Chapter 0

Historical Background

The theory of composition of quadratic forms over fields had its start in the 19th century with the search for n-square identities of the type

$$(x_1^2 + x_2^2 + \cdots + x_n^2) \cdot (y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2$$

where $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ are systems of indeterminates and each $z_k = z_k(X, Y)$ is a bilinear form in X and Y. For example when $n = 2$ there is the ancient identity

$$(x_1^2 + x_2^2) \cdot (y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2.$$

In this example $z_1 = x_1 y_1 + x_2 y_2$ and $z_2 = x_1 y_2 - x_2 y_1$ are bilinear forms in X, Y with integer coefficients. This formula for $n = 2$ can be interpreted as the "law of moduli" for complex numbers: $|\alpha| \cdot |\beta| = |\alpha\beta|$ where $\alpha = x_1 - i x_2$ and $\beta = y_1 + i y_2$.

A similar 4-square identity was found by Euler (1748) in his attempt to prove Fermat's conjecture that every positive integer is a sum of four integer squares. This identity is often attributed to Lagrange, who used it (1770) in his proof of that conjecture of Fermat. Here is Euler's formula, in our notation:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

where

$$z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4$$

$$z_2 = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3$$

$$z_3 = x_1 y_3 - x_2 y_4 - x_3 y_1 + x_4 y_2$$

$$z_4 = x_1 y_4 + x_2 y_3 - x_3 y_2 - x_4 y_1.$$

After Hamilton's discovery of the quaternions (1843) this 4-square formula was interpreted as the law of moduli for quaternions. Hamilton's discovery came only after he spent years searching for a way to multiply "triplets" (i.e. triples of numbers) so that the law of moduli holds. Such a product would yield a 3-square identity. Already in his *Théorie des Nombres* (1830), Legendre showed the impossibility of such an identity. He noted that 3 and 21 can be expressed as sums of three squares of rational numbers, but that $3 \times 21 = 63$ cannot be represented in this way. It follows

that a 3-square identity is impossible (at least when the bilinear forms have rational coefficients). If Hamilton had known of this remark by Legendre he might have given up the search to multiply triplets! Hamilton's great insight was to move on to four dimensions and to allow a non-commutative multiplication.

Hamilton wrote to John Graves about the discovery of quaternions in October 1843 and within two months Graves wrote to Hamilton about his discovery of an algebra of "octaves" having 8 basis elements. The multiplication satisfies the law of moduli, but is neither commutative nor associative. Graves published his discovery in 1848, but Cayley independently discovered this algebra and published his results in 1845. Many authors refer to elements of this algebra as "Cayley numbers". In this book we use the term "octonions".

The multiplication of octonions provides an 8-square identity. Such an identity had already been found in 1818 by Degen in Russia, but his work was not widely read. After the 1840s a number of authors attempted to find 16-square identities with little success. It was soon realized that no 16-square identity with integral coefficients is possible, but the arguments at the time were incomplete. These "proofs" were combinatorial in nature, attempting to insert $+$ and $-$ signs in the entries of a 16×16 Latin square to make the rows orthogonal.

In 1898 Hurwitz published the definitive paper on these identities. He proved that there exists an n-square identity with complex coefficients if and only if $n = 1, 2, 4$ or 8. His proof involves elementary linear algebra, but these uses of matrices and linear independence were not widely known in 1898. At the end of that paper Hurwitz posed the general problem: For which positive integers r, s, n does there exist a "composition formula":

$$(x_1^2 + x_2^2 + \cdots + x_r^2) \cdot (y_1^2 + y_2^2 + \cdots + y_s^2) = z_1^2 + z_2^2 + \cdots + z_n^2$$

where $X = (x_1, x_2, \ldots, x_r)$ and $Y = (y_1, y_2, \ldots, y_s)$ are systems of indeterminates and each $z_k = z_k(X, Y)$ is a bilinear form in X and Y?

Here is an outline of Hurwitz's ideas, given without all the details. Suppose there is a composition formula of size $[r, s, n]$ as above. View X, Y and Z as column vectors. Then, for example, $z_1^2 + z_2^2 + \cdots + z_n^2 = Z^\top \cdot Z$, where the superscript $\top$ denotes the transpose. The bilinearity condition becomes $Z = AY$ where A is an $n \times s$ matrix whose entries are linear forms in X. The given composition formula can then be written as

$$(x_1^2 + x_2^2 + \cdots + x_r^2) Y^\top \cdot Y = Z^\top \cdot Z = Y^\top A^\top A Y.$$

Since Y consists of indeterminates this equation is equivalent to

$$A^\top \cdot A = (x_1^2 + x_2^2 + \cdots + x_r^2) I_s,$$

where A is an $n \times s$ matrix whose entries are linear forms in X.

Of course I_s here denotes the $s \times s$ identity matrix. Since the entries of A are linear forms we can express $A = x_1A_1 + x_2A_2 + \cdots + x_rA_r$ where each A_i is an $n \times s$ matrix with constant entries. After substituting this expression into the equation and canceling like terms, we find:

There are $n \times s$ matrices $A_1, A_2, \ldots, A_r$ over F satisfying

$$A_i^\top \cdot A_i = I_s \quad \text{for } 1 \le i \le r,$$
$$A_i^\top \cdot A_j + A_j^\top \cdot A_i = 0 \quad \text{for } 1 \le i, j \le r \text{ and } i \ne j.$$

This system is known as the "Hurwitz Matrix Equations". Such matrices exist if and only if there is a composition formula of size $[r, s, n]$.

Hurwitz considered these matrices to have complex entries, but his ideas work just as well using any field of coefficients, provided that the characteristic is not 2. Those matrices are square when $s = n$. In that special case the system of equations can be greatly simplified by defining the $n \times n$ matrices $B_i = A_1^{-1}A_i$ for $1 \le i \le r$. Then $B_1, \ldots, B_r$ satisfy the Hurwitz Matrix Equations and $B_1 = I_n$. It follows that:

There are $n \times n$ matrices $B_2, \ldots, B_r$ over F satisfying:

$$B_i^\top = -B_i, \quad B_i^2 = -I_n, \quad \text{for } 2 \le i \le r;$$
$$B_iB_j = -B_jB_i \quad \text{whenever } i \ne j.$$

Such a system of $n \times n$ matrices exists if and only if there is a composition formula of size $[r, n, n]$. Hurwitz proved that the 2^{r-2} matrices $B_{i_1}B_{i_2}\ldots B_{i_k}$ for $2 \le i_1 \le \cdots \le i_k \le r-1$ are linearly independent. This shows that $2^{r-2} \le n^2$ and in the case of n-square identities (when $r = n$) quickly leads to the "1, 2, 4, 8 Theorem".

In 1922 Radon determined the exact conditions on r and n for such a system of matrices to exist over the real field $\mathbb{R}$. This condition had been found independently by Hurwitz for formulas over the complex field $\mathbb{C}$ and was published posthumously in 1923. They proved that:

A formula of size $[r, n, n]$ exists if and only if $r \le \rho(n)$,

where the "Hurwitz–Radon function" $\rho(n)$ is defined as follows: if $n = 2^{4a+b}n_0$ where n_0 is odd and $0 \le b \le 3$, then $\rho(n) = 8a + 2^b$. There are several different ways

this function can be described. The following one is the most convenient for our purposes:

$$\text{If } n = 2^m n_0 \text{ where } n_0 \text{ is odd then } \rho(n) = \begin{cases} 2m+1 & \text{if } m \equiv 0, \\ 2m & \text{if } m \equiv 1, \\ 2m & \text{if } m \equiv 2, \\ 2m+2 & \text{if } m \equiv 3 \end{cases} \pmod 4.$$

For example, $\rho(n) = n$ if and only if $n = 1, 2, 4$ or 8, as expected from the earlier theorem of Hurwitz. Also $\rho(16) = 9$, $\rho(32) = 10$, $\rho(64) = 12$ and generally $\rho(16n) = 8 + \rho(n)$. New proofs of the Hurwitz–Radon Theorem for compositions of size $[r, n, n]$ were found in the 1940s. Eckmann (1943b) applied the representation theory of certain finite groups to prove the theorem over $\mathbb{R}$, and Lee (1948) modified Eckmann's ideas to prove the result using representations of Clifford algebras. Independently, Albert (1942a) generalized the 1, 2, 4, 8 Theorem to quadratic forms over arbitrary fields, and Dubisch (1946) used Clifford algebras to prove the Hurwitz–Radon Theorem for quadratic forms over $\mathbb{R}$ (allowing indefinite forms). Motivated by a problem in geometry, Wong (1961) analyzed the Hurwitz–Radon Theorem using matrix methods and classified the types of solutions over $\mathbb{R}$. In the 1970s Shapiro proved the Hurwitz–Radon Theorem for arbitrary (regular) quadratic forms over any field where $2 \neq 0$, and investigated the quadratic forms which admit compositions. One goal of our presentation is to explain the curious periodicity property of the Hurwitz–Radon function $\rho(n)$:

$$\text{Why does } \rho(2^m) \text{ depend only on } m \pmod 4?$$

The explanation comes from the shifting properties of (s, t)-families as explained in Chapter 2.

Here are some of the questions which have motivated much of the work done in Part I of this book. Suppose σ and q are regular quadratic forms over the field F, where $\dim \sigma = s$ and $\dim q = n$. Then σ and q "admit a composition" if there is a formula

$$\sigma(X)q(Y) = q(Z),$$

where as usual $X = (x_1, x_2, \ldots, x_s)$ and $Y = (y_1, y_2, \ldots, y_n)$ are systems of indeterminates and each z_k is a bilinear form in X and Y, with coefficients in F. The quadratic forms involved in these compositions are related to Pfister forms.

In the 1960s Pfister found that for every m there do exist 2^m-square identities, provided some denominators are allowed. He generalized these identities to a wider class: a quadratic form is a *Pfister form* if it expressible as a tensor product of binary quadratic forms of the type $\langle 1, a\rangle$. In particular its dimension is 2^m for some m. Here we use the notation $\langle a_1, \ldots, a_n\rangle$ to stand for the n-dimensional quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$.

Theorem (Pfister). *If φ is a Pfister form and X, Y are systems of indeterminates, then there is a multiplication formula*

$$\varphi(X)\varphi(Y) = \varphi(Z),$$

where each component $z_k = z_k(X, Y)$ is a linear form in Y with coefficients in the rational function field $F(X)$. Conversely if φ is an anisotropic quadratic form over F satisfying such a multiplication formula, then φ must be a Pfister form.

The theory of Pfister forms is described in the textbooks by Lam (1973) and Scharlau (1985). When $\dim \varphi = 1, 2, 4$ or 8, such a multiplication formula exists using no denominators, since the Pfister forms of those sizes are exactly the norm forms of composition algebras. But if $\dim \varphi = 2^m > 8$, Hurwitz's theorem implies that any such formula must involve denominators. Examples of such formulas can be written out explicitly (see Exercise 5).

The quadratic forms appearing in the Hurwitz–Radon composition formulas have a close relationship to Pfister forms. For any Pfister form φ of dimension 2^m there is an explicit construction showing that φ admits a composition with some form σ having the maximal dimension $\rho(2^m)$. The converse is an interesting open question.

Pfister Factor Conjecture. Suppose q is a quadratic form of dimension 2^m, and q admits a composition with some form of the maximal dimension $\rho(2^m)$. Then q is a scalar multiple of a Pfister form.

This conjecture is one of the central themes driving the topics chosen for the first part of the book. In Chapter 9 it is proved true when $m \leq 5$, and for larger values of m over special classes of fields.

The second part of this book focuses on the more general compositions of size $[r, s, n]$. In 1898 Hurwitz already posed the question: Which sizes are possible? The cases where $s = n$ were settled by Hurwitz and Radon in the 1920s. Further progress was made around 1940 when Stiefel and Hopf applied techniques of algebraic topology to the problem, (for compositions over the field of real numbers). In Part II we discuss these topological arguments and their generalizations, as well as considering the question for more general fields of coefficients. Further details are described in the Introduction to Part II.

Exercises for Chapter 0

Note: For the exercises in this book, most of the declarative statements are to be proved. This avoids writing "prove that" in every problem.

1. In any (bilinear) 4-square identity, if $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$ then z_2, z_3, z_4 must be skew-symmetric. (Compare 4-square identity of Euler above.)

2. **Doubling Lemma.** From an $[r, s, n]$-formula over F construct an $[r+1, 2s, 2n]$-formula.

(Hint. Given the Hurwitz Matrix Equations consider the $2n \times 2s$ matrices

$$C_1 = \begin{pmatrix} A_1 & 0 \\ 0 & A_1 \end{pmatrix},\ C_j = \begin{pmatrix} A_j & 0 \\ 0 & -A_j \end{pmatrix} \text{ for } 2 \le j \le r \text{ and } C_{r+1} = \begin{pmatrix} 0 & A_1 \\ -A_1 & 0 \end{pmatrix}.)$$

3. Let $x_1, x_2, \ldots, x_n$ be indeterminates and consider the set $\mathcal{S}$ of all the vectors $(\pm x_{\alpha(1)}, \pm x_{\alpha(2)}, \ldots, \pm x_{\alpha(n)})$ where α is a permutation of the n subscripts and $+/-$ signs are arbitrary. What is the largest number of mutually orthogonal elements of this set of $2^n n!$ vectors, using the usual dot product? Answer: The sharp bound is the Hurwitz–Radon function $\rho(n)$.

(Hint. If $v_1, \ldots, v_s$ is a set of mutually orthogonal vectors in $\mathcal{S}$ let A be the $n \times s$ matrix with columns v_j. Then $A^\top \cdot A = \sigma I_s$ where $\sigma = x_1^2 + x_2^2 + \cdots + x_n^2$. This provides a composition formula of size $[n, s, n]$.)

4. **Integer compositions.** Suppose a composition formula of size $[r, s, n]$ is given with *integer* coefficients. As above, let $Z = AY$ where A is an $n \times s$ matrix whose entries are linear forms in X, and $A^\top \cdot A = \sigma I_s$ where $\sigma = x_1^2 + x_2^2 + \cdots + x_r^2$.

(1) The columns of A are orthogonal vectors, and each column consists of the entries $\pm x_1, \ldots, \pm x_r$, placed (in some order) in r of the n positions, with zeros elsewhere. When $r = n$ the columns of A are signed permutations of X.

(2) The matrix A for the 2-square identity is $\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$, where we write only the subscript of each x_i. Similarly express A for the 4-square identity. Try to construct the 8-square identity directly in this way. (Explicit matrices A were listed by Hurwitz (1898).)

(3) Write down the matrix A for a composition of size $[3, 5, 7]$.

(Hint: (3) Express $(x_1^2 + x_2^2 + x_3^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2)$ as 4 squares.

5. Define $D_F(n)$ to be the set of those non-zero elements of the field F which are expressible as sums of n squares of elements of F.

Theorem (Pfister). *$D_F(n)$ is a group whenever $n = 2^m$.*

This result motivated Pfister's theorem on multiplicative quadratic forms. Here is a proof.

(1) If $D_F(n)$ is closed under multiplication then it is a group.

(2) **Lemma.** *Suppose $c = c_1^2 + c_2^2 + \cdots + c_n^2$ where $n = 2^m$. Then there exists an $n \times n$ matrix C having first row $(c_1, c_2, \ldots, c_n)$ and satisfying $C \cdot C^\top = C^\top \cdot C = cI_n$.*

(3) *Proof of Theorem.* Let $c, d \in D_F(n)$, with the corresponding matrices C, D from the lemma. Then $A = CD^\top$ satisfies $AA^\top = cdI_n$, hence $cd \in D_F(n)$.

(4) **Corollary.** *Let $n = 2^m$ and $x_1, , \ldots, x_n, y_1, \ldots, y_n$ be indeterminates. Then there exist $z_1, \ldots, z_n \in F(X)[Y]$ such that*

$$(x_1^2 + \cdots + x_n^2) \cdot (y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2. \qquad (*)$$

In fact we can choose each z_i to be a linear form in Y and $z_1 = x_1 y_1 + \cdots + x_n y_n$.

If $n = 16$, there exists such an identity where $z_1, , \ldots, z_8$ are bilinear forms in X, Y while $z_9, \ldots, z_{16}$ are linear forms in Y. What denominators are involved in the terms z_j?

(Hint. (1) Note that $F^{\bullet 2} \subseteq D_F(n)$.

(2) Express $c = a + b$ where a, b are the sums of 2^{m-1} of the c_k^2. Let A, B be the corresponding matrices which exist by induction. If $a \neq 0$ define $C = \begin{pmatrix} A & B \\ \diamond & A^\top \end{pmatrix}$, where the entry $\diamond$ is to be filled in. If $b \neq 0$ use $C = \begin{pmatrix} A & B \\ B^\top & \diamond \end{pmatrix}$. What if $a = b = 0$?

(4) When $n = 16$, start from a bilinear 8-square identity, then build up the matrix C.)

6. **Hurwitz–Radon function.**

(1) If $n = 2^m \cdot (\text{odd})$ then $\rho(n) = \begin{cases} 8a + 1 & \text{if } m = 4a, \\ 8a + 2 & \text{if } m = 4a + 1, \\ 8a + 4 & \text{if } m = 4a + 2, \\ 8a + 8 & \text{if } m = 4a + 3. \end{cases}$

(2) Given r define $v(r)$ to be the minimal n for which there exists an $[r, n, n]$ formula. Then $v(r) = 2^{\delta(r)}$ where $\delta(r) = \min\{m : r \leq \rho(2^m)\}$. Then $\rho(2^m) = \max\{r : \delta(r) = m\}$ and

$$\delta(r) = \#\{k : 0 < k < r \text{ and } k \equiv 0, 1, 2 \text{ or } 4 \pmod 8\}.$$

Here are the first few values:

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\delta(r)$	0	1	2	2	3	3	3	3	4	5	6	6	7	7	7	7

(3) $r \leq \rho(2^m)$ if and only if $\delta(r) \leq m$. Equivalently: $r \leq \rho(n)$ iff $2^{\delta(r)} | n$. Note: $r \leq 2^{\delta(r)}$ with equality if and only if $r = 1, 2, 4, 8$.

7. **Vector fields on spheres.** Let S^{n-1} be the unit sphere in the euclidean space $\mathbb{R}^n$.

A (tangent) *vector field* on S^{n-1} is a continuous map $f : S^{n-1} \to \mathbb{R}^n$ for which $f(x)$ is a vector tangent to S^{n-1} at x, for every $x \in S^{n-1}$. Using $\langle x, y \rangle$ for the dot product on $\mathbb{R}^n$, this says: $\langle x, f(x) \rangle = 0$ for every x. Define a vector field to be *linear* if the map f is the restriction of a linear map $\mathbb{R}^n \to \mathbb{R}^n$. A set of vector fields satisfies a property if that property holds at every point x. For instance, a vector field f is non-vanishing if $f(x) \neq 0$ for every $x \in S^n$.

(1) There is a non-vanishing linear vector field on S^{n-1} if and only if n is even.

(2) There exist r independent, linear vector fields on S^{n-1} if and only if $r \leq \rho(n) - 1$. Consequently, S^{n-1} admits $n-1$ independent linear vector fields if and only if $n = 1, 2, 4$ or 8.

(Hint. (1) A linear vector field is given by an $n \times n$ matrix A with $A^\top = -A$. It is non-vanishing iff A is nonsingular.

(2) The vector fields, and Gram–Schmidt, provide r mutually orthogonal, unit length, linear vector fields on S^{n-1}. These lead to the Hurwitz matrix equations.)

Remark. With considerable topological work, the hypothesis "linear" can be removed here. For example, the fact that S^2 has no non-vanishing vector field (the "Hairy Ball Theorem") is a result often proved in beginning topology courses. Finding the maximal number of linearly independent tangent vector fields on S^{n-1} is a famous topic in algebraic topology. Adams finally solved this problem in 1962, showing that the maximal number is just $\rho(n) - 1$. In particular, S^{n-1} is "parallelizable" (i.e. it has $n-1$ linearly independent tangent vector fields) if and only if $n = 1, 2, 4$ or 8.

8. **Division algebras.** Let F be a field. An *F-algebra* is defined to be an F-vector space A together with an F-bilinear map $m : A \times A \to A$. (Note that there are no assumptions of associativity, commutativity or identity element here.) Writing $m(x, y)$ as xy we see that the distributive laws hold and the scalars can be moved around freely. For $a \in A$ define the linear maps $L_a, R_a : A \to A$ by $L_a(x) = ax$ and $R_a(x) = xa$. Define A to be a *division algebra* if L_a and R_a are bijective for every $a \neq 0$.

(1) Suppose A is a finite dimensional F-algebra. Then A is a division algebra if and only if it has no zero-divisors.

(2) Suppose D is a division algebra over F, choose non-zero elements $u, v \in D$, and define a new multiplication $\diamond$ on D by: $x \diamond y = (R_u^{-1}(x))(L_v^{-1}(y))$. Then $(xu) \diamond (vy) = xy$ and $(D, \diamond)$ is a division algebra over F with identity element vu.

(3) F-algebras $(A, \cdot)$ and $(B, *)$ are defined to be *isotopic* (written $A \sim B$) if there exist bijective linear maps $\alpha, \beta, \gamma : A \to B$ such that $\gamma(x \cdot y) = \alpha(x) * \beta(y)$ for every $x, y \in A$. Isotopy is an equivalence relation on the category of F-algebras, and $A \cong B$ implies $A \sim B$. If A is a division algebra and $A \sim B$ then B is a division algebra. Every F-division algebra is isotopic to an F-division algebra with identity.

Remark. Since we are used to the associative law, great care must be exercised when dealing with such general division algebras. Suppose A is a division algebra with 1 and $0 \neq a \in A$. There exist $b, c \in A$ with $ba = 1$ and $ac = 1$. These left and right "inverses" are unique but they can be unequal. Even if $b = c$ it does not follow that $b \cdot ax = x$ for every x. See Exercise 8.7.

9. **Division algebras and vector fields.** Suppose there is an n-dimensional real division algebra (with no associativity assumptions).

(1) There is such a division algebra D with identity element e. (Use Exercise 8(2).)

(2) If $d \in D$ let $f_d(x)$ be the projection of $d * x$ to $(x)^{\perp}$. Then f_d is a vector field on S^{n-1} which is non-vanishing if $d \notin \mathbb{R} \cdot e$. A basis of D induces $n-1$ linearly independent vector fields on S^{n-1}.

(3) Deduce the "1, 2, 4, 8 Theorem" for real division algebras from Adams' theorem on vector fields (mentioned in Exercise 7).

10. **Hopf maps.** Suppose there is a real composition formula of size $[r, s, n]$. Then there is a bilinear map $f : \mathbb{R}^r \times \mathbb{R}^s \to \mathbb{R}^n$ satisfying $|f(x, y)| = |x| \cdot |y|$ for every $x \in \mathbb{R}^r$ and $y \in \mathbb{R}^s$. Construct the associated Hopf map $h : \mathbb{R}^r \times \mathbb{R}^s \to \mathbb{R} \times \mathbb{R}^n$ by $h(x, y) = (|x|^2 - |y|^2, 2f(x, y))$.

(1) $|h(x, y)| = |(x, y)|^2$, using the usual Euclidean norms.

(2) h restricts to a map on the unit spheres $h_0 : S^{r+s-1} \to S^n$.

(3) If $x \in S^{r-1}$ and $y \in S^{s-1}$ then $(\cos(\theta) \cdot x, \sin(\theta) \cdot y) \in S^{r+s-1} \subseteq \mathbb{R}^r \times \mathbb{R}^s$. This provides a covering $S^1 \times S^{r-1} \times S^{s-1} \to S^{r+s-1}$. The Hopf map h_0 carries

$$(\cos(\theta) \cdot x, \sin(\theta) \cdot y) \mapsto (\cos(2\theta), \sin(2\theta) \cdot f(x, y)).$$

(4) When $r = s = n = 1$ the map $h_0 : S^1 \to S^1$ wraps the circle around itself twice. When $r = s = n = 2$ the map $h : \mathbb{C} \times \mathbb{C} \to \mathbb{R} \times \mathbb{C}$ induces $h_0 : S^3 \to S^2$. This map is surjective and each fiber is a circle. Further properties of Hopf maps are described in Chapter 15.

Notes on Chapter 0

Further details on the history of n-square identities appear in Dickson (1919), van der Blij (1961), Curtis (1963), Halberstam and Ingham (1967), Taussky (1970), (1981) and van der Waerden (1976), (1985). The interesting history of Hamilton and his quaternions is described in Crowe (1967). Veldkamp (1991) also has some historical remarks on octonions.

The terminology for the 8-dimensional composition algebra has changed over the years. The earliest name was "octaves" used by Graves and others in the 19th century. This term remained in use in German articles (e.g. Freudenthal in the 1950s), and some authors followed that tradition in English. Many papers in English used "Cayley numbers", the "Cayley algebra" or the "Cayley–Dickson algebra". The term "octonions" came into use in the late 1960s, and may have first appeared in Jacobson's book (1968). Several of Jacobson's students were using "octonions" shortly after that and this terminology has become fairly standard. Jacobson himself says that this term was motivated directly from "the master of terminology" J. J. Sylvester, who introduced quinions, nonions and sedenions. See Sylvester (1884).

In proving his 1, 2, 4, 8 Theorem, Hurwitz deduced the linear independence of the 2^{r-2} matrices formed by products of subsets of $\{B_2, \ldots, B_{r-1}\}$. His argument used the skew-symmetry of the B_j. The more general independence result, proved in

(1.11), first appeared in Robert's thesis (1912), written under the direction of Hurwitz. It also appears in the posthumous paper of Hurwitz (1923). Compare Exercise 1.12.

It is interesting to note that the law of multiplication of quaternions had been discovered, but not published, by Gauss as early as 1820. See the reference in van der Waerden (1985), p. 183.

The theory of Pfister forms appears in a number of books, including Lam (1973) and Scharlau (1985) and in Knebusch and Scharlau (1980). The basic multiplicative properties of Pfister forms are derived in Chapter 5.

Basic topological results (Hairy Ball Theorem, vector fields on spheres, etc.) appear in many topology texts, including Spanier (1966) and Husemoller (1975). Further information on these topics is given in Chapter 12.

Exercise 5. This property of $D_F(2^m)$ was foreshadowed by the 8 and 16 square identities of Taussky (1966) and Zassenhaus and Eichhorn (1966). The multiplicative properties of $D_F(n)$ were discovered by Pfister (1965a) and generalized in (1965b). The simple matrix proof here is due to Pfister and appears in Lam (1973), pp. 296–298 and in Knebusch and Scharlau (1980), pp. 12–14. Pfister's analysis of the more general products $D_F(r) \cdot D_F(s)$ is presented in Chapter 14.

Exercise 6. The function $\delta(r)$ arises later in (2.15) and Exercise 2.3, and comes up in K-theory as mentioned in (12.17) and (12.19).

Exercise 7. Further discussion of Adams' work in K-theory is mentioned in Chapter 12.

Exercise 8. (2) This trick to get an identity element goes back to Albert (1942b) and was also used by Kaplansky (1953).

(3) Isotopies were probably first introduced by Albert (1942b). He mentions that this equivalence relation on algebras was motivated by some topological results of Steenrod.

Exercise 9. The statement of the 1, 2, 4, 8 Theorem on real division algebras is purely algebraic, but the only known proofs involve non-trivial topology or analysis. The original proofs (due to Milnor and Bott, and Kervaire in 1958) were simplified using the machinery of K-theory. Gilkey (1987) found an analytic proof. Real division algebras are also mentioned in Chapter 8 and Chapter 12. Hirzebruch (1991) provides a well-written outline of the geometric ideas behind these applications of algebraic topology.

Exercise 10. The Hopf map $S^3 \to S^2$ is an important example in topology. Hopf (1931) proved that this map is not homotopic to a constant, providing early impetus for the study of homotopy theory and fiber bundles. Further information on Hopf maps appears in Gluck, Warner and Ziller (1986), and Yiu (1986). Also see Chapter 15.

Part I

Classical Compositions and Quadratic Forms

Chapter 1

Spaces of Similarities

In order to understand the Hurwitz matrix equations we formulate them in the more general context of bilinear forms and quadratic spaces over a field F. The first step is to use linear transformations in place of matrices, and adjoint involutions in place of transposes. Then we will see that a composition formula becomes a linear subspace of similarities. This more abstract approach leads to more general results and simpler proofs, but of course the price is that readers must be familiar with more notations and terminology.

Rather than beginning with the Hurwitz problem here, we introduce some standard notations from quadratic form theory, discuss spaces of similarities, and then remark in (1.9) that these subspaces correspond with composition formulas. The chapter ends with a quick proof of the Hurwitz 1, 2, 4, 8 Theorem.

We follow most of the standard notations in the subject as given in the books by T. Y. Lam (1973) and W. Scharlau (1985). Throughout this book we work with a field F having characteristic not 2. (For if $2 = 0$ then every sum of squares is itself a square, and the original question about composition formulas becomes trivial.)

Suppose (V, q) is a *quadratic space* over F. This means that V is a (finite dimensional) F-vector space $q : V \to F$ is a regular quadratic form. To explain this, we define

$$B = B_q : V \times V \to F \quad \text{by} \quad 2B(x, y) = q(x + y) - q(x) - q(y).$$

Then q is a *quadratic form* if this B_q is a bilinear map and if $q(ax) = a^2 q(x)$ for every $a \in F$ and $x \in V$. The form q (or the bilinear form B) is *regular* if $V^\perp = 0$, that is:

$$\text{if } x \in V \text{ and } B(x, y) = 0 \text{ for every } y \in V, \text{ then } x = 0.$$

If q is not regular it is called *singular*. (Regular forms are sometimes called nonsingular or nondegenerate.) Since 2 is invertible in F, the bilinear form B can be recovered from the associated quadratic form q by:

$$q(x) = B(x, x) \quad \text{for all } x \in V.$$

Depending on the context we use several notations to refer to such a quadratic space. It could be called (V, q) or (V, B), or sometimes just V or just q.

To get the matrix interpretation of a quadratic space (V, q), choose a basis $\{e_1, \ldots, e_n\}$ of V. The form q can then be regarded as a homogeneous degree 2 polynomial by setting $q(X) = q(x_1, \ldots, x_n) = q(x_1e_1 + \cdots + x_ne_n)$. The *Gram matrix* of q is $M = (B(e_i, e_j))$, an $n \times n$ symmetric nonsingular matrix. Then $q(X) = X^\top \cdot M \cdot X$, where X is viewed as a column vector and $X^\top$ denotes the transpose. Another basis for V furnishes a matrix M' congruent to M, that is: $M' = P^\top \cdot M \cdot P$ where P is the basis-change matrix.

Here is a list of some of the terminology used throughout this book. Further explanations appear in the texts by Lam and Scharlau.

1_V denotes the identity map on a vector space V. Then $1_V \in \mathrm{End}(V)$.

$F^\bullet = F - \{0\}$, the multiplicative group of F.

$F^{\bullet 2} = \{a^2 : a \in F^\bullet\}$, the group of squares.

$\langle c \rangle = cF^{\bullet 2}$ is the coset of c in the group of square classes $F^\bullet / F^{\bullet 2}$. We also use $\langle c \rangle$ to denote the 1-dimensional quadratic form with a basis element of length c.

$\langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$ is the quadratic space (V, q) where V has a basis whose corresponding Gram matrix is $\mathrm{diag}(a_1, \ldots, a_n)$. Interpreted as a polynomial this form is $q(X) = a_1x_1^2 + \cdots + a_nx_n^2$.

$\langle\langle a_1, a_2, \ldots, a_n \rangle\rangle = \langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle$ is the n-fold Pfister form. It is a quadratic form of dimension 2^n. For example $\langle\langle a, b \rangle\rangle = \langle 1, a, b, ab \rangle$.

$\det(q) = \langle d \rangle$ if the determinant of a Gram matrix M_q equals d. Choosing a different basis alters $\det(M_q)$ by a square, so $\det(q)$ is a well-defined element in $F^\bullet / F^{\bullet 2}$.

$dq = (-1)^{n(n-1)/2} \det(q)$ when $\dim q = n$.

$q_1 \perp q_2$ and $q_1 \otimes q_2$ are the orthogonal direct sum and tensor product of the quadratic forms q_1 and q_2.

$q_1 \simeq q_2$ means that q_1 and q_2 are isometric.

$q_1 \subset q_2$ means that q_1 is isometric to a subform of q_2.

$nq = q \perp \cdots \perp q$ (n terms). In particular, $n\langle 1 \rangle = \langle 1, 1, \ldots, 1 \rangle$.

$\langle a \rangle q = \langle a \rangle \otimes q$ is a form *similar* to q.

$D_F(q) = \{a \in F^\bullet : q \text{ represents } a\}$ is the value set.

$G_F(q) = \{a \in F^\bullet : \langle a \rangle q \simeq q\}$ is the group of "norms", or "similarity factors" of q.

1.1 Definition. Let (V, q) be a quadratic space over F with associated bilinear form B. If $c \in F$, a linear map $f : V \to V$ is a *c-similarity* if

$$B(f(x), f(y)) = cB(x, y)$$

for every $x, y \in V$. The scalar $c = \mu(f)$ is the *norm* (also called the multiplier, similarity factor or ratio) of f. A map is a *similarity* if it is a c-similarity for some scalar c. An *isometry* is a 1-similarity.

Let $\mathrm{Sim}(V, q)$ be the set of all such similarities. Sometimes it is denoted by $\mathrm{Sim}(V)$, $\mathrm{Sim}(V, B)$ or $\mathrm{Sim}(q)$. It is easy to check that the composition of similarities is again a similarity and the norms multiply: $\mu(fg) = \mu(f)\mu(g)$. If f is a similarity and b is a scalar: $\mu(bf) = b^2\mu(f)$.

Suppose $f \in \mathrm{Sim}(V)$ and $\mu(f) = c \neq 0$. Then f must be bijective (using the hypothesis that V is regular to conclude that f is injective), so that f induces an isometry from $(V, \langle c\rangle q)$ to (V, q). Then $\langle c\rangle q \simeq q$ and the norm $c = \mu(f)$ lies in the group $G_F(q)$.

Define $\mathrm{Sim}^\bullet(V, q) = \{f \in \mathrm{Sim}(V, q) : \mu(f) \neq 0\}$, the set of invertible elements in $\mathrm{Sim}(V, q)$. Then $\mathrm{Sim}^\bullet(V, q)$ is a group containing the non-zero scalar maps and the orthogonal group $\mathrm{O}(V, q)$ as subgroups.[1] The norm map $\mu : \mathrm{Sim}^\bullet(V, q) \to F^\bullet$ is a group homomorphism yielding the exact sequence:

$$1 \longrightarrow \mathrm{O}(V, q) \longrightarrow \mathrm{Sim}^\bullet(V, q) \longrightarrow G_F(q) \longrightarrow 1.$$

The subgroup $F^\bullet \mathrm{O}(V, q)$ consists of all elements $f \in \mathrm{Sim}^\bullet(V, q)$ where $\mu(f) \in F^{\bullet 2}$. For instance if F is algebraically closed, everything in $\mathrm{Sim}^\bullet(V, q)$ is a scalar multiple of an isometry. The notation "$\mathrm{Sim}(V, q)$" is an analog of "$\mathrm{End}(V)$", emphasizing the *additive* structure of the similarities, so it is important to include 0-similarities.

The adjoint involution I_q is essential to our analysis of similarities. This map I_q is a generalization of the transpose of matrices.[2]

1.2 Definition. Let (V, q) be a quadratic space with associated bilinear form B. The adjoint map $I_q : \mathrm{End}(V) \to \mathrm{End}(V)$ is characterized by the formula:

$$B(v, I_q(f)(w)) = B(f(v), w)$$

for $f \in \mathrm{End}(V)$ and $v, w \in V$. When convenient we write $\tilde{f}$ instead of $I_q(f)$.

It follows from the regularity of the form that I_q is a well-defined map which is an F-linear anti-automorphism of $\mathrm{End}(V)$ whose square is the identity. If a basis of V is chosen we obtain the Gram matrix M of the form q, and the matrix A of the map $f \in \mathrm{End}(V)$. Then the matrix of $\tilde{f} = I_q(f)$ is just $M^{-1}A^\top M$, a conjugate of the transpose matrix $A^\top$. If $q \simeq n\langle 1\rangle = \langle 1, \ldots 1\rangle$ and an orthonormal basis is chosen, then I_q coincides with the transpose of matrices.

1.3 Lemma. *Let (V, q) be a quadratic space.*

(1) *If $f \in \mathrm{End}(V)$ then f is a c-similarity if and only if $\tilde{f}f = c1_V$.*

---

1 There seems to be no standard notation for this group. Some authors call it $\mathrm{GO}(V, q)$.

2 The notation I_q should not cause confusion with the $n \times n$ identity matrix I_n (we hope).

(2) *If* $f, g \in \mathrm{Sim}(V)$ *the following statements are equivalent:*
   (i) $f + g \in \mathrm{Sim}(V)$.
   (ii) $af + bg \in \mathrm{Sim}(V)$ *for every* $a, b \in F$.
   (iii) $\tilde{f}g + \tilde{g}f = c1_V$ *for some* $c \in F$.

Proof. Part (1) follows easily from the definitions and (2) is a consequence of (1). □

Similarities $f, g \in \mathrm{Sim}(V)$ are called *comparable* if $f + g \in \mathrm{Sim}(V)$ as well. The lemma implies that if $f_1, f_2, \ldots, f_r$ are pairwise comparable similarities in $\mathrm{Sim}(V)$ then the whole vector space $S = \mathrm{span}\{f_1, f_2, \ldots, f_r\}$ is inside $\mathrm{Sim}(V)$. For if $g \in S$ then g is a linear combination of the maps f_i, and $\tilde{g}g$ is a linear combination of the terms $\tilde{f}_i f_i$ and $\tilde{f}_i f_j + \tilde{f}_j f_i$. Since these terms are scalars by hypothesis, $\tilde{g}g$ is also a scalar and $g \in \mathrm{Sim}(V)$.

Such a subspace $S \subseteq \mathrm{Sim}(V)$ is more than just a linear space. The map μ restricted to S induces a quadratic form σ on S. (To avoid notatonal confusion we have not used the letter μ again for this form on S.) Generally if $f, g \in \mathrm{Sim}(V)$ are comparable, define $B_\mu(f, g) \in F$ by:

$$\tilde{f}g + \tilde{g}f = 2B_\mu(f, g)1_V.$$

Then B_μ is bilinear whenever it is defined, and $\mu(f) = B_\mu(f, f)$. This map $\mu : \mathrm{Sim}(V) \to F$ has all the properties of a quadratic form except that its domain is not necessarily closed under addition.

The induced quadratic form σ on a subspace $S \subseteq \mathrm{Sim}(V)$ could be singular. Of course, this can occur only when there are non-trivial 0-similarities of V. A map $f \in \mathrm{End}(V)$ is a 0-similarity if and only if the image $f(V)$ is a totally isotropic subspace of V (i.e. the quadratic form vanishes identically on $f(V)$). Then if (V, q) is anisotropic, the only 0-similarity is the zero map.

> We will restrict attention to those $S \subseteq \mathrm{Sim}(V)$
> whose induced quadratic form is regular.

If S is a subspace of similarities with induced (regular) quadratic form σ, we write $(S, \sigma) \subseteq \mathrm{Sim}(V, q)$. If σ is a quadratic form over F we write

$$\sigma < \mathrm{Sim}(V, q)$$

if there exists a subspace $S \subseteq \mathrm{Sim}(V, q)$ whose induced quadratic form is isometric to σ.

Given q what is the largest possible σ?

Given σ what is the smallest possible q?

Various aspects of these questions comprise Part I of this book.

1.4 Proposition. *Suppose* $(S, \sigma) \subseteq \mathrm{Sim}(q)$ *is a regular subspace of similarities.*

(1) *If* $a \in D_F(q)$ *then* $\langle a \rangle \sigma \subset q$. *In particular,* $\dim \sigma \leq \dim q$.

(2) *If* σ *is isotropic then* q *is hyperbolic.*

Proof. (1) For any $v \in V$, the evaluation map $S \to V$ sending $f \mapsto f(v)$ is a $q(v)$-similarity. If $q(v) \neq 0$ then this map must be injective, since (S, σ) is regular.

(2) If $\dim V = n$ then any totally isotropic subspace of V has dimension $\leq n/2$, and (V, q) is hyperbolic if and only if there exist totally isotropic subspaces of dimension equal to $n/2$. We are given a 0-similarity $f \in S$ with $f \neq 0$. Since $\tilde{f} f = 0$, image $f = f(V)$ is totally isotropic. Also $\ker f$ is totally isotropic, for if $v \in V$ has $q(v) \neq 0$ then the proof of part (1) shows that $f(v) \neq 0$. Then $\dim \text{image } f$ and $\dim \ker f$ are both $\leq n/2$, but their sum equals n. Therefore these dimensions equal $n/2$ and (V, q) is hyperbolic. □

We can also generalize the Hurwitz Matrix Equations mentioned in Chapter 0.

1.5 Lemma. *Let* (V, q) *be a quadratic space and* $(S, \sigma) \subseteq \mathrm{Sim}(V)$. *If the form* σ *on* S *has Gram matrix* $M_\sigma = (c_{ij})$, *then there exist* $f_i \in S$ *satisfying*

$$\tilde{f}_i f_j + \tilde{f}_j f_i = 2c_{ij} 1_V, \quad \textit{for all } 1 \leq i, j \leq s.$$

Conversely if maps $f_i \in \mathrm{End}(V)$ *satisfy these equations then they span a subspace* $S \subseteq \mathrm{Sim}(V)$ *where the induced form has Gram matrix* $M = (c_{ij})$.

Proof. By definition of the Gram matrix, there is a basis $\{f_1, \ldots, f_s\}$ of S such that $c_{ij} = B_\mu(f_i, f_j)$. The required equations are immediate from the definition of B_μ. Conversely, given f_i satisfying those equations, the remarks after Lemma 1.3 imply that $S = \mathrm{span}\{f_1, \ldots, f_n\}$ is a subspace of $\mathrm{Sim}(V, q)$. □

Suppose that we choose an *orthogonal* basis $\{f_1, \ldots, f_n\}$ of S. Then $\sigma \simeq \langle a_1, \ldots, a_s \rangle$ and

$$\begin{aligned} \tilde{f}_i f_i &= a_i 1_V \qquad \text{for } 1 \leq i \leq s, \\ \tilde{f}_i f_j + \tilde{f}_j f_i &= 0 \qquad \text{for } 1 \leq i, j \leq s. \end{aligned}$$

When $\sigma = s\langle 1 \rangle = \langle 1, 1, \ldots, 1 \rangle$ and $q = n\langle 1 \rangle = \langle 1, 1, \ldots, 1 \rangle$ and we use matrices, these equations become the Hurwitz Matrix Equations mentioned in Chapter 0.

Here are some ways to manipulate subspaces of $\mathrm{Sim}(V)$.

1.6 Lemma. *Let* $(S, \sigma) \subseteq \mathrm{Sim}(V, q)$ *over the field* F.

(1) *If* (W, δ) *is another quadratic space then* $\sigma < \mathrm{Sim}(q \otimes \delta)$.

(2) *If* K *is an extension field of* F *then* $\sigma \otimes K < \mathrm{Sim}(q \otimes K)$.

(3) *If* $f, g \in \mathrm{Sim}^\bullet(V, q)$ *then* $fSg \subseteq \mathrm{Sim}(V, q)$.

Proof. (1) Use $S \otimes 1_w$ acting on $V \otimes W$.

(2) If $f_i \in S$ and $c_i \in K$ then Lemma 1.3 implies that $\sum f_i c_i$ lies in $\mathrm{Sim}(V \otimes K)$.

(3) This is clear since $\mathrm{Sim}(V, q)$ is closed under composition. □

The ideas developed so far can be generalized to subspaces of $\mathrm{Sim}(V, W)$ for two quadratic spaces (V, q) and (W, q'). (See Exercise 2.) In this case the matrices are rectangular and the involution is replaced by the map $J = J_W^V : \mathrm{Hom}(V, W) \to \mathrm{Hom}(W, V)$. Since our main concern is the case $V = W$, we will not pursue this generality here. The main advantage of this restriction is that we can arrange the identity map 1_V to be in S.

1.7 Proposition. *Let $\sigma \simeq \langle 1, a_2, \ldots, a_s \rangle$ be a quadratic form representing* 1.

Then $\sigma < \mathrm{Sim}(V, q)$ if and only if there exist maps $f_2, \ldots, f_s$ in $\mathrm{End}(V)$ *satisfying:*

$$\begin{aligned} \tilde{f}_i &= -f_i \\ f_i^2 &= -a_i 1_V \end{aligned} \qquad \text{for } 2 \le i \le s,$$

$$f_i f_j = -f_j f_i \qquad \text{whenever } i \ne j.$$

Proof. Given $S \subseteq \mathrm{Sim}(V)$ with induced form σ we can choose maps f_i as above. Replacing S by the isometric space $f_1^{-1} S$ we may assume that $f_1 = 1_V$. Then the equations above reduce to those given here. The converse follows similarly. □

The conditions above correspond to the second form of the Hurwitz Matrix Equations. With this formulation an experienced reader will notice that the algebra generated by the f_i is related to the Clifford algebra $C(\langle -a_2, \ldots, -a_s \rangle)$. This connection is explored in Chapter 4.

1.8 Example. Let $q = \langle 1, a \rangle$ with corresponding basis $\{e_1, e_2\}$ of V. The adjoint involution I_q on $\mathrm{End}(V)$ is translated into matrices as follows:

$$\text{if} \quad f = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \quad \text{then} \quad \tilde{f} = \begin{pmatrix} x & az \\ a^{-1}y & w \end{pmatrix}.$$

Let $f_2 = \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix}$, $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$. One can quickly check that $\tilde{f}_2 = -f_2$ and $f_2^2 = -a 1_V$. Then $S = \mathrm{span}\{1_V, f_2\} = \left\{ \begin{pmatrix} x & -ay \\ y & x \end{pmatrix} : x, y \in F \right\}$ is a subspace of $\mathrm{Sim}(\langle 1, a \rangle)$ and the induced form is $(S, \sigma) \simeq \langle 1, a \rangle$. Similarly g_1 and g_2 are comparable (in fact, orthogonal) similarities and $T = \mathrm{span}\{g_1, g_2\}$ is also a subspace of $\mathrm{Sim}(\langle 1, a \rangle)$ with induced form $\langle 1, a \rangle$.

This 2-dimensional example contains the germs of several ideas exploited below. One way to understand this example is to interpret $\langle 1, a\rangle$ as the usual norm form on the quadratic extension $K = F(\theta)$ where $\theta^2 = -a$. (When $-a \notin F^{\bullet 2}$, K is a field.) Let $\mathcal{L} : K \to \mathrm{End}(K)$ be the regular representation: $\mathcal{L}(x)(y) = xy$. With $\{1, \theta\}$ as the F-basis of K, the matrix of $\mathcal{L}(\theta)$ is f_2, and the subspace S above is just $\mathcal{L}(K) \subseteq \mathrm{Sim}(K)$. Similarly to get T define the twisted representation $\mathcal{L}' : K \to \mathrm{End}(K)$ by $\mathcal{L}'(x)(y) = x\bar{y}$. Then $T = \mathcal{L}'(K) \subseteq \mathrm{Sim}(K)$.

More generally suppose there is an F-algebra A furnished with a "norm" quadratic form q which is multiplicative: $q(xy) = q(x)q(y)$ for all $x, y \in A$. Using the left regular representation in a similar way, we get $q < \mathrm{Sim}(q)$. For instance the quaternion algebra $A = \left(\frac{-a,-b}{F}\right)$ with basis $\{1, i, j, k\}$ has the norm form $q \simeq \langle 1, a, b, ab\rangle$. Conversely if $q < \mathrm{Sim}(q)$ then q does arise as the norm form of some "composition algebra" A. Any subspace $\sigma < \mathrm{Sim}(q)$ can be viewed as coming from a "partial multiplication" $S \times V \to V$.

1.9 Proposition. *Suppose (V, q) and (S, σ) are quadratic spaces over F. The following conditions are equivalent:*

(1) $\sigma < \mathrm{Sim}(q)$.

(2) *There is a bilinear pairing $* : S \times V \to V$ satisfying $q(f * v) = \sigma(f)q(v)$ for every $f \in S$ and $v \in V$.*

(3) *There is a formula $\sigma(X)q(Y) = q(Z)$ where each z_k is a bilinear form in the systems of indeterminates X, Y with coefficients in F.*

Proof. (1) $\Longleftrightarrow$ (2). Given $S \subseteq \mathrm{Sim}(V, q)$ where the induced form on S is isometric to σ. For $f \in S$ and $v \in V$, define $f * v = f(v)$. Since f is a $\sigma(f)$-similarity we get required equation. Conversely, the map $*$ induces a linear map $\lambda : S \to \mathrm{End}(V)$ by $\lambda(f)(v) = f * v$. For each $f \in S$, $\lambda(f)$ is a $\sigma(f)$-similarity and therefore λ is an isometry from (S, σ) to the subspace $\lambda(S) \subseteq \mathrm{Sim}(V, q)$. Since (S, σ) is regular, this λ is injective and $\sigma < \mathrm{Sim}(q)$.

(1) $\Longrightarrow$ (3). Given $(S, \sigma) \subseteq \mathrm{Sim}(V, q)$ as before, choose bases $\{f_1, \ldots, f_s\}$ of S and $\{v_1, \ldots, v_n\}$ of V. Let $M = M_q$ be the $n \times n$ Gram matrix of q, $M_\sigma = (c_{ij})$ the $s \times s$ Gram matrix of σ, and A_i the $n \times n$ matrix of the map f_i. Then the matrix of $\tilde{f}_i$ is $M^{-1}A_i^\top M$ and the equations given in (1.5) become:

$$A_i^\top M A_j + A_j^\top M A_i = 2c_{ij}M, \quad \text{for } 1 = i, j = s.$$

Let $A = x_1A_1 + \cdots + x_sA_s$. Since the x_i are indeterminates the system of equations above is equivalent to the single equation:

$$A^\top M A = \sigma(X)M.$$

Since $q(Y) = Y^\top MY$ we see that $Z = AY$ satisfies the condition: $q(Z) = \sigma(X)q(Y)$.

(3) $\Longrightarrow$ (1). Reverse the steps above. □

If $\sigma < \mathrm{Sim}(q)$ and $\dim \sigma \geq 2$, then $\dim q$ must be even. One way to see this is to scale σ to represent 1 and get a map $f = f_2$ as in (1.7). Since f is nonsingular and skew-symmetric, the dimension must be even. (In matrix notation in the proof of (1.9) we see that MA is a skew-symmetric matrix.) For a different proof, let K be an extension field of F where σ becomes isotropic. Since $\sigma \otimes K < \mathrm{Sim}(q \otimes K)$, (1.4) implies $q \otimes K$ hyperbolic and hence of even dimension. The next proposition shows that more can be said about the structure of q.

1.10 Proposition. (1) *If* $\langle 1, a\rangle < \mathrm{Sim}(q)$ *then* $q \simeq \langle\langle a\rangle\rangle \otimes \varphi$ *for some form* φ.
(2) *If* $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ *then* $q \simeq \langle\langle a, b\rangle\rangle \otimes \psi$ *for some form* ψ.

Proof. (1) By hypothesis there is $f \in \mathrm{Sim}(V)$ with $\mu(f) = a$ and $\tilde{f} = -f$. This skew-symmetry implies $B(v, f(v)) = 0$ for every $v \in V$. Choose v with $q(v) \neq 0$. Then the line $U = Fv$ is a regular subspace such that U and $f(U)$ are orthogonal. Let U_0 be maximal among such regular subspaces. Then $U_0 \perp f(U_0)$ is a regular subspace of V. If this subspace is proper, choose $w \in (U_0 \perp f(U_0))^{\perp}$ with $q(w) \neq 0$ and note that $U_0 + Fw$ contradicts the maximality. Therefore $V = U_0 \perp f(U_0) \simeq \langle 1, a\rangle \otimes \varphi$, where φ is the quadratic form on U_0.

(2) Given a basis $1_V, f, g$ corresponding to $\langle 1, a, b\rangle$, choose W_0 maximal among the regular subspaces W for which W, $f(W)$, $g(W)$ and $fg(W)$ are mutually orthogonal. The argument above generalizes to show that $V = W_0 \perp f(W_0) \perp g(W_0) \perp fg(W_0) \simeq \langle 1, a, b, ab\rangle \otimes \psi$, where ψ is the quadratic form on W_0. □

This elementary proof in part (1) can perhaps be better understood by considering the given f as inducing an action of $K = F(\sqrt{-a})$ on V. The formation of U_0 corresponds to choosing a K-basis of V. Similarly part (2) corresponds to the action of the quaternion algebra $\left(\frac{-a,-b}{F}\right)$ on V. These ideas are explored in Chapter 4 when we view V as a module over a certain Clifford algebra.

We conclude this chapter with an independence argument, due to Hurwitz, which suffices to prove the "1, 2, 4, 8 Theorem". Let us first set up a multi-index notation. Let $\mathbb{F}_2 = \{0, 1\}$ be the field of 2 elements. If $\delta \in \mathbb{F}_2$ define

$$a^{\delta} = \begin{cases} 1 & \text{if } \delta = 0 \\ a & \text{if } \delta = 1. \end{cases}$$

Let $\Delta = (\delta_1, \ldots, \delta_n)$ be a vector in $\mathbb{F}_2^n$. If $f_1, f_2, \ldots, f_n$ are elements of some ring, define

$$f^{\Delta} = f_1^{\delta_1} \ldots f_n^{\delta_n}.$$

By convention $f^0 = 1$ here. Define $|\Delta|$ to be the number of indices i such that $\delta_i = 1$. Then f^{Δ} is a product of $|\Delta|$ elements f_i.

1.11 Proposition. *Suppose A is an associative F-algebra with 1 and $\{f_1, \ldots, f_n\}$ is a set of pairwise anti-commuting invertible elements of A. If n is even then $\{f^{\Delta} : \Delta \in \mathbb{F}_2^n\}$ is a linearly independent set of 2^n elements of A.*

Proof. Suppose there exists a non-trivial dependence relation and let $\sum c_\Delta f^\Delta = 0$ be such a relation having the fewest non-zero coefficients $c_\Delta \in F$. We may assume $c_0 \neq 0$ by multiplying the relation by $(f^\Delta)^{-1}$ for some Δ where $c_\Delta \neq 0$. For fixed i, conjugate the given relation by f_i and subtract, noting that $f_i f^\Delta f_i^{-1} = \pm f^\Delta$. The result is a shorter relation among the f^Δ (since the f^0 terms cancel). By the minimality of the given relation, this shorter one must be trivial. Therefore if $c_\Delta \neq 0$ then f^Δ must commute with f_i. Since this holds for every index i it follows that either $\Delta = 0$ or else $\Delta = (1, 1, \ldots, 1)$ and n is odd. Since n is even the dependence relation must have just one term: $c_0 f^0 = 0$, which is absurd. □

1.12 Corollary. *If* $\sigma < \mathrm{Sim}(V, q)$ *where* $\dim \sigma = s$ *and* $\dim q = n$, *then* $2^{s-2} \leq n^2$. *Consequently,* $s = n$ *is possible only when* $n = 1, 2, 4$ *or* 8.

Proof. By (1.7) there are $s - 1$ anti-commuting invertible elements in $\mathrm{End}(V)$. Since $\dim \mathrm{End}(V) = n^2$, Proposition 1.11 provides the inequality. If $s = n$ the inequality $2^{n-2} \leq n^2$ implies that $n \leq 8$. The restrictions given in (1.10) show that n must equal 1, 2, 4 or 8. □

Appendix to Chapter 1. Composition algebras

This appendix contains another proof of the 1, 2, 4, 8 Theorem. This approach uses the classical "doubling process" to construct the composition algebras, so it provides information on the underlying algebras and not just their dimensions. This appendix is self-contained, using somewhat different notation for the quadratic and bilinear forms. The theorem here is well- known, first proved by Albert (1942a), who also handled the case when the characteristic is 2. The organization of the ideas here follows a lecture by J. H. Conway (1980).

Suppose F is a field with characteristic $\neq 2$ and let A be an F-algebra. This algebra is not assumed to be associative or finite dimensional: A is simply an F-vector space and the multiplication is an F-bilinear map $A \times A \to A$. We do assume that A has an identity element 1.

A.1 Definition. An F-algebra A with 1 is called a *composition algebra* if there is a regular quadratic form $A \to F$, denoted $a \mapsto [a]$, such that

$$[a] \cdot [b] = [ab] \quad \text{for every } a, b \in A. \tag{$*$}$$

Let $[a, b]$ denote the associated symmetric bilinear form: $2[a, b] = [a+b] - [a] - [b]$. This differs from our previous notation: $[a] = q(a)$ and $[a, b] = B(a, b)$. This notation will not be used elsewhere in this book because the square brackets stand for so many other things (like quaternion symbols and cohomology classes).

We will determine all the possible composition algebras over F. The classical examples over the field $\mathbb{R}$ include the real numbers (dim $= 1$), the complex numbers (dim $= 2$), the quaternions (dim $= 4$) and the octonions (dim $= 8$). We assume no knowledge of these examples and consider an arbitrary composition algebra A over F. This appendix is organized as a sequence of numbered statements, with hints for their proofs.

A.2. $[ac, ad] = [a] \cdot [c, d]$. (Set $b = c + d$ in $(*)$).
Symmetrically, $[ac, bc] = [a, b] \cdot [c]$.

A.3. *The "Flip Law":* $[ac, bd] = 2[a, b] \cdot [c, d] - [ad, bc]$.
(Replace a by $a + b$ in (A.2)).

A.4. *Define "bar" by:* $\bar{c} = 2[c, 1] - c$.
Then $[ac, b] = [a, b\bar{c}]$. (Apply (A.3) with $d = 1$.)
Symmetrically, $[ca, b] = [a, \bar{c}b]$.

Repeating property (A.4) yields a "braiding sequence" of six equal quantities:

$$\cdots = [a, bc] = [a\bar{c}, b] = [\bar{c}, \bar{a}b] = [\bar{c}\bar{b}, \bar{a}] = [\bar{b}, c\bar{a}] = [\bar{b}a, c] = [a, bc] = \cdots$$

Basic Principle: to prove $X = Y$ show that $[X, t] = [Y, t]$ for every $t \in A$.

A.5. *Properties of "bar":*

$\overline{a + b} = \bar{a} + \bar{b}$.

c *is scalar if and only if* $\bar{c} = c$.

$[a, b] = [\bar{a}, \bar{b}]$. (Apply the braiding sequence when $c = 1$.)

$\bar{\bar{c}} = c$. (Use the Basic Principle.)

$\overline{bc} = \bar{c}\bar{b}$. (Use $[a, bc] = [\bar{c}\bar{b}, \bar{a}]$ from braiding.)

$\bar{b} \cdot ac = 2[a, b]c - \bar{a} \cdot bc$. (Use (A.3), isolate d, apply the Basic Principle: $[\bar{b} \cdot ac, d] = [2[a, b]c, d] - [\bar{a} \cdot bc, d]$.)

$\bar{a} \cdot ab = ba \cdot \bar{a} = [a]b$. (Set $a = b$ in previous line.)

$\bar{a}a = a\bar{a} = [a]$. (Set $b = 1$ in previous line.)

Since $\bar{a} = 2[a, 1] - a$ we have $a \cdot ab = a^2 b$ and $ba \cdot a = ba^2$. These are the "Alternative Laws", a weak version of associativity.

Now suppose that $H \subseteq A$ is a composition subalgebra (that is, H is an F-subalgebra on which the quadratic form is regular, i.e. $H \cap H^{\perp} = 0$.) Suppose $H \neq A$. Then we may choose $i \in H^{\perp}$ with $[i] = \alpha \neq 0$.

A.6. *H and Hi are orthogonal, $H' = H + Hi$ is a subspace on which the form is regular and* $\dim H' = 2 \cdot \dim H$. *Moreover, if $a, b, c, d \in H$ then:*

$$(a + bi) \cdot (c + di) = (ac - \alpha \bar{d} b) + (da + b\bar{c})i.$$

Consequently H' is also a composition subalgebra of A.

Proof. H is invariant under "bar" since $1 \in H$. If $a, b \in H$ then $[a, bi] = [\bar{b}a, i] = 0$. Then H and Hi are orthogonal and $H \cap Hi = \{0\}$ since the form is regular.

To verify the formula for products it suffices to analyze three cases.

(1) $$\begin{aligned}[bi \cdot c, t] &= [bi, t\bar{c}] = -[b\bar{c}, ti] \quad \text{using the Flip Law (A.3),} \\ &= [b\bar{c} \cdot i, t].\end{aligned}$$

Hence $bi \cdot c = b\bar{c} \cdot i$.

(2) If $x \in H$ then $\bar{x} \cdot iy = i \cdot xy$, since $[iy, xt] = -[it, xy]$ by the Flip Law. In particular, $\bar{x}i = ix$. Hence if $a, d \in H$ then $a \cdot di = a \cdot i\bar{d} = i \cdot \bar{a}\bar{d} = i \cdot \overline{da} = da \cdot i$.

(3) $$\begin{aligned}[bi \cdot di, t] &= [di, \overline{bi} \cdot t] = [d \cdot i, -bi \cdot t] \quad \text{since } [bi, 1] = 0, \\ &= [d \cdot t, bi \cdot i] \quad \text{by the Flip Law,} \\ &= -[dt \cdot i, bi] = -\alpha[dt, b] = [t, -\alpha\bar{d}b].\end{aligned}$$

Hence $bi \cdot di = -\alpha\bar{d}b$. □

This observation imposes severe restrictions on the structure of a composition algebra A. The smallest composition subalgebra is $A_0 = F$. If $A \neq F$ there must be a 2-dimensional subalgebra $A_1 \subseteq A$ built as $A_1 = F + Fi$ for some $i \in F^{\perp}$. If $A \neq A_1$ there must be a 4-dimensional subalgebra $A_2 \subseteq A$ built as $A_2 = A_1 + A_1 j$ for some $j \in A_2^{\perp}$. If $A \neq A_2$ there must be an 8-dimensional subalgebra $A_3 \subseteq A$, etc. This doubling process cannot continue very long.

A.7. *Suppose H is a composition subalgebra of A, and H' is formed as in* (A.6). *Then:*

H is associative.

H' is associative if and only if H is a commutative and associative.

H' is commutative and associative if and only if $H = F$.

Proof. We know that $H' = H \oplus Hi$ is a composition algebra. Then $[(a + bi) \cdot (c + di)] = [a + bi] \cdot [c + di]$, for every $a, b, c, d \in H$. The left side equals $[(ac - \alpha\bar{d}b) + (da + b\bar{c})i] = [ac - \alpha\bar{d}b] + \alpha[da + b\bar{c}]$ and the right side equals $([a] + \alpha[b]) \cdot ([c] + \alpha[d])$. Expanding the two sides and canceling like terms yields: $[ac, \bar{d}b] = [da, b\bar{c}]$. Then $[d \cdot ac, b] = [da \cdot c, b]$ and we conclude that $d \cdot ac = da \cdot c$ and H is associative. The converse follows since these steps are reversible.

The proofs of the other statements are similar direct calculations. □

A.8 Theorem. *If A is a composition algebra over F then A is obtained from the algebra F by "doubling" 0, 1, 2 or 3 times. In particular,* $\dim A = 1, 2, 4$ *or* 8.

Proof. As remarked before (A.7), if $\dim A \notin \{1, 2, 4, 8\}$ then there is a chain of subalgebras $F = A_0 \subset A_1 \subset A_2 \subset A_3 \subset A_4 \subseteq A$, where $\dim A_k = 2^k$. Applying the statements in (A.7) repeatedly we deduce that A_1 is commutative and associative but not equal to F; A_2 is associative but not commutative; A_3 is not associative and therefore A_4 cannot exist inside the composition algebra A. This contradiction proves the assertion. □

This argument does more than compute the dimensions. It characterizes all the composition algebras. These are

(0) F,

(1) $F\langle\alpha\rangle \simeq F[x]/(x^2 - \alpha)$, a quadratic extension of F,

(2) $\left(\frac{\alpha,\beta}{F}\right)$, a quaternion algebra over F,

(3) $\left(\frac{\alpha,\beta,\gamma}{F}\right)$, an octonion algebra over F.

These algebras are defined recursively by the formulas in (A.6). Further properties of quaternion algebras are mentioned in Chapter 3. Further properties of octonions algebras appear in Chapters 8 and 12.

This relationship between H' and H in (A.6) is clarified by formalizing the idea of doubling an F-algebra. A map $a \mapsto \bar{a}$ on an F-algebra is called an *involution* if it is F-linear, $\bar{\bar{a}} = a$ and $\overline{ab} = \bar{b}\bar{a}$. Suppose H is an F-algebra with 1, $a \mapsto [a]$ is a regular quadratic form on H, and $a \mapsto \bar{a}$ is an involution on H. Let $\alpha \in F^\bullet$.

Definition. The *α-double*, $\mathcal{D}_\alpha(H)$, is the F-algebra with underlying vector space $H \times H$, and with multiplication given by the formula in (A.6), viewing $1 = (1, 0)$ and $i = (0, 1)$. For $(a, b) = a + bi \in \mathcal{D}_\alpha(H)$, define $\overline{a + bi} = \bar{a} - bi$, and $[a + bi] = [a] + \alpha[b]$.

A.9. *$\mathcal{D}_\alpha(H)$ is an F-algebra containing H as a subalgebra;* $\dim \mathcal{D}_\alpha(H) = 2 \cdot \dim H$*; $[a]$ is a regular quadratic form on $\mathcal{D}_\alpha(H)$; and $a \mapsto \bar{a}$ is an involution on $\mathcal{D}_\alpha(H)$. If the elements of H satisfy the following properties then so do the elements of $\mathcal{D}_\alpha(H)$:*

$a = \bar{a}$ *if and only if* $a \in F$;

$[a, b] = [\bar{a}, \bar{b}]$;

$[ax, b] = [a, b\bar{x}]$ *and* $[xa, b] = [a, \bar{x}b]$;

$a\bar{a} = [a] = \bar{a}a$;

$a\bar{b} + b\bar{a} = 2[a, b] = \bar{a}b + \bar{b}a$;

$T(x) = x + \bar{x}$ *satisfies* $T(ab) = T(ba)$ *and* $T(a \cdot bc) = T(ab \cdot c)$.

Proof. These are straightforward calculations. □

The algebras built from F by repeated application of this doubling process are called Cayley–Dickson algebras. Given a sequence of scalars $\alpha_1, \ldots, \alpha_n \in F^\bullet$ define

$$A(\alpha_1, \ldots, \alpha_n) = \mathcal{D}_{\alpha_n} \ldots \mathcal{D}_{\alpha_1}(F).$$

When $n \leq 3$ we obtain the composition algebras mentioned above. For example, $A(\alpha, \beta) \simeq \left(\frac{-\alpha,-\beta}{F}\right)$ is the quaternion algebra with norm form $\langle\langle \alpha, \beta \rangle\rangle = \langle 1, \alpha, \beta, \alpha\beta \rangle$.

Every Cayley–Dickson algebra $A(\alpha_1, \ldots, \alpha_n)$ satisfies the properties listed in (A.9), even though it is not a composition algebra when $n > 3$. Further properties are given in Exercise 25. Here are a few properties of composition algebras, not all valid for larger Cayley–Dickson algebras.

A.10. *If A is a composition algebra and $a, b, x, y, z \in A$ then:*

$a \cdot ba = ab \cdot a$. *(The "Flexible Law". Hence, it is unambiguous to write aba.)*
$aba \cdot x = a \cdot (b \cdot ax)$,
$a(xy)a = ax \cdot ya$. *(These are the Moufang identities.)*

Proof. From (A.5) $\bar{b} \cdot ac = 2[a, b]c - \bar{a} \cdot bc$. Substitute a for $\bar{b}$, b for a and ax for c, to deduce: $a \cdot (b \cdot ax) = (2[\bar{a}, b]a - [a]\bar{b}) \cdot x$. When $x = 1$ this is $a \cdot ba = 2[\bar{a}, b]a - [a]\bar{b}$, so that: $a \cdot (b \cdot ax) = (a \cdot ba) \cdot x$. Apply "bar" to the formula for $a \cdot ba$ and replace a, b by $\bar{a}, \bar{b}$ to find: $ab \cdot a = 2[a, \bar{b}]a - [\bar{a}]\bar{b} = a \cdot ba$.

The second Moufang identity also follows directly from the Flip Law.

$$\begin{aligned}[ax \cdot ya, t] &= [a \cdot x, t \cdot \overline{ya}] \\ &= 2[a, t] \cdot [xy, \bar{a}] - [a] \cdot [\bar{y}, tx] \quad \text{by the Flip Law and (A.5)}, \\ &= 2[a, t] \cdot [\overline{xy}, a] - [a] \cdot [\overline{xy}, t].\end{aligned}$$

Then for fixed a the value $ax \cdot ya$ depends only on the quantity xy. The stated formula is clear from this independence. □

These identities hold in any alternative ring. See Exercise 26.

Exercises for Chapter 1

1. **Composition algebras.** Suppose $S \subseteq \mathrm{Sim}(V, q)$ with $\dim S = \dim V$. Explain how this yields a composition algebra, as defined in (A.1) of the appendix.

(Hint. Scale q to assume it represents 1 and choose $e \in V$ with $q(e) = 1$. Identify S with V by $f \mapsto f(e)$. (1.9) provides a pairing. Apply Exercise 0.8 to obtain an algebra with 1.)

2. Let (V, q) and (W, q') be two quadratic spaces. Define the "adjoint" map $J = J_W^V : \mathrm{Hom}(V, W) \to \mathrm{Hom}(W, V)$.

(1) The inverse of J_W^V is J_V^W. How does J behave on matrices?

(2) Define subspaces of $\mathrm{Sim}(V, W)$ and generalize (1.3), (1.5), (1.6) and (1.9).

(3) $\sigma < \mathrm{Sim}(q, q')$ if and only if $\mathrm{q}< \mathrm{Sim}(\sigma, q')$.

3. Let (V, q) be a quadratic space and $f, g \in \mathrm{End}(V)$.

(1) f is a c-similarity if and only if $q(f(v)) = cq(v)$ for every $v \in V$.

(2) $\tilde{f}g + \tilde{g}f = 0$ if and only if $f(v)$ and $g(v)$ are orthogonal for every $v \in V$.

(3) If f, g are comparable similarities, then $B(f(v), g(v)) = B_\mu(f, g)q(v)$. In euclidean space over $\mathbb{R}$, the notion of the angle between two vectors is meaningful. Similarities f and g are comparable iff the angle between $f(v)$ and $g(v)$ is constant, independent of v.

4. (1) Suppose $q \simeq \langle 1, a\rangle$. If $f \in \mathrm{Sim}^\bullet(q)$ then either $f = \begin{pmatrix} x & -ay \\ y & x \end{pmatrix}$ or $f = \begin{pmatrix} x & ay \\ y & -x \end{pmatrix}$ for some $x, y \in F$ with $\mu(f) = x^2 + ay^2$. Consequently, every (regular) subspace of $\mathrm{Sim}(q)$ is contained in one of the spaces S, T in Example 1.8. If $q \simeq \langle 1, -1\rangle$, list all the 0-similarities.

(2) Let $D = \left(\frac{-1,-1}{F}\right)$ be the quaternion algebra with norm form $q = \langle 1, 1, 1, 1\rangle$. Let $L_0 = \mathcal{L}(D) \subseteq \mathrm{Sim}(D, q)$ arising from the left regular representation of D. Then L_0 is the set of all $\begin{pmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{pmatrix}$. Similarly $R_0 = \mathcal{R}(D)$ is the set of all $\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$. Then L_0 and R_0 are subalgebras of $\mathrm{End}(D)$ which commute with each other and they are 4-dimensional subspaces of $\mathrm{Sim}(q)$. Also, $R_0 \cdot J = J \cdot L_0$ where $J =$ "bar". These subspaces of similarities are unique in a strong sense:

Lemma. *If $U \subseteq \mathrm{Sim}(D, q)$ is a (regular) subspace and $f \in U^\bullet$, either $U \subseteq f \cdot L_0$ or $U \subseteq f \cdot R_0$.*

(3) What are the possibilities for the intersections $f \cdot L_0 \cap L_0$ and $f \cdot L_0 \cap R_0$?

(Hint. (2) Reduce to the case $1_V \in U$. If $A^2 \in F^\bullet$ for a 4×4 skew-symmetric matrix A show that $A \in L_0$ or $A \in R_0$. Deduce that $U \subseteq L_0$ or $U \subseteq R_0$.

5. **Characterizing similarities.** Let (V, q) be a quadratic space and $f \in \mathrm{End}(V)$.

(1) If f preserves orthogonality (i.e. $B(v, w) = 0$ implies $B(f(v), f(w)) = 0$), then f is a similarity.

(2) If q is isotropic and f preserves isotropy (i.e. $q(v) = 0$ implies $q(f(v)) = 0$), then f is a similarity. (This also follows from Exercise 14, at least if F is infinite.)

(3) If q represents 1 and f preserves the unit sphere (i.e. $q(v) = 1$ implies $q(f(v)) = 1$), then f is an isometry.

6. **Multiplication formulas.** (1) Suppose $q = 2^m\langle 1\rangle$. If q represents $c \in F^\bullet$ then $\langle c\rangle q \simeq q$. Equivalently, $D_F(q) = G_F(q)$.

(2) Follow the notations of Proposition 1.9. There is an equivalence:

(i) There is a formula $\sigma(X)q(Y) = q(Z)$ such that each $z_k \in F(X)[Y]$ is a linear form in Y.

(ii) $\sigma(X) \in G_{F(X)}(q \otimes F(X))$.

(Hint. (1) The matrix in Exercise 0.5 provides a c-similarity.)

7. Let (V, B) be an *alternating space*, that is, B is a nonsingular skew-symmetric bilinear form on the F-vector space V.

(1) The adjoint involution I_B is well defined. The set $\mathrm{Sim}(V, B)$ is defined as usual and if $S \subseteq \mathrm{Sim}(V, B)$ is a linear subspace then the norm map induces a quadratic form σ on S.

(2) When $\dim V = 2$ then $\mathrm{Sim}(V, B) = \mathrm{End}(V)$ and the map $\mu : \mathrm{End}(V) \to F$ is the determinant. That is, the 2-dimensional alternating space admits a 4-dimensional subspace of similarities.

(3) $\dim V = 2m$ is even and $(V, B) \simeq m\boldsymbol{H} \simeq \boldsymbol{H} \perp \cdots \perp \boldsymbol{H}$, where H is the 2-dimensional alternating space where the Gram matrix of the form is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. If B is allowed to be singular then $(V, B) \simeq r\langle 0\rangle \perp m\boldsymbol{H}$.

(4) Let $J_{r,m}$ be the $n \times n$ matrix $\begin{pmatrix} 0_r & 0 & 0 \\ 0 & 0_m & -I_m \\ 0 & I_m & 0_m \end{pmatrix}$ where $n = r + 2m$. Any skew-symmetric $n \times n$ matrix is of the type $P^\top \cdot J_{r,m} \cdot P$ for some r, m and some $P \in \mathrm{GL}_n(F)$. In particular rank $M = 2m$ is even and $\det M$ is a square.

8. **Jordan forms.** Let (V, q) be a quadratic space over an algebraically closed field F. Let $f \in \mathrm{O}(V, q)$, that is, $\tilde{f} f = 1_V$. For each $a \in F$ define the general eigenspace $V((a)) = \{x \in V : (f - a1_V)^k(x) = 0 \text{ for some } k\}$.

(1) If $ab \neq 1$ then $V((a))$ and $V((b))$ are orthogonal. In particular if $a \neq \pm 1$ then $V((a))$ is totally isotropic.

(2) Therefore $V = V((1)) \perp V((-1)) \perp \perp(V((a)) \oplus V((a^{-1})))$, summed over some scalars $a \neq \pm 1$. Then $\det f = (-1)^m$ where $m = \dim V((-1))$.

(3) If $f \in \mathrm{End}(V)$, what condition on the Jordan form of f ensures the existence of a quadratic form q on V having $f \in \mathrm{O}(V, q)$? Certainly f must be similar to f^{-1}.

Proposition. *If $f \in \mathrm{GL}(V)$ then $f \in \mathrm{O}(V, q)$ for some regular quadratic form q if and only if $\tilde{f} \sim f^{-1}$ and every elementary divisor $(x \pm 1)^m$ for m even occurs with even multiplicity.*

(Hint. (3) ($\Longleftarrow$) If f has matrix $\begin{pmatrix} B & 0 \\ 0 & B^{-\top} \end{pmatrix}$ in block form, we can use $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as the Gram matrix of q. By canonical form theory we need only find M in the case f has the single elementary divisor $(x-1)^m$ for odd m.

($\Longrightarrow$) Trickier to prove. See Gantmacher (1959), §11.5, Milnor (1969), §3, or Shapiro (1992).)

9. **More Jordan forms.** Let $f \in \mathrm{End}(V)$. What conditions on the Jordan form of f are needed to ensure the existence of a quadratic form q on V for which f is symmetric: $I_q(f) = f$? (Answer. Such q always exists. In matrix terms this says that for any square matrix A there is a nonsingular symmetric matrix S such that $SAS^{-1} = A^\top$. This result was proved by Frobenius (1910) and has appeared in the literature in various forms. Similar questions arise: When does there exist a quadratic form q such that $I_q(f) = -f$? When does there exist an alternating form B on V such that $I_B(f) = \pm f$? These are questions are addressed in Chapter 10.)

10. **Determinants of skew matrices.** If (V, q) is a quadratic space then all the invertible skew-symmetric matrices have the same determinant, modulo squares. In fact:

$$\text{if } f \in \mathrm{GL}(V) \text{ and } I_q(f) = -f \text{ then } \langle \det f \rangle = \det q \text{ in } F^\bullet / F^{\bullet 2}.$$

(Hint. The determinant of a skew-symmetric matrix is always a square.)

11. **Multi-indices.** In the notation of Proposition 1.11:

(1) For any Δ, Γ note that $f^\Delta \cdot f^\Gamma = \pm f^\Gamma \cdot f^\Delta$. Determine this sign explicitly.

(2) Suppose further that $f_i^2 = a_i \in F^\bullet$. Define $a_\Delta = a_1^{\delta_1} \dots a_n^{\delta_n}$. Then $(f^\Delta)^2 = \pm a_\Delta$. Determine exactly when that sign is "+". Further investigation of such signs appears in Exercise 3.18 below.

(3) The "multi-index" Δ can be viewed as the subset of $\{1, 2, \dots, n\}$ consisting of all indices i such that $\delta_i = 1$. Listing this subset as $\Delta = \{i_1, \dots, i_k\}$ such that $i_1 < i_2 < \cdots < i_k$, we have $f^\Delta = f_{i_1} f_{i_2} \dots f_{i_k}$. Then $|\Delta|$ is the cardinality of Δ, $\Delta\Gamma = \Delta \cap \Gamma$, and $\Delta + \Gamma = (\Delta \cup \Gamma) - (\Delta \cap \Gamma)$, the symmetric difference.

(Hint. (1) The answer involves only $|\Delta|$, $|\Gamma|$ and $|\Delta\Gamma|$.)

12. **Anticommuting matrices.** (1) **Proposition.** *Suppose $n = 2^m n_0$ where n_0 is odd. There exist k elements of $\mathrm{GL}_n(F)$ which anticommute pairwise, if and only if $k \le 2m+1$.*

(2) Suppose $f_1, \dots, f_{2m+1}$ is a maximal anticommuting system in $\mathrm{GL}_n(F)$ as above. If $n = 2^m$ then f_i^2 must be a scalar. For other values of n this claim may fail.

(Hint. (1) ($\Longleftarrow$) Inductively construct such $f_1, \dots, f_{2m+1}$ in $\mathrm{GL}(n)$ with $f_i^2 = \pm 1$. To get the system in $\mathrm{GL}_{2n}(F)$ use block matrices: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & f_i \\ -f_i & 0 \end{pmatrix}$.

($\Longrightarrow$) We may assume F is algebraically closed and $k = 2k_0$ is even. *To show*: $2^{k_0}|n$. Use notations of Exercise 8 with $V = F^n$. Then V is a direct sum of the $V((a))$'s and $f_j : V((a)) \to V((-a))$ is a bijection, for every $j > 1$. Let $n_a = \dim V((a))$, so that $n = \sum 2n_a$, summed over certain eigenvalues a. The maps $f_2 f_j$ induce $k-2$ anticommuting elements of $\mathrm{GL}\big(V((a))\big)$, and hence $2^{k_0-1}|n_a$, by induction hypothesis.

(2) By (1.11) the matrices f^Δ span all of $\mathbb{M}_n(F)$ and f_i^2 commutes with every f_j.)

13. **Trace forms.** The map $\mu : \mathrm{Sim}(V) \to F$ induces a quadratic form on every linear subspace.

(1) In fact μ extends to a quadratic form on $\mathrm{End}(V)$, at least if $\dim V$ is not divisible by the characteristic of F.

(2) If (V, q) is a quadratic space define $\tau : \mathrm{End}(V) \to F$ by $\tau(f) = \mathrm{trace}(\tilde{f} f)$. Then $(\mathrm{End}(V), \tau) \simeq q \otimes q$.

(3) Let $A = \{f \in \mathrm{End}(V) : \tilde{f} = -f\}$, the space of skew-symmetric maps. Compute the restriction τ_A of the trace form τ to $A \times A$.

(4) If (V, B) is a alternating space what can be said about the trace form τ?

(5) Suppose (V, α) and (W, β) are quadratic spaces and use the isomorphism $\theta_\alpha : V \to \hat{V}$ to find an isomorphism $V \otimes W \to \mathrm{Hom}(V, W)$. Does the quadratic form $\alpha \otimes \beta$ get carried over to the trace form τ on $\mathrm{Hom}(V, W)$ defined by $\tau(f) = \mathrm{trace}(J_W^V(f) \circ f)$? (See Exercise 2 for J_W^V.)

(Hint. (1) Consider $\mathrm{trace}(\tilde{f} f)$.

(2) The bilinear form $b = B_q$ induces an isomorphism $\theta : V \to \hat{V}$ where $\hat{V}$ is the dual vector space. Then $\varphi : V \otimes V \to \hat{V} \otimes V \to \mathrm{End}(V)$ is an isomorphism. Verify that

(i) $\varphi(v_1 \otimes w_1) \circ \varphi(v_2 \otimes w_2) = b(w_1, v_2) \cdot \varphi(v_1 \otimes w_2)$.

(ii) $\mathrm{trace}(\varphi(v \otimes w)) = b(v, w)$.

(iii) $I_q(\varphi(v \otimes w)) = \varphi(w \otimes v)$. Show that φ carries $q \otimes q$ to τ.

(3) If $q \simeq \langle a_1, \ldots, a_n \rangle$ define $P_2(q) = \langle a_1 a_2, a_1 a_3, \ldots, a_{n-1} a_n \rangle$. Then $\tau_A \simeq \langle 2 \rangle P_2(q)$. To see this let $\{v_1, \ldots, v_n\}$ be the given orthogonal basis and note that $\varphi^{-1}(A)$ is spanned by $v_i \otimes v_j - v_j \otimes v_i$ for $i < j$.) Compare Exercise 3.13.)

14. **Geometry lemma.** Let $X = (x_1, \ldots, x_n)$ be indeterminates. If $f \in F[X]$ define the zero-set $\mathcal{Z}(f) = \{a \in F^n : f(a) = 0\}$. If $f|p$ then p vanishes on $\mathcal{Z}(f)$, or equivalently, $\mathcal{Z}(f) \subseteq \mathcal{Z}(p)$. The converse is false in general even if f is irreducible. (Hilbert's Nullstellensatz applies when F is algebraically closed.) However, the converse does hold in some cases:

(1) **Lemma.** *Let F be an infinite field and let $x, Y = (y_1, \ldots, y_n)$ be indeterminates. Suppose $f(x, Y) = x \cdot g(Y) + h(Y) \in F[x, Y]$ where $g(Y)$, $h(Y)$ are non-zero and relatively prime in $F[Y]$. Then f is irreducible and if $p \in F[x, Y]$ vanishes on $\mathcal{Z}(f)$ then $f|p$.*

Proof outline. Express $p = c_0(Y)x^d + \cdots + c_d(Y)$. Since $xg \equiv -h \pmod f$, we have $g^d p \equiv Q \pmod f$ where $Q = c_0(Y)(-h(Y))^d + \cdots + c_d(Y)g(Y)^d \in F[Y]$. Since p vanishes on $\mathcal{Z}(f)$ it follows that $Q(B) = 0$ for every $B \in F^n$ with $g(B) \neq 0$. Therefore $g \cdot Q$ vanishes identically on F^n. Hence $Q = 0$ as a polynomial and $f | g^d p$ and we conclude that $f | p$.

(2) Suppose $\deg p = d$ and $\deg f = m$ above. If F is finite and $|F| \geq (m+1)\cdot(d+1)$, the conclusion still holds.

(3) Suppose q is an isotropic quadratic form over an infinite field F, and $\dim q > 2$. If $p \in F[X]$ vanishes on $\mathcal{Z}(q)$, then $q | p$. In particular if q, q' are quadratic forms with dimension > 2 and if $\mathcal{Z}(q) \subseteq \mathcal{Z}(q')$ then $q' = c \cdot q$ for some $c \in F$. For what finite fields F do these statements hold?

(Hint. (2) If $k(Y) \in F[Y]$ vanishes on F^n and if $|F| > \deg k$ then $k = 0$.

(3) Change variables to assume $q(X) = xy + h(Z)$ where h is a quadratic form of dim ≥ 1. Analyze (1) to show that $\deg Q \leq 2d$. The argument works if $|F| \geq 2 \cdot \deg p + 2$.)

15. **Transversality.** Suppose F is a field with more than 5 elements.

(1) If $a \in F^\bullet$ there exist non-zero $r, s \in F$ such that $r^2 + as^2 = 1$.

(2) Suppose $q \simeq \langle a_1, \ldots, a_n \rangle$ represents c. That is, there exists $0 \neq v \in F^n$ such that $q(v) = \sum a_i v_i^2 = c$. Then there exists $w \in F^n$ such that $q(w) = c$ and $w_i \neq 0$ for *every* i.

(3) **Transversality Lemma.** *Suppose (V, α) and (W, β) are quadratic spaces over F and $\alpha \perp \beta$ represents c. Then there exist $v \in V$ and $w \in W$ such that $c = \alpha(v) + \beta(w)$ and $\alpha(v) \neq 0$ and $\beta(w) \neq 0$.*

(4) Generalize (2) to non-diagonal forms. The answer reduces to the case $c = 0$:

Proposition. *Let (V, q) be an isotropic quadratic space with $\dim q = n \geq 3$ and let $H_1, \ldots, H_n$ be linearly independent hyperplanes in V. Then there exists an isotropic vector $v \in V$ such that $v \notin H_1 \cup \cdots \cup H_n$.*

For example, relative to a given basis the coordinate hyperplanes are linearly independent. If F is infinite we can avoid any finite number of hyperplanes in V. (Use Exercise 14 with p a product of linear forms.) If F is finite the result follows from Exercise 14 provided that $|F| \geq 2n + 2$. The stated result (valid if $|F| > 5$) is due to Leep (unpublished) and seems quite hard to prove.

(Hint. (1) Use the formulas $r = \frac{t^2-a}{t^2+a}$ and $s = \frac{2t}{t^2+a}$.

(2) Suppose $n = 2$. Re-index to assume $v_1 \neq 0$ and scale to assume $a_1 = 1$. If $v_2 = 0$ scale again to assume $c = 1$. Apply (1). What if $n > 2$?

(3) If α, β are anisotropic diagonalize them and apply (2). If α is isotropic choose w so that $\beta(w) \neq 0, c$ and note that α represents $c - \beta(w)$.)

16. **Conjugate subspaces. Lemma.** *Suppose $S, S' \subseteq \mathrm{Sim}(V, q)$ are subspaces containing 1_V and such that $S \simeq S'$ as quadratic spaces (relative to the induced quadratic form). If $\dim S \leq 3$ then $S' = gSg^{-1}$ for some $g \in \mathrm{O}(V, q)$.*

(Hint. Compare (1.10). Induct on $\dim V$. Restate the hypotheses in the case $\dim S = 2$: For $i = 1, 2$ we have isometric spaces (V_i, q_i) and $f_i \in \mathrm{End}(V_i)$ such that $\tilde{f_i} = -f_i$ and $f_i^2 = -a \cdot 1_V$. Choose $v_i \in V_i$ such that $q_1(v_1) = q_2(v_2) \neq 0$ and let $W_i = \mathrm{span}\{v_i, f_i(v_i)\}$. Define $g : W_1 \to W_2$ with $g(v_1) = v_2$ and $g(f(v_1)) = f(v_2)$. Then g is an isometry and $f_2 = g f_1 g^{-1}$ on W_2. Apply induction to $W_i^{\perp}$.)

17. **Proper similarities.** If $f \in \mathrm{Sim}^{\bullet}(V, q)$ where $\dim V = n$ then $(\det f)^2 = \mu(f)^n$.

(1) If n is odd then $\mu(f) \in F^{\bullet 2}$ and $f \in F^{\bullet}\,\mathrm{O}(V)$.

(2) Suppose $n = 2m$. Define f to be *proper* if $\det f = \mu(f)^m$. The proper similarities form a subgroup $\mathrm{Sim}^{+}(V)$ of index 2 in $\mathrm{Sim}^{\bullet}(V)$. This is the analog of the special orthogonal group $\mathrm{O}^{+}(n) = \mathrm{SO}(n)$.

(3) Suppose $\tilde{f} = -f$. If $g = a1_V + bf$ for $a, b \in F$ then g is proper.

(4) **Wonenburger's Theorem.** *Suppose $f, g \in \mathrm{Sim}^{\bullet}(V)$ and $\tilde{f} = -f$. If g commutes with f, then g is proper. If g anticommutes with f and $4 \mid n$ then g is proper.*

(5) Let $L_0, R_0 \subseteq \mathrm{Sim}(\langle 1, 1, 1, 1\rangle)$ be the subspaces described in Exercise 4(2). Let G be the group generated by $L_0^{\bullet}$ and $R_0^{\bullet}$. Then G is the set of all maps $g(x) = axb$ for $a, b \in D^{\bullet}$.

Lemma. $G = \mathrm{Sim}^{+}(q)$**.**

(Hint. (1) Show $\mu(f) \in F^{\bullet 2}$.

(4) Assume F algebraically closed and $f^2 = 1_V$. The eigenspaces U^{+} and U^{-} are totally isotropic of dimension m. Examine the matrix of g relative to $V = U^{+} \oplus U^{-}$ using the Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(5) $G \subseteq \mathrm{Sim}^{+}(V)$ by Wonenburger. Conversely it suffices to show that $\mathrm{SO}(q) \subseteq G$. The maps τ_a generate $\mathrm{O}(q)$, where τ_a is the reflection fixing the hyperplane $(a)^{\perp}$. Therefore the maps $\tau_a \tau_1$ generate $\mathrm{SO}(q)$. Writing $[a]$ for $q(a)$ as in the appendix, we have $\tau_a(x) = x - \frac{2[x,a]}{[a]} \cdot a = x - [a]^{-1}(x\bar{a} + a\bar{x})a = -[a]a\bar{x}a$. Then $\tau_a\tau_1(x) = [a]^{-1}axa$ so that $\tau_a\tau_1$ lies in G.)

18. **Zero-similarities.** Let $h \in \mathrm{End}(V)$ where (V, q) is a quadratic space.

(1) $(\mathrm{image}\, h)^{\perp} = \ker \tilde{h}$ and $(\ker h)^{\perp} = \mathrm{image}\, \tilde{h}$.

(2) If $h \in \mathrm{Sim}(V)$, it is possible that $\tilde{h} \notin \mathrm{Sim}(V)$. However if h is comparable to some $f \in \mathrm{Sim}^{\bullet}(V)$ then $\tilde{h} \in \mathrm{Sim}(V)$.

(3) Suppose $h \in S \subseteq \mathrm{Sim}(V)$ where $\mu(h) = 0$ and S is a regular subspace. Then $h\tilde{h} = \tilde{h}h = 0$ and $\dim \ker h = \dim \mathrm{image}\, h$, as in the proof of (1.4). Conversely if $h \in \mathrm{End}(V)$ satisfies these conditions then h is in some regular $S \subseteq \mathrm{Sim}(V)$.

(Hint: (3) $U = \ker h = \mathrm{image}\, \tilde{h}$ and $U' = \mathrm{image}\, h = \ker \tilde{h}$ are totally isotropic of dimension $n/2$. Replace h by gh for a suitable $g \in \mathrm{O}(V, q)$, to assume $U = U'$. Choose a totally isotropic complement W and use matrices relative to $V = U \oplus W$ to construct a 0-similarity k with $\tilde{h}k + \tilde{k}h = 1_V$.)

19. **Singular subspaces.** (1) Find an example of a regular quadratic space (V, q) admitting a (singular) subspace $S \subseteq \mathrm{Sim}(V, q)$ where $\dim S > \dim V$.

(2) Find such an example where $1_V \in S$.

(Hint. Let $(V, q) = m\mathbb{H}$ be hyperbolic and choose a basis so that the matrix of q is $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in $m \times m$ blocks. If $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $\tilde{f} = \begin{pmatrix} d^\top & b^\top \\ c^\top & a^\top \end{pmatrix}$. Consider the cases $f = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.)

20. **Extension Theorem.** (1) **Lemma.** *Suppose (V, q) is a quadratic space, $W \subseteq V$ is a regular subspace and $f : W \to V$ is a similarity. If $\mu(f) \in G_F(q)$. Then there exists $\hat{f} \in \mathrm{Sim}(V, q)$ extending f.*

(2) **Corollary.** *If D is an $n \times r$ matrix over F satisfying $D^\top \cdot D = aI_r$ and $a \in G_F(n\langle 1\rangle)$ then D can be enlarged to an an $n \times n$ matrix $\hat{D} = (D|D')$ which satisfies $\hat{D}^\top \cdot \hat{D} = aI_n$.*

(Hint. (1) There exists $g \in \mathrm{Sim}(V, q)$ with $\mu(g) = \mu(f)$. Then $g^{-1} \circ f : W \to V$ is an isometry and Witt's Extension Theorem for isometries applies. See Scharlau (1985) Theorem 1.5.3.)

21. **Bilinear terms in Pfister Form Formulas.** According to Pfister's Theory, if $n = 2^m$ and X, Y are systems of n indeterminates over F, there exists a formula

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2, \qquad (*)$$

where each z_k is a linear form in Y with coefficients in the rational function field $F(X)$. In Exercise 0.5 we found formulas where several of the z_k's were also linear in X. Question. How many of the terms z_k can be taken to be bilinear in X, Y?

Proposition. *Suppose F is a formally real field, $n = 2^m$ and X, Y are systems of n indeterminates. There is an n-square identity $(*)$ as above with each z_k linear in Y and with $z_1, \ldots, z_r$ also linear in X if and only if $r \leq \rho(n)$.*

Proof outline. Suppose $z_1, \ldots, z_r$ are also linear in X. Then $Z = AY$ for an $n \times n$ matrix A over $F(X)$ such that the entries in the first r rows of A are linear forms in X. Then $(*)$ becomes: $A^\top \cdot A = \left(\sum x_i^2\right) \cdot I_n$. Consequently $A \cdot A^\top = \left(\sum x_i^2\right) \cdot I_n$. Express A in block form as $A = \begin{pmatrix} B \\ C \end{pmatrix}$ where B is an $r \times n$ matrix whose entries are linear forms in X and C is an $(n-r) \times n$ matrix over $F(X)$. Then $B \cdot B^\top = \left(\sum x_i^2\right) \cdot I_r$, so that $B^\top$ satisfies the Hurwitz conditions for a formula of size $[n, r, n]$. The Hurwitz–Radon Theorem implies $r \leq \rho(n)$.

Conversely if $r \leq \rho(n)$ there exists an $r \times n$ matrix B, linear in X, with $B \cdot B^\top = \left(\sum x_i^2\right) \cdot I_r$. Note that $\left(\sum x_i^2\right)$ is in $G_{F(X)}(n\langle 1\rangle)$ by Pfister's theorem. (Use Exercise 6 or invoke (5.2) (1) below.) Apply Exercise 20(2) to $B^\top$ over $F(X)$ to find the matrix A.

22. **Isoclinic planes.** If $U \subseteq \mathbb{R}^n$ is a subspace and ℓ is a line in $\mathbb{R}^n$ let $\angle(\ell, U)$ be the angle between them. If $\ell \not\subseteq U^\perp$ then $\angle(\ell, U)$ is the angle between the lines ℓ and $\pi_U(\ell)$, where $\pi_U : \mathbb{R}^n \to U$ is the orthogonal projection. Subspaces $U, W \subseteq \mathbb{R}^n$ are *isoclinic* if $\angle(\ell, U)$ is the same for every line $\ell \subseteq W$.

(1) U, W are isoclinic if and only if π_U is a similarity when restricted to W.

(2) If $\dim U = \dim W$ this relation "isoclinic" is symmetric.

(3) Suppose $\mathbb{R}^{2n} = U \perp U'$ where $\dim U = \dim U' = n$. If $f \in \mathrm{Hom}(U, U')$ define its graph to be $U[f] = \{u + f(u) : u \in U\} \subseteq \mathbb{R}^{2n}$. Let $W \subseteq \mathbb{R}^{2n}$ be a subspace of dimension n.

Lemma. *U, W are isoclinic if and only if either $W = U'$ or $W = U[f]$ for some similarity f.*

Proposition. *Suppose $f, g \in \mathrm{Sim}(U, U')$. Then $U[f], U[g]$ are isoclinic if and only if f, g are comparable similarities.*

(4) If $T \subseteq \mathrm{Sim}(U, U')$ is a subspace define $\mathcal{S}(T) = \{U[f] : f \in T\} \cup \{U'\}$. Then $\mathcal{S}(T)$ is a set of mutually isoclinic n-planes in $\mathbb{R}^{2n}$. It is called an isoclinic sphere since it is a sphere when viewed as a subset of the Grassmann manifold of n-planes in $2n$-space.

(5) If $n \in \{1, 2, 4, 8\}$ there exists such T with $\dim T = n$. In these cases $\mathcal{S}(T)$ is "space filling": whenever $0 \neq x \in \mathbb{R}^{2n}$ there is a unique n-plane in $\mathcal{S}(T)$ containing x.

23. **Normal sets of planes.** Define two n-planes U, V in $\mathbb{R}^{2n}$ to be *normally related* if $U \cap V = \{0\} = U \cap V^\perp$. A set of n-planes is *normal* if every two distinct elements are either normally related or orthogonal.

(1) Suppose $\mathcal{S}$ is a maximal normal set of n-planes in $\mathbb{R}^{2n}$. If $U \in \mathcal{S}$ then $U^\perp \in \mathcal{S}$. A linear map $f : U \to U^\perp$ has a corresponding graph $U[f] \subseteq U \perp U^\perp = \mathbb{R}^{2n}$, as in Exercise 22. If $W \in \mathcal{S}$ then either $W = U^\perp$ or $W = U[f]$ for some bijective f. Note that $U[f]^\perp = U[-f^{-\top}]$, and that $U[f]$ and $U[g]$ are normally related iff $f - g$ and $f + g^{-\top}$ are bijective.

(2) Let $\mathbb{O} = \mathbb{R}^n \times \{0\}$ be the basic n-plane. If $T \subseteq \mathbb{M}_n(\mathbb{R})$ define

$$\mathcal{S}(T) = \{\mathbb{O}[A] : A \in T\} \cup \{\mathbb{O}^\perp\}.$$

Any maximal normal set of n-planes in $\mathbb{R}^{2n}$ containing $\mathbb{O}$ equals $\mathcal{S}(T)$ for some subset T such that: T is *nonsingular* (i.e. every non-zero element is in $\mathrm{GL}_n(\mathbb{R}^n)$), T is an additive subgroup and T is closed under the operation $A \mapsto A^{-\top}$.

(3) Consider the case $T \subseteq \mathbb{M}_n(\mathbb{R})$ is a linear subspace. (If $\mathcal{S}(T)$ is maximal normal must T be a subspace?)

Proposition. *If $T \subseteq \mathbb{M}_n(\mathbb{R})$ is a linear subspace such that $\mathcal{S}(T)$ is a maximal normal set of n-planes, then $T \subseteq \mathrm{Sim}(\mathbb{R}^n)$ and $\mathcal{S}(T)$ is a maximal isoclinic sphere.*

(Hint. (3) If $0 \neq A \in T$ express $A = PDQ^\top$ where $P, Q \in \mathrm{O}(n)$ and D is diagonal with positive entries. (This is a singular value decomposition.) If $a, b \in \mathbb{R}$ then $aA + bA^{-\top} \in T$. Then if $aD + bD^{-\top}$ is non-zero it must be nonsingular. Deduce $D =$ scalar so that $A \in \mathrm{Sim}(\mathbb{R}^n)$.

24. **Automorphisms.** Suppose C is a composition algebra and $a \in C$.

(1) If a is invertible, must $x \mapsto axa^{-1}$ be an automorphism of C?

Define $L_a(x) = ax$, $R_a(x) = xa$ and $B_a(x) = axa$.

(2) $B_a(xy) = L_a(x) \cdot R_a(y)$. Consequently $B_a B_b(xy) = L_a L_b(x) \cdot R_a R_b(y)$, etc. These provide examples of maps $\alpha, \beta, \gamma : C \to C$ satisfying: $\gamma(xy) = \alpha(x) \cdot \beta(y)$.

(3) For such α, β, γ if $\alpha(1) = \beta(1) = 1$ then $\alpha = \beta = \gamma$ is an automorphism of C. If C is associative this automorphism is the identity. Suppose C is octonion and $\gamma = B_{a_1} B_{a_2} \dots B_{a_n}$, etc. There exist non-trivial automorphisms built this way (but they require $n \geq 4$).

(4) Suppose C_1 and C_2 are composition algebras. If $\varphi : C_1 \to C_2$ is an isomorphism then φ commutes with the involutions: $\varphi(\bar{x}) = \overline{\varphi(x)}$, and φ is an isometry of the norm forms $[x]$. Conversely if the norm forms of C_1 and C_2 are isometric then the algebras must be isomorphic. (However not every isometry is an isomorphism.)

(Hint. (2) Moufang identities.

(3) $\alpha(1) = 1 \Longrightarrow \gamma = \beta$, and $\beta(1) = 1 \Longrightarrow \gamma = \alpha$. Case $n = 2$: $ab = 1$ implies $a \cdot bx = x$ since alternative. Case $n = 3$: Given $a \cdot bc = 1 = cb \cdot a$, show a, b, c lie in a commutative subalgebra. Then a, b, c, x lie in an associative subalgebra and $L_a L_b L_c(x) = x$.

(4) $a \in C$ is pure (i.e. $\bar{a} = -a$) iff $a \notin F$ and $a^2 \in F$. Any isomorphism preserves "purity". Given an isometry $\eta : C_1 \to C_2$ assume inductively that C_i is the double of a subalgebra B_i, that $\eta(B_1) = B_2$ and that the restriction of η to B_1 is an isomorphism. By Witt Cancellation the complements $B_i^{\perp}$ are isometric.)

25. Suppose $A = A(\alpha_1, \dots, \alpha_n)$ is a Cayley–Dickson algebra. Then elements of A satisfy the identities in (A.9).

(1) The elements of A also satisfy:

$yx \cdot x = x \cdot xy$

$a \cdot ba = ab \cdot a$ (the flexible law)

$[ab] = [\bar{a}b] = [ba]$

$a^n \cdot a^m = a^{n+m}$ (A is power-associative).

(2) If $ab = 1$ in A does it follow that $ba = 1$? If $a, b, c \in A$ does it follow that $[ab \cdot c] = [a \cdot bc]$?

(3) $\dim A = 2^n$ and A is a composition algebra if and only if $n \leq 3$. Define $A^{\circ} = \ker(T)$, the subspace of "pure" elements, so that $A = F \perp A^{\circ}$. If a, b are anisotropic, orthogonal elements of A° (using the norm form) then $a^2, b^2 \in F^{\bullet}$ and $ab = -ba$. These elements might fail to generate a quaternion subalgebra.

(4) There exists a basis $e_0, e_1, \dots, e_{2^n-1}$ of A such that:

$e_0 = 1$

$e_1, \dots, e_{2^n-1} \in A^{\circ}$ pairwise anti-commute and $e_i^2 \in F^{\bullet}$.

For each i, j: $e_i e_j = \lambda e_k$ for some index $k = k(i, j)$ and some $\lambda \in F^{\bullet}$.

The basis elements are "alternative": $e_ie_i \cdot x = e_i \cdot e_ix$ and $xe_i \cdot e_i = x \cdot e_ie_i$.

(5) The norm form $x \mapsto [x]$ on A is the Pfister form $\langle\langle -\alpha_1, \ldots, -\alpha_n \rangle\rangle$.

(6) Let $A_n = A(\alpha_1, a_2, \ldots \alpha_n)$. We proved that the identity $a \cdot bc = ab \cdot c$ holds in every A_2 and fails in every A_3. Similarly the identity $a \cdot ab = aa \cdot b$ holds in A_3 and fails in A_4.

Open question. Is there some other simple identity which holds in A_4 and fails in A_5?

(Hints. (1) If $\bar{a} = -a$ we know $[x, ax] = 0 = [x, xa]$. The flexible law for $\mathcal{D}_\alpha(H)$ follows from the properties of H, after some calculation. It suffices to prove power-associativity for pure elements, that is, when $\bar{a} = -a$. But then $a^2 \in F$.

(2) The $ab = 1$ property holds, at least when the form $[x]$ is anisotropic: Express $a = \alpha + e$ and $b = \beta + \gamma e + f$ where $1, e, f$ are orthogonal and $[e], [f] \neq 0$. Then $\{1, e, f, ef\}$ is linearly independent.

(4) Construct the basis inductively.)

26. **Alternative algebras.** Suppose A is a ring. If $x, y, z \in A$ define the associator $(x, y, z) = xy \cdot z - x \cdot yz$. Suppose A is alternative: $(a, a, b) = (a, b, b) = 0$.

(1) (x, y, z) is an alternating function of the three variables. In particular, $a \cdot ba = ab \cdot a$, which is the "Flexible Law".

(2) $xax \cdot y = x(a \cdot xy)$
$y \cdot xax = (yx \cdot a)x$ (the Moufang identities)
$bx \cdot yb = b \cdot xy \cdot b$

(3) $(y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x$.

(4) **Proposition.** *Any two elements of A generate an associative subalgebra.*

(Hint. (2) $xax \cdot y - x(a \cdot xy) = (xa, x, y) + (x, a, xy) = -(x, xa, y) - (x, xy, a) = -x^2a \cdot y - x^2y \cdot a + x(xa \cdot y + xy \cdot a) = -(x^2, a, y) - (x^2, y, a) + x \cdot [(x, a, y) + (x, y, a)] = 0$. For the second, use the opposite algebra. Finally, $bx \cdot yb - b \cdot xy \cdot b = (b, x, yb) - b(x, y, b) = -(b, yb, x) - b(x, y, b) = b \cdot [(y, b, x) - (x, y, b)] = 0$, using the first identity.

(3) $(y, xa, x) = -(y, x, a)x$ by (2). Replace x by $x + z$.

(4) If $u, v \in A$, examine "words" formed from products of u's and v's. It suffices to show that $(p, q, r) = 0$ for any such words p, q, r. Induct on the sum of the lengths of p, q, r. Rename things to assume that words q and r begin with u. Apply (3) when $x = u$.)

27. **The nucleus.** The *nucleus* $\mathcal{N}(A)$ of an algebra A is the set of elements $g \in A$ which associate with every pair of elements in A. That is, $xy \cdot z = x \cdot yz$ whenever one of the factors x, y, z is equal to g. Then $\mathcal{N}(A)$ is an associative subalgebra of A.

(1) If A is alternative it is enough to require $g \cdot xy = gx \cdot y$ for every x, y.

(2) If A is an octonion algebra over F then $\mathcal{N}(A) = F$.

(3) Does this hold true for all the Cayley–Dickson algebras A_n when $n > 3$?

28. Suppose A is an octonion algebra and $a, b \in A$. Then: $(a, b, x) = 0$ for every $x \in A$ iff $1, a, b$ are linearly dependent.

(Hint. ($\Longrightarrow$) $a, b \in H$ for some quaternion subalgebra H. Use (A.6) to deduce that $ab = ba$.)

Notes on Chapter 1

The independence result in (1.11) was proved by Hurwitz (1898) for skew symmetric matrices. The general result (for matrices) is given in Robert's thesis (1912) and in Dickson (1919). Similar results are mentioned in the Notes for Exercise 12.

The notation $\langle\langle a_1, \ldots, a_n \rangle\rangle$ for Pfister forms was introduced by T. Y. Lam. Other authors reverse the signs of the generators, writing $\langle\langle a \rangle\rangle$ for $\langle 1, -a \rangle$. In particular this is done in the monumental work on involutions by Knus, Merkurjev, Rost and Tignol (1998). We continue to follow Lam's notation, hoping that readers will not be unduly confused.

The topics in the appendix have been described in several articles and textbooks. The idea of the "doubling process", building the octonions from pairs of quaternions, is implicit in Cayley's works, but it was first formally introduced in Dickson's 1914 monograph. Dickson was also the first to note that the real octonions form a division ring. E. Artin conjectured that the octonions satisfy the alternative law. This was first proved by Artin's student M. Zorn (1930).

Perhaps the first study of the Cayley–Dickson algebras of dimension > 8 was given by Albert (1942a). He analyzed the algebras A_n of dimension 2^n over an arbitrary field F (allowing F to have characteristic 2), and proved a general version of Theorem A.8. Properties of A_n appear in Schafer (1954), Khalil (1993), Khalil and Yiu (1997), and Moreno (1998). Further information on composition algebras appears in Jacobson (1958), Kaplansky (1953), Curtis (1963).

Are there infinite dimensional composition algebras? Kaplansky (1953) proved that every composition algebra with (2-sided) identity element must be finite dimensional. However there do exist infinite dimensional composition algebras having only a left identity element. Further information is given in Elduque and Pérez (1997).

Define an algebra A over the real field $\mathbb{R}$ to be an *absolute-valued algebra* if A is a normed space (in the sense of real analysis) and $|xy| = |x| \cdot |y|$. Urbanik and Wright (1960) proved that an absolute-valued algebra with identity must be isomorphic to one of the classical composition algebras. Further information and references appear in Palacios (1992).

Exercise 3. (3) Let $V^\bullet = \{v \in V : q(v) \neq 0\}$ be the set of anisotropic vectors in (V, q). If $x, y \in V^\bullet$ define the angle-measure $\angle(x, y) = \frac{B(x,y)}{q(x)q(y)}$. If $f \in \mathrm{End}(V)$ preserves all such angle-measures, must f be a similarity? Alpers and Schröder (1991) investigate this question (without assuming f is linear).

Exercise 5. (1) In fact if $A, B : V \times W \to F$ are bilinear forms such that $A(x, y) = 0$ implies $B(x, y) = 0$, then B is a scalar multiple of A. This is proved in Rothaus (1978). A version of this result for p-linear maps appears in Shaw and Yeadon (1989). In a different direction, Alpers and Schröder (1991) study maps $f : V \to V$ (not assumed linear) which preserve the orthogonality of the vectors in $V^\bullet$ (the set of anisotropic vectors).

(2) See Samuel (1968), de Géry (1970), Lester (1977).

Exercise 6. This is part of the theory of Pfister forms. See Chapter 5.

Exercise 9. Compare Exercise 10.13. Also see Gantmacher (1959), §11.4, Taussky and Zassenhaus (1959), Kaplansky (1969), Theorem 66, Shapiro (1992).

Exercise 12. This generalizes (1.11). Variations include systems where the matrices are skew-symmetric, or have squares which are scalars. Results of these types were obtained by Eddington (1932), Newman (1932), Littlewood (1934), Dieudonné (1953), Kestelman (1961), Gerstenhaber (1964), and Putter (1967). The skew-symmetric case appears in Exercise 2.13. A system of anticommuting matrices whose squares are scalars becomes a representation of a Clifford algebra, and the bounds are determined by the dimension of an irreducible module. Another variation on the problem is considered by Eichhorn (1969), (1970).

Exercises 14. This Geometry Lemma was pointed out to me by A. Wadsworth with further comments by D. Leep.

Exercise 15 (1), (2) appears in Witt (1937). There is a related Transversality Theorem for quadratic forms over semi-local rings, due to Baeza and Knebusch.

Exercise 16. Compare (7.16).

Exercise 17. (4) Wonenburger (1962b).

(5) This lemma appears in Coxeter (1946). It is also valid in more general quaternion algebras.

Exercise 21. **Remark.** There is very little control on the denominators that arise in the process of extending the similarity B to the full matrix A. Even writing out an explicit 16-square identity having 9 bilinear terms seems difficult. There are so many choices for extending the given 9×16 matrix to a 16×16 matrix that nothing interesting seems to arise.

One can generalize these results to formulas $\varphi(X)\varphi(Y) = \varphi(Z)$ for any Pfister form φ. There are similar results on multiplication formulas for hyperbolic forms, but difficulties arise in cases of singular spaces of similarities.

Exercise 22. Details and further results about isoclinic planes are given in: Wong (1961), Wolf (1963), Tyrrell and Semple (1971), Shapiro (1978b), and Wong and Mok (1990). Isoclinic spaces are briefly mentioned after (15.23) below.

Exercise 23. These ideas follow Wong and Mok (1990), and Yiu (1993). Yiu proves:

Theorem. *Every maximal subspace in* $\mathrm{Sim}(\mathbb{R}^n)$ *is maximal as a subspace of nonsingular matrices.*

The proof uses homotopy theory. Related results appear in Adams, Lax and Philips (1965).

Exercise 24. Information on automorphisms appears in Jacobson (1958). Jacobson defines the inner automorphisms of an octonion algebra to be the ones defined in (3), and he proves that every automorphism is inner. That construction of inner automorphisms works for any alternative algebra. Also see Exercise 8.16 below. Automorphisms may also be considered geometrically. For the real octonion division algebra $\mathbb{K}$ the group $\mathrm{Aut}(\mathbb{K})$ is a compact Lie group of dimension 14, usually denoted G_2. The map $\sigma_a(x) = axa^{-1}$ is not often an automorphism of an octonion algebra. In fact, H. Brandt proved that if $[a] = 1$ then σ_a is an automorphism $\Longleftrightarrow a^6 = 1$. Proofs appear in Zorn (1935) and Khalil (1993).

Exercise 25. See Schafer (1954), Adem (1978b) and Moreno (1998). The Cayley–Dickson algebras are also mentioned in Chapter 13. The 2^n basis elements e_i of Exercise 25 (4) can instead be indexed by $V = \mathbb{F}_2^n$, using notation as in (1.11). If $e_i^2 = -1$ then: $e^\Delta \cdot e^\Gamma = (-1)^{\beta(\Delta,\Gamma)} e^{\Delta+\Gamma}$ for some map $\beta : V \times V \to \mathbb{F}_2$. Gordan et al. (1993) discuss the following question: If $n = 3$, which maps β yield an octonion algebra? These results can also be cast in terms of intercalate matrices defined in Chapter 13. A related situation for Clifford algebras is mentioned in Exercise 3.19.

Exercise 26. The proposition (due to Artin) follows Schafer (1966), pp. 27–30. See also Zhevlakov et al. (1982), p. 36.

Chapter 2

Amicable Similarities

Analysis of compositions of quadratic forms leads us quickly to the Hurwitz–Radon function $\rho(n)$ as defined in Chapter 0. This function enjoys a property sometimes called "periodicity 8". That is: $\rho(16n) = 8 + \rho(n)$. This and similar properties of the function $\rho(n)$ can be better understood in a more general context. Instead of considering $s - 1$ skew symmetric maps as in the original Hurwitz Matrix Equations (1.7), we allow some of the maps to be symmetric and some skew symmetric. This formulation exposes some of the symmetries of the situation which were not evident at the start. For example we can use these ideas to produce explicit 8-square identities without requiring previous knowledge of octonion algebras.

2.1 Definition. Two (regular) subspaces $S, T \subseteq \mathrm{Sim}(V, q)$ are *amicable* if

$$\tilde{f} g = \tilde{g} f \quad \text{for every } f \in S \text{ and } g \in T.$$

In this case we write $(S, T) \subseteq \mathrm{Sim}(V, q)$. If σ and τ are quadratic forms, the notation

$$(\sigma, \tau) < \mathrm{Sim}(V, q)$$

means that there is a pair $(S, T) \subseteq \mathrm{Sim}(V, q)$ where the induced quadratic forms on S and T are isometric to σ and τ, respectively.

It follows from the definition that if $(S, T) \subseteq \mathrm{Sim}(V)$ and $h, k \in \mathrm{Sim}^{\bullet}(V)$, then $(hSk, hTk) \subseteq \mathrm{Sim}(V)$. On the level of quadratic forms this says:

$$\text{If } (\sigma, \tau) < \mathrm{Sim}(q) \text{ and } d \in G_F(q) \text{ then } (\langle d \rangle \sigma, \langle d \rangle \tau) < \mathrm{Sim}(q).$$

If $S \neq 0$ we may translate by some f to assume $1_V \in S$. Since this normalization is so useful we give it a special name.

2.2 Definition. An (s, t)-*family* on (V, q) is a pair $(S, T) \subseteq \mathrm{Sim}(V, q)$ where $\dim S = s$, $\dim T = t$ and $1_V \in S$. If $(\sigma, \tau) < \mathrm{Sim}(V, q)$ and σ represents 1, we abuse the notation and say that (σ, τ) is an (s, t)-family on (V, q).

2.3 Lemma. *Suppose* $\sigma \simeq \langle 1, a_2, \ldots, a_s \rangle$ *and* $\tau \simeq \langle b_1, \ldots, b_t \rangle$. *Then* $(\sigma, \tau) < \mathrm{Sim}(V, q)$ *if and only if there exist* $f_2, \ldots, f_s; g_1, \ldots, g_t$ *in* $\mathrm{End}(V)$ *satisfying the*

following conditions:

$$\tilde{f}_i = -f_i, \quad f_i^2 = -a_i 1_V \qquad \text{for } 2 \le i \le s.$$
$$\tilde{g}_j = g_j, \quad g_j^2 = b_j 1_V \qquad \text{for } 1 \le j \le t.$$

The $s + t - 1$ *maps* $f_2, \ldots, f_s; g_1, \ldots, g_t$ *pairwise anti-commute.*

Proof. If $(\sigma, \tau) < \mathrm{Sim}(V, q)$ let $(S, T) \subseteq \mathrm{Sim}(V, q)$ be the corresponding amicable pair. Since σ represents 1, we may translate by an isometry to assume $1_V \in S$. Let $\{1_V, f_2, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ be orthogonal bases of S and T, respectively, corresponding to the given diagonalizations. The conditions listed above quickly follow. The converse is also clear. □

An (s, t)-family corresponds to a system of $s + t - 1$ anti-commuting matrices where $s - 1$ of them are skew-symmetric and t of them are symmetric. Stated that way our notation seems unbalanced. The advantage of the terminology of (s, t)-families is that s and t behave symmetrically:

$$(\sigma, \tau) < \mathrm{Sim}(V, q) \quad \text{if and only if} \quad (\tau, \sigma) < \mathrm{Sim}(V, q).$$

Example 1.8 provides an explicit $(2, 2)$-family on a 2-dimensional space: $(\langle 1, d\rangle, \langle 1, d\rangle) < \mathrm{Sim}(\langle 1, d\rangle)$. More trivially, $(\langle 1\rangle, \langle 1\rangle) < \mathrm{Sim}(V)$ for every space V.

2.4 Basic sign calculation. Continuing the notation of (2.3), let $z = f_2 \ldots f_s g_1 \ldots g_t$. Let $\det(\sigma)\det(\tau) = \langle d\rangle$. Then $\tilde{z} = \pm z$ and $\mu(z) = \tilde{z}z = d$, up to a square factor. In fact, $\tilde{z} = z$ if and only if $s \equiv t$ or $t + 1 \pmod 4$.

Proof. The formula for $\tilde{z}z$ is clear since $\tilde{}$ reverses the order of products. If $e_1, e_2, \ldots, e_n$ is a set of n anti-commuting elements, then $e_n \ldots e_2 e_1 = (-1)^k e_1 e_2 \ldots e_n$ where $k = (n-1) + (n-2) + \cdots + 2 + 1 = n(n-1)/2$. Since z is a product of $s + t - 1$ anti-commuting elements and the tilde $\tilde{}$ produces another minus sign for $s - 1$ of those elements, we find that $\tilde{z} = (-1)^{s-1}(-1)^k z$ where $k = (s + t - 1)(s + t - 2)/2$. The stated calculation of the sign is now a routine matter. □

2.5 Expansion Lemma. *Suppose* $(\sigma, \tau) < \mathrm{Sim}(V)$ *with* $\dim \sigma = s$ *and* $\dim \tau = t$. *Let* $\det(\sigma)\det(\tau) = \langle d\rangle$.

If $s \equiv t - 1 \pmod 4$, *then* $(\sigma \perp \langle d\rangle, \tau) < \mathrm{Sim}(V)$.

If $s \equiv t + 1 \pmod 4$, *then* $(\sigma, \tau \perp \langle d\rangle) < \mathrm{Sim}(V)$.

If (σ', τ') *is the amicable pair obtained from* (σ, τ) *then* $\dim \sigma' \equiv \dim \tau' \pmod 4$ *and* $d\sigma' = d\tau'$.

Proof. First suppose σ represents 1, arrange $1_V \in S$ and choose bases as in (2.3). Let $z = f_2 \ldots f_s g_1 \ldots g_t$ as before. Then $z \in \mathrm{Sim}^\bullet(V)$ and $\mu(z) = d$, up to a square

factor. If $s + t$ is odd, then z anti-commutes with each f_i and g_j. If $\tilde{z} = -z$ then z can be adjoined to S while if $\tilde{z} = z$ then it can be adjoined to T. The congruence conditions follow from (2.4) and the properties of (σ', τ') follow easily. □

2.6 Shift Lemma. *Let σ, τ, φ, ψ be quadratic forms and suppose* $\dim\varphi \equiv \dim\psi \pmod 4$. *Let* $\langle d\rangle = (\det\varphi)(\det\psi)$. *Then:*

$$(\sigma \perp \varphi, \tau \perp \psi) < \mathrm{Sim}(V, q) \text{ if and only if } (\sigma \perp \langle d\rangle\psi, \tau \perp \langle d\rangle\varphi) < \mathrm{Sim}(V, q).$$

This remains valid when φ or ψ is zero. That is, if α is a quadratic form with $\dim\alpha \equiv 0 \pmod 4$ and $\langle d\rangle = \det\alpha$ then:

$$(\sigma \perp \alpha, \tau) < \mathrm{Sim}(q) \text{ if and only if } (\sigma, \tau \perp \langle d\rangle\alpha) < \mathrm{Sim}(q).$$

This shifting result exhibits some of the flexibility of these families: an $(s+4, t)$-family is equivalent to an $(s, t+4)$-family.

Proof of 2.6. Suppose $(S \perp H, T \perp K) \subseteq \mathrm{Sim}(V, q)$ and $a \equiv b \pmod 4$, where $a = \dim H$ and $b = \dim K$. We may assume $S \neq 0$. (For if $T \neq 0$ interchange the eigenspaces. If $S = T = 0$ the lemma is clear.) Scale by suitable f to assume $1_V \in S$. Choose orthogonal bases $\{1_V, f_2, \ldots, f_s, h_1, \ldots, h_a\}$ and $\{g_1, \ldots, g_t, k_1, \ldots, k_b\}$ and define $y = h_1 h_2 \ldots h_a k_1 \ldots k_b$. Then $\tilde{y} = y$ and y commutes with elements of S and T, and anticommutes with elements of H and K. Therefore $(S + yK, T + yH) \subseteq \mathrm{Sim}(V, q)$. The converse follows since the same operation applied again leads back to the original subspaces. □

2.7 Construction Lemma. *Suppose* $(\sigma, \tau) < \mathrm{Sim}(q)$ *where* σ *represents* 1. *If* $a \in F^\bullet$ *then*

$$(\sigma \perp \langle a\rangle, \tau \perp \langle a\rangle) < \mathrm{Sim}(q \otimes \langle\langle a\rangle\rangle).$$

Proof. Recall that $\langle\langle a\rangle\rangle = \langle 1, a\rangle$ is a binary form. Let (S, T) be an (s, t)-family on (V, q) corresponding to (σ, τ), and express $S = F1_V \perp S_1$. Recall the $(2, 2)$-family constructed in Example 1.8 given by certain 2×2 matrices f_2, g_1 and g_2 in $\mathrm{Sim}(\langle\langle a\rangle\rangle)$. We may verify that $S' = F(1_V \otimes 1) + S_1 \otimes g_1 + F(1_V \otimes f_2)$ and $T' = T \otimes g_1 + F(1_V \otimes g_2)$ does form an $(s+1, t+1)$-family on $q \otimes \langle\langle a\rangle\rangle$. Compare Exercise 1. □

2.8 Corollary. *If* $\varphi \simeq \langle\langle a_1, \ldots, a_m\rangle\rangle$ *is a Pfister form of dimension* 2^m, *then there is an* $(m+1, m+1)$*-family* $(\sigma, \sigma) < \mathrm{Sim}(\varphi)$, *where* $\sigma \simeq \langle 1, a_1, \ldots, a_m\rangle$.

Proof. Starting from the $(1, 1)$-family on $\langle 1\rangle$, repeat the Construction Lemma m times. □

The construction here is explicit. The $2m+2$ basis elements of this family can be written out as $2^m \times 2^m$ matrices. Each entry of one of these matrices is either 0 or $\pm a_{i_1} \dots a_{i_r}$ for some $1 \le i_1 < \cdots < i_r \le m$. In particular if every $a_i = 1$ then the matrix entries lie in $\{0, 1, -1\}$.

These lemmas can be used to construct large spaces of similarities. Suppose φ is an m-fold Pfister form as above. Then there is an $(m+1, m+1)$-family $(\sigma, \sigma) < \mathrm{Sim}(\varphi)$. Now use the Shift Lemma to shift as much as possible to the left. The resulting sizes are:

$$\begin{array}{rl} (2m+1, 1) & \text{if } m \equiv 0 \\ (2m, 2) & \text{if } m \equiv 1 \\ (2m-1, 3) & \text{if } m \equiv 2 \\ (2m+2, 0) & \text{if } m \equiv 3 \end{array} \qquad (\mathrm{mod}\ 4)$$

Ignoring the "t" parts of these families we get some large subspaces of $\mathrm{Sim}(\varphi)$. In the case $m \equiv 2$ we have $2m - 1 \equiv 3 \pmod 4$, and the Expansion Lemma furnishes a subspace of dimension $2m$. We have found subspaces of dimension $\rho(2^m)$.

2.9 Proposition. *Suppose $n = 2^m n_0$ where n_0 is odd. Suppose q is a quadratic form of dimension n expressible as $q \simeq \varphi \otimes \gamma$ where φ is an m-fold Pfister form and $\dim \gamma = n_0$. Then there exists $\sigma < \mathrm{Sim}(q)$ with $\dim \sigma = \rho(n)$.*

Proof. From the definition of $\rho(n)$ given in Chapter 0 and the remarks above we see that there exists $\sigma < \mathrm{Sim}(\varphi)$ with $\dim \sigma = \rho(2^m) = \rho(n)$. Then also $\sigma < \mathrm{Sim}(q)$ as mentioned in (1.5). □

Using a little linear algebra we prove the following converse to the Construction Lemma.

2.10 Eigenspace Lemma. *Suppose $(\sigma \perp \langle a\rangle, \tau \perp \langle a\rangle) < \mathrm{Sim}(q)$ is an $(s+1, t+1)$-family, where $s \ge 1$. Then $q \simeq \varphi \otimes \langle\langle a\rangle\rangle$ for some quadratic form φ such that $(\sigma, \tau) < \mathrm{Sim}(\varphi)$.*

Proof. Translating the given family if necessary we may assume it is given by $(S, T) \subseteq \mathrm{Sim}(V, q)$ where $\{1_V, f_2, \dots, f_s, f\}$ and $\{g_1, \dots, g_t, g\}$ are orthogonal bases and $\mu(f) = \mu(g) = a$. Then $\tilde{f} = -f$ and $f^2 = -a1_V$, $\tilde{g} = g$ and $g^2 = a1_V$. Then $h = f^{-1}g = -a^{-1}fg$ satisfies $\tilde{h} = h$and $h^2 = 1_V$. Let U and U' be the ± 1-eigenspaces for h. Since $\tilde{h} = h$ these spaces are orthogonal and $V = U \perp U'$. Let φ, φ' be the quadratic forms on U and U' induced by q, so that $q \simeq \varphi \perp \varphi'$. Since f anti-commutes with h we have $f(U) = U'$ and $f(U') = U$. Consequently $\dim U = \dim U' = \frac{1}{2}\dim V$, $\varphi \simeq \langle a\rangle\varphi$ and $q \simeq \varphi \otimes \langle\langle a\rangle\rangle$. Furthermore $1_V, f_2, \dots, f_s, g_1, \dots, g_t$ all commute with h so they preserve U. Their restrictions to U provide the family $(\sigma, \tau) < \mathrm{Sim}(U, \varphi)$. □

We now have enough information to find all the possible sizes of (s, t)-families on quadratic spaces of dimension n.

2.11 Theorem. *Suppose $n = 2^m n_0$ where n_0 is odd. There exists an (s, t)- family on some quadratic space of dimension n if and only if $s \geq 1$ and one of the following holds:*

(1) $s + t \leq 2m$,

(2) $s + t = 2m + 1$ *and* $s \equiv t - 1$ *or* $t + 1 \pmod 8$,

(3) $s + t = 2m + 2$ *and* $s \equiv t \pmod 8$.

Proof. ("if") Suppose that there exist numbers s', t' such that $s \leq s'$, $t \leq t'$, $s' + t' = 2m + 2$ and $s' \equiv t' \pmod 8$. Then there is an (s', t')-family and hence an (s, t)-family on some quadratic space of dimension n. To see this first use the Construction Lemma to get an $(m + 1, m + 1)$-family on a space of dimension 2^m and tensor it up (as in (1.6)) to get such a family on an n-dimensional space (V, q). A suitable application of the Shift Lemma then provides an (s', t')-family in $\mathrm{Sim}(q)$.

If s, t satisfy one of the given conditions then such s', t' do exist, except in the case $s + t = 2m$ and $s \equiv t + 4 \pmod 8$. In this case, suppose $s \geq 2$. Then $s - 1 \equiv t + 3 \pmod 8$ and the work above implies that there is an $(s - 1, t + 3)$-family in $\mathrm{Sim}(q)$ for some n-dimensional form q. Restrict to an $(s - 1, t)$-family and apply the Expansion Lemma 2.5 to obtain an (s, t)-family. Similarly if $t \geq 1$ there is an $(s + 3, t - 1)$-family which restricts and expands to an (s, t)-family.

("only if") Suppose there is an (s, t)-family on some n-dimensional space and proceed by induction on m. If $m = 0$ Proposition 1.10 implies $s, t \leq 1$ and therefore $s + t \leq 2$. If $s + t = 2$ then certainly $s = t$. Similarly, if $m = 1$ Proposition 1.10 implies $s, t \leq 2$ so that $s + t \leq 4$. If $s + t = 4$ then $s = t$.

Suppose $m \geq 2$. If $s + t \leq 4$ the conditions are satisfied. Suppose $s + t > 4$ and apply the Shift Lemma and the symmetry of (s, t) and (t, s) to arrange $s \geq 2$ and $t \geq 1$. If $(\sigma, \tau) < \mathrm{Sim}(q)$ is the given (s, t)-family where $\dim q = n$, pass to an extension field of F to assume σ and τ represent a common value. The Eigenspace Lemma then implies that there is an $(s - 1, t - 1)$-family on some space of dimension $n/2$. The induction hypothesis implies the required conditions. □

2.12 Corollary. *If $\sigma < \mathrm{Sim}(q)$ where $\dim q = n$ then $\dim \sigma \leq \rho(n)$.*

Proof. Suppose $s = \dim \sigma > \rho(n)$ where $n = 2^m n_0$ and n_0 is odd. If $m \equiv 0 \pmod 4$ then $s > \rho(n) = 2m + 1$ so there is a $(2m + 2, 0)$-family in $\mathrm{Sim}(q)$. But $2m + 2 \equiv 2 \pmod 8$ contrary to the requirement in the Theorem 2.11. The other cases follow similarly. □

This corollary is the generalization of the Hurwitz–Radon Theorem to quadratic forms over any field (of characteristic not 2). A refinement of Theorem 2.11 appears in (7.8) below.

Theorem 2.11 contains all the information about possible sizes of families. This information can be presented in a number of ways. For example, given n and t we can determine the largest s for which an (s, t)-family exists on some n-dimensional quadratic space.

2.13 Definition. Given n and t, define $\rho_t(n)$ to be the maximum of 0 and the value indicated in the following table. Here $n = 2^m n_0$ where n_0 is odd.

$m \pmod 4$	$\rho_t(n)$
$m \equiv t$	$2m + 1 - t$
$m \equiv t + 1$	$2m - t$
$m \equiv t + 2$	$2m - t$
$m \equiv t + 3$	$2m + 2 - t$

2.14 Corollary. *Suppose (V, q) is an n-dimensional quadratic space.*

(1) *If there is an (s, t)-family in* $\mathrm{Sim}(V, q)$ *then $s \le \rho_t(n)$.*

(2) *Suppose $s = \rho_t(n)$. Then there is some (s, t)-family in* $\mathrm{Sim}(V, q)$*, provided that q can be expressed as a product $\varphi \otimes \gamma$ where φ is a Pfister form and* $\dim \gamma$ *is odd.*

The proof is left as an exercise for the reader.

Here is another way to codify this information. Given s, t we determine the minimal dimension of a quadratic space admitting an (s, t)-family.

2.15 Corollary. *Let $s \ge 1$ and $t \ge 0$ be given. The smallest n such that there is an (s, t)-family on some n-dimensional quadratic space is $n = 2^{\delta(s,t)}$ where the value $m = \delta(s, t)$ is defined as follows.*

Case $s + t$ is even:

if $s \equiv t \pmod 8$ then $s + t = 2m + 2$ and $\delta(s, t) = \frac{s+t-2}{2}$,

if $s \not\equiv t \pmod 8$ then $s + t = 2m$ and $\delta(s, t) = \frac{s+t}{2}$.

Case $s + t$ is odd:

if $s \equiv t \pm 1 \pmod 8$ then $s + t = 2m + 1$ and $\delta(s, t) = \frac{s+t-1}{2}$,

if $s \equiv t \pm 3 \pmod 8$ then $s + t = 2m - 1$ and $\delta(s, t) = \frac{s+t+1}{2}$.

Proof. This is a restatement of Theorem 2.11. The value $\delta(r) = \delta(r, 0)$ was calculated in Exercise 0.6. Further properties of $\delta(s, t)$ appear in Exercise 3. □

If $q = \varphi \otimes \gamma$ where φ is a large Pfister form, then (2.14) implies that $\mathrm{Sim}(V, q)$ admits a large (s, t)-family. We investigate the converse. By Proposition 1.10 subspaces of $\mathrm{Sim}(q)$ provide certain Pfister forms which are tensor factors of q. The following consequence of the Eigenspace Lemma is a similar sort of result: certain (s, t)- families in $\mathrm{Sim}(q)$ provide Pfister factors of q.

2.16 Corollary. *Suppose* $(\sigma \perp \alpha, \tau \perp \alpha) < \mathrm{Sim}(q)$ *where* $\dim \sigma \geq 1$ *and* $\alpha \simeq \langle a_1, \ldots, a_k \rangle$. *Then* $q \simeq \langle\langle a_1, \ldots, a_k \rangle\rangle \otimes \gamma$ *for some quadratic form* γ *such that* $(\sigma, \tau) < \mathrm{Sim}(\gamma)$.

Proof. Repeated application of (2.10). □

Suppose $\dim q = 2^m n_0$ where n_0 is odd. If there is an $(m + 1, m + 1)$- family $(\sigma, \tau) < \mathrm{Sim}(q)$ with $\sigma \simeq \tau \simeq \langle 1, a_1, \ldots, a_m \rangle$ then $q \simeq \langle\langle a_1, \ldots, a_m \rangle\rangle \otimes \gamma$ for some form γ of odd dimension n_0. The Pfister Factor Conjecture is a stronger version of this idea.

2.17 Pfister Factor Conjecture. *Suppose that* q *is a quadratic form of dimension* $n = 2^m n_0$ *where* n_0 *is odd. If there exists an* $(m + 1, m + 1)$*-family in* $\mathrm{Sim}(q)$ *then* $q \simeq \langle\langle a_1, \ldots, a_m \rangle\rangle \otimes \gamma$ *for some quadratic form* γ *of dimension* n_0.

This conjecture is true for $m \leq 2$ by Proposition 1.10. We cannot get much further without more tools. We take up the analysis of this conjecture again in Chapter 9. The Decomposition Theorem and properties of unsplittable modules (Chapters 4–7) reduce the Conjecture to the case $\dim q = 2^m$. Properties of discriminants and Witt invariants of quadratic forms (Chapter 3) can then be used to prove the conjecture when $m \leq 5$. The answer is not known when $m > 5$ over arbitrary fields, but over certain nice fields (e.g. global fields) the conjecture can be proved for all values of m. After learning some properties of the invariants of quadratic forms (stated in (3.21)), the reader is encouraged to skip directly to Chapter 9 to see how they relate to the Pfister Factor Conjecture.

The Conjecture can be stated in terms of compositions of quadratic forms in the earlier sense: If $\dim q = n = 2^m n_0$ as usual and if there is a subspace $\sigma < \mathrm{Sim}(q)$ where $\dim \sigma = \rho(n)$, then there is an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$. In fact in Proposition 7.6 we prove that $\dim \sigma \geq 2m - 1$ suffices to imply that there is an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$. This "expansion" result seems to require some knowledge of algebras and involutions.

Exercises for Chapter 2

1. **Construction Lemma revisited.** (1) Write out the elements of the $(s+1, t+1)$-family in (2.7) using block matrices: if S has basis $\{1, h_2, \ldots, h_s\}$ then for example $h_i \otimes g_1 = \begin{pmatrix} h_i & 0 \\ 0 & -h_i \end{pmatrix}$ while $1 \otimes f_2 = \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix}$.

(2) Let (S, T) and (G, H) be commuting pairs of amicable subspaces of $\mathrm{Sim}(V)$. That is, every element of $S \cup T$ commutes with every element of $G \cup H$. Choose anisotropic $f \in S$, $g \in G$ and define $S_1 = (f)^\perp$ and $G_1 = (g)^\perp$. Then $(\tilde{f} S_1 + \tilde{g} H, \tilde{g} G_1 + \tilde{f} T)$ is an amicable pair in $\mathrm{Sim}(V)$.

(3) An (s, t)-family on V and an (a, b)-family on W where $s, a \geq 1$ yield an $(s + b - 1, t + a - 1)$-family on $V \otimes W$.

2. **When σ does not represent 1.** Define the *norm group* $G_F(q) = \{a \in F^\bullet : \langle a \rangle q \simeq q\}$, the group of norms of all elements of $\mathrm{Sim}^\bullet(q)$. For any form q, $G_F(q) \cdot D_F(q) \subseteq D_F(q)$. If $\sigma < \mathrm{Sim}(q)$ then $D_F(\sigma) \subseteq G_F(q)$. Let σ, τ be quadratic forms over F.

(1) Suppose $c \in D_F(\sigma)$ and let $\sigma_0 = \langle c \rangle \sigma$ and $\tau_0 = \langle c \rangle \tau$. Then $(\sigma, \tau) < \mathrm{Sim}(q)$ if and only if $c \in G_F(q)$ and $(\sigma_0, \tau_0) < \mathrm{Sim}(q)$.

(2) The Expansion Lemma 2.5 remains true without assuming σ represents 1.

(3) If $(S \perp A, T) \subseteq \mathrm{Sim}(V, q)$ where $\dim A = 4$, there is a shifted amicable family $(S, T \perp A') \subseteq \mathrm{Sim}(V, q)$. If $\{h_1, \ldots, h_4\}$ is an orthogonal basis of A, what is an explicit basis of A'?

(4) The Construction Lemma remains true without assuming σ represents 1.

(Hint. (4) If $c \in G_F(q)$ then $q \otimes \langle\langle ca \rangle\rangle \simeq q \otimes \langle\langle a \rangle\rangle$.)

3. (1) Deduce the following formulas directly from the early lemmas about (s, t)-families.

$$\delta(s, t) = \delta(t, s) \quad \delta(s+1, t+1) = 1 + \delta(s, t) \quad \delta(s+4, t) = \delta(s, t+4).$$

(2) Recall the definition of $\delta(r)$ from Exercise 0.6: $r \leq \rho(n)$ iff $2^{\delta(r)} \,|\, n$. Note that $\delta(r+8) = \delta(r) + 4$ and use this to extend the definition to $\delta(-r)$.

Lemma. $\delta(s, t) = t + \delta(s - t)$.

(3) $\delta(s) = \begin{cases} \frac{s-2}{2} & \text{if } s \equiv 0 \\ \frac{s-1}{2} & \text{if } s \equiv \pm 1 \\ \frac{s}{2} & \text{if } s \equiv \pm 2, 4 \\ \frac{s+1}{2} & \text{if } s \equiv \pm 3 \end{cases} \pmod 8.$

4. **More Shift Lemmas.** (1) If $\dim \varphi \equiv 2 + \dim \psi \pmod 4$ in the Shift Lemma then $(\sigma \perp \varphi, \tau \perp \psi)$ is equivalent to $(\sigma \perp \langle d \rangle \varphi, \tau \perp \langle d \rangle \psi)$.

(2) Let $(\sigma, \tau) = (\langle 1, a, b, c\rangle, \langle x, y\rangle)$ and $d = abcxy$. Then we can shift it to $(\sigma', \tau') = (\langle 1, a, b, c, dx, dy\rangle, 0)$. Similarly if $(\sigma, \tau) = (\langle 1, a, b\rangle, \langle x, y, z\rangle)$, and $d = abxyz$ we can shift it to $(\sigma', \tau') = (\langle 1, a, bd\rangle, \langle x, y, zd\rangle)$.

(3) Generalize this idea to other (s, t)-pairs where $s + t$ is even. If $s \equiv t \pmod 4$ explain why $\delta(s, t + 2) = \delta(s + 2, t)$.

5. (1) If $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q)$ then $\langle 1, abx\rangle < \mathrm{Sim}(q)$.

(2) Generalize this observation to $(\sigma, \tau) < \mathrm{Sim}(q)$ where $s \equiv t+2$ or $t+3 \pmod 4$.

(Hint. (1) Examine the element z as in (2.4).)

6. **Alternating spaces.** (1) **Lemma.** *Let σ, τ and α be quadratic forms and V a vector space. Suppose* $\dim \alpha \equiv 2 \pmod 4$. *Then $(\sigma \perp \alpha, \tau) < \mathrm{Sim}(V, q)$ for some quadratic form q on V if and only if $(\sigma, \tau \perp \alpha) < \mathrm{Sim}(V, B)$ for some alternating form B on V.*

(2) **Theorem.** *Suppose $n = 2^m n_0$ where n_0 is odd. There exists an (s, t)- family on some alternating space of dimension n if and only if one of the following holds:*

(i) $s + t \leq 2m$,

(ii) $s + t = 2m + 1$ *and* $s \equiv t - 3$ *or* $t + 3 \pmod 8$,

(iii) $s + t = 2m + 2$ *and* $s \equiv t + 4 \pmod 8$.

(3) Let $\delta'(s, t)$ be the corresponding function for alternating spaces. Then $\delta'(s + 2, t) = \delta(s, t + 2)$. Note that $\delta(s, t) = \delta'(s, t)$ iff $s \equiv t \pm 2 \pmod 8$. How does Exercise 4 help "explain" this? Does $\delta'(s, t) = t + \delta'(s - t)$?

(4) Let $\rho'(n)$ be the Hurwitz–Radon function for alternating spaces. Note that $\rho'(1) = 0$ and $\rho'(2) = 4$. (See Exercise 1.7.) The formula for $\rho'(n)$ in terms of $m \pmod 4$ is a "cycled" version of the formula for $\rho(n)$. In other words, $\rho'(4n) = 4 + \rho(n)$ whenever $n \geq 1$.

(Hint:. (1) Let $(S \perp A, T) \subseteq \mathrm{Sim}(V, q)$ and z be given as in the Shift Lemma 2.6. Define the form B' on V by: $B'(u, v) = B(u, z(v))$. Then $(S, T \perp A) \subseteq \mathrm{Sim}(V, B')$.)

7. **Hurwitz–Radon functions.** (1) Write out the formulas for $\rho'_t(n)$, the alternating version of the functions $\rho_t(n)$ given in (2.13) and prove the analog of (2.14).

(2) We write $\rho^\lambda(n)$ to denote $\rho(n)$ if $\lambda = 1$ and $\rho'(n)$ if $\lambda = -1$. The following properties of the Hurwitz–Radon functions are consequences of the formulas, assuming in each case that the function values are large enough.

$$\rho^\lambda_{t+1}(2n) = 1 + \rho^\lambda_t(n), \qquad \rho^\lambda_t(n) = 4 + \rho^\lambda_{t+4}(n), \qquad \rho_t^{-\lambda}(4n) = 4 + \rho^\lambda_t(n),$$
$$\rho^\lambda_t(n) = 2 + \rho^{-\lambda}_{t+2}(n), \qquad \max\{\rho(n), \rho'(n)\} = \begin{cases} 2m + 1 & \text{if } m \text{ is even,} \\ 2m + 2 & \text{if } m \text{ is odd.} \end{cases}$$

(3) Explain each of these formulas more theoretically.

8. **That element "z".** The element $z = z(S) \cdot z(T)$ was used in (2.4) and (2.5). What if a different orthogonal basis is chosen for S? Is there a suitable definition for z when S does not contain 1_V? We use the following result originally due to Witt:

Chain-Equivalence Theorem. *Let (V, q) be a quadratic space with two orthogonal bases $\mathcal{X}$ and $\mathcal{X}'$. Then there exists a chain of orthogonal bases $\mathcal{X} = \mathcal{X}_0, \mathcal{X}_1, \ldots, \mathcal{X}_m = \mathcal{X}'$ such that $\mathcal{X}_i$ and $\mathcal{X}_{i-1}$ differ in at most 2 vectors.*

Proofs appear in Scharlau (1985), pp. 64–65 and O'Meara (1963), p. 150. Compare Satz 7 of Witt (1937).

(1) Let $S \subseteq \mathrm{Sim}(V, q)$ be a subspace of dimension s. If $\mathcal{B} = \{f_1, f_2, \ldots, f_s\}$ is an orthogonal basis of S, define $z(\mathcal{B}) = f_1 \cdot \tilde{f}_2 \cdot f_3 \cdot \tilde{f}_4 \ldots$ and $w(\mathcal{B}) = \tilde{f}_1 \cdot f_2 \cdot \tilde{f}_3 \cdot f_4 \ldots$.

Lemma. *If $\mathcal{B}'$ is another orthogonal basis, then $z(\mathcal{B}') = \lambda \cdot z(\mathcal{B})$ and $w(\mathcal{B}') = \lambda \cdot w(\mathcal{B})$ for some $\lambda \in F^\bullet$.*

Define $z(S) = z(\mathcal{B})$ and $w(S) = w(\mathcal{B})$. These values are uniquely determined by the subspace S, up to non-zero scalar multiple. Note that $z(S) \cdot z(S)^\sim = w(S) \cdot w(S)^\sim = \det(\sigma) \cdot 1_V$.

Let $z = z(\mathcal{B})$ and $w = w(\mathcal{B})$.

(2) If s is odd: $w = (-1)^{(s-1)/2} \cdot \tilde{z}$. For every $f \in S^\bullet$, $z \cdot \tilde{f} = f \cdot \tilde{z}$.

If s is even: $\tilde{z} = (-1)^{s/2} \cdot z$ and $\tilde{w} = (-1)^{s/2} \cdot w$. For every $f \in S^\bullet$, $zf = fw$.

Consequently if s is even then $z^2 = w^2 = d\sigma \cdot 1_V$.

(3) Suppose $\varphi : S \to S$ is a similarity. Then $\varphi(\mathcal{B})$ is another orthogonal basis and

$$z(\varphi(\mathcal{B})) = (\det \varphi) \cdot z(\mathcal{B}).$$

(4) Let $g, h \in \mathrm{Sim}^\bullet(V, q)$ with $\alpha = \mu(g)\mu(h)$.

If s is odd: $z(g\mathcal{B}h) = \alpha^{(s-1)/2} \cdot g \cdot z(\mathcal{B}) \cdot h$.

If s is even: $z(g\mathcal{B}h) = \alpha^{s/2} \cdot g \cdot z(\mathcal{B}) \cdot g^{-1}$.

(5) Analyze the Expansion and Shift Lemmas using these ideas. (Compare Exercise 2.)

9. **Symmetric similarities.** (1) **Lemma** (Dieudonné). *Suppose $f \in \mathrm{Sim}^\bullet(V, q)$ where $\dim V = 2m$ is even. Then there exists $g \in \mathrm{O}(V, q)$ and a decomposition $V = V_1 \perp \cdots \perp V_m$ such that $gf(V_i) = V_i$, $\dim V_i = 2$ and $\widetilde{gf} = gf$. Furthermore, given anisotropic $v \in V$, there is such a decomposition with $v \in V_1$.*

(2) $\langle a \rangle < \mathrm{Sim}(q)$ if and only if $(\langle 1 \rangle, \langle a \rangle) < \mathrm{Sim}(q)$.

(3) If $\dim q$ is even then $G_F(q) \subseteq D_F(\langle\langle -dq \rangle\rangle)$.

(Hint. (1) Assume $\mu(f) \notin F^{\bullet 2}$ and let $V_1 = \mathrm{span}\{v, f(v)\}$. Then V_1 is a regular 2-plane and there exists $g_1 \in \mathrm{O}(V)$ with $g_1 f(v) = f(v)$ and $g_1 f^2(v) = \mu(f)v$. Then $g_1 f$ preserves V_1. Apply induction to construct g. Note that $(gf)^2 = \mu(f)1_V$.

(3) If $a \in G_F(q)$ with $a \notin F^{\bullet 2}$ then $q \simeq \langle x_1 \rangle\langle\langle -d_1 \rangle\rangle \perp \cdots \perp \langle x_m \rangle\langle\langle -d_m \rangle\rangle$ where $\langle\langle -d_j \rangle\rangle$ represents a. Then $\langle\langle -a \rangle\rangle$ represents $\langle d_1 d_2 \ldots d_m \rangle = dq$.)

10. An *orthogonal design* of order n and type $(s_1, \ldots, s_k)$ is an $n \times n$ matrix A with entries from $\{0, \pm x_1, \ldots, \pm x_k\}$ such that the rows of A are orthogonal and each row

of A has s_i entries of the type $\pm x_i$. Here the x_i are commuting indeterminates and s_i is a positive integer. Then $A \cdot A^\top = \sigma \cdot I_n$ where $\sigma = \sum_{i=1}^k s_i x_i^2$.

Proposition. (1) *If there is such a design then* $\langle s_1, \ldots, s_k \rangle < \mathrm{Sim}(n\langle 1 \rangle)$. *In particular* $k \leq \rho(n)$.

(2) *If the* s_i *are positive integers and* $s_1 + \cdots + s_k \leq \rho(n)$ *then there is an orthogonal design of order* n *and type* $(s_1, \ldots, s_k)$.

(Hint. The Construction, Shift and Expansion Lemmas provide $A_i \in \mathbb{M}_n(\mathbb{Z})$, for $1 \leq i \leq \rho(n)$, which satisfy the Hurwitz Matrix Equations. This yields an integer composition formula as in Exercise 0.4, hence an orthogonal design of order n and type $(1, 1, \ldots, 1)$. Set some of the variables equal.)

11. **Constructing composition algebras.** (1) From the Construction and Expansion Lemmas there is a 4-dimensional subspace $\langle 1, a, b, ab \rangle < \mathrm{Sim}(\langle\langle a, b \rangle\rangle)$. This induces a 4-dimensional composition algebra (see Exercise 1.1). This turns out to be the usual quaternion algebra.

(2) The Construction and Shift Lemmas provide an explicit $\sigma < \mathrm{Sim}(\langle\langle a, b, c \rangle\rangle)$ with $\dim \sigma = 8$, and we get an induced 8-dimensional composition algebra. This turns out to be the standard octonion algebra.

12. **Amicable spaces of rectangular matrices.** Let V, W be two regular quadratic spaces and consider subspaces $S, T \subseteq \mathrm{Sim}(V, W)$ as in Exercise 1.2. Suppose S and T are "amicable" in the sense generalizing (2.1). If $\dim S = s$, $\dim T = t$, $\dim V = r$ and $\dim W = n$ we could call this an (s, t)-family of $n \times r$ matrices.

(1) If there is an (s, t)-family of $n \times r$ matrices then there is an $(s+1, t+1)$-family of $2n \times 2r$ matrices. This is the analog of the Construction Lemma.

(2) Why do the analogs of the Expansion and Shift Lemmas fail in this context?

13. **Systems of skew-symmetric matrices. Definition.** $\alpha_F(n) = \max\{t :$ there exist $A_1, \ldots, A_t \in \mathrm{GL}_n(F)$ such that $A_i^\top A_j + A_j^\top A_i = 0$ whenever $i \neq j\}$. Certainly $\rho(n) \leq \alpha_F(n)$.

Open question. Is this always an equality?

(1) $\alpha_F(n) - 1 = \max\{k :$ there exist k skew-symmetric elements of $\mathrm{GL}_n(F)$ which pairwise anticommute$\}$.

(2) If $n = 2^m n_0$ where n_0 is odd, then $\alpha_F(n) \leq 2m + 2$.

(3) If n_0 is odd then $\alpha_F(n_0) = 1$ and $\alpha_F(2n_0) = 2$.

(4) **Proposition.** $\alpha_F(2^m) = \rho(2^m)$.

(5) Let $\{I, f_2, \ldots, f_s\}$ be a system over F as above. Let $V = F^n$ with the standard inner product, and view $f_i \in \mathrm{End}(V)$. Define $W \subseteq V$ to be invariant if $f_i(W) \subseteq W$ for every i. The system is "decomposable" if V is an orthogonal sum of non-zero invariant subspaces.

Lemma. *If* $\{f_i\}$ *is an indecomposable system over* $\mathbb{R}$, *then* $f_i^2 = $ *scalar.*

(6) **Proposition.** *If* F *is formally real then* $\alpha_F(n) = \rho(n)$.

(Hint. (2) See Exercise 1.12.

(3) For $2n_0$ apply the "Pfaffians" defined in Chapter 10. If f, g are nonsingular, skew-symmetric, anti-commuting, then $pf(fg) = pf(gf) = pf(-fg)$.

(4) If $\alpha_F(2^m) > \rho(2^m)$ there exist $2m$ skew-symmetric, anti-commuting elements $f_i \in \mathrm{GL}_{2^m}(F)$. Then $f_i^2 =$ scalar as in Exercise 1.12(2), and Hurwitz–Radon applies.

(5) The Spectral Theorem implies V is the orthogonal sum of the eigenspaces of the symmetric matrix f_j^2. Since every f_i commutes with f_j^2 these eigenspaces are invariant.

(6) Generalize (5) to real closed fields and note that F embeds in a real closed field. Apply Hurwitz–Radon. Over $\mathbb{R}$ we could apply Adams' theorem (see Exercise 0.7) to the orthogonal vector fields $f_2(v), \ldots, f_s(v)$ on S^{n-1}.)

14. A *Hadamard design* of order n on k letters $\{x_1, \ldots, x_k\}$ is an $n \times n$ matrix H such that each entry is some $\pm x_j$ and the inner product of any two distinct rows is zero. If there is such a design then there exist $n \times n$ matrices $H_1, \ldots, H_k$ with entries in $\{0, 1, -1\}$ such that $H_j \cdot H_i^\top + H_i \cdot H_j^\top = 0$ if $i \neq j$ and $H_i \cdot H_i^\top =$ diagonal.

Proposition. *If there exists a Hadamard design of order n on k letters, each of which occurs at least once in every column of H, then $k \leq \rho(n)$.*

(Hint. Note that each H_i is nonsingular and apply Exercise 13.)

15. **Hermitian compositions.** A *hermitian (r, s, n)-formula* is:

$$(|x_1|^2 + \cdots + |x_r|^2) \cdot (|y_1|^2 + \cdots + |y_s|^2) = |z_1|^2 + \cdots + |z_n|^2$$

where $X = (x_1, \ldots, x_r)$ and $Y = (y_1, \ldots, y_s)$ are systems of complex indeterminants over $\mathbb{C}$, and each z_k is bilinear in X, Y. Such a formula can be viewed as a bilinear map $f : \mathbb{C}^r \times \mathbb{C}^s \to \mathbb{C}^n$ satisfying $|f(x, y)| = |x| \cdot |y|$. We consider three versions of bilinearity:

Type 1: each z_k is bilinear in $(X, \bar{X})$ and $(Y, \bar{Y})$.

Type 2: each z_k is bilinear in $(X, \bar{X})$ and Y.

Type 3: each z_k is bilinear in X and Y.

Note that if $X = X_1 + iX_2$ then z is linear (over $\mathbb{C}$) in $(X, \bar{X})$ if and only if z is $\mathbb{C}$-linear in the system of real variables (X_1, X_2). For example $z_1 = x_1y_1 + x_2y_2$ and $z_2 = \bar{x}_1y_2 - \bar{x}_2y_1$ provides a $(2, 2, 2)$-formula of types 1 and 2.

Proposition. (1) *A hermitian (r, s, n)-formula of type 1 exists if and only if there exists an ordinary $(2r, 2s, 2n)$-formula over $\mathbb{R}$.*

(2) *A hermitian (r, s, n)-formula of type 2 exists if and only if there exist two amicable subspaces of dimension r in $\mathrm{Sim}^{\mathrm{herm}}(\mathbb{C}^s, \mathbb{C}^n)$, the set of hermitian similarities.*

(3) *A hermitian (r, s, n)-formula of type 3 exists if and only if $n \geq rs$.*

(Hints. (2) The formula exists iff there is an $n \times s$ matrix A whose entries are linear forms in $(X, \bar{X})$ and satisfying $A^* \cdot A = \left(\sum_1^r \bar{x}_j x_j\right) I_s$, where $*$ denotes the conjugate-transpose. Express $x_j = u_j + v_j\sqrt{-1}$ where u_j, v_j are real variables. Then

$A = \sum_1^r u_j B_j + v_j \sqrt{-1} C_j$, where B_j and C_j are $n \times s$ matrices over $\mathbb{C}$. Then $S = \text{span}\{B_1, \ldots, B_r\}$ and $T = \text{span}\{C_1, \ldots, C_r\}$ are the desired subspaces.

(3) Here we get the same equation for A, where $A = x_1 A_1 + \cdots + x_r A_r$ and each A_j is a complex $n \times s$ matrix. Then $A_j^* A_j = I_s$ and $A_j^* A_k = 0$ if $j \neq k$. Choose $A_1 = \begin{pmatrix} I_s \\ 0 \end{pmatrix}$.)

16. Consider the analogous composition formulas of the type

$$(x_1^2 + \cdots + x_r^2) \cdot (|y_1|^2 + \cdots + |y_s|^2) = |z_1|^2 + \cdots + |z_n|^2$$

where X is a system over $\mathbb{R}$, Y is a system over $\mathbb{C}$ and each z_k is bilinear in X, Y. Is the existence of such a formula equivalent to the existence of $A_2, \ldots, A_r \in \text{GL}_n(\mathbb{C})$ which are anti-hermitian ($A_j^* = -A_j$), unitary ($A_j^* \cdot A_j = 1$) and pairwise anticommute?

Notes on Chapter 2

The notion of amicable similarities was pointed out to me by W. Wolfe in 1974 (see Wolfe (1976)). He introduced the term "amicable" in analogy with a related idea in combinatorics.

The idea of allowing some symmetric elements in the Hurwitz Matrix Equations has occurred independently in Ławrynowicz and Rembieliński (1990). They do this to obtain some further symmetries in their approach to the theory.

Exercise 9 follows Dieudonné (1954). Compare the appendix of Elman and Lam (1974). The decomposition of V is closely related to the "β-decomposition" in Corollary 2.3 of Elman and Lam (1973b). See Exercise 5.7 below.

Exercise 10. Orthogonal designs are investigated extensively in Geramita and Seberry (1979).

Exercise 13. The lemma in (5) follows Putter (1967). Further information on anticommuting matrices is given in the Notes on Chapter 1.

Exercise 14 generalizes ideas of Storer (1971).

Exercise 15–16. The observation on $\mathbb{C}$-bilinear hermitian compositions in 15 (3) is due to Alarcon and Yiu (1993). Hermitian compositions are discussed further in Exercise 4.7. Compositions as in Exercise 16 are also considered in Furuoya et al. (1994). They work with a slightly more general situation, allowing forms of arbitrary signature over $\mathbb{R}$. Compare Exercise 4.7.

Chapter 3

Clifford Algebras

This is essentially a reference chapter, containing the definitions and basic properties of Clifford algebras and Witt invariants, along with some related technical results that will be used later. The reader should have some acquaintance with central simple algebras, the Brauer group $\mathrm{Br}(F)$ and the Witt ring $W(F)$. This background is presented in a number of texts, including Lam (1973), Scharlau (1985).

Clifford algebras have importance in algebra, geometry and analysis. We need the basic algebraic properties of Clifford algebras over an arbitrary field F. We include the proofs of some of the basic results, assuming familiarity with the classical theory of central simple algebras. The exposition is simplified since we assume that the characteristic of F is not 2.

Every F-algebra considered here is a finite dimensional, associative F-algebra with an identity element denoted by 1. The field F is viewed as a subset of the algebra. An unadorned tensor product $\otimes$ always denotes $\otimes_F$, the tensor product over F.

The first non-commutative algebra was the real quaternion algebra discovered by Hamilton in 1843. That motivates the general definition of a quaternion algebra over F.

Definition. If $a, b \in F^\bullet$, the quaternion algebra $A = \left(\frac{a,b}{F}\right)$ is the associative F-algebra with generators i, j satisfying the multiplication rules:

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ij = -ji.$$

The associativity implies that A is spanned by $\{1, i, j, ij\}$ and it follows that $\dim A = 4$. An element of A is called "pure" if its scalar part is 0. Then the set $A^\circ = A_0$ of pure quaternions is the span of $\{i, j, ij\}$. Direct calculation shows that

$$A_0 = \{u \in A : u \notin F^\bullet \text{ and } u^2 \in F\}.$$

Consequently A_0 is independent of the choice of generators i, j. Define the "bar" map on A to be the linear map which acts as 1 on F and as -1 on A_0. Then $\bar{\bar{a}} = a$ and: $\bar{a} = a$ if and only if $a \in F$. Another calculation shows: $\overline{uv} = \bar{v} \cdot \bar{u}$. Then "bar" is the unique anti-automorphism of A with $\bar{i} = -i$ and $\bar{j} = -j$.

The norm $N : A \to F$, defined by $N(a) = \bar{a} \cdot a$, is a quadratic form on A and calculation on the given basis shows that $(A, N) \simeq \langle\langle -a, -b \rangle\rangle$. Moreover, $N(ab) = N(a) \cdot N(b)$ so that A is a composition algebra as described in Chapter 1, Appendix.

3.1 Lemma. (1) $\left(\frac{a,b}{F}\right)$ *is split if and only if its norm form* $\langle\langle -a, -b \rangle\rangle$ *is hyperbolic.*

(2) *The isomorphism class of* $\left(\frac{a,b}{F}\right)$ *is determined by the isometry class of* $\langle\langle -a, -b \rangle\rangle$.

Proof. An explicit isomorphism $\left(\frac{1,-1}{F}\right) \to \mathbb{M}_2(F)$ is provided by sending $i \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. It suffices to prove (2). An isomorphism of quaternion algebras preserves the pure parts, so it commutes with "bar" and is an isometry for the norms. If A is a quaternion algebra and $(A, N) \simeq \langle\langle -a, -b \rangle\rangle$, Witt Cancellation implies $(A_0, N) \simeq \langle -a, -b, ab \rangle$, so there exist orthogonal elements i, j in A_0 with $N(i) = -a$ and $N(j) = -b$. Therefore $i^2 = a$, $j^2 = b$ and $ij + ji = 0$ and these generators provide an isomorphism $A \cong \left(\frac{a,b}{F}\right)$. □

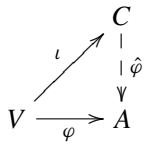
These results on quaternion algebras, together with the systems of equations in (1.6) and (2.3), help to motivate the investigation of algebras having generators $\{e_1, e_2, \ldots, e_n\}$ which anticommute and satisfy $e_i^2 \in F^\bullet$. An efficient method for defining these algebras is to use their universal property.

Suppose (V, q) is a quadratic space over F and A is an F-algebra. A linear map $\iota : V \to A$ is *compatible with* q if it satisfies:

$$\iota(v)^2 = q(v) \quad \text{for every } v \in V.$$

For such a map ι, the quadratic structure of (V, q) is related to the algebra structure of A. For example, if $v, w \in V$ are orthogonal then $\iota(v)$ and $\iota(w)$ anticommute in A. (For $2B_q(v, w) = q(v + w) - q(v) - q(w) = \iota(v + w)^2 - \iota(v)^2 - \iota(w)^2 = \iota(v)\iota(w) + \iota(w)\iota(v)$.)

The Clifford algebra $C(V, q)$ is the F-algebra universal with respect to being compatible with q. More formally, define a *Clifford algebra* for (V, q) to be an F-algebra C together with an F-linear map $\iota : V \to C$ compatible with q and such that for any F-algebra A and any F-linear map $\varphi : V \to A$ which is compatible with q, there exists a unique F-algebra homomorphism $\hat{\varphi} : C \to A$ such that $\varphi = \hat{\varphi} \circ \iota$.



3.2 Lemma. *For any quadratic space (V, q) over F there is a Clifford algebra $(C(V, q), \iota)$, which is unique up to a unique isomorphism.*

Proof. The uniqueness of the Clifford algebra follows by the standard argument for universal objects. (See Exercise 1.) To prove existence we use the tensor algebra

$$T(V) = \oplus_k T^k(V) \quad \text{where } T^k(V) \text{ is the } k\text{-fold tensor product of } V.$$

Then $T(V) = F \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$. Let $C = T(V)/\mathfrak{I}$ where $\mathfrak{I}$ is the two-sided ideal of $T(V)$ generated by all elements $v \otimes v - q(v) \cdot 1$ for $v \in V$. Let $\iota : V \to C$ be the canonical map $V \to T(V) \to T(V)/\mathfrak{I} = C$.

Claim. (C, ι) is a Clifford algebra for (V, q). For if $\varphi : V \to A$ is an F-linear map compatible with q then the universal property of tensor algebras implies that φ extends to a unique F-algebra homomorphism $\tilde{\varphi} : T(V) \to A$. Since φ is compatible with q we find that $\tilde{\varphi}(\mathfrak{I}) = 0$ and therefore $\tilde{\varphi}$ induces a unique homomorphism $\hat{\varphi} : C \to A$ such that $\varphi = \hat{\varphi} \circ \iota$. □

Since the Clifford algebra is unique we are often sloppy about the notations, writing $C(q)$ rather than $C(V, q)$. A major advantage of using the universal property to define Clifford algebras is that the "functorial" properties follow immediately:

3.3 Lemma. (1) *An isometry $f : (V, q) \to (V', q')$ induces a unique algebra homomorphism $C(f) : C(V, q) \to C(V', q')$. Consequently if $q \simeq q'$ then $C(q) \cong C(q')$.*

(2) *If K is an extension field of F then there is a canonical isomorphism $C(K \otimes_F (V, q)) \cong K \otimes_F C(V, q)$.*

Proof. Exercise 1. □

The isomorphism class of $C(q)$ depends only on the isometry class of the quadratic form q. It is natural to ask the converse question: If $C(q) \cong C(q')$ does it follow that the quadratic forms q and q' are isometric? The answer is "no" in general, but the study of those quadratic forms which have isomorphic Clifford algebras is one of the major themes of this theory.

With the universal definition of Clifford algebras given above it is not immediately clear what the dimensions are. We spend some time presenting a proof that if $\dim q = n$ then $\dim C(q) = 2^n$.

3.4 Lemma. (1) *$C(V, q)$ is an F-algebra generated by $\iota(V)$.*

(2) *If $\dim q = n$ then $\dim C(q) \leq 2^n$.*

Proof. (1) Exercise 1.

(2) If $\{v_1, \dots, v_n\}$ is an orthogonal basis of V let $e_i = \iota(v_i)$. As mentioned earlier, $e_1, \dots, e_n$ anticommute and $e_j^2 = q(v_j) \in F$. By part (1), $C(q)$ is spanned by the products $e_1^{\delta_1} \dots e_n^{\delta_n}$ where each $\delta_i = 0$ or 1. There are 2^n of these products. □

3.5 Lemma. *Suppose q is a quadratic form on V, A is an F-algebra and $\varphi : V \to A$ is a linear map compatible with q such that A is generated by $\varphi(V)$. If* $\dim q = n$ *and* $\dim A = 2^n$ *then $A \cong C(q)$. If such an algebra A exists then* $\dim C(q) = 2^n$ *and $\iota : V \to C(q)$ is injective.*

Proof. There is an algebra homomorphism $\hat{\varphi} : C(q) \to A$ such that $\varphi = \hat{\varphi} \circ \iota$. Since $\iota(V)$ generates $C(q)$, $\varphi(V) = \hat{\varphi}(\iota(V))$ generates $\hat{\varphi}(C(q)) \subseteq A$. By hypothesis $\varphi(V)$ generates A and we see that $\hat{\varphi}$ is surjective. Then $\dim C(q) = 2^n + \dim(\ker \hat{\varphi})$ and (3.4) implies that $\dim C(q) = 2^n$ and $\ker \hat{\varphi} = \{0\}$. Therefore $\hat{\varphi}$ is an isomorphism. If ι is not injective then $\dim \iota(V) < n$ and the argument in (3.4) would imply that $\dim C(q) < 2^n$. □

This criterion can be used to provide some explicit examples of Clifford algebras. If $a \in F^\bullet$ define the quadratic extension to be $F\langle\sqrt{a}\rangle = F[x]/(x^2 - a)$. If $\langle a\rangle \not\simeq \langle 1\rangle$ (that is, a is not a square in F) this algebra is just the quadratic field extension $F(\sqrt{a})$. However if $\langle a\rangle \simeq \langle 1\rangle$ then $F\langle\sqrt{a}\rangle \cong F \times F$, the direct product of two copies of F.

3.6 Examples. (1) $C(\langle a\rangle) \cong F\langle\sqrt{a}\rangle$, the quadratic extension.

(2) $C(\langle a, b\rangle) \cong \left(\frac{a,b}{F}\right)$, the quaternion algebra.

(3) If q is the zero form on V then $C(V, q) = \Lambda(V)$ is the exterior algebra.

Proof. (1) The space $\langle a\rangle$ is given by $V = Fe$ with $q(xe) = ax^2$. If $A = F\langle\sqrt{a}\rangle$ define $\varphi : Fe \to A$ by $\varphi(xe) = x\sqrt{a}$. Then φ is compatible with q and (3.5) applies.

(2) The space $\langle a, b\rangle$ is given by $V = Fe_1 + Fe_2$ with $q(xe_1 + ye_2) = ax^2 + by^2$. Define $\varphi : V \to \left(\frac{a,b}{F}\right)$ by $\varphi(xe_1 + ye_2) = xi + yj$. Then φ is compatible with q and (3.5) applies.

(3) If $q = 0$ the definition of the Clifford algebra coincides with the definition of the exterior algebra. □

Perhaps the best way to prove the general result that $\dim C(q) = 2^n$ is to develop the theory of graded tensor products, prove that $C(\alpha \perp \beta) \cong C(\alpha) \hat{\otimes} C(\beta)$ and use induction. That approach has the advantage that it gives a unified treatment of the theory, combining the "even" and "odd" cases. Furthermore it is valid for quadratic forms over a commutative ring, provided that the forms can be diagonalized. Graded tensor products are discussed in the books by Lam and Scharlau, but see the booklets by Chevalley (1955) and Knus (1988) for further generality.

Rather than repeating that treatment, we provide an elementary, direct argument using the independence result (1.11). This method works only over fields of charac-

teristic not 2, but that is the case of interest here anyway. The quadratic form q may be singular here.

3.7 Proposition. *If q is a quadratic form on V with* $\dim q = n$ *then* $\dim C(q) = 2^n$ *and the map $\iota : V \to C(q)$ is injective.*

Proof. First suppose q is a regular form of even dimension n. Choose an orthogonal basis $\{v_1, \ldots, v_n\}$ yielding the diagonalization $q \simeq \langle a_1, \ldots, a_n \rangle$. Then $C(q)$ contains elements $e_i = \iota(v_i)$ which anticommute and with $e_i^2 = a_i \in F^\bullet$. Then (1.11) implies that the 2^n elements e^Δ are linearly independent. Therefore $2^n \leq \dim C(q)$ and (3.4) and (3.5) complete the argument.

If n is odd let $q' = q \perp \langle 1 \rangle$ and choose an isometry $\psi : (V, q) \to (V', q')$. Then (V', q') has an orthogonal basis $\{w_1, \ldots, w_n, w_{n+1}\}$ where $w_i = \psi(v_i)$ for $i = 1, \ldots, n$. Let $e_i = \iota(w_i)$ in $C(q')$. As before (1.11) implies that the elements e^Δ are linearly independent. Let A be the subalgebra generated by $e_1, \ldots, e_n$, so that $\dim A = 2^n$. Then $\iota \circ \psi : V \to A$ is compatible with q and (3.5) completes the argument.

If (V, q) is singular the same idea works. Choose an isometry $\varphi : (V, q) \to (V', q')$ where q' is regular. (Why does such φ exist? See Exercise 20.) First step: if $\{w_1, \ldots, w_m\}$ is any basis of V' (not necessarily orthogonal) and $f_i = \iota(w_i)$ then the 2^n elements f^Δ are linearly independent. Second step: choose $\{w_1, \ldots, w_m\}$ so that $w_i = \varphi(v_i)$ for $1 \leq i \leq n$ and let A be the subalgebra generated by $f_1, \ldots, f_n$. Then $\dim A = 2^n$ and $\iota \circ \psi : V \to A$ is compatible with q. □

Since $\iota : V \to C(V, q)$ is always injective we simplify the notation by considering V as a subset of $C(V, q)$. If $U \subseteq V$ is a subspace and q induces the quadratic form φ on U, then $C(U, \varphi)$ is viewed as a subalgebra of $C(V, q)$. If $\{e_1, \ldots, e_n\}$ is a basis of V then $\{e^\Delta : \Delta \in \mathbb{F}_2^n\}$ is sometimes called the *derived basis* of $C(V, q)$.

If $f : (V, q) \to (V', q')$ is an isometry the universal property implies that there is a unique algebra homomorphism $C(f) : C(V, q) \to C(V', q')$ extending f. Consequently, if $g \in \mathrm{O}(V, q)$ there is an automorphism $C(g)$ of $C(V, q)$ extending g. When $g = -1_V$ we get an automorphism $\alpha = C(-1_V)$ of particular importance.

3.8 Definition. The *canonical automorphism* α of $C(V, q)$ is the automorphism with $\alpha(x) = -x$ for every $x \in V$. Define $C_0(V, q)$ to be the 1-eigenspace of α and $C_1(V, q)$ to be the (-1)-eigenspace of α. This subalgebra $C_0(V, q)$ is called the *even Clifford algebra* (or the second Clifford algebra) of q.

This notation α for an automorphism should not cause confusion even though we sometimes use α to denote a quadratic form. The meaning of the 'α' ought to be clear from the context.

Note that $\alpha^2 = \alpha \circ \alpha$ is the identity map on $C(q)$ and therefore $C(q) = C_0(q) \oplus C_1(q)$. Note that $\alpha(v_1 v_2 \ldots v_m) = (-1)^m v_1 v_2 \ldots v_m$ for any $v_1, v_2, \ldots, v_m \in V$.

Therefore $C_0(V,q)$ is the span of all such products where m is even. Suppose $\{e_1, e_2, \ldots, e_n\}$ is an orthogonal basis of V corresponding to $q \simeq \langle a_1, a_2, \ldots, a_n\rangle$. Then

$$\alpha(e^\Delta) = (-1)^{|\Delta|} e^\Delta.$$

Therefore $\{e^\Delta : |\Delta| \text{ is even}\}$ is a basis of $C_0(q)$ while $\{e^\Delta : |\Delta| \text{ is odd}\}$ is a basis of $C_1(q)$. In particular, $\dim C_0(q) = \dim C_1(q) = 2^{n-1}$.

Furthermore, $C_0 \cdot C_1 \subseteq C_1$ and $C_1 \cdot C_1 \subseteq C_0$. If $u \in C_1(q)$ is an invertible element then $C_1(q) = C_0(q) \cdot u$. The next lemma shows that this subalgebra $C_0(q)$ can itself be viewed as a Clifford algebra, at least if q is regular.

3.9 Lemma. *If $q \simeq \langle a\rangle \perp \beta$ and $a \neq 0$ then $C_0(q) \simeq C(\langle -a\rangle\beta)$.*

Proof. Let $\{e_1, e_2, \ldots, e_n\}$ be an orthogonal basis of V where e_1 corresponds to $\langle a\rangle$. Then the elements $e_1 e_i \in C_0(q)$ anticommute and $(e_1 e_i)^2 = -a \cdot q(e_i)$ for $i = 2, \ldots, n$. Then the inclusion map from $W = \operatorname{span}\{e_1e_2, \ldots, e_1e_n\}$ to $C_0(q)$ is compatible with the form $\langle -a\rangle\beta$ on W and the universal property provides an algebra homomorphism $\hat{\varphi} : C(\langle -a\rangle\beta) \to C_0(q)$. Since $a \neq 0$ the elements e_1e_i generate $C_0(q)$ so that $\hat{\varphi}$ is surjective. Counting dimensions we conclude that $\hat{\varphi}$ is an isomorphism. □

Let us now restrict attention again to regular quadratic forms. The next goal is to define the "Witt invariant" $c(q)$ of a regular quadratic form and to derive some of its properties. The first step is to prove that if q has even dimension then $C(q)$ is a central simple algebra. Then $c(q)$ will be defined to be the class of $C(q)$ in the Brauer group $\operatorname{Br}(F)$.

To begin this sequence of ideas we determine the centralizer of $C_0(q)$ in $C(q)$. The argument here is reminiscent of the proof of (1.11).

3.10 Definition. If $\{e_1, \ldots, e_n\}$ is an orthogonal basis of (V,q) define the element $z(V,q) = e_1e_2 \ldots e_n \in C(V,q)$.

Define the subalgebra $Z(V,q) = \operatorname{span}\{1, z(V,q)\} \subseteq C(V,q)$.

We sometimes write $z(q)$ or $z(V)$ for the element $z(V,q)$. If $e_i^2 = a_i \in F^\bullet$ then $z(q)^2 = (e_1 \ldots e_n)\cdot(e_1 \ldots e_n) = (-1)^{n(n-1)/2} a_1 \ldots a_n$. Abusing notation slightly we have

$$z(q)^2 = dq \quad \text{and} \quad Z(q) \cong F(\sqrt{dq}).$$

Then if $dq \not\simeq \langle 1\rangle$ the subalgebra $Z(q) \cong F(\sqrt{dq})$ is a field. If $dq \simeq \langle 1\rangle$ then $Z(q) \cong F \times F$. From the next proposition it follows that $Z(q)$ is independent of the choice of basis. Furthermore, the element $z(q)$ is unique up to a non-zero scalar multiple.

3.11 Proposition. *Suppose q is a regular form on V and $\dim q = n$.*

(1) *$Z(V, q)$ is the centralizer of $C_0(V, q)$ in $C(V, q)$.*

(2) *The center of $C(V, q)$ is* $\begin{cases} F & \text{if } n \text{ is even,} \\ Z(V, q) & \text{if } n \text{ is odd.} \end{cases}$

(3) *The center of $C_0(V, q)$ is* $\begin{cases} Z(V, q) & \text{if } n \text{ is even,} \\ F & \text{if } n \text{ is odd.} \end{cases}$

Proof. (1) Suppose c is an element of that centralizer. Let $\{e_1, e_2, \ldots, e_n\}$ be the orthogonal basis used in (3.10) and express $c = \sum c_\Delta e^\Delta$ for coefficients $c_\Delta \in F$. Since c commutes with every $e_i e_j$ and $(e_i e_j)^{-1} e^\Delta (e_i e_j) = \pm e^\Delta$ it follows that if $c_\Delta \neq 0$ then e^Δ commutes with every $e_i e_j$. If $\Delta = (\delta_1, \ldots, \delta_n)$ and $\delta_r \neq \delta_s$ for some r, s then $e_r e_s$ anticommutes with e^Δ. Therefore either $\Delta = (0, \ldots, 0)$ and $e^\Delta = 1$ or $\Delta = (1, \ldots, 1)$ and $e^\Delta = z(q)$. Hence c is a combination of 1 and $z(q)$ so that $c \in Z(q)$.

(2) If c is in the center then $c \in Z(q)$ by part (1). If n is even every e_i commutes with $z(q)$ and the center is $Z(q)$. If n is odd every e_i anticommutes with $z(q)$ and the center is F.

(3) $z(q)$ is in $C_0(q)$ if and only if n is even. □

3.12 Lemma. *If n is odd and q is regular then $C(V, q) \cong C_0(V, q) \otimes Z(V, q)$.*

Proof. Since $C_0(q)$ and $Z(q)$ are subalgebras of $C(q)$ which centralize each other there is an induced algebra homomorphism $\psi : C_0(q) \otimes Z(q) \to C(q)$. Since n is odd these two subalgebras generate $C(q)$ so that ψ is surjective. Counting dimensions we see that ψ is an isomorphism. □

3.13 Structure Theorem. *Let $C = C(V, q)$ be the Clifford algebra of a regular quadratic space over the field F. Let $C_0 = C_0(V, q)$ and $Z = Z(V, q)$.*

(1) *If* $\dim V$ *is even then C is a central simple algebra over F, and C_0 has center Z.*

(2) *If* $\dim V$ *is odd then C_0 is a central simple algebra over F and $C \cong C_0 \otimes Z$.*

If $dq \not\simeq \langle 1 \rangle$ then C is a central simple algebra over Z. If $dq = \langle 1 \rangle$ then $C \cong C_0 \times C_0$.

Proof. Suppose $n = \dim V$ so that $\dim C = 2^n$. The centers of these algebras are given in (3.11).

(1) Suppose n is even and $\mathfrak{I}$ is a proper ideal of C so that $\bar{C} = C/\mathfrak{I}$ is an F-algebra with $\dim \bar{C} = 2^n - \dim \mathfrak{I}$. If $\{e_1, \ldots, e_n\}$ is an orthogonal basis of (V, q), the images $\bar{e}_1, \ldots, \bar{e}_n$ are anticommuting invertible elements of $\bar{C}$. Since n is even (1.11) implies that $\dim \bar{C} \geq 2^n$ and therefore $\mathfrak{I} = 0$. Hence C is simple.

(2) Apply (3.9), part (1) and (3.12). The final assertions follow since Z is a field if $\mathrm{d}q \not\simeq \langle 1 \rangle$ and $Z \cong F \times F$ if $dq \simeq \langle 1 \rangle$. □

If q is a regular quadratic form of even dimension then $C(q)$ is a central simple algebra. In fact it is isomorphic to a tensor product of quaternion algebras. Before beginning the analysis of the Witt invariant we describe an explicit decomposition of $C(q)$ which will be useful later on. This decomposition provides another proof that $C(q)$ is central simple, since the class of central simple F-algebras is closed under tensor products.

3.14 Proposition. *If $q \simeq \langle a_1, \ldots, a_{2m}\rangle$ define $u_k = e_1 e_2 \ldots e_{2k-1}$ and $v_k = e_{2k-1}e_{2k}$ for $k = 1, 2, \ldots, m$. The subalgebra Q_k generated by u_k and v_k is a quaternion algebra and $C(q) \cong Q_1 \otimes \cdots \otimes Q_m$.*

Proof. Check that u_k anticommutes with v_k but commutes with every u_i and with every v_j for $j \neq k$. Since $u_k^2 = (-1)^{k-1} a_1 a_2 \ldots a_{2k-1}$ and $v_k^2 = -a_{2k-1}a_{2k}$ are scalars, each Q_k is a quaternion subalgebra. The induced map $Q_1 \otimes \cdots \otimes Q_m \to C(q)$ is injective since the domain is simple. By counting dimensions we see it is an isomorphism. □

If A is an F-algebra, the "opposite algebra" A^{op} is the algebra defined as the vector space A with the multiplication $*$ given by: $a * b = ba$. An algebra isomorphism $\varphi : A \to A^{\mathrm{op}}$ can be interpreted as an anti-automorphism $\varphi : A \to A$. That is, φ is a vector space isomorphism and $\varphi(ab) = \varphi(b)\varphi(a)$ for every $a, b \in A$. If (V, q) is a quadratic space and $g \in \mathrm{O}(V, q)$ then the map $\iota \circ g : V \to C(V, q)^{\mathrm{op}}$ is compatible with q. The universal property provides a homomorphism $\hat{\varphi} : C(V, q) \to C(V, q)^{\mathrm{op}}$. This map is surjective and therefore it is an isomorphism. As above we may interpret this map as an anti-automorphism

$$C'(g) : C(V, q) \to C(V, q).$$

This is the unique anti-automorphism of $C(V, q)$ which extends $g : V \to V$.

The involutions of $C(V, q)$ will be particularly important for our work. By definition, an *involution* of an F-algebra is an F-linear anti-automorphism whose square is the identity. (These are sometimes called "involutions of the first kind".) For example, the transpose map on the matrix algebra $\mathbb{M}_n(F)$ and the usual "bar" on a quaternion algebra are involutions. If $g \in \mathrm{O}(V, q)$ satisfies $g^2 = 1_V$ then $C'(g)$ is an involution on $C(V, q)$.

3.15 Definition. If $V = R \perp T$, define $J_{R,T}$ to be the involution on $C(V, q)$ which is -1_R on R and 1_T on T. The *canonical involution* (denoted J_0 or $^\top$) is $J_{0,V}$ and the *bar involution* (denoted J_1 or $^-$) is $J_{V,0}$.

This $J_{R,T}$ is the anti-automorphism of $C = C(V, q)$ extending the reflection $(-1_R) \perp (1_T)$ on $V = R \perp T$. These involutions will be important when we analyze (s, t)- families using Clifford algebras.

The canonical involution acts as the identity on V. If $v_1, v_2, \ldots, v_m \in V$ then $(v_1 v_2 \ldots v_m)^\top = v_m \ldots v_2 v_1$, reversing the order of the product. A simple sign calculation shows that $(e^\Delta)^\top = (-1)^{k(k-1)/2} e^\Delta$ where $k = |\Delta|$. The bar involution is the composition of α and $^\top$, and similar remarks hold. For the quaternion algebras, the bar involution is the usual "bar".

For the discussion of the Witt invariant below we assume some familiarity with the theory of central simple algebras. If A is a central simple algebra over F, then Wedderburn's theory implies that A is a matrix ring over a division algebra. That is, $A \cong \mathbb{M}_k(D)$ where D is a central division algebra over F, which is uniquely determined (up to isomorphism) by A. Two central simple algebras A, B are equivalent ($A \sim B$) if their corresponding division algebras are isomorphic. That is, $A \sim B$ if and only if $\mathbb{M}_m(A) \cong \mathbb{M}_n(B)$ for some m, n. Let $[A]$ denote the equivalence class of a central simple algebra A. Each such class contains a unique division algebra. The Brauer group $\mathrm{Br}(F)$ is the set of these equivalence classes, with a multiplication induced by $\otimes$.

The inverse of $[A]$ in $\mathrm{Br}(F)$ is $[A^{\mathrm{op}}]$, the class of the opposite algebra. (For there is a natural isomorphism $A \otimes A^{\mathrm{op}} \cong \mathrm{End}_F(A)$.) Since quaternion algebras possess involutions, $[A]^2 = 1$ whenever A is a tensor product of quaternion algebras. Let $\mathrm{Br}_2(F)$ be the subgroup of $\mathrm{Br}(F)$ consisting of all $[A]$ with $[A]^2 = 1$.

3.16 Definition. Let (V, q) be a (regular) quadratic space over F. The *Witt invariant* $c(q)$ is the element of $\mathrm{Br}_2(F)$ defined as:

$$c(q) = \begin{cases} [C(V,q)] & \text{if } \dim V \text{ is even,} \\ [C_0(V,q)] & \text{if } \dim V \text{ is odd.} \end{cases}$$

By the Structure Theorem the indicated algebras are central simple, so $c(q)$ is well-defined. To derive the basic properties of $c(q)$ we must recall some of the properties of quaternion algebras. The class of the quaternion algebra is written $[a, b]$.

3.17 Lemma. (1) $[a, b] = [a', b']$ *if and only if* $\langle\langle -a, -b\rangle\rangle \simeq \langle\langle -a', -b'\rangle\rangle$. *In particular,* $[a, b] = 1$ *if and only if* $\langle\langle -a, -b\rangle\rangle$ *is hyperbolic if and only if* $\langle a, b\rangle$ *represents* 1.

(2) $[a, b] = [b, a]$, $[a, a] = [-1, a]$, $[a, b]^2 = 1$ *and* $[a, b] \cdot [a, c] = [a, bc]$.

Proof. (1) This is a standard result about quaternion algebras: the isomorphism class of the algebra $\left(\frac{a,b}{F}\right)$ is determined by the isometry class of its norm form $\langle\langle -a, -b\rangle\rangle$. In particular the symbol $[a, b]$ depends only on the square classes $\langle a\rangle$ and $\langle b\rangle$.

(2) The first and second statements follow from (1), and the third one is clear. The last statement is equivalent to the isomorphism:

$$\left(\frac{a, b}{F}\right) \otimes \left(\frac{a, c}{F}\right) \cong \left(\frac{a, bc}{F}\right) \otimes \mathbb{M}_2(F).$$

To prove this let i, j be the generators of the algebra $B = \left(\frac{a,b}{F}\right)$ so that $i^2 = a$ and $j^2 = b$. Similarly let i', j' be the generators of the algebra $C = \left(\frac{a,c}{F}\right)$ so that $i'^2 = a$ and $j'^2 = c$. Then the subalgebra of $B \otimes C$ generated by $i \otimes 1$ and $j \otimes j'$ is isomorphic to $\left(\frac{a,bc}{F}\right)$ and the subalgebra generated by $i \otimes i'$ and $1 \otimes j'$ is isomorphic to $\left(\frac{a^2,c}{F}\right) \cong \mathbb{M}_2(F)$. Since those subalgebras centralize each other and together span the algebra $B \otimes C$ the claim follows. □

The same sorts of arguments are used to prove the various isomorphisms of Clifford algebras stated below.

3.18 Lemma. (1) *If* $\dim \alpha$ *and* $\dim \beta$ *are even then* $c(\alpha \perp \beta) = c(\alpha) \cdot c((d\alpha) \cdot \beta)$.
(2) *If* $\dim \alpha$ *is odd and* $\dim \beta$ *is even then* $c(\alpha \perp \beta) = c(\alpha) \cdot c((-d\alpha) \cdot \beta)$.

Proof. (1) We must prove that $C(\alpha \perp \beta) \cong C(\alpha) \otimes C((d\alpha) \cdot \beta)$. In fact this holds whenever $\dim \alpha$ is even. Let $v_1, \ldots, v_r, w_1, \ldots, w_s$ be an orthogonal basis corresponding to $\alpha \perp \beta$. The subalgebra of $C(\alpha \perp \beta)$ generated by $\{v_1, \ldots, v_r\}$ is isomorphic to $C(\alpha)$. Since r is even the element $u = z(\alpha) = v_1 \ldots v_r$ anticommutes with each v_i, commutes with each w_j and $\langle u^2 \rangle = d\alpha$. Then the subalgebra generated by $\{uw_1, \ldots, uw_s\}$ is isomorphic to $C((d\alpha)\beta)$ and centralizes $C(\alpha)$. Since these subalgebras together generate the whole algebra $C(\alpha \perp \beta)$ the isomorphism follows.

(2) We must show that $C_0(\alpha \perp \beta) \cong C_0(\alpha) \otimes C((d\alpha) \cdot \beta)$. In fact this holds whenever $\dim \alpha$ is odd. Either use an argument similar to (1) above or apply (1) and Lemma 3.9. We omit the details. □

By applying (3.18) (1) successively to $q \simeq \langle a_1, \ldots, a_{2m} \rangle$ we find that $C(q)$ is isomorphic to a tensor product of quaternion subalgebras. These are the same subalgebras found in (3.14) above.

3.19 Proposition. *Let* α, β *be (regular) quadratic forms over* F *and let* $x, y, z \in F^\bullet$.

(1) $c(\alpha \perp \beta) = \begin{cases} c(\alpha) \cdot c(\beta) \cdot [d\alpha, d\beta] & \text{if } \dim \alpha \text{ and } \dim \beta \text{ are both even} \\ & \text{or both odd,} \\ c(\alpha) \cdot c(\beta) \cdot [-d\alpha, d\beta] & \text{if } \dim \alpha \text{ is odd and } \dim \beta \text{ is even.} \end{cases}$

(2) $c(\langle x \rangle \alpha) = \begin{cases} c(\alpha)[x, d\alpha] & \text{if } \dim \alpha \text{ is even,} \\ c(\alpha) & \text{if } \dim \alpha \text{ is odd.} \end{cases}$

(3) $c(\alpha \perp \mathbb{H}) = c(\alpha)$ *where* $\mathbb{H} = \langle 1, -1 \rangle$ *is the hyperbolic plane.*

(4) $c(\langle\langle x \rangle\rangle \otimes \alpha) = [-x, d\alpha]$. *Hence* $c(\langle\langle x, y \rangle\rangle) = [-x, -y]$ *and* $c(\langle\langle x, y, z \rangle\rangle) = 1$.

Proof. (3) follows immediately from (3.18) when $\beta = \mathbb{H}$. To prove (2) first note that $C_0(\langle x \rangle q) \cong C_0(q)$ for any form q. This settles the case $\dim \alpha$ is odd. For the even case of (2) we apply (3.18) in two ways: $c(\alpha \perp \langle -1, x \rangle) = c(\alpha) \cdot c((d\alpha) \cdot \langle -1, x \rangle) =$

$c(\langle -1, x\rangle) \cdot c(\langle x\rangle \cdot \alpha)$. Therefore $c(\langle x\rangle \cdot \alpha) = c(\alpha)[-d\alpha, (d\alpha)\cdot x] \cdot [-1, x] = c(\alpha)\cdot[d\alpha, x]$, using the properties in (3.17).

(1) If $\dim\alpha$ and $\dim\beta$ are even then $c(\alpha \perp \beta) = c(\alpha)\cdot c((d\alpha)\cdot\beta) = c(\alpha)\cdot c(\beta)\cdot [d\alpha, d\beta]$ by (3.18) and part (2). A similar argument works when $\dim\alpha$ is odd and $\dim\beta$ is even. Suppose $\dim\alpha$ and $\dim\beta$ are odd. One way to proceed is to express $\alpha = \langle a\rangle \perp \alpha'$ and $\beta = \langle b\rangle \perp \beta'$ so that $c(\alpha \perp \beta) = c(\langle a, b\rangle \perp \alpha' \perp \beta')$ and $c(\alpha) = c(\langle -a\rangle\alpha')$, $c(\beta) = c(\langle -b\rangle\beta')$ by (3.9). The desired equality follows after expanding both sides using the properties for forms of even dimension. Alternatively we can prove the isomorphism $C(\alpha \perp \beta) \cong C_0(\alpha) \otimes C_0(\beta) \otimes \left(\frac{d\alpha, d\beta}{F}\right)$ by directly examining basis elements. Further details are left to the reader.

The formula for $c(\langle\langle x\rangle\rangle \otimes \alpha) = c(\alpha \perp \langle x\rangle\alpha)$ in (4) follows from (1) and (2). □

Recall that if a (regular) quadratic form q is isotropic, then $q \simeq \mathbb{H} \perp \alpha$ for some form α. A form φ is *hyperbolic* if $\varphi \simeq m\mathbb{H} \simeq \mathbb{H} \perp \mathbb{H} \perp \cdots \perp \mathbb{H}$. Then every form q can be expressed as $q \simeq q_0 \perp H$ where q_0 is anisotropic and H is hyperbolic. (This is the "Witt decomposition" of q.) Witt's Cancellation Theorem implies that this form q_0 is uniquely determined by q (up to isometry). Two forms α and β are *Witt equivalent* (written $\alpha \sim \beta$) if $\alpha \perp -\beta$ is hyperbolic. If $\dim\alpha > \dim\beta$ and $\alpha \sim \beta$ then $\alpha \simeq \beta \perp H$ for some hyperbolic space H. Consequently every Witt class contains a unique anisotropic form. These classes form the elements of the Witt ring $W(F)$, where the addition is induced by $\perp$ and the multiplication by $\otimes$.

We often abuse the notations, using symbols like q, φ, α to stand for regular quadratic forms, and writing $q \in W(F)$ rather than stating that the Witt class of q lies in $W(F)$.

Define IF to be the ideal in the Witt ring $W(F)$ consisting of all quadratic forms of even dimension. (This is well-defined since $\dim\mathbb{H}$ is even.) Then IF is additively generated by all the forms $\langle\langle a\rangle\rangle = \langle 1, a\rangle$ for $a \in F^\bullet$. The square I^2F is additively generated by the 2-fold Pfister forms $\langle\langle a, b\rangle\rangle$, and similarly for higher powers.

The determinant $\det\alpha \in F^\bullet/F^{\bullet 2}$ does not generally induce a map on $W(F)$. The "correct" invariant is the signed discriminant $d\alpha = (-1)^{n(n-1)/2}\det\alpha$, because $d(\alpha \perp \mathbb{H}) = d\alpha$. This discriminant induces a map $d : W(F) \to F^\bullet/F^{\bullet 2}$. The ideal I^2F is characterized by this discriminant: $\alpha \in I^2F$ if and only if $\dim\alpha$ is even and $d\alpha = \langle 1\rangle$.

The Witt invariant $c(q)$ induces a map $c : W(F) \to \mathrm{Br}(F)$. The formulas in (3.19) imply that the restriction $c : I^2F \to \mathrm{Br}(F)$ is a homomorphism. One natural question is: Which quadratic forms q have all three invariants trivial? That is:

$$\dim q = \text{even}, \quad dq = \langle 1\rangle, \quad c(q) = 1.$$

It is easy to check that any 3-fold Pfister form $\langle\langle a, b, c\rangle\rangle$ has trivial invariants. Consequently so does everything in the ideal I^3F. For convenience we let $J_3(F)$ be the ideal of elements in $W(F)$ which have trivial invariants. That is:

$$J_3(F) = \ker(c : I^2F \to \mathrm{Br}(F)).$$

Does $J_3(F) = I^3F$ for every field F? This was a major open question until Merkurjev proved it true in 1981 using techniques from K-theory (which are well beyond the scope of this book). Before 1981 the only result in this direction valid over arbitrary fields was the one of Pfister (1966): if $q \in J_3(F)$ and $\dim q \leq 12$ then $q \in I^3F$. An important tool used in the proof is the following easy lemma about the behavior of forms under quadratic extensions.

3.20 Lemma. *Let q be an anisotropic quadratic form over F.*

(1) *$q \otimes F(\sqrt{d})$ is isotropic iff $q \simeq \langle x\rangle\langle 1, -d\rangle \perp \alpha$ for some $x \in F^\bullet$ and some form α over F.*

(2) *$q \otimes F(\sqrt{d})$ is hyperbolic iff $q \simeq \langle\langle -d\rangle\rangle \otimes \beta$ for some form β over F.*

Proof. Exercise 8. □

With this lemma, and some clever arguments with quaternion algebras, Pfister (1966) characterized the small forms in I^3F up to isometry.

3.21 Pfister's Theorem. *Let φ be a regular quadratic form over F with $\dim\varphi$ even, $d\varphi = \langle 1\rangle$ and $c(\varphi) = 1$.*

(1) *If $\dim\varphi < 8$ then $\varphi \sim 0$.*

(2) *If $\dim\varphi = 8$ then $\varphi \simeq \langle a\rangle\langle\langle x, y, z\rangle\rangle$ for some $a, x, y, z \in F^\bullet$.*

(3) *If $\dim\varphi = 10$ then φ is isotropic.*

(4) *If $\dim\varphi = 12$ then $\varphi \simeq \langle\langle x\rangle\rangle \otimes \delta$ for some $x \in F^\bullet$ and some quadratic form δ where $\dim\delta = 6$ and $d\delta = \langle 1\rangle$. Furthermore if $\langle a\rangle\langle\langle -b\rangle\rangle \subset \varphi$ then $\varphi \simeq \varphi_1 \perp \varphi_2 \perp \varphi_3$ where $\dim\varphi_i = 4$, $d\varphi_i = \langle 1\rangle$ and $\langle a\rangle\langle\langle -b\rangle\rangle \subset \varphi_1$.*

The proof is given in Exercises 9 and 10.

The three basic invariants described above induce group homomorphisms

$$\overline{\dim} : W(F)/IF \to \mathbb{Z}/2\mathbb{Z}, \quad \bar{d} : IF/I^2F \to F^\bullet/F^{\bullet 2}, \quad \bar{c} : I^2F/I^3F \to \mathrm{Br}_2(F).$$

The first two maps above are easily seen to be isomorphisms. Milnor (1970) conjectured that these maps are the first three of a sequence of well defined isomorphisms $e_n : I^nF/I^{n+1}F \to H^n(F)$, where H^n is a suitable Galois cohomology group. Many mathematicians have worked on various aspects of these conjectures. Merkurjev (1981) proved that $e_2 = \bar{c}$ is always an isomorphism. Recently Voevodsky proved that Milnor's conjecture is always true. For an outline of these ideas and further references see Morel (1998).

Exercises for Chapter 3

1. **Universal property.** (1) If $f : (V, q) \to (V', q')$ is an isometry then there is a unique algebra homomorphism $\psi : C(V, q) \to C(V', q')$ such that $\psi \circ \iota = \iota' \circ f$. If f is bijective then ψ is an isomorphism. The uniqueness of the Clifford algebra follows.

(2) $1 \otimes \iota : K \otimes V \to K \otimes C(V, q)$ is compatible with $K \otimes q$ and satisfies the universal property. This proves (3.3) (2).

(3) $C(V, q)$ is generated as an F-algebra by $\iota(V)$. This proves (3.4) (1):

(Hint. (3) Apply the proof of (3.2). Or directly from the definitions: Let A be the subalgebra generated by $\iota(V)$ so that ι induces a map $\iota' : V \to A$ which is compatible with q. Apply the definition of $C(q)$ to get an induced algebra homomorphism $\psi : C(q) \to C(q)$ with $\psi \circ \iota = \iota$. The uniqueness implies $\psi = 1_C$.)

2. **Homogeneous components.** (1) Let $\{e_1, e_2, \ldots, e_n\}$ be an orthogonal basis of (V, q), and define the subspace $V_{(k)} = \operatorname{span}\{e^\Delta : |\Delta| = k\}$. Then $\dim V_{(k)} = \binom{n}{k}$. For instance, $V_{(0)} = F$ and $V_{(1)} = V$. Each $V_{(k)}$ is independent of the choice of orthogonal basis.

(2) Since $V_{(n)} = F \cdot z(q)$, the element $z(q)$ in Definition 3.10 is uniquely determined up to a non-zero scalar multiple. For any subspace $U \subseteq V$, the line spanned by $z(U)$ is uniquely determined.

(Hint. (1) Use the Chain-Equivalence Theorem stated in Exercise 2.8.)

3. Prove (3.19) (1), (2) by exhibiting explicit algebra isomorphisms, similar to the proof of (3.18). For instance if $\dim \alpha$ and $\dim \beta$ are odd,

$$C(\alpha \perp \beta \perp \mathbb{H}) \cong C(\alpha) \otimes C(\beta) \otimes \left(\frac{d\alpha, d\beta}{F}\right).$$

4. **Discriminants.** Suppose $\dim \alpha = m$ and $\dim \beta = n$.

(1) $d(\alpha \perp \beta) = (-1)^{mn} d\alpha \cdot d\beta$. In particular $d(\alpha \perp \mathbb{H}) = d\alpha$.

(2) $d(\langle c \rangle \alpha) = \langle c \rangle^m \cdot d\alpha$.

(3) $d(\alpha \otimes \beta) = (d\alpha)^n \cdot (d\beta)^m$.

(4) If $q \simeq p\langle 1 \rangle \perp r\langle -1 \rangle$ define the signature $\operatorname{sgn}(q) = p - r$. Then

$$dq = \begin{cases} \langle 1 \rangle & \text{if } \operatorname{sgn}(q) \equiv 0, 1 \\ \langle -1 \rangle & \text{if } \operatorname{sgn}(q) \equiv 2, 3 \end{cases} \pmod 4.$$

5. **Witt invariant calculations.** (1) $c(\langle a, b \rangle) = [a, b]$, and $c(\langle a, b, c \rangle) = [-ab, -ac]$.

(2) If $d\alpha = d\beta$, $c(\alpha) = c(\beta)$ and $\dim \alpha = \dim \beta \leq 3$ then $\alpha \simeq \beta$.

(3) Let $\beta = \langle 1 \rangle \perp \beta_1$. Then $d(\beta) = d(-\beta_1)$ and $c(\beta) = c(-\beta_1)$.

(4) $c(\alpha \otimes \beta) = \begin{cases} [d\alpha, d\beta] & \text{if } \dim\alpha \text{ and } \dim\beta \text{ are even,} \\ c(\alpha)c(\beta) & \text{if } \dim\alpha \text{ and } \dim\beta \text{ are odd,} \\ c(\beta)[d\alpha, d\beta] & \text{if } \dim\alpha \text{ is odd and } \dim\beta \text{ is even.} \end{cases}$

(5) If $q \simeq p\langle 1\rangle \perp r\langle -1\rangle$ define the signature $\operatorname{sgn}(q) = p - r$. Then

$$c(q) = \begin{cases} 1 & \text{if } \operatorname{sgn}(q) \equiv -1, 0, 1, 2 \\ [-1, -1] & \text{if } \operatorname{sgn}(q) \equiv 3, 4, 5, 6 \end{cases} \pmod 8.$$

6. **Hasse invariant.** If $q \simeq \langle a_1, \ldots, a_n\rangle$ define the Hasse invariant

$$h(q) = \prod_{i \le j} [a_i, a_j].$$

(1) If $\dim q = n$ then $h(q) = c(q \perp n\langle -1\rangle)$. Consequently $h(q)$ depends only on the isometry class of q.

(2) This independence of $h(q)$ can be proved without Clifford algebras. Use the Chain-Equivalence Theorem stated in Exercise 2.8.

(3) $h(\alpha \perp \beta) = h(\alpha) \cdot h(\beta) \cdot [\det\alpha, \det\beta]$.

(4) Another version of the Hasse invariant is given by $s(q) = \prod_{i<j}[a_i, a_j]$. How are $h(q)$ and $s(q)$ related?

(Hint. (1) Apply (3.14) to $q \perp n\langle -1\rangle \simeq \langle a_1, -1, a_2, -1, \ldots, a_n, -1\rangle$.)

7. (1) Prove from the definition of I^2F that:
If $\dim q$ is even then $q \equiv \langle 1, -dq\rangle \pmod{I^2F}$.
If $\dim q$ is odd then $q \equiv \langle dq\rangle \pmod{I^2F}$.
(2) $q \in I^2F$ if and only if $\dim q$ is even and $dq = \langle 1\rangle$.
(3) If $\dim q$ is even and $\langle a\rangle q \simeq q$ then $a \in D_F(\langle\langle -dq\rangle\rangle)$.
(4) If α is a form of even dimension then $\langle\langle d\alpha\rangle\rangle \otimes \alpha \in I^3F$.
(5) Suppose $q \equiv \langle\langle x\rangle\rangle \otimes \alpha \pmod{I^3F}$, where $dq = \langle 1\rangle$ and $c(q) = 1$. Then $q \in I^3F$.

(Hint. (3) Use Witt invariants. Compare Exercise 2.9(3).)

8. **Quadratic extensions.** (1) Prove Lemma 3.20.

(2) If A is a central simple F-algebra and $K = F(\sqrt{d})$, then:

$$A \otimes K \sim 1 \iff A \sim \left(\frac{d, x}{F}\right) \quad \text{for some } x \in F^\bullet.$$

(3) $c(q) =$ quaternion $\iff c(q_K) = 1$ in $\operatorname{Br}(K)$ for some quadratic extension K/F.

(Hint. (1) If $q(v) = 0$ for $v \in V \otimes K$, express $v = v_0 + v_1\sqrt{d}$ and conclude: $q(v_0) + dq(v_1) = 0$ and $B_q(v_0, v_1) = 0$. The second statement follows by repeated application of the first.

(2) The theory of division algebras implies: If D is a central F-division algebra of degree n and K is a splitting field, then $[K : F] \geq n$. A central simple algebras of degree 2 must be quaternion.)

9. **Trivial invariants.** Suppose φ is a quadratic form over F.

(1) If $\dim \varphi = 2, 4$ or 6, $d\varphi = \langle 1 \rangle$ and $c(\varphi) = 1$, then $\varphi \sim 0$.

(2) Suppose $\dim \varphi = 6$, $d\varphi = \langle 1 \rangle$ and $c(\varphi) =$ quaternion, then φ is isotropic.

(3) Prove the cases where $\dim \varphi \leq 10$ in (3.21).

(Hint. (1) If $\dim \varphi = 6$, express $\varphi \simeq \langle a \rangle \langle 1, -b \rangle \perp \psi$. If $K = F(\sqrt{b})$ then $\varphi_K \sim 0$ because ψ_K has trivial invariants over K. If φ is anisotropic, (3.20) implies $\varphi \simeq \langle\langle -b \rangle\rangle \otimes \beta$. Discriminants show that $\langle b \rangle = \langle 1 \rangle$ so that $\varphi \sim 0$.

(2) $c(\varphi)$ is split over some $K = F(\sqrt{b})$. Finish as in part (1).

(3) Let $\dim \varphi = 8$, anisotropic with trivial invariants. Express $\varphi \simeq \langle a \rangle \langle\langle -b \rangle\rangle \perp \psi$, so that $d\psi = \langle b \rangle$ and $c(\psi) = [-a, b]$. Part (1) over $F(\sqrt{b})$ and (3.20) imply that $\psi \simeq \langle\langle -b \rangle\rangle \otimes \langle u, v, w \rangle$. Witt invariants show that $[b, auvw] = 1$ and $\langle\langle -b \rangle\rangle$ represents $auvw$. Therefore $\psi \simeq \langle\langle -b \rangle\rangle \otimes \langle u, v, auv \rangle$ and $\varphi \simeq \langle a \rangle \langle\langle -b, au, av \rangle\rangle$.

Let $\dim \varphi = 10$, anisotropic with trivial invariants. Express $\varphi \simeq \langle w \rangle \langle 1, a, b, c \rangle \perp \psi$. Then $\dim \psi = 6$, $d\psi = \langle abc \rangle$. Let $K = F(\sqrt{abc})$ so that $c(\psi_K) =$ quaternion. Part (2) implies ψ_K is isotropic, so that $\psi \simeq \langle u \rangle \langle\langle -abc \rangle\rangle \perp \delta$ where $\dim \delta = 4$ and $d\delta = \langle 1 \rangle$. Then $\varphi \cong \omega \perp \delta$ where $\omega = \langle w \rangle \langle 1, a, b, c \rangle \perp \langle u \rangle \langle\langle -abc \rangle\rangle$. Since $d\omega = \langle 1 \rangle$ and $c(\omega) = c(-\delta)$ is quaternion, (2) leads to a contradiction.)

10. **Linked Pfister forms.** If a Pfister form $\varphi \simeq \langle 1 \rangle \perp \varphi'$ then φ' is called the *pure part* of φ. For instance, if $\varphi = \langle\langle a, b \rangle\rangle$ then $\varphi' = \langle a, b, ab \rangle$. In this case, if φ' represents d then we may use d as one of the "slots": $\varphi \simeq \langle\langle d, x \rangle\rangle$ for some x. The 2-fold Pfister forms φ and ψ are *linked* if there is a common slot: $\varphi \simeq \langle\langle a, x \rangle\rangle$ and $\psi \simeq \langle\langle a, y \rangle\rangle$ for some $a, x, y \in F^\bullet$. This occurs if and only if φ' and ψ' represent a common value, if and only if $\varphi' \perp -\psi'$ is isotropic.

(1) φ and ψ are linked $\Longleftrightarrow c(\varphi)c(\psi) =$ quaternion.

(2) Suppose ψ_1, ψ_2, ψ_3 are 2-fold Pfister forms and $c(\psi_1)c(\psi_2)c(\psi_3) = 1$. Then $\psi_1 \simeq \langle\langle a, x \rangle\rangle$, $\psi_2 \simeq \langle\langle a, y \rangle\rangle$ and $\psi_3 \simeq \langle\langle a, -xy \rangle\rangle$ for some $a, x, y \in F^\bullet$.

(3) Suppose β is anisotropic, $\dim \beta = 8$, $d\beta = \langle 1 \rangle$ and $c(\beta) =$ quaternion. Then $\beta \simeq \langle\langle a \rangle\rangle \otimes \gamma$ for some $a \in F^\bullet$ and some form γ.

(4) Complete the proof of (3.21).

(5) Let Q_1 and Q_2 be quaternion algebras with norm forms φ_1 and φ_2. Let $\alpha = \varphi_1' \perp -\varphi_2'$. Then $Q_1 \otimes Q_2$ is a division algebra if and only if α is anisotropic.

(Hint. (1) $q = \varphi' \perp -\psi'$ has $\dim q = 6$, $dq = \langle 1 \rangle$ and $c(q) = c(\varphi)c(\psi)$. Apply Exercise 9(2).

(2) $c(\psi_1)c(\psi_2) = c(\psi_3)$ and (1) imply $\psi_1 \simeq \langle\langle a, x \rangle\rangle$, $\psi_2 \simeq \langle\langle a, y \rangle\rangle$ for some a, x, y. Witt invariants then imply $\psi_3 \simeq \langle\langle a, -xy \rangle\rangle$.

(3) Let $\beta = \langle x \rangle \langle\langle -b \rangle\rangle \perp \delta$. Exercise 9(2) over $K = F(\sqrt{b})$ and (3.20) imply $\langle y \rangle \langle\langle -b \rangle\rangle \subset \delta$ for some y. Then $\beta \simeq \varphi_1 \perp \varphi_2$ where $\dim \varphi_i = 4$ and $d\varphi_i = \langle 1 \rangle$.

(Here $\varphi_1 \simeq \langle\langle -b\rangle\rangle \otimes \langle x, y\rangle$.) Express $\varphi_i \simeq \langle x_i\rangle\psi_i$ for some x_i and some 2-fold Pfister forms ψ_i. Apply part (1).

(4) Suppose $\dim\varphi = 12$, and φ is anisotropic with trivial invariants. Express $\varphi = \langle a\rangle\langle\langle -b\rangle\rangle \perp \alpha$. By (3.21) (3), α is isotropic over $K = F(\sqrt{b})$. Then $\varphi \simeq \varphi_1 \perp \beta$ where $\varphi_1 = \langle\langle -b\rangle\rangle \otimes \langle a, u\rangle$, $\dim\beta = 8$, $d\beta = \langle 1\rangle$ and $c(\beta) = [b, -au]$. Part (3) implies $\beta = \varphi_2 \perp \varphi_3$ where $\dim\varphi_i = 4$ and $d\varphi_i = \langle 1\rangle$. Express $\varphi_i = \langle x_i\rangle\psi_i$ and apply part (2).)

11. **Graded algebras.** Let A be an associative F-algebra with 1. Then A is graded (or more precisely, "$\mathbb{Z}/2\mathbb{Z}$-graded") if $A = A_0 \oplus A_1$, a direct sum as F-vector spaces, such that $A_i \cdot A_j \subseteq A_{i+j}$, where the subscripts are taken mod 2. It follows that $1 \in A_0$ and A_0 is a subalgebra of A. Every Clifford algebra $C(q)$ is a graded algebra using $C(q) = C_0(q) \oplus C_1(q)$. An element of A is *homogeneous* if it lies in $A_0 \cup A_1$. If a is homogeneous define the *degree* $\partial(a) = i$ if $a \in A_i$. The graded F-algebras A and B are *graded-isomorphic*, if there exists $f : A \to B$ which is an F-algebra isomorphism satisfying $f(A_i) = B_i$ for $i = 0, 1$.

Define the *graded tensor product* $A\hat{\otimes}B$ by taking the vector space $A \otimes B$ with the new multiplication induced by: $(a \otimes b) \cdot (a' \otimes b') = (-1)^{\partial(a)\partial(b)}aa' \otimes bb'$. Then $A \hat{\otimes} B$ is a graded algebra with $(A \hat{\otimes} B)_0 = A_0 \otimes B_0 + A_1 \otimes B_1$ and $(A \hat{\otimes} B)_1 = A_1 \otimes B_0 + A_0 \otimes B_1$. Then $A \hat{\otimes} 1$ and $1 \hat{\otimes} B$ are graded subalgebras of $A \hat{\otimes} B$. In the category of graded F-algebras the graded tensor product is commutative and associative, and it distributes through direct sums.

(1) **Lemma.** *If α, β are quadratic forms then $C(\alpha \perp \beta) \cong C(\alpha)\hat{\otimes}C(\beta)$ as graded algebras.*

(2) **Lemma.** *The Clifford algebras $C(\alpha)$ and $C(\beta)$ are graded-isomorphic if and only if*

$$\dim\alpha = \dim\beta, \quad d\alpha = d\beta \quad \textit{and} \quad c(\alpha) = c(\beta).$$

(3) Let A be a graded F-algebra. An A-module V is a *graded A-module* if V has a decomposition $V = V_0 \oplus V_1$ such that $A_i \cdot V_j \subseteq V_{i+j}$ whenever $i, j \in \mathbb{Z}/2\mathbb{Z}$. Let C be the Clifford algebra of some regular quadratic form. If V is a graded C-module then $V \cong C \otimes_{C_0} V_0$. Thus there is a one-to-one correspondence: {graded C-modules} $\leftrightarrow$ {C_0-modules}.

12. **4-dimensional forms.** Suppose $\dim\alpha = 4$, $d\alpha = \langle d\rangle$, and $L = F(\sqrt{d})$.

(1) $c(\alpha \otimes L) = 1$ iff α is isotropic.

(2) $c(\alpha) =$ quaternion iff $\alpha \perp \langle -1, d\rangle$ is isotropic.

(3) Suppose $\dim\alpha = \dim\beta = 4$, $d\alpha = d\beta = \langle d\rangle$, and $L = F(\sqrt{d})$.

Then α and β are similar over F if and only if $\alpha \otimes L$ and $\beta \otimes L$ are similar over L.

(4) If $\dim\alpha = \dim\beta = 4$, $d\alpha = d\beta$ and $c(\alpha) = c(\beta)$ then α and β are similar.

(5) If α and β are 4-dimensional forms then α, β are similar if and only if $C_0(\alpha) \cong C_0(\beta)$.

(Hint. (3) Scale α, β to assume $\alpha \simeq \langle 1\rangle \perp \alpha'$ and $\beta \simeq \langle 1\rangle \perp \beta'$. Since α_L and β_L are similar Pfister forms they are isometric and Exercises 8(3) and 9(2) imply that $\alpha' \perp -\beta'$ is isotropic (see Exercise 10). If $\alpha \simeq \langle\langle u\rangle\rangle \perp \langle a\rangle\langle\langle ud\rangle\rangle$ and $\beta \simeq \langle\langle u\rangle\rangle \perp \langle b\rangle\langle\langle ud\rangle\rangle$ then by (3.20), $\langle 1, -ab, u, -abud\rangle$ is isotropic. Choose $x \in D_F(\langle\langle u\rangle\rangle) \cap D_F(\langle ab\rangle\langle\langle ud\rangle\rangle)$, to obtain $\langle x\rangle\alpha \simeq \beta$.

(4) If $\langle d\rangle \neq \langle 1\rangle$ apply (3).)

13. (1) Suppose $\dim \varphi = 5$. Then $\varphi \subset \langle a\rangle\rho$ for some 3-fold Pfister form ρ if and only if φ represents $d\varphi$, if and only if $c(\varphi) =$ quaternion.

(2) Suppose $\dim \varphi = 6$. Then $\varphi \subset \langle a\rangle\rho$ for some 3-fold Pfister form ρ if and only if $\varphi \simeq \langle\langle x\rangle\rangle \otimes \delta$ for some $x \in F^\bullet$ and some form δ if and only if $c(\varphi)$ is split by $F(\sqrt{d\varphi})$.

14. **Trace forms.** Let $C = C(V, q)$ be a Clifford algebra of dimension 2^m. Define the "trace" map $\ell : C \to F$ to be the scalar multiple of the regular trace having $\ell(1) = 1$. Then for a derived basis $\{e^\Delta\}$ we have $\ell(e^\Delta) = 0$ whenever $\Delta \neq 0$. Recall that "bar" $= J_0$ is the involution extending -1_V. Define the associated trace form $\mathrm{B}_0 : C \times C \to F$ by $B_0(x, y) = \ell(x\bar{y})$.

(1) B_0 is a regular symmetric bilinear form on C. If $q \simeq \langle a_1, \ldots, a_m\rangle$ then $(C, B_0) \simeq \langle\langle -a_1, \ldