, \lambda_n] / \langle a_1\lambda_1^2 + \cdots + a_n\lambda_n^2 \rangle,$$

שאפשר לתאר בצורה פחות סימטרית כהרחבה ריבועית של שדה טרנסצנדנטי טהור:

$$F(q) = F(\lambda_1, \dots, \lambda_{n-1})[\lambda_n] \,/\, (a_1\lambda_1^2 + \cdots + a_{n-1}\lambda_{n-1}^2 + a_n\lambda_n^2)F(\lambda_1, \dots, \lambda_{n-1}).$$

הערה 7.3.1 *Nagata, 1957* הוכיח שאם $\dim(q) > 4$, אז חוג הפונקציות $F(q)$ הוא תחום פריקות יחידה.

7.3.1 התבנית מעל שדה הפונקציות של עצמה

תהי q תבנית מעל F. אם מצמצמים את q לשדה הפונקציות $F(q)$, הנקודה $(\lambda_1, \dots, \lambda_n)$ נמצאת על יריעת האפסים $Z(q_{F(q)})$, והיא נקראת **הנקודה הגנרית** של היריעה. בפרט, הוכחנו:

טענה 7.3.2 לכל תבנית q, $q_{F(q)}$ איזוטרופית.

ולפי תכונת הפיצול של תבניות פיסטר, משפט 6.4.1:

מסקנה 7.3.3 אם φ תבנית פיסטר אז $\varphi_{F(\varphi)}$ היפרבולית.

טענה 7.3.4 $F(q)$ היא הרחבה טרנסצנדנטית טהורה של F אם ורק אם q איזוטרופית.

הוכחה. אם q איזוטרופית אז אפשר לפרק $q = h \perp q'$ כאשר h היא תבנית היפרבולית דו־ממדית. על־ידי החלפת משתנים אפשר להניח שהרכיב הזה הוא התבנית $h(x,y) = xy$. לכן $F(q)$ מוגדר על־ידי היחס $\lambda_1\lambda_2 + q'(\lambda_3, \dots, \lambda_n) = 0$, שפתרונו $\lambda_1 = -\lambda_2^{-1}q'(\lambda_3, \dots, \lambda_n)$. לכן $F(q)$ טרנסצנדנטי מסדר $n-1$.

מאידך, אם q אינה איזוטרופית, לא יתכן ש־$F(q)$ הרחבה טרנסצנדנטית טהורה, משום שבמקרה זה q היתה אנאיזוטרופית מעל $F(q)$ לפי 2.4.1, בסתירה לטענה 7.3.2. $\square$

7.3.2 התפצלות מעל שדה פונקציות

תהי q תבנית אנאיזוטרופית. כפי שראינו (טענה 7.3.2), $q_{F(q)}$ נעשית איזוטרופית. עובדה זו מעוררת שאלה טבעית: מתי נעשית $q_{F(q)}$ היפרבולית? לפי מסקנה 7.3.3, ברור שזה המצב אם q תבנית פיסטר. מתברר שתכונת הפיצול הזו מאפיינת תבניות פיסטר עד כדי "דמיון". נאמר ששתי תבניות q, q' הן **דומות** אם קיים a כך ש־$q' \cong \langle a \rangle \cdot q$.

תרגיל 7.3.5 הראה שלשתי תבניות דומות יש אותו שדה פונקציות.

טענה 7.3.6 *תהיינה q, φ תבניות, $n = \dim(\varphi)$, כך ש־$1 \in D(\varphi)$. נניח ש־q נעשית היפרבולית מעל $F(\varphi)$. אז הנקודה הגנרית של φ היא גורם דמיון של q מעל $E = F(\Lambda)$.*

הוכחה. לפי ההנחה אפשר לכתוב $\varphi = \varphi' \perp \langle 1 \rangle$. נסמן $\Lambda' = (\lambda_1, \dots, \lambda_{n-1})$. בהרחבה $E' = F(\Lambda')$ של F נסמן $\Delta = \varphi'(\Lambda')$. שדה הפונקציות של φ הוא $F(\varphi) = E'[\sqrt{-\Delta}]$. אפשר להניח ש־$q$ אנאיזוטרופית. לכן היא נשארת אנאיזוטרופית מעל E' (טענה 2.4.1), ונעשית היפרבולית בהרחבה הריבועית $E'[\sqrt{-\Delta}]/E'$. לפי משפט 2.4.3, נובע מזה ש־$q_{E'}$ מתחלקת ב־$\langle\langle -\Delta \rangle\rangle = \langle 1, \Delta \rangle$. תבנית ריבועית זו מציגה את $\Delta + \lambda_n^2$. לכן $\Delta + \lambda_n^2 \in D(\langle\langle -\Delta \rangle\rangle_{E'}) = G(\langle\langle -\Delta \rangle\rangle_{E'}) \subseteq G(q_{E'})$, והרי $\Delta + \lambda_n^2$ היא הנקודה הגנרית של φ. $\square$

משפט 7.3.7 *תהי q תבנית לא היפרבולית מעל F. אם q נעשית היפרבולית מעל $F(q)$, אז q דומה לתבנית פיסטר.*

הוכחה. אם q איזוטרופית, אז $F(q)$ טרנסצנדנטי ולפי טענה 2.4.1 מכך ש־$q_{F(q)}$ היפרבולית נובע שגם q היפרבולית.

נניח, אם כך, ש־q אנאיזוטרופית. ככל תבנית, q דומה לתבנית המציגה את 1, ואפשר להחליף את q בתבנית הזו. לכן הנקודה הגנרית של q היא גורם דמיון של q (טענה 7.3.6), ולפי משפט 7.2.2 נובע מזה ש־q תבנית פיסטר. $\square$

הערה 7.3.8 תהיינה φ, q תבניות מעל F, כך ש־$\dim \varphi \leq 2^n < \dim q$ לאיזשהו n, ונניח ש־q אנאיזוטרופית. אם φ איזוטרופית מעל $F(q)$, אז היא איזוטרופית מעל F *[7, Thm. 26.5]*.

משפט 7.3.7 מעורר שאלה כללית יותר: מה קורה לתבנית q_1 מעל שדה הפונקציות של התבנית q_2? אילו תבניות נעשות היפרבוליות מעל שדה הפונקציות של התבנית q?

מסקנה 7.3.9 תהי φ תבנית. נניח שתבנית q נעשית היפרבולית מעל $F(\varphi)$. אז לכל $a \in D_F(q)$ ו־$c \in D_F(\varphi)$, q מכילה תת־תבנית איזומורפית ל־$\langle ac\rangle \cdot \varphi$.

הוכחה. נסמן $n = \dim(\varphi)$. לפי טענה 7.3.6, הנקודה הגנרית של $\varphi\langle c\rangle$ היא גורם דמיון של q מעל השדה החופשי $E = F(\lambda_1,\dots,\lambda_n)$. כלומר $q \cong q \cdot c\varphi(\lambda_1,\dots,\lambda_n)$. מכאן ש־$ac\varphi(\lambda_1,\dots,\lambda_n) \in D(q)$, ומכיוון ש־$q$ אנאיזוטרופית, משפט תת־התבנית 7.2.1 קובע ש־$\varphi\langle ac\rangle$ היא תת־תבנית של q. $\Box$

מסקנה 7.3.10 תהיינה q,φ תבניות, כאשר φ תבנית פיסטר לא היפרבולית. אם $F(q) \cong F(\varphi)$ (כשדות מעל F) אז q דומה ל־φ.

הוכחה. לפי ההנחה φ נעשית היפרבולית מעל $F(q)$, ומכאן ש־q מחלק את φ. אבל האיזומורפיזם מספק שוויון לדרגות הטרנסצנדנטיות, ומכאן גם לממדים של q, φ. $\Box$

משפט 7.3.11 *תהי φ תבנית פיסטר, ותהי q תבנית אנאיזוטרופית כלשהי. אז $q_{F(\varphi)}$ היפרבולית אם ורק אם φ מחלקת את q.*

הוכחה. ראשית נניח ש־φ מחלקת את q. אז q נעשית היפרבולית מעל $F(\varphi)$ משום שכבר φ נעשית שם היפרבולית (מסקנה 7.3.3). בכיוון ההפוך, נניח ש־q נעשית היפרבולית מעל $F(\varphi)$. נבחר $a_1 \in D_F(q)$. לפי מסקנה 7.3.9, אפשר לפרק $q = \langle a_1\rangle\varphi \perp q'$. מעל שדה הפונקציות $F(\varphi)$, גם q וגם $\langle a_1\rangle\varphi$ נעשות היפרבוליות. לכן גם q' נעשית שם היפרבולית. לפי הנחת האינדוקציה φ מחלק את q' ולכן את q. $\Box$

מסקנה 7.3.12 אם φ תבנית פיסטר, אז $\mathrm{Ker}(W(F)\to W(F(\varphi)) = \varphi \cdot W(F)$.

הערה 7.3.13 תהי q תבנית אנאיזוטרופית; נסמן $F_1 = F(q)$. כפי שראינו (טענה 7.3.2), q_{F_1} נעשית איזוטרופית, ולכן יש לה חלק אנאיזוטרופי $q_1 = (q_{F_1})_{an}$, שהממד שלו קטן משל q. כעת אפשר להגדיר $F_2 = F_1(q_1)$, $q_2 = ((q_1)_{F_2})_{an}$, וכן הלאה. מכיוון ש־

$$\dim(q) > \dim(q_1) > \dim(q_2) > \cdots,$$

הסדרה מתאפסת עד מהרה עם $q_{\ell+1} = 0$. היינו, q_ℓ נעשית היפרבולית מעל שדה הפונקציות שלה, ולפי משפט 7.3.7 היא תבנית פיסטר. הממדים של התבניות $q, q_1, q_2, \dots$ והסדר של q_ℓ הם נושא חשוב במחקר המודרני של תבניות ריבועיות.

7.4 מסנן החזקות של $I(F)$

משפט 7.4.1 (ארסון־פיסטר (Arason-Pfister)) *הממד של תבנית לא היפרבולית $q \in I^n(F)$ הוא לפחות 2^n. אם יש שוויון, אז q דומה לתבנית פיסטר מסדר n.*

האידיאל $I^n(F)$ נוצר על־ידי תבניות פיסטר מממד 2^n. הבעיה היא כמובן שבסכום של תבניות עלול להופיע צמצום חלקי; ראה בעיה 7.4.2.

(במקרה הלא מפותל ההוכחה קלה. נניח ש־q אינה מפותלת. אז יש סדר שעבורו הסימן של q שונה מאפס (משפט 5.5.8); אבל הסימן של כל תבנית ב־$I^n(F)$ מתחלק ב־2^n (הערה 5.5.20). לכן הערך המוחלט של הסימן הוא לפחות 2^n, וזה חסם תחתון לממד.)

הוכחה. לפי ההנחה אפשר לכתוב את q כצירוף שלם $q = \epsilon_1\varphi_1 \perp \cdots \perp \epsilon_r\varphi_r$ של תבניות פיסטר φ_i מסדר n, כאשר $\epsilon_i = \pm 1$. ההוכחה היא באינדוקציה על r. אם $r = 1$ סיימנו, ולכן נניח ש־$r > 1$. נתבונן בשדה $F' = F(\varphi_r)$. מכיוון ש־φ_r נעשית היפרבולית מעל F' (מסקנה 7.3.3),

$$q_{F'} \cong \epsilon_1(\varphi_1)_{F'} \perp \cdots \perp \epsilon_{r-1}(\varphi_{r-1})_{F'};$$

בנוסף $q_{F'} \in I^n(F')$, ולכן אפשר להפעיל את הנחת האינדוקציה: אם $q_{F'}$ אינה היפרבולית, אז $\dim(q) = \dim(q_{F'}) \geq 2^n$. מצד שני אם $q_{F'}$ היפרבולית, אז לפי משפט 7.3.11, q היא כפולה של φ והממד שלה מתחלק ב־2^n.

לבסוף, נניח ש־$\dim(q) = 2^n$. נתבונן בשדה $K = F(q)$. נסמן ב־q_0 את החלק האנאיזוטרופי של q_K. לפי טענה 7.3.2, $\dim(q_0) < \dim(q_K) = \dim(q) = 2^n$, ולפי החלק הראשון של המשפט $q_0 = 0$. כלומר, q_K היפרבולית, ולפי משפט 7.3.7 זה אומר ש־q דומה לתבנית פיסטר. $\square$

בעיה 7.4.2 מצא ב־$I^2(F)$ תבנית אנאיזוטרופית ממימד 6 (והסק ש־2^n אינו בהכרח מחלק את הממד של תבנית ב־$I^n(F)$).

מסקנה 7.4.3 $\bigcap_{n\geq 1} I^n(F) = 0$.

בעיה 7.4.4 הראה שהטופולוגיה ה־I אדית (שבסיס שלה הוא ההזזות $q + I^n(F)$) מקיימת את תכונת ההפרדה T_1. תהי K/F הרחבה. הראה שהעתקת הצמצום $W(F){\rightarrow}W(K)$ רציפה. נסמן $T = \mathrm{Ker}(W(F){\rightarrow}W(K))$. הראה ש־$T = \mathrm{Ker}(WF{\rightarrow}WK)$ הוא אידיאל סגור. הסק ש־$\bigcap_{n\geq 1}(T + I^n(F)) = T$.

ממשפט ארסון־פיסטר נובע שתבניות פיסטר שונות מסדר n שונות זו מזו גם במנה I^n/I^{n+1}:

מסקנה 7.4.5 תהיינה φ, ψ תבניות פיסטר מסדר n. אם $\varphi \equiv \psi \pmod{I^{n+1}}$ אז $\psi \cong \varphi$.

הוכחה. **לפי ההנחה $\varphi + \langle -1\rangle\psi \in I^{n+1}$ $\varphi' - \psi' \sim \mathbb{H} + \varphi' + \langle -1\rangle\psi' \cong$. זה מוכיח לפי משפט ארסון־פיסטר 7.4.1 ש־$\varphi' - \psi' \sim 0$, כלומר $\varphi' \cong \psi'$ ו־$\varphi \cong \psi$.** $\square$

פרק 8

אריתמטיקה של תבניות ריבועיות

פרק זה כלול בחוברת למרות שאינו מוכן לפרסום.

התורה האריתמטית של תבניות ריבועיות עוסקת במיון של תבניות מעל "השדות האריתמטיים", כלומר אלו שקרובים במובנים שונים לשדה המספרים הרציונליים. שאלה חשובה נוספת באריתמטיקה, שיש לה משקל היסטורי משמעותי, היא השאלה אלו ערכים (שלמים) אפשר לבטא באמצעות תבנית נתונה.

הערה 8.0.6 תהי φ תבנית רגולרית מעל שדה F, ויהי $a \in F^\times$. אז φ מציגה את a אם ורק אם $\varphi \perp \langle -a \rangle$ איזוטרופית. (אכן, אם φ איזוטרופית היא מציגה כל ערך, ואם היא אנאיזוטרופית אבל $\varphi \perp \langle -a \rangle$ איזוטרופית, זה בהכרח משום ש־a הוא ערך של φ.)

8.1 תבניות מעל שדות סופיים

טענה 8.1.1 יהי F שדה סופי.

א. אם $|F| \equiv 1 \pmod 4$ אז $W(F) \cong \mathbb{F}_2[\epsilon \mid \epsilon^2 = 0]$.

ב. אם $|F| \equiv -1 \pmod 4$ אז $W(F) \cong \mathbb{Z}/4\mathbb{Z}$.

הוכחה. **כידוע $F^\times/F^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$. יהי $s \in F^\times$ איבר שאינו ריבוע.**

1. נניח ש־$|F| \equiv 1 \pmod 4$. מכיוון ש־-1 הוא ריבוע, $\langle 1, 1 \rangle$ איזוטרופית ולכן היפרבולית, כך ש־$W(F) = \{0, \langle 1 \rangle, \langle s \rangle, \langle 1, s \rangle\}$. מכיוון ש־$\langle s \rangle^2 = \langle 1 \rangle$, החוג איזומורפי ל־$\mathbb{F}_2[\epsilon \mid \epsilon^2 = 0]$, עם $\epsilon = \langle 1, s \rangle$.

2. נניח ש־$|F| \equiv -1 \pmod 4$. אפשר לקחת $s = -1$. כפל בריבועים מפרק את F לשלושה מסלולים: ריבועים, לא־ריבועים ואפס. נתבונן בקבוצה $A = F^{\times 2} + F^{\times 2}$, שהיא איחוד של מסלולים. היא אינה מכילה את אפס כי -1 אינו ריבוע; היא מכילה את כל הריבועים, אבל לא רק אותם משום ש־$F^{\times 2}$ סגורה לכפל ולכן אינה סגורה לחיבור (היא אינה תת־שדה). מכאן ש־$-1 \in F^\times = F^{\times 2} + F^{\times 2}$. לכן $\langle -1, -1 \rangle \cong \langle 1, 1 \rangle$ (לפי מסקנה 3.3.11), אבל תבנית זו אינה איזוטרופית, ומכאן ש־$W(F) \cong \mathbb{Z}/4\mathbb{Z}$; אכן $W(F) = \{0, \langle 1 \rangle, \langle -1 \rangle, \langle 1, 1 \rangle\}$.

□

מסקנה 8.1.2 לכל שדה סופי F, $I^2(F) = 0$.

מסקנה 8.1.3 מעל שדה סופי, כל תבנית ממימד 3 (או יותר) היא איזוטרופית. בפרט, כל תבנית ממימד 2 (או יותר) מעל שדה סופי היא **אוניברסלית**, כלומר מציגה כל ערך שונה מאפס.

דוגמא 8.1.4 נתבונן בהרחבה $\mathbb{F}_{25}/\mathbb{F}_5$. מכיוון ש־2 אינו ריבוע ב־$\mathbb{F}_5$, $W(\mathbb{F}_5) \cong \mathbb{F}_2[\epsilon \mid \epsilon^2 = 1]$ עם הזיהוי $\epsilon = \langle 2 \rangle$. בדומה לזה $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{2}]$ ו־$\sqrt{2}$ אינו ריבוע ב־$\mathbb{F}_{25}$ (כי אם $t^2 = \sqrt{2}$ אז $t^{24} = (t^8)^3 = (-1)^3 = -1$), ולכן $W(\mathbb{F}_{25}) \cong \mathbb{F}_2[\epsilon' \mid \epsilon'^2 = 1]$ עם הזיהוי $\epsilon' = \langle \sqrt{2} \rangle$. ראה גם תרגיל 8.1.1. העתקת הצמצום $R \to R'$ שולחת $\epsilon \mapsto 1$, ולכן התמונה שלה היא $\{0, \langle 1 \rangle\}$, והגרעין הוא האידיאל הנוצר על־ידי $\epsilon + 1 = \langle 1, 2 \rangle$.

בעיה 8.1.5 הוכח שיש שלושה חוגים עם יחידה עם ארבעה אברים. הראה שאחד מהם (החוג $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$) אינו יכול להיות חוג ויט של אף שדה.

אתגר 8.1.6 קבע אלו חוגים בני שמונה אברים עשויים להיות חוגי ויט של שדה כלשהו (ממאפיין שונה מ־2).

אתגר 8.1.7 תאר את כל השדות F שחוג ויט שלהם איזומורפי לזה של שדה סופי.

8.2 תבניות מעל שדות מקומיים

8.2.1 שדות עם הערכה

הגדרה 8.2.1 ***הערכה בדידה*** *(מדרגה 1) של שדה F היא פונקציה $\nu : F \to \mathbb{Z} \cup \{\infty\}$ כך ש־$\nu(0) = \infty$ ו־$\nu(a) \in \mathbb{Z}$ בכל מקרה אחר, המקיימת לכל $a, b \in F^\times$:*

1. $\nu(ab) = \nu(a) + \nu(b)$;
2. $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$.

דוגמא 8.2.2 יהי R תחום פריקות יחידה, עם איבר ראשוני $p \in R$. יהי $F = \mathrm{q}(R)$ שדה השברים. לכל איבר $a \in R$ אפשר להגדיר $\nu_p(a) = \max\{n :\ a \in Rp^n\}$. הפונקציה ν_p היא הערכה בדידה.

כך מתקבלות **ההערכה ה־p־אדית** של $\mathbb{Q}$ (עבור p ראשוני) וההערכה ה־p־אדית של $F[\lambda]$ (עבור p פולינום אי־פריק).

הגדרה 8.2.3 *יהי F שדה עם הערכה בדידה $\nu : F^\times \to \mathbb{Z}$.* ***חוג השלמים*** *של ν הוא*

$$O_\nu = \{a \in F :\ \nu(a) \geq 0\}.$$

אידיאל ההערכה *הוא*

$$I_\nu = \{a \in F :\ \nu(a) > 0\}.$$

שדה השאריות *של F הוא שדה המנה O_ν / I_ν. איבר $\pi \in I_\nu$ עם ערך מינימלי נקרא* ***יוניפורמיזר*** *(בדרך כלל מנרמלים את ההערכה כך ש־$\nu(\pi) = 1$).*

תרגיל 8.2.4 כפי שהשמות רומזים, F הוא שדה השברים של O_ν; O_ν הוא חוג מקומי ש־I_ν הוא האידיאל המקסימלי שלו; $\bar{F}$ הוא אכן שדה.

תרגיל 8.2.5 יהי $a \in F$. אז a הוא איבר הפיך ב־O_ν אם ורק אם $\nu(a) = 0$.

תרגיל 8.2.6 כחבורה כפלית אפשר לפרק $F^\times = \pi^{\mathbb{Z}} O_\nu^\times$. כלומר, לכל $a \in F^\times$ יש $\ell \in \mathbb{Z}$ יחיד ו־$u \in O_\nu^\times$ יחיד כך ש־$a = \pi^\ell u$.

8.2.2 שדות שלמים ושדות מקומיים

יהי F שדה עם הערכה בדידה. ההערכה משרה על F מטריקה, באופן הבא. נקבע $0 < \gamma < 1$, ונגדיר $d(a,b) = \gamma^{\nu(a-b)}$.

תרגיל 8.2.7 זו אכן מטריקה.

תרגיל 8.2.8 הטופולוגיה המטרית אינה תלויה בערך של γ.

ככל ש־$\nu(a)$ גדול יותר, a קרוב יותר לאפס. למשל, אם π יוניפורמיזר, אז $\pi^n \to 0$. המטריקה מגדירה בשדה סדרות קושי. השדה הוא **שדה שלם** (ביחס להערכה ν) אם כל סדרת קושי מתכנסת.

דוגמא 8.2.9 השדות המקומיים (סעיף 8.2.5) הם שלמים. דוגמא נוספת: לכל שדה k, $F = k((t))$ הוא שלם ביחס להערכה $\nu(\sum_{i=N}^{\infty} a_i t^i) = N$ כאשר $a_N \neq 0$.

תרגיל 8.2.10 אם $x_1, x_2, \ldots$ סדרת קושי ו־$\nu(x_n) \geq 0$ עבור n מספיק גדול, אז $\lim x_n \in O_\nu$. כלומר, חוג השלמים O_ν הוא מרחב מטרי שלם ("חוג השלמים הוא חוג שלם").

השלמה של שדות

בהמשך נראה שהאריתמטיקה של שדה שלם היא פשוטה יחסית. למרבה הנוחות, כל שדה עם הערכה מוכל בשדה שלם יחיד.

טענה 8.2.11 יהי F שדה עם הערכה. אז יש שדה שלם $\hat{F}$ שכל איבר בו הוא גבול של סדרת קושי של אברים מ־F. ההערכה מוגדרת בשדה הזה לפי $\nu(\lim a_n) = \lim \nu(a_n)$; הסדרה באגף ימין מתכנסת בטופולוגיה הדיסקרטית של $\mathbb{Z}$, משום שהיא קבועה לבסוף. השדה $\hat{F}$ יחיד עד כדי איזומורפיזם של שדות עם הערכה.

משפט 8.2.12 (משפט אוסטרובסקי (Ostrovsky)) *ההערכות הבדידות היחידות של $\mathbb{Q}$ הן ההערכות ה־p־אדיות.*

הערה 8.2.13 כתוצאה ממשפט אוסטרובסקי 8.2.12, ההשלמות היחידות של $\mathbb{Q}$ לשדות שלמים בטופולוגיה מטרית שתחתיה פעולות השדה רציפות, הן $\mathbb{Q}_p$ עבור p ראשוני, ו־$\mathbb{R}$. (ההשלמה ל־$\mathbb{R}$ קשורה **בערכים מוחלטים ארכימדיים**, מושג שלא נבאר כאן; כל הערכה בדידה משרה ערך מוחלט לא ארכימדי).

שדות מקומיים

נפגוש כעת מחלקה חשובה של שדות שלמים. נזכיר שמרחב מטרי הוא **קומפקטי מקומית** אם לכל נקודה יש סביבה פתוחה שהסגור שלה קומפקטי.

הגדרה 8.2.14 *שדה עם הערכה בדידה הוא **מקומי** אם הוא קומפקטי מקומית (בטופולוגיה המטרית המושרית על־ידי ההערכה).*

תרגיל 8.2.15 שדה מקומי הוא בהכרח שלם.

טענה 8.2.16 יהי F שדה שלם. הוא מקומי אם ורק אם $\bar{F}$ הוא שדה סופי.

הגדרה 8.2.17 *$\mathbb{Q}_p$, **שדה המספרים ה־p־אדיים**, הוא ההשלמה של $\mathbb{Q}$ ביחס להערכה ה־p־אדית ν_p.*

את חוג השלמים של $\mathbb{Q}_p$ מסמנים ב־$\mathbb{Z}_p$. שימו לב ש־$\operatorname{char}\mathbb{Q}_p = 0$: זוהי הרחבה של $\mathbb{Q}$.

משפט 8.2.18 *כל שדה מקומי הוא אחד מהשדות הבאים:*

1. *הרחבה סוף־ממדית של $\mathbb{Q}_p$, עם ההערכה (היחידה) הממשיכה את ההערכה ה־p־אדית.*
2. *השדה של טורי לורן מעל שדה סופי, היינו $\mathbb{F}_q((t))$, עם ההערכה $\nu(\sum a_i t^i) = \min\{i : a_i \neq 0\}$.*

בעיה 8.2.19 אם F שדה מקומי, אז לכל מרחב ריבועי (V,q) מתקיים $O(V,q) = O^+(V,q)$.

8.2.3 תבניות מעל חוג השלמים בשדה שלם

היתרון בשדות שלמים הוא שאפשר לפתור בהם משוואות באופן איטרטיבי. הרעיון הבסיסי הוא שכל מה שאפשר לעשות בשדה השאריות, אפשר להרים לחוג השלמים עצמו, באמצעות לינאריזציה של הבעיה בכל אחד מהמקטעים $\pi^n O_\nu/\pi^{n+1}O_\nu$. כדי שהאסטרטגיה הזו תעבוד, המשוואה צריכה להיות "ספרבילית" בשדה השאריות, וזה מסבך את הדברים עבור תבניות ריבועיות אם יש מקדמים לא הפיכים, או כאשר $\mathrm{char}F = 2$.

נדגים זאת במקרה פשוט, ואחר־כך נציג תוצאה כללית יותר.

למה 8.2.20 (הלמה של הנזל Hensel) נניח ש־$\mathrm{char}\bar{F} \neq 2$. אם $a \in O_\nu^\times$ ו־$\bar{a} \in \bar{F}^{\times 2}$ הוא איבר ריבועי, אז גם a ריבוע ב־O_ν.

הוכחה. נבנה סדרה $x_1,\dots$ באינדוקציה. עבור $n \geq 1$, נניח ש־$x_n^2 \equiv a \pmod{\pi^n}$ (לפי ההנחה x_1 קיים). כתוב $x_{n+1} = x_n + \pi^n y$, עבור y שנבחר מיד. ממילא יוצא ש־$\{x_n\}$ היא סדרת קושי. כדי לבחור את y, נחשב:

$$\begin{aligned} x_{n+1}^2 - a &= (x_n^2-a) + 2\pi^n y + \pi^{2n}y^2 \\ &\equiv x_n^2 + 2\pi^n y \\ &= \pi^n(\pi^{-n}(x_n^2-a)+2y) \pmod{\pi^{n+1}}. \end{aligned}$$

נבחר $y \in \mathcal{O}$ כך ש־$y \equiv -\frac{1}{2}\pi^{-n}(x_n^2-a) \pmod{\pi}$, ואז $x_{n+1}^2 \equiv a \pmod{\pi^{n+1}}$. הגבול $x = \lim_{n\to\infty} x_n$ מקיים $x^2 = \lim_{n\to\infty} x_n^2 = a$. □

הנה הגרסה הכללית על הרמת הצגות של תבנית ריבועית.

למה 8.2.21 תהי $q(x_1,\dots,x_t) = \sum_i a_i x_i^2$ תבנית ריבועית אלכסונית מעל O_ν. יהי $a \in O_\nu$. נניח שיש $x_1,\dots,x_t \in O_\nu$ כך ש־$q(x_1,\dots,x_t) \equiv a \pmod{4\pi}$, ויש i כך ש־$a_i x_i$ הפיך (ב־O_ν). אז q מציגה את a מעל O_ν.

הוכחה. נקבע יוניפורמיזר $\pi \in O_\nu$. ראשית, נסמן $e = \nu(2)$, כך ש־$2O_\nu = \pi^e O_\nu$ (אם $e = 0$ אז $\mathrm{char}F \neq 2$).

לכל $x_1,\dots,x_t \in \mathcal{O}_\nu$ ו־$\delta_1,\dots,\delta_t \in O_\nu$, אם נציב $x_i' = x_i + \pi^n\delta_i$, נוכל לחשב ש־

$$\begin{aligned} q(x_1',\dots,x_t') &= \sum_i a_i x_i'^2 \\ &= \sum_i a_i(x_i+\pi^n\delta_i)^2 \\ &= \sum_i a_i(x_i^2 + 2\pi^n\delta_i x_i + \pi^{2n}\delta_i^2) \\ &= q(x_1,\dots,x_t) + 2\pi^n \sum_i a_i\delta_i x_i + \pi^{2n}\sum_i a_i\delta_i^2. \end{aligned}$$

בפרט, אם $n \geq e+1$ אז $\pi^{2n} \mid 2\pi^{n+1}$, ולכן

$$q(x_1',\dots,x_t') \equiv q(x_1,\dots,x_t) + 2\pi^n \sum_i a_i\delta_i x_i \pmod{2\pi^{n+1}}.$$

נאמר שהווקטור $x_1,\dots,x_t$ הוא 'n־טוב' אם $q(x_1,\dots,x_t) \equiv a \pmod{2\pi^n}$, ויש i כך ש־$a_i x_i$ הפיך. לפי ההנחה קיים וקטור $(e+1)$־טוב, $x_1^{(e+1)},\dots,x_t^{(e+1)}$. יהי $n \geq e+1$, ונניח ש־$x_1^{(n)},\dots,x_t^{(n)}$ הוא וקטור n־טוב. כתוב $q(x_1^{(n)},\dots,x_t^{(n)}) \equiv a + 2\pi^n\theta \pmod{2\pi^{n+1}}$ עבור $\theta \in O_\nu$ מתאים. נגדיר

$x_i^{(n+1)} = x_i^{(n)} + \pi^n\delta_i$ עבור ערכים $\delta_i \in O_\nu$ שנבחר מיד (ממילא נובע שלכל i, הסדרה $x_i^{(n)}$ היא סדרת קושי). אז

$$q(x_1^{(n+1)},\dots,x_t^{(n+1)}) \equiv q(x_1^{(n)},\dots,x_t^{(n)}) + 2\pi^n\sum_i a_i\delta_i x_i \equiv a + 2\pi^n\theta + 2\pi^n\sum_i a_i\delta_i x_i \pmod{2\pi^{n+1}}.$$

מכיוון ש-$x_1^{(n)},\dots,x_t^{(n)}$ הוא טוב, אפשר לפתור את $\theta + \sum_i a_i\delta_i x_i \equiv 0 \pmod{\pi}$ עבור $\delta_1,\dots,\delta_t \in O_\nu$, ואז $q(x_1^{(n+1)},\dots,x_t^{(n+1)}) \equiv a \pmod{2\pi^{n+1}}$ כך ש-$x_1^{(n+1)},\dots,x_t^{(n+1)}$ הוא $(n+1)$-טוב. במעבר לגבול $x_i = \lim_{n\to\infty} x_i^{(n)}$, מתקבלת הצגה של a על-ידי q מעל O_ν. □

בפרט, אם בוחרים $q = \langle 1\rangle$, מקבלים גרסה של למה 8.2.20 המכסה גם את המקרה $\mathrm{char}\bar{F} = 2$:

מסקנה 8.2.22 אם ל-$a \in \mathcal{O}^\times$ יש שורש מודולו 4π, אז יש ל-a שורש ב-$\mathcal{O}$.

מסקנה 8.2.23 בכל שדה שלם ביחס להערכה בדידה, $1 + 4\pi O \subseteq \mathcal{O}^{\times 2}$.

מסקנה 8.2.24 תהי q תבנית ריבועית אלכסונית מעל O_ν, ויהי $a \in O_\nu^\times$. אם q מציגה את a מודולו 4π, אז q מציגה את a מעל O_ν.

הוכחה. **זו גרסה של למה 8.2.21: ההנחה a אומרת שבהצגה $a \equiv \sum a_i x_i^2$ מודולו 4π, בהכרח יש $a_i x_i$ הפיך, ולכן הלמה מספקת הצגה מעל השלמים.** □

וקטור $\vec{x} = (x_1,\dots,x_n)$ מעל חוג השלמים O_ν (או חוג מנה שלו) נקרא **פרימיטיבי** אם יש לו לפחות רכיב הפיך אחד. הצגה של a באמצעות וקטור פרימיטיבי נקראת **הצגה פרימיטיבית**. מן ההומוגניות ברור שאם תבנית q המוגדרת מעל O_ν היא איזוטרופית מעל F, אז היא מציגה את אפס באופן פרימיטיבי. בשפה זו, 8.2.21 מספקת את התוצאה הבאה:

מסקנה 8.2.25 תהי q תבנית ריבועית אלכסונית מעל O_ν, הנשארת רגולרית מודולו π. יהי $a \in O_\nu$. אם q מציגה את a באופן פרימיטיבי מודולו 4π, אז q מציגה את a מעל O_ν.

מסקנה 8.2.26 תהי q תבנית ריבועית אלכסונית מעל O_ν, הנשארת רגולרית מודולו π. אם q מציגה את אפס באופן פרימיטיבי מודולו 4π, אז היא איזוטרופית.

הוכחה. **זהו המקרה $a = 0$ של מסקנה 8.2.25.** □

תרגיל 8.2.27 במסקנה 8.2.26, הדרישה שהתבנית תשאר רגולרית היא חיונית. הראה שהתבנית $\langle 1,1,\pi,\pi\rangle$ מעל $\mathbb{Q}_2[\pi \mid \pi^2 = 2]$ היא אנאיזוטרופית: למרות שהיא מציגה את אפס פרימיטיבית מודולו 4π, היא אינה יכולה להציג את אפס פרימיטיבית מודולו 8.

בעיה 8.2.28 הצע גרסה של למה 8.2.21 שתתאים לתבנית כללית, לאו דווקא אלכסונית.

בעיה 8.2.29 יהי $e \geq 1$. התבונן בשדה $\mathbb{Q}_2[\pi]/\langle \pi^e - 2\rangle$ (הקבוע e ממשפט 8.2.21 מתלכד עם הערך שניתן לו כאן). הראה ש-5 אינו ריבוע בשדה, משום שהוא אינו ריבוע מודולו 4π, למרות שהוא ריבוע מודולו 4. מכאן שהדרישה לקיום הצגה מודולו 4π במסקנה 8.2.24 היא המינימום ההכרחי להבטיח הצגה שלמה.

8.2.4 חוג ויט של שדה שלם

מסקנה 8.2.23 מאפשרת להוכיח את המשפט הבא:

משפט 8.2.30 (הלמה של פיסטר) יהי F שדה הערכה שלם. נניח ש־$\mathrm{char}\bar{F} \neq 2$. אז יש איזומורפיזם של חבורות אדיטיביות $W(F) \cong W(\bar{F}) \oplus W(\bar{F})$.

הוכחה. יהיו $\mathcal{O}$ חוג השלמים של F, $\pi \in \mathcal{O}$ יוניפורמיזר, ו־$\bar{F} = \mathcal{O}/\pi\mathcal{O}$ שדה השאריות. נגדיר העתקה $W(F) \to W(\bar{F}) \oplus W(\bar{F})$ על היוצרים, בעזרת תרגיל 8.2.6, לפי

$$\left\langle \pi^\ell u \right\rangle \mapsto \begin{array}{ll} (\langle \bar{u} \rangle\, , 0) & \ell \text{ זוגי} \\ (0\, , \langle \bar{u} \rangle) & \ell \text{ אי־זוגי} \end{array} .$$

יש לוודא שההעתקה מוגדרת היטב. נעשה זאת לפי היחסים במשפט 3.3.19. היחסים $\left\langle ac^2 \right\rangle = \langle a \rangle$ ו־$\langle 1 \rangle + \langle -1 \rangle = 0$ עוברים לטענות נכונות בתמונה. נשאר לבדוק את היחס $\langle a \rangle + \langle b \rangle = \langle a+b \rangle + \langle ab(a+b) \rangle$. נכתוב $a = \pi^\ell u$ ו־$b = \pi^{\ell'} v$ כאשר u, v שלמים הפיכים. אם $\ell < \ell'$ נסמן $w = u + \pi^{\ell'-\ell} v$; אז $w \equiv u$ מודולו ריבועים, ולכן $\langle \bar{w} \rangle = \langle \bar{u} \rangle$ ו־$\langle \bar{u}\bar{v}\bar{w} \rangle = \langle \bar{v} \rangle$. בדיקה של המקרים השונים מראה שתמיד מתקבל שוויון בתמונה. כך גם כאשר $\ell' < \ell$. נשאר המקרה $\ell = \ell'$. אם $u+v$ הפיך, אז $\langle \bar{w} \rangle + \langle \bar{u}\bar{v}\bar{w} \rangle = \langle \bar{u} \rangle + \langle \bar{v} \rangle$. אחרת, $w = \pi^t s$ עבור $s \in \mathcal{O}^\times$, ואז $\bar{u} = -\bar{v}$, $\langle \bar{u} \rangle + \langle \bar{v} \rangle = 0$ ו־$\langle \bar{s} \rangle + \langle \bar{u}\bar{v}\bar{s} \rangle = \langle \bar{s} \rangle (\langle 1 \rangle + \langle -1 \rangle) = 0$.

בכיוון ההפוך, אפשר להגדיר

$$(\langle \bar{u} \rangle, \langle \bar{v} \rangle) \mapsto \langle u, \pi v \rangle;$$

זו העתקה מוגדרת היטב (משום שכל איבר ב־$1 + \pi O_\nu$ הוא ריבוע), ההופכת את הפונקציה הקודמת, ולכן שתיהן איזומורפיזמים. □

בעיה 8.2.31 הלמה של פיסטר מגדירה (בין השאר) הומומורפיזם של חבורות $W(F) \to W(\bar{F})$ לפי $\langle u \rangle \mapsto \langle \bar{u} \rangle$ ו־$\langle \pi u \rangle \mapsto 0$. מצא הטלה מ־$W(F)$ במקרה ש־$\mathrm{char} F = 0$ ו־$\mathrm{char}\bar{F} = 2$.

נמשיך בהנחה ש־F שדה שלם, וששדה השברים $\bar{F}$ הוא ממאפיין שונה מ־2.

מסקנה 8.2.32 כל תבנית רגולרית מעל F אפשר לפרק באופן יחיד (עד כדי שקילות ויט) בצורה $q = q_0 \perp \langle \pi \rangle q_1$ כאשר q_0, q_1 הן תבניות המוגדרות מעל O_ν ונשארות רגולריות מעל $\bar{F}$.

תרגיל 8.2.33 לכל $a \in F^\times$ מתקיים $\langle\langle a \rangle\rangle^2 = 2\langle\langle a \rangle\rangle$. **הדרכה.** $\langle\langle a, a \rangle\rangle = \langle\langle -1 \rangle\rangle \langle\langle a \rangle\rangle$ לפי למה 6.3.1.(1).

טענה 8.2.34 (אם F שלם ו־$\mathrm{char}\bar{F} \neq 2$) יש איזומורפיזם של חוגים

$$W(F) \cong W(\bar{F})[\theta \mid \theta^2 = 2\theta].$$

הוכחה. האיזומורפיזם הוא $[q_0 + \langle \pi \rangle q_1] \mapsto [\bar{q_0}] + (1-\theta)[\bar{q_1}]$, ובכיוון ההפוך $\langle\langle \pi \rangle\rangle \mapsto \theta$. □

האיזומורפיזם $W(F) \to W(\bar{F})[\theta \mid \theta^2 = 2\theta]$ נושא את האידיאל היסודי $I(F)$ ל־$I(\bar{F}) + \theta W(\bar{F})$, משום ש־$\langle\langle u \rangle\rangle \mapsto \langle\langle \bar{u} \rangle\rangle$ ו־$\langle\langle \pi u \rangle\rangle \mapsto \langle\langle \bar{u} \rangle\rangle + \langle \bar{u} \rangle \theta$. כך אפשר לחשב את החזקות: לכל $n \geq 1$,

$$I^n(F) \mapsto I^n(\bar{F}) + I^{n-1}(\bar{F})\theta.$$

מסקנה 8.2.35 יהי F שדה שלם עם $\mathrm{char}\bar{F} \neq 2$. אז

$$I^n(F)/I^{n+1}(F) \;\cong\; I^n(\bar{F})/I^{n+1}(\bar{F}) \;\oplus\; I^{n-1}(\bar{F})/I^n(\bar{F}).$$

בעיה 8.2.36 מצא את הקשר בין העתקת השארית בלמה של פיסטר, לבין תת־סעיף 4.2.1.

בעיה 8.2.37 השמורה u של שדה F מוגדרת כממד המקסימלי האפשרי עבור תבנית אנאיזוטרופית מעל F. מסמנים אותה ב־$u(F)$. הוכח ש־$u(F((t))) = 2u(F)$, כאשר F שדה ממאפיין שונה מ־2.

8.2.5 חוג ויט של שדות מקומיים

בסעיף הזה נחשב את $W(\mathbb{Q}_p)$ כאשר $p \neq 2$ (בעזרת טענה 8.2.34), וכאשר $p = 2$ (כשהטענה אינה ישימה).

טענה 8.2.38 נתבונן בשדה $\mathbb{Q}_p$.

1. אם p אי־זוגי, $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong (\mathbb{Z}/2)^2$, כאשר החבורה נוצרת על־ידי p ואיבר $s \in \mathbb{Z}$ שאינו ריבוע מודולו p.
2. $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \cong (\mathbb{Z}/2)^3$, כשהחבורה נוצרת על־ידי $-1, 2, 3$.

דוגמא 8.2.39 יהי $p \equiv -1 \pmod 4$ ראשוני. אז כל תבנית ריבועית רגולרית מעל $F = \mathbb{Q}_p$ שקולה בדיוק לאחת מהתבניות הבאות:

$$\begin{gathered} 0; \qquad \langle 1\rangle, \langle -1\rangle, \langle p\rangle, \langle -p\rangle, \\ \langle 1,1\rangle, \langle 1,p\rangle, \langle 1,-p\rangle, \langle -1,p\rangle, \langle -1,-p\rangle, \langle p,p\rangle \\ \langle 1,p,p\rangle, \langle -1,p,p\rangle, \langle 1,1,p\rangle, \langle 1,1,-p\rangle, \\ \langle 1,1,p,p\rangle. \end{gathered}$$

בפרט (בעקבות טענה 8.2.34)

$$W(\mathbb{Q}_p) = (\mathbb{Z}/4)[\theta \,|\, \theta^2 = 2\theta],$$

כאשר $\langle 1\rangle = 1$ כרגיל, ו־$\langle\langle p\rangle\rangle = \theta$. האידיאל היסודי נוצר אדיטיבית על־ידי $2, \theta$. לכן $I^2(F) = \{0, 2\theta\}$, וכמובן $I^3(F) = 0$.

מסקנה 8.2.40 יהי $p \equiv -1 \pmod 4$ ראשוני. אז $\mathrm{k}_2(\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z}$, כאשר האיבר השונה מאפס הוא $\{p,p\}$.

הוכחה. לפי משפט 4.4.8 $\mathrm{k}_2(\mathbb{Q}_p) \cong I^2(\mathbb{Q}_p)/I^3(\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z}$, כאשר האיזומורפיזם f_2 נושא את $\{p,p\}$ ל־$\langle\langle p,p\rangle\rangle = \theta^2 \neq 0$. □

בעיה 8.2.41 כידוע, יש מישור פרוייקטיבי מכל סדר שהוא חזקת ראשוני; השאלה האם יש מישור פרוייקטיבי מסדרים אחרים, עודנה פתוחה. משפט Bruck-Ryser (1949) הוא התוצאה החזקה ביותר הידועה בכיוון זה: אם יש מישור פרוייקטיבי מסדר n כאשר $n \equiv 1,2 \pmod 4$, אז n הוא סכום של שני ריבועים. השלם את הפרטים בהוכחה (ראה [9, Thm. 5.18]):

1. נסמן $N = n^2+n+1$. נסמן ב־T את מטריצת החילה של הגאומטריה. חשב את $A = T^{\mathrm{t}}T$. לפיכך, T הוא איזומטריה של $\langle 1,\dots,1\rangle$ לתבנית המיוצגת על־ידי A.

2. נסמן $S = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ n^{-1} & 1 & & \\ \vdots & & \ddots & \\ n^{-1} & & & 1 \end{pmatrix}$. הראה ש־$S^{\mathrm{t}}\mathrm{diag}(1,n,\dots,n)S = A$, כלומר S הוא איזומטריה של $\langle 1,n,\dots,n\rangle$ לתבנית המיוצגת על־ידי A.

3. הסק ש־$(N-1)\langle 1\rangle \cong (N-1)\langle n\rangle$ מעל $\mathbb{Q}$.

4. נניח ש־$p \equiv -1 \pmod 4$ ו־$\nu_p(n)$ אי־זוגי; הסק ש־$(N-1)\langle\langle p\rangle\rangle = 0$ מעל $\mathbb{Q}_p$.

5. נניח ש־$n \equiv 1,2 \pmod 4$; אז $N-1 \equiv 2 \pmod 4$, ולכן $2\langle\langle p\rangle\rangle = 0$, בסתירה לחישוב בדוגמא 8.2.39.

בעיה 8.2.42 **גרף רגולרי בחזקה** עם הפרמטרים (v,k,λ,μ) הוא גרף k־רגולרי על v קודקודים, שבו לכל שני קודקודים סמוכים יש λ שכנים משותפים ולכל שני קודקודים שאינם שכנים יש μ שכנים משותפים. מטריצת החילה של גרף רגולרי בחזקה מקיימת את התנאים $AJ = JA = kJ$ ו־$A^2 + (\mu-\lambda)A + (\mu-k)I = \mu J$. האם אפשר להסיק מקיומו של גרף כזה איזומורפיזם לא טריוויאלי כלשהו של תבניות ריבועיות?

דוגמא 8.2.43 יהי $p \equiv 1 \pmod 4$ ראשוני. קבע $s \in \mathbb{Z}$ שאינו שארית ריבועית מודולו p. אז כל תבנית ריבועית רגולרית מעל $F = \mathbb{Q}_p$ שקולה בדיוק לאחת מהתבניות הבאות:

$$\begin{gathered} 0; \qquad \langle 1\rangle, \langle s\rangle, \langle p\rangle, \langle sp\rangle, \\ \langle 1,s\rangle, \langle 1,p\rangle, \langle 1,sp\rangle, \langle s,p\rangle, \langle s,sp\rangle, \langle p,sp\rangle \\ \langle 1,s,p\rangle, \langle 1,s,sp\rangle, \langle 1,p,sp\rangle, \langle s,p,sp\rangle, \\ \langle 1,s,p,sp\rangle. \end{gathered}$$

חוג ויט הוא $W(\mathbb{Q}_p) = (\mathbb{Z}/2)[\sigma,\theta \mid \sigma^2 = \theta^2 = 0]$, עם ההתאמה $\sigma = \langle\langle s\rangle\rangle$ ו־$\theta = \langle\langle p\rangle\rangle$. במקרה זה $I(F)$ נוצר אדיטיבית על־ידי $\sigma,\theta,\sigma\theta$. לכן $I^2(F) = \{0,\sigma\theta\}$, ושוב $I^3(F) = 0$.

טענה 8.2.44 יש 32 תבניות אנאיזוטרופיות מעל $\mathbb{Q}_2$. חוג ויט של $\mathbb{Q}_2$ הוא

$$W(\mathbb{Q}_2) \cong (\mathbb{Z}/8)[x,y \mid x^2 = y^2 = 2x = 2y = 0,\ xy = 4],$$

עם $x = \langle\langle 2\rangle\rangle$ ו־$y = \langle\langle -3\rangle\rangle$. בחוג הזה $I(\mathbb{Q}_2) = \langle 2,x,y\rangle$, $I^2(\mathbb{Q}_2) = \langle 4\rangle$ ו־$I^3(\mathbb{Q}_2) = 0$.

הוכחה. ראינו (טענה 8.2.38) ש־$\mathbb{Q}_2^{\times}/\mathbb{Q}_2^{\times 2} = \langle -1,2,3\rangle$. מכאן ש־$W(\mathbb{Q}_2)$ נוצר אדיטיבית על־ידי התבניות $1 = \langle 1\rangle$, $x = \langle\langle 2\rangle\rangle$ ו־$y = \langle\langle -3\rangle\rangle$. התבנית $\langle\langle -1,-1,-1\rangle\rangle$ היא איזוטרופית ($\sqrt{-7} \in \mathbb{Q}_2$ לפי למה 8.2.22) ולכן היפרבולית (משפט 6.4.1). מכאן ש־$8 = 0$ בחוג.

את היחסים אפשר להוכיח ישירות בעזרת ההצגות השונות לתבנית בינארית. מ־$\langle 2,2\rangle = \langle 1,1\rangle$ נובע $2x = 0$. מ־$\langle 1,1\rangle = \langle 1,4\rangle = \langle 5,5\rangle = \langle -3,-3\rangle$ נובע $2y = 0$. מ־$\langle 1,-6\rangle = \langle -2,3\rangle$ נובע $xy = \langle 1,-2,3,-6\rangle = 2\langle -2,3\rangle = 2(x+y-2) = 4$, ולבסוף $x^2 = 2x = 0$ ו־$y^2 = 2y = 0$ לפי תרגיל 8.2.33.

כדי להוכיח שכל התבניות $q = n\langle 1\rangle + \alpha\langle\langle 2\rangle\rangle + \beta\langle\langle -3\rangle\rangle$ שונות זו מזו ($n = 0,\dots,7$, $\alpha,\beta = 0,1$), אפשר להפעיל את השמורות. די להוכיח שהתבנית ההיפרבולית היחידה מתקבלת עבור $n = \alpha = \beta = 0$. $q \in I(\mathbb{Q}_2)$ אם ורק אם $n \equiv 0 \pmod 2$; ועבור תבניות ב־$I(\mathbb{Q}_2)$, $\mathrm{disc}(q) = (-1)^{n/2+\beta}2^{\alpha}3^{\beta}$, שהוא ריבוע אם ורק אם $\alpha = \beta = 0$ ו־$n \equiv 0 \pmod 4$. זה משאיר רק תבנית אחת לבדוק, $q = \langle 1,1,1,1\rangle$. אבל התבנית הזו אינה איזוטרופית כי אם יש הצגה $x_1^2 + \cdots + x_4^2 = 0$ אפשר להניח ש־$x_1,\dots,x_4 \in \mathbb{Z}_2$ ולא כולם זוגיים, אלא שזה בלתי אפשרי מודולו 8. □

בעיה 8.2.45 הוכח את הטענות הבאות לגבי התבניות האנאיזוטרופיות מעל $\mathbb{Q}_2$:

1. יש 8 תבניות ממימד 1. **הדרכה.** $\left|\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}\right|$. (בסימוני המשפט, אלו התבניות ± 1, $x \pm 1$, $y \pm 1$, $x + y \pm 3$).
2. יש 7 תבניות ממימד 2 המציגות את 1. **הדרכה.** אלו התבניות $\langle 1, -a\rangle$ עבור $\langle\langle a\rangle\rangle =$ $a \neq 1$.
3. לכל תבנית מהסעיף הקודם $G(\langle\langle a\rangle\rangle)$ היא מסדר 4 (מתקבלות שבע תת־החבורות מסדר 4 של $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$).
4. יש 14 תבניות ממימד 2. **הדרכה.** כל תבנית דומה לתבנית המציגה את 1.
5. יש בסך־הכל 16 תבניות (אנאיזוטרופיות) ממימד זוגי. **הדרכה.** עד כדי שקילות אלו הן $2m + \alpha x + \beta y$.
6. יש תבנית אנאיזוטרופית יחידה ממימד 4, והיא $\langle 1, 1, 1, 1\rangle$. **הדרכה.** $16 = 1 + 14 + 1$.
7. אין תבניות אנאיזוטרופיות ממימד 5. **הדרכה.** אם $q = \langle a_1, \dots, a_n\rangle$ אנאיזוטרופית אז כל תת־תבנית שלה אנאיזוטרופית, אבל $\langle 1, 1, 1, 1, 1\rangle$ איזוטרופית.
8. שמונה התבניות (האנאיזוטרופיות) ממימד 3 שקולות לתבניות $\langle a\rangle \perp \langle 1, 1, 1, 1\rangle$.
9. נסמן ב־A_2 את קבוצת התבניות האנאיזוטרופית ממימד 2. לכל $q \in A_2$ יש $q' \in A_2$ יחידה כך ש־$q \perp q' \cong \langle 1, 1, 1, 1\rangle$.
10. הראה שיש 26 דרכים להציג את התבנית $4\langle 1\rangle$ בצורה $\langle a_1, a_2, a_3, a_4\rangle$ (הצגות הן שקולות אם הן מתקבלות מכפל של מקדם בריבוע או מהחלפת סדר).

מסקנה 8.2.46 כל תבנית ממימד 5 מעל $\mathbb{Q}_p$ (p כלשהו) היא איזוטרופית.

(בנושא זה ראה [15, Sec. 63].)

בעיה 8.2.47 חשב את חוג ויט של $F = \mathbb{Q}_2[\sqrt{2}]$. **הדרכה.** $F^\times/F^{\times 2}$ נוצרת על־ידי $\{-1, 3, 1 + \pi, \pi\}$ כאשר $\pi = \sqrt{2}$. בחוג הזה $4 = \langle 1, 1, 1, 1\rangle = 0$ (לפי השוויון $\pi^2 + (1 + \pi)^2 + (1 + \pi)^2 \equiv 0 \pmod{4\pi}$ ומסקנה 8.2.26).

8.3 תבניות מעל שדות גלובליים

שדה גלובלי הוא שדה המקיים נוסחת מכפלה $\prod |x|_\nu = 1$ ביחס לערכים מוחלטים. כל השלמה (ביחס להערכה) של שדה כזה היא היא שדה מקומי (לוקלי). הרעיון היסודי באריתמטיקה הוא שאפשר ללמוד בעיות גלובליות על־ידי מיקום שלהן בכל הדרכים האפשריות.

משפט 8.3.1 *השדות הגלובליים הם ההרחבות הסופיות של אחד השדות $\mathbb{Q}$ או $\mathbb{F}_p(t)$.*

נתאר את המבנה של חוג ויט של $\mathbb{Q}$. התאור תקף, בשינויים המתחייבים, לכל שדה גלובלי. נסמן $W_p = W(\mathbb{F}_p)$ עבור ראשוני $p \neq 2$, $W_\infty = W(\mathbb{R}) = \mathbb{Z}$, ו־$W_2 = \mathbb{Z}/2$.

משפט 8.3.2 *כחבורות אדיטיביות, $W(\mathbb{Q}) \cong \bigoplus W_p$ כאשר הסכום כולל את הראשוניים (לרבות 2) ואת אינסוף.*

הוכחה. (בעקבות [4, p. 94]). נגדיר $\psi_\infty : W(\mathbb{Q}) \to W(\mathbb{R})$ על־ידי צמצום; $\psi_p : W(\mathbb{Q}) \to W_p$ על ידי ההטלה $\langle pu \rangle \mapsto \langle \bar{u} \rangle$ ו־$0 \mapsto \langle\langle u \rangle\rangle$ עבור $u \in \mathbb{Q}$ כך ש־$\nu_p(u) = 0$; ו־$\psi_2 : W(\mathbb{Q}) \to W_{2^-}$ לפי $\psi_2 : \langle 2^\ell u \rangle \mapsto \ell$. שני הראשונים הם הומומורפיזמים של חוגים. האחרון, בסימוני טענה 8.2.44, מוגדר לפי $n\langle 1 \rangle + \alpha x + \beta y \mapsto \alpha$, והוא הומומורפיזם של חבורות אבל לא של חוגים.

לכל ראשוני p, נסמן ב־p' את הראשוני הגדול ביותר הקטן מ־p (עם $2' = 1$). תהי P תת־החבורה של $\mathbb{Q}^\times$ הנוצרת על־ידי האברים a עם $|a| \leq p$, ו־P' החבורה הנוצרת על־ידי האברים a עם $p < |a|$.

נסמן ב־L_p את תת־החוג של $W(\mathbb{Q})$ הנוצר על־ידי התבניות $\langle a \rangle$ עם $|a| \leq p$. אז $L_1 \subseteq L_2 \subseteq L_3 \subseteq L_5 \subseteq L_7 \subseteq \cdots$, כאשר האיחוד הוא $W(\mathbb{Q}) = \bigcup L_p$. לפי ההגדרה L_1 נפרש על־ידי $\langle 1 \rangle$, ולכן $\psi_\infty : L_1 \to \mathbb{Z}$ הוא איזומורפיזם.

ברור ש־$\psi_p(L_{p'}) = 0$, ולכן ψ_p מוגדר היטב על חבורת המנה $L_p/L_{p'}$, וקל לראות שהוא על. נוכיח ש־$L_p/L_{p'} \cong W_p$. עבור $p = 2$, $L_2 = \mathbb{Z} \cup (\mathbb{Z}\langle 1 \rangle + \langle 2 \rangle)$ מכיוון ש־$\langle 2 \rangle + \langle 2 \rangle = \langle 1, 1 \rangle \in \mathbb{Z}\langle 1 \rangle$, ו־$\psi_2 : n\langle 1 \rangle + \alpha\langle 2 \rangle \mapsto \alpha$, כך ש־$\mathrm{Ker}(\psi_2) = L_1$.

יהי $p > 2$. ראשית נראה שאם $u \equiv v \pmod{p}$ עבור $u, v \in P'$, אז $\langle pu \rangle \equiv \langle pv \rangle \pmod{L_{p'}}$. לכל $u, v, w, t \in P'$ אם $uw = v + pt$ אז $\langle vp, t \rangle = \langle vp, tp^2 \rangle = \langle (v + pt)p, vt(v + tp) \rangle = \langle uwp, tuvw \rangle$, וכך $\langle vp \rangle \equiv \langle uwp \rangle \pmod{L_{p'}}$. הטענה נובעת מנימוק אינדוקציה מפותל שלא נכסה כאן (ראה [4, p. 95]).

כעת נגדיר העתקה $W_p = W(\mathbb{F}_p) \to L_p/L_{p'}$ על־ידי $\langle \alpha \rangle \mapsto \langle ap \rangle$, כאשר $a \in \mathbb{Z}$ בעל שארית α, ו־$|a| < p/2$. כדי להראות שזה מוגדר היטב, יש לבדוק את היחסים ב־טענה 3.3.19. היחס הלא טריוויאלי הוא השלישי: נניח ש־$\langle \beta \rangle \mapsto \langle pb \rangle$ עבור α ו־a; אז $|a + b| < p$, ולכן $a, b, a + b, ab(a + b) \in P'$, ומתקיים $\langle ap, bp \rangle = \langle (a + b)p \rangle + \langle ab(a + b)p \rangle \equiv \langle cp, dp \rangle \pmod{L_{p'}}$ כאשר $c \equiv a + b \pmod{p}$ ו־$d \equiv ab(a + b) \pmod{p}$ מקיימים $|c|, |d| < p/2$. זה מראה ש־$L_p/L_{p'} \cong W_p$, כפי שרצינו. $\square$

מסקנה 8.3.3 נניח שתבנית q מעל $\mathbb{Q}$ נעשית היפרבולית מעל $\mathbb{R}$ ובכל השלמה ל־$\mathbb{Q}_p$. אז היא היפרבולית כבר מעל $\mathbb{Q}$.

מסקנה 8.3.4 (עקרון הסה החלש) אם q, q' הן תבניות מעל $\mathbb{Q}$, השקולות מעל $\mathbb{R}$ ומעל כל $\mathbb{Q}_p$, אז הן שקולות מעל $\mathbb{Q}$.

משפט חזק יותר, שאינו נובע מן התאור של חוג ויט, עוסק בתבניות עצמן:

משפט 8.3.5 (עקרון הסה החזק) *(ראו למשל [20, Thm. IV.8]) אם תבנית ריבועית מעל $\mathbb{Q}$ נעשית איזוטרופית מעל $\mathbb{R}$ ומעל כל $\mathbb{Q}_p$, אז היא איזוטרופית מעל $\mathbb{Q}$.*

מסקנה 8.3.6 אם תבנית רגולרית מעל $\mathbb{Q}$ מציגה את $a \in \mathbb{Q}$ מעל $\mathbb{R}$ ומעל כל $\mathbb{Q}_p$, אז היא מציגה את a כבר מעל $\mathbb{Q}$.

מסקנה 8.3.7 כל תבנית q ממימד $\dim(q) \geq 5$ מעל $\mathbb{Q}$, שאינה חיובית או שלילית לחלוטין, היא איזוטרופית.

הערה 8.3.8 ב־*1969/70* הציע נבוש (*Knebusch*) הכללה של חוגי ויט מעל שדות, כשהגדיר וחקר את חוג ויט של התבניות האלכסוניות מעל חוג קומוטטיבי. האובייקט הבסיסי הוא מרחב ריבועי מעל החוג, היינו מודול פרוייקטיבי נוצר סופית, עם תבנית בילינארית רגולרית. עבור תחום דדקינד R עם שדה שברים $F = \mathrm{q}(R)$, שהסדרה הבאה היא מדוייקת:

$$0 \longrightarrow W(R) \longrightarrow W(F) \longrightarrow \bigoplus W(\bar{F_\mathfrak{p}})$$

[16, (3.3)]. אפשר להוכיח ש־$\langle a \rangle \in W(F)$ הוא בתמונה של $W(R)$ אם ורק אם Ra הוא ריבוע של אידיאל.

8.4 תבניות מעל חוגי דדקינד

בסעיף זה נעסוק (עם הוכחות מעטות בלבד) בתבניות ריבועיות מעל חוגי דדקינד, ובפרט מעל השלמים. מהי תבנית ריבועית מעל השלמים? כשגאוס חקר תבניות בינאריות, הוא הגדיר תבנית שלמה כתבנית מהצורה $ax^2+2bxy+cy^2$, כלומר, בפועל, כתבנית שאפשר להציג באצעות מטריצה $A\in\mathrm{M}_2(\mathbb{Z})$. זו תהיה ההגדרה שלנו כאן: תבנית ריבועית מעל תחום שלמות R היא תבנית שאפשר להציג בצורה $\sum a_{ij}x_ix_j$, כאשר $a_{ii}\in R$ ו־$a_{ij}\in 2R^{-1}$ (לכל $i\neq j$). ההגדרה של לגרנז', המחלישה את התנאי ל־$a_{ij}\in R$, מתאימה יותר לטיפול בשדות וחוגים ממאפיין 2.

כמו במקרה של שדות גלובליים, הרעיון המרכזי הוא ללמוד את האובייקט הגלובלי (סריג או תבנית מעל $\mathbb{Z}$, למשל), דרך ההתנהגות המקומית שלו. במקרה של $\mathbb{Z}$ המיקום מעביר אותנו אל חוגי השלמים ה־p־אדיים $\mathbb{Z}_p$; תופעה דומה מתרחשת מעל כל חוג דדיקנד.

8.4.1 חוגי דדקינד

תחום דדקינד הוא תחום שלמות נתרי, בעל ממד קרול 1, וסגור בשלמות בשדה השברים שלו. תכונה זו שקולה לכך שאפשר להציג כל אידיאל באופן יחיד כמכפלה של אידיאלים ראשוניים. יהי R תחום דדקינד. כל קבוצה מהצורה aI, כאשר $I\lhd R$ ו־$a\in F^{\times}$, נקראת **אידיאל שברי** של R (או של F). לכל אידיאל I בחוג דדקינד יש אידאל שברי הפכי $I^{-1}=\{x\in R\colon\ xI\subseteq R\}$.

דוגמא 8.4.1 יהי F שדה עם הערכה בדידה ν. אז חוג השלמים O_ν הוא תחום דדקינד.

דוגמא זו מראה שסעיף 8.4, על חוגי דדקינד, מכליל את תת־סעיף 8.2.3 העוסק בחוגי השלמים של שדה שלם.

דוגמא טיפוסית יותר מתקבלת מחוג השלמים בשדה גלובלי, K. נניח ש־$\mathbb{Q}\subseteq K$ (למרות שהנחה זו אינה מהותית). לכן $\mathbb{Z}\subseteq K$, ומגדירים את **חוג השלמים** של K להיות חוג השלמים האלגבריים (מעל $\mathbb{Z}$) ב־K. לחילופין, O_K הוא החיתוך של כל חוגי השלמים ביחס להערכות הבדידות של K. למעשה, ההערכות הבדידות של K מושרות כולן על־ידי אידיאלים ראשוניים $\mathfrak{p}\lhd O_K$. נסמן ב־$K_{\mathfrak{p}}$ את ההשלמה של K המושרית על־ידי ההערכה ה־$\mathfrak{p}$־אדית.

דוגמא 8.4.2

1. חוג השלמים של $\mathbb{Q}$ הוא כמובן $\mathbb{Z}$.
2. חוג השלמים של $\mathbb{Q}[\sqrt{d}]$, כאשר d חופשי מריבועים, הוא $\mathbb{Z}[\sqrt{d}]$ אם $d\not\equiv 1\pmod 4$ ו־$\mathbb{Z}[\frac{\sqrt{d}+1}{2}]$ אם $d\equiv 1\pmod 4$.
3. חוג השלמים של $\mathbb{Q}[\rho_n]$ הוא $\mathbb{Z}[\rho_n]$.

8.4.2 הגנוס

המיון היסודי של תבניות מעל שדה עוסק במחלקות איזומטריה: אם שני מרחבים ריבועיים הם איזומטריים, אז מבחינתנו אי אפשר להבדיל ביניהם. כשעוסקים בתבניות מעל חוגים, מושג האיזומטריה חזק מדי, וצריך לבחון גם גרסאות חלשות שלו.

אם שתי תבניות מוגדרות מעל O_K, הן עשויות להיות איזומטריות כבר שם (כלומר יתכן שקיימת $T\in\mathrm{GL}_n(O_K)$ הפיכה כך ש־$q'(x)=q(Tx)$), ויתכן שיש איזומטריה חלשה יותר, מעל השדה, או מעל השלמים מקומית (בכל מקום), וכן הלאה. תכונות אלה מוצגות עם הגרירות ביניהן ברשימה הבאה. החץ הפשוט הוא עקרון הסה החלש, 8.3.4. נאמר שתכונה מסויימת מתקיימת "מקומית" הם היא נכונה בכל השלמה של K.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathbb{Z}_p \arrow[d, Rightarrow] \\ \mathbb{Q} \arrow[r, Rightarrow, shift left] & \mathbb{Q}_p \arrow[l, shift left] \end{tikzcd}$$

"$\mathbb{Z}$". התבניות q,q' איזומטריות מעל O_K.

"$\mathbb{Z}_p$". התבניות q,q' איזומטריות מקומית מעל השלמים (=שייכות לאותו **גנוס**).

"$\mathbb{Q}$". התבניות q,q' איזומטריות מעל K.

"$\mathbb{Q}_p$". התבניות q,q' איזומטריות מקומית מעל השדה

הגדרה 8.4.3 *הגנוס של תבנית ריבועית q כולל את התבניות מעל O_K שהן כך שלכל $\mathfrak{p}\lhd O_K$, q,q' איזומטריות מעל $O_{\mathfrak{p}}$.*

טענה 8.4.4 אם q,q' איזומטריות מעל O_K, אז הן שייכות לאותו גנוס.

משפט 8.4.5 *מספר התבניות (עד כדי איזומטריה) בגנוס הוא תמיד סופי* [4, Thm. 9.4.1].

הצגת ערך שלם

בדומה לאפשרויות השונות לאיזומטריות של תבניות, אפשר לדון בסוגים שונים של הצגות של ערך שלם. תהי q תבנית אנאיזוטרופית, המוגדרת מעל חוג השלמים של K; ויהי $a \in O_K$. יש כמה אפשרויות טבעיות:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathbb{Z}_p \arrow[d, Rightarrow] \\ \mathbb{Q} \arrow[r, Rightarrow, shift left] & \mathbb{Q}_p \arrow[l, shift left] \end{tikzcd}$$

"$\mathbb{Z}$". q מציגה את a מעל O_K.

"$\mathbb{Z}_p$". מציגה את a מקומית מעל השלמים (כלומר מעל כל O_ν).

"$\mathbb{Q}$". q מציגה את a מעל K.

"$\mathbb{Q}_p$". q מציגה את a מקומית מעל השדה (כלומר מעל כל השלמה של K).

הגרירות המסומנות בחץ כפול בדיאגרמה משמאל כולן טריוויאליות: הצגה של a מעל K היא הצגה מעל כל השלמה; והצגה מעל חוג השלמים הוא הצגה מעל השדה. החץ הפשוט הוא העקרון החזק של הסה, משפט 8.3.5, התקף לשדות אבל לא לחוגי השלמים שלהם.

במקום עקרון הסה, תקף מעל השלמים עקרון חלש יותר, המבוסס על הגנוס של התבנית.

משפט 8.4.6 ([4, Thm. 9.1.3]) ***אם $t \in O_K$ ניתן להצגה מקומית מעל השלמים על ידי q, אז t ניתן להצגה מעל השלמים על־ידי תבניות מאותו גנוס.***

הערה 8.4.7 לא קשה למצוא דוגמאות לתבניות בינאריות שבהן הצגת ערך שלם דורשת מעבר לתבנית אחרת מאותו גנוס.

הדוגמא הראשונה לתבנית ריבועית טרנרית לא מוחלטת, המייצגת מספר מקומית בכל מקום (כל $\mathbb{Z}_p$ ו־ $\mathbb{R}$) אבל לא מעל $\mathbb{Z}$ היא של זיגל (*Siegel*), *[22]*.

בעיה 8.4.8 (דוגמא של בורובוי ורודניק (Borovoi-Rudnick), 1995). הראה שהתבנית $q = -9x^2+2xy+7y^2+2z^2$ מציגה את 1 מקומית בכל מקום, אבל אינה מציגה את 1 מעל $\mathbb{Z}$. **הדרכה**. אם $p|x-y$ אז 2 שארית ריבועית מודולו p, אבל $p \equiv \pm 3 \pmod{16}$. מצא תבנית אחרת מאותו גנוס המציגה את 1 מעל $\mathbb{Z}$.

בעיה 8.4.9 (מבוא להתאמה של גאוס בין תבניות לאידיאלים). הדיסקרימיננטה של תבנית ריבועית $q = ax^2 + bxy + cy^2$ מעל השלמים היא $d = b^2 - 4ac$.

1. נגדיר $z(q) = \frac{b+\sqrt{d}}{2a}$ ו־$\bar{z}(q) = \frac{b-\sqrt{d}}{2a}$. בדוק שמעל $\mathbb{Q}[\sqrt{d}]$ מתקבל פירוק לגורמים לינאריים $q = a(x + zy)(x + \bar{z}y)$.
2. החבורה $\mathrm{SL}_2(\mathbb{Z})$ פועלת על מטריצות לפי $X \mapsto AXA^{\mathrm{t}}$ ועל חצי המישור העליון (הסגור, בניכוי החלק הרציונלי של ציר ה־x) לפי $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot z = \frac{\alpha z+\beta}{\gamma z+\delta}$.
3. הראה ש־$z(A \cdot X) = A^{-\mathrm{t}} \cdot z(X)$. הראה ששתי תבניות הן איזומטריות (מעל $\mathbb{Z}$) אם ורק אם מקדמי z שלהן שקולים (ביחס לפעולה של $\mathrm{SL}_2(\mathbb{Z})$ על חצי המישור העליון).
4. נסמן את האידיאל $I(q) = \left\langle a, \frac{b-\sqrt{d}}{2} \right\rangle$ בחוג השלמים של $\mathbb{Q}[\sqrt{d}]$. הראה ש־$|\mathcal{O}_d/I(q)| = |a| \cdot (a,b,c)$, כאשר (a,b,c) הוא המחלק המשותף המקסימלי של שלושת המקדמים. **הדרכה**. חשב את $I(q)\overline{I(q)}$; אם R תחום שלמות, הפונקציה $I \mapsto |R/I|$ היא כפלית.
5. הראה שאם האידיאלים $I(q)$ ו־$I(q')$ שקולים בחבורת המחלקה של השדה, אז $q \sim q'$ תחת פעולת $\mathrm{SL}_2(\mathbb{Z})$.
6. הראה שאם q' מתקבל מ־q על־ידי פעולת $A \in \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/a\mathbb{Z}))$, אז $I(q') \subseteq I(q')$.

8.4.3 הגנוס הספינורי

הגנוס הספינורי של תבנית הוא מושג ביניים: כל גנוס מורכב מכמה גנוסים ספינוריים, וכל גנוס ספינורי מורכב מכמה מחלקות איזומטריה.

את החבורות $\Theta(V, q)$ הגדרנו בהגדרה 3.4.63. נתבונן בהשלמה $K_{\mathfrak{p}}$ של K. אם V מרחב ריבועי מעל K, אז $V_{K_{\mathfrak{p}}}$ הוא מרחב ריבועי מעל $K_{\mathfrak{p}}$. במקום לכתוב $\Theta(K_{\mathfrak{p}} \otimes_K V, q_{K_{\mathfrak{p}}})$, נכתוב פשוט $\Theta(K_{\mathfrak{p}})$.

הגדרה 8.4.10 *תהיינה q, q' תבניות מעל חוג השלמים $\mathcal{O}_K$. אומרים ש־q, q' שייכות לאותו גנוס ספינורי אם q איזומטרית לתבנית q'' כך שמקומית, יש איזומטריה ב־$\Theta(K_{\mathfrak{p}})$ המעבירה את q' ל־q'' ([15, sec. 102A]).*

הערה 8.4.11 אם שתי תבניות הן איזומטריות מעל השלמים, אז הן שייכות לאותו גנוס ספינורי; ואם שתי תבניות שייכות לאותו גנוס ספינורי, אז הן שייכות לאותו גנוס.

הגנוס מורכב ממספר סופי (שהוא חזקת 2) של גנוסים ספינוריים [15, Thm. 108:2a]; וכל גנוס ספינורי מורכב ממספר סופי של מחלקות איזומטריה. עבור תבניות לא מוחלטות מממד 3 או יותר, כל התבניות בגנוס ספינורי הן איזומטריות מעל השלמים [4, Thm. 11.1.4].

כדי לחשב את מספר הגנוסים הספינוריים בגנוס, יש לחשב **נורמה ספינורית** בהשלמות של K [4, Subsec. 11.3]. למשל, ידוע שאם לכל אידיאל מקסימלי $\mathfrak{p} \lhd O_K$ חבורת הנורמות הספינוריות $\theta(O^+(q))$ מעל $O_{\mathfrak{p}}$ מכילה את כל האברים ההפיכים $O_{\mathfrak{p}}^{\times}$, אז הגנוס של q מכיל גנוס ספינורי יחיד.

את החישוב של חבורות נורמה ספינוריות באופן מקומי, התחיל קנזר (Kneser) ב־[11], שהצליח לחשב את החבורות מעל הראשוניים האי־זוגיים. המקרה של שדות דיאדיים (אלו שבהם 2 אינו שלם הפיך) הרבה יותר קשה. (הפניה למאמר שיצא בעקבות KSV2).

שילוב [4, Lemma 11.3.7] ו־[25, Lemma 2.2(2)] מאפשר להוכיח את התוצאה הבאה:

משפט 8.4.12 *יהי K שדה מספרים, ויהיו a_1, a_2, a_3 שלמים אלגבריים, כך ש־$d = a_1a_2a_3$ אינו מתחלק באף חזקה שלישית (של אידיאל ראשוני), והוא שלילי בכל סידור של K. אז יש רק מחלקת איזומטריה אחת בגנוס של $\langle a_1, a_2, a_3 \rangle$.*

בעיה 8.4.13 נסח את מושגי הגנוס והגנוס הספינורי במונחי פעולת החבורה האורתוגונלית מעל האדלים (Adéles), על מרחב התבניות הריבועיות.

8.4.4 סריגים מעל חוגי דדקינד

מתת־סעיף זה ואילך נעסוק בסריגים ריבועיים מעל חוג דדקינד כללי. יהי R חוג דדקינד, ויהי F שדה השברים שלו. אנו עוקבים בעיקר אחרי [15, Section 82]. נקבע מרחב וקטורי (מממד סופי) V מעל F, עם תבנית בילינארית סימטרית $B : V \times V \to F$.

תת־מודול $L \subseteq V$ מעל R המכיל בסיס של V, ושהוא פרוייקטיבי ונוצר סופית כמודול, נקרא **סריג**. (ב־[15, Section 81] מסתפקים בדרישה ש־L יהיה מוכל במודול חופשי נוצר סופית). איננו מניח ש־$B(L, L) \subseteq R$, אם כי אפשר להשיג תכונה זו על־ידי כפל של התבנית בקבוע.

כמו במקרה של מרחבים ריבועיים, הבעיה היסודית היא לזהות את הסריגים עד כדי איזומורפיזם. כלומר, בהנתן סריגים L, L', האם יש איזומטריה $\sigma \in O(V)$ כך ש־$\sigma L = L'$? יש שתי דרכים שבהן הבעיה עבור סריגים מסובכת יותר מן הבעיה עבור שדות. ראשית, אם הסריג חופשי כמודול, אפשר לתרגם את הבעיה למטריצות; אבל במקרה הכללי יש סריגים לא חופשיים. ושנית, כפי שכבר ראינו, אפילו הבעיה עבור מטריצות קשה בהרבה מעל חוג שלמים מאשר מעל שדה.

על פי המיון של מודולים נוצרים סופית מעל חוג דדקינד, ידוע שכל סריג ניתן להצגה בצורה

$$L = I_1x_1 + \dots + I_nx_n \tag{8.1}$$

כאשר $I_1, \dots, I_n \lhd R$ הם אידיאלים, ו־$x_1, \dots, x_n \in V$.

הסריג הדואלי מוגדר לפי $L^{\#} = \{x \in V : \ B(x, L) \subseteq R\}$. אם L נתון לפי ההצגה (8.1), אז הסריג הדואלי הוא $L^{\#} = \sum I_i^{-1}x_i'$ כאשר $x_1', \dots, x_n'$ הוא בסיס דואלי לבסיס $x_1, \dots, x_n$.

8.4.5 תבניות וסריגים חופשיים

תהי $A \in \mathrm{M}_n(F)$ מטריצה הפיכה (זה המקרה הרגולרי). **המחלקה** של A כוללת את המטריצות מהצורה PAP^{t}, כאשר $P \in \mathrm{GL}_n(R)$ הפיכה מעל השלמים. כמו במקרה של שדות, שני סריגים ריבועיים הם איזומורפיים אם ורק אם המטריצות המייצגות אותם שייכות לאותה מחלקה. מבחינה זו, התאוריה של סריגים חופשיים היא התאוריה של תבניות ריבועיות (והתאוריה מעל תחומים ראשיים דומה לזו של שדות, לפחות בכך שכל הסריגים חופשיים).

מסקנה 8.4.14 הדטרמיננטה של המטריצה המייצגת היא שמורה מוגדרת היטב ב־$F^{\times}/R^{\times 2}$.

טענה 8.4.15 ([15, 82:7]) נניח ש־$L' = L_1' \perp L_2'$ הם סריגים רגולריים, ו־$L' \subseteq L$, שגם הוא סריג. אז L' הוא מרכיב אורתוגונלי של L אם ורק אם כל L_i' הוא מרכיב אורתוגונלי של L.

8.4.6 שמורות אריתמטיות

מקדם **המידה** (scale) של L הוא האידאל השברי $\mathfrak{s}L = B(L, L) \lhd R$. **הנורמה** $\mathfrak{n}L = RQ(L)$ היא תת־המודול של F הנוצר מעל R על ידי כל הערכים $Q(v) = B(v, v)$, $v \in L$. מכיוון ש־$2B(x, y) = Q(x + y) - Q(x) - Q(y) \in \mathfrak{n}L$, מתקבלת ההכלה

$$2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L.$$

שתי השמורות האלה אדיטיביות לפריוק אורתוגונלי.

הערה 8.4.16 שינוי קנה מידה: אם $I \lhd F$, אידיאל שברי מעל R, אז $\mathfrak{s}(IL) = I^2\mathfrak{s}L$ ו־$\mathfrak{n}(IL) = I^2\mathfrak{n}L$.

טענה 8.4.17 נניח ש־$V = V_1 \perp V_2$, ו־$L_1 \subseteq V_1$ סריג רגולרי. אז יש סריג $L_2 \subseteq V_2$ כך של־$L_1 \perp L_2$ אותם מידה ונורמה כמו ל־L_1.

הוכחה. קח סריג כלשהו $L_2' \subseteq V_2$, אז יש $\alpha \in R$ כך ש־$\alpha^2\mathfrak{s}L_2' \subseteq \mathfrak{s}L_1$ ו־$\alpha^2\mathfrak{n}L_2' \subseteq \mathfrak{n}L_1$; לכן $L_1 \perp \alpha L_2'$ מקיים את הדרישות. $\square$

הנפח

נניח ש־L נתון בצורה (8.1). **הנפח** של L מוגדר כ־$\mathfrak{v}L = I_1^2 \cdots I_n^2 \det(x_1,\dots,x_n)$ כאשר $\det(\cdot)$ הוא הדטרמיננטה. זהו אידיאל שברי של F.

תרגיל 8.4.18 הנפח אינו תלוי בהצגה של הסריג.

טענה 8.4.19 $\mathfrak{v}(L_1 \perp L_2) = \mathfrak{v}L_1 \cdot \mathfrak{v}L_2$.

טענה 8.4.20 $\mathfrak{v}L \subseteq (\mathfrak{s}L)^n$ כאשר $n = \mathrm{rank}L$.

טענה 8.4.21 ([15, 82:11]) אם $K \subseteq L'$ אז יש אידאל $I \lhd R$ כך ש־$\mathfrak{v}L' = I^2\mathfrak{v}L$.

טענה 8.4.22 אם $L' \subset L$ אז $\mathfrak{v}L' \subset \mathfrak{v}L$.

אפשר לחשב ישירות ש־$\mathfrak{v}L^{\#} = (\mathfrak{v}L)^{-1}$. טענה 8.4.22 מאפשרת להוכיח ש־$L^{\#\#} = L$.

המיקום ב־P של מרחב בילינארי V מעל F הוא המרחב הריבועי $V_P = F_PV$ עם התבנית המושרית מ־V. המיקום של L מוגדר באותו אופן, כ־$L_P = R_PL$.

תרגיל 8.4.23 $\mathfrak{s}L_P = (\mathfrak{s}L)_P$, $\mathfrak{n}L_P = (\mathfrak{n}L)_P$, $\mathfrak{v}L_P = (\mathfrak{v}L)_P$.

(ראה [4, Thm. 11.1.1] על קיום סריגים גלובליים לפי מידע לוקלי.)

8.4.7 מודולריות

סריג רגולרי L נקרא **מודולרי** (ביחס ל־$I = \mathfrak{v}L$) אם $\mathfrak{v}L = \mathfrak{s}L^n$, **ויונימודולרי** אם הוא מודולרי ו־$\mathfrak{v}L = R$.

אם L מודולרי, אז כך גם JL לכל אידיאל שברי $J \subseteq F$. בפירוק אורתוגונלי, $L_1 \perp L_2$ מודולרי ביחס לאידיאל I אם ורק אם L_1, L_2 הם כאלה.

טענה 8.4.24 ([15, 82:13]) הסריג החופשי עם מטריצה מייצגת A הוא יונימודולרי אם ורק אם $A \in \mathrm{GL}_n(R)$.

טענה 8.4.25 ([15, 82:14] + [15, 82:14a]) סריג רגולרי הוא מודולרי ביחס ל־I אם ורק אם $L = IL^{\#}$. במקרה כזה $L = \{v \in V :\ B(v, L) \subseteq I\}$.

מסקנה 8.4.26 L יונימודולרי אם ורק אם $L^{\#} = L$.

טענה 8.4.27 ([15, 82:15]) אם P תת־סריג I־מודולרי של L ו־$\mathfrak{s}L = I$ אז $L = P \perp P'$ עבור P' מתאים.

טענה 8.4.28 ([15, 82:16]) יהי L סריג מודולרי, ו־$x \in L$ וקטור איזוטרופי. אז יש תת־סריג $I'x+I''y$ שהוא מחובר אורתוגונלי של L.

מסקנה 8.4.29 (מתרגיל 8.4.23) L הוא I־מודולרי אם ורק אם הוא מודולרי מקומית מכל מקום.

8.4.8 סריגים מקסימליים

יהי $I \lhd R$. סריג $L \subseteq V$ נקרא **I־מקסימלי** אם הוא מקסימלי בין הסריגים המקיימים $\mathfrak{n}L \subseteq I$. אם L מקסימלי, כל גם JL לכל $J \lhd R$.

תרגיל 8.4.30 כל מחובר ישר של סריג I־מקסימלי הוא I־מקסימלי.

טענה 8.4.31 אם $\mathfrak{n}L \subseteq I$ אז L מוכל בסריג I־מקסימלי.

הוכחה. אם $\mathfrak{n}L \subseteq I$ אז $\mathfrak{v}L \subseteq (\mathfrak{s}L)^n \subseteq (\frac{1}{2}I)^n$. לכל שרשרת עולה של סריגים המתחילה ב־L, הנפח חסום, ולכן אורך השרשרת חסום. $\square$

בעיה 8.4.32 יהי L סריג כלשהו כך ש־$\mathfrak{n}L \subseteq I$. אם באידאל השלם $2^n\mathfrak{v}LI^{-n}$ אין גורמים ריבועיים, אז L מקסימלי. **הדרכה**. אחרת הפעל את טענה 8.4.21.

טענה 8.4.33 ([15, 82:20]) יהי L סריג מקסימלי, ו־$x \in L$ וקטור איזוטרופי. אז יש מרכיב אורתוגונלי של L מדרגה 2 המכיל את x.

(ההוכחה בונה תת־סריג מודולרי מדרגה 2, ומפעילה את טענה 8.4.27.)

טענה 8.4.34 ([15, 82:21]) סריג L במישור היפרבולי הוא $2I$־מקסימלי אם ורק אם L I־מודולרי ו־$\frac{n}{2}L \subseteq 2I$.

מסקנה 8.4.35 (מתרגיל 8.4.23) L הוא I־מקסימלי אם ורק אם הוא I_P־מקסימלי בכל מקום I_P.

פרק 9

מטלות לסוף הקורס

להלן רשימה של מטלות לסוף הקורס. יש לתאם את המטלה עם המרצה מראש.

1. פתור שלושה-חמישה מהתרגילים המסומנים ב"בעיה", או אחד מאלה המסומנים ב"אתגר".
2. תאר את חוג ויט של תבניות בילינאריות סימטריות במקרה של מאפיין 2 (קבוצת התבניות המטאבוליות מכילה ממש את קבוצת התבניות ההיפרבוליות, ומחליפה אותה כאיבר האפס של החוג).
3. סכם את התאוריה של קדם־סדרים ושדות סדורים (סגור סדור וכדומה) על־פי [13].
4. הסבר את עקרון הסה לשדות גלובליים (עבוד מעל $\mathbb{Q}$ לשם הפשטות): השמורה של הסה, משפט ההיפוך של הילברט $\sum_p(\alpha,\beta)_{k_p}=0$, העובדה ש־
$$0\longrightarrow {}_2\mathrm{Br}(F)\longrightarrow \bigoplus {}_2\mathrm{Br}(F_p)\longrightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z}\longrightarrow 0$$
היא סדרה מדוייקת קצרה.
5. כתוב על אברים אלגבריים ב־$W(F)$ לפי [6, III.5.5] (אלו המחלקות של תבניות עקבה בהרחבות אלגבריות).
6. סריגים: ראה [10, Section 5.2] על הפירוק של סריגים יונימודולריים מעל $\mathbb{Q}_p$ (ההגדרה בסעיף 8.4.7).
7. למד את היחסים $<$ ו־$\gg$ בין תבניות ($\phi<\psi$ או $\phi\gg\psi$ אם ϕ נעשה איזוטרופי או היפרבולי מעל $F(\psi)$, בהתאמה). ראה פרקים 9, 10 אצל [14].
8. הוכח את משפט מרקורייב ש־$\mathrm{K}_2(F)/2\cong {}_2\mathrm{Br}(F)$ בעזרת [23]; או סכם את [17].
9. תאר את השמורה $C_0(q)$ והמבנה שלה, בדומה למה שעשינו כאן עבור $C(q)$ ([12]).
10. כתוב על excellence של תבניות (נסה לפתח גרסה כמותית).
11. כתוב על מספר פיתגורס ועל ה־u-invariant (בעיה 8.2.37). ראה [7, Section 77] על בניה של שדה עם מספר פיתגורס כרצונך.
12. כתוב ערכים טובים בוויקיפדיה על המושגים "חוג ויט", "תבנית פיסטר", "רמה של שדה".
13. תאר את העבודה של גאוס על מיון תבניות ריבועיות, ואת הקשר לאידיאלים בשדות ריבועיים; בעיה 8.4.9 ו־[4, Chap. 14].

14. הוכח את עקרון הסה החזק, משפט 8.3.5.

15. כתוב על נושא כלשהו השייך לסעיף 8.4.

16. כתוב סעיף על גאומטריה פולרית והקשר שלה לתת־מרחבים איזוטרופיים של תבנית ריבועית.

17. כתוב על התנאי (C_r) או ממד קוהומולוגי, והקשר לתנאי $I^n(F) = 0$, בעזרת [21].

18. סכם את התוצאות המרכזיות לגבי הצגת מספר כסכום של שני ריבועים, מן הספר [8].

19. עיין במאמרים [2], [3] על הצגת פולינום מעל שדה סופי כסכום של ריבועים, וסכם את התוצאות המרכזיות. (לפי הצעה של אופיר גורודצקי, 2017).

ביבליוגרפיה

[1] V. Astier and T. Unger, *Signatures of hermitian forms and the Knebusch trace formula*, Math. Ann. **358**(3–4), 925–947, (2014).

[2] L. Carlitz, *On the Representation of a Polynomial In a Galois Field as the Sum of an Even Number of Squares*, Transactions of the American Mathematical Society, **35**(2), 397–410. `http://www.jstor.org/stable/1989773`.

[3] L. Carlitz, *On the representation of a polynomial in a Galois field as the sum of an odd number of squares*, Duke Math. J. **1**(3), (1935), 298–315.

[4] J.W.S. Cassels, "Rational Quadratic Forms", Dover, 2008.

[5] D.B Coleman and Joel Cunningham, *Harrison's Witt ring of a commutative ring*, Journal of Algebra Volume 18, Issue 4, 549–564, (1971).

[6] P.E. Conner and R. Perlis, "A survey of trace forms of algebraic Number fields", World Scientific, 1984.

[7] R.S. Elman, N. Karpenko and A. Merkurjev, "The Algebraic and Geometric Theory of Quadratic Forms", AMS, 2008.

[8] E. Grosswald, "Representations of Integers as Sums of Squares", 1985.

[9] L.J. Gerstein, "Basic Quadratic Forms", Graduate Studies in Mathemtaics **90**, AMS.2008

[10] Y. Kitaoka, "Arithmetic of Quadratic Forms", Cambridge tracts in math **106**, 1993.

[11] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen*, Archiv d. Math. **7**, 323–332, (1956).

[12] M.-A. Knus, M. Rost, J.-P. Tignol, A. Merkurjev, "The Book of Involutions", AMS, Coll. Pub. **44**, 1998..

Available at `https://sites.ualberta.ca/ karpenko/publ/Kniga.pdf`.

[13] T.Y. Lam, "Orderings, valuations and quadratic forms", CBMS **52**, 1983.

[14] T.Y. Lam, Ten lectures on Quadratic Forms over Fields, Queen's University, 1977.

[15] O.T. O'Meara, "Introduction to Quadratic Forms", Spinger, Classics in Mathematics, 2000; reprint of a 1973 edition.

[16] J. Milnor and Husemoller, "Symmetric Bilinear Forms", Springer, Ergeb. Math. Grenzgeb **73**, 1973.

[17] D. Orlov, A. Vishik and V. Voevodsky, *An exact sequence for $K_*^M/2$ with applications to quadratic forms*, Annals of Mathematics **165**, 1–13, (2007).

[18] A. Pfister, Quadratic Forms with Applications to Algebraic Geometry and Topology, LMS-LNS **217**, 1995.

[19] A.R. Rajwade, "Squares", LMS **171**, 1993.

[20] J.P. Serre, "A course in Arithmetic", Springer, 1973.

[21] J.P. Serre, "Galois Cohomology", Springer, 1996.

[22] C.L. Siegel, *Indefinite quadratische Formen und Funktionentheorie I.*, Math Ann. **124**, 17–54, (1951).

[23] A.R. Wadsworth, *Merkurjev's elementary proof of Merkurjev's theorem*, Contemp. Math. **55**, 741–776, (1986).

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

[25] F. Xu, *Generation of integral orthogonal groups over dyadic local fields*, Pacific J. Math. **167**(2), 385–398, (1995).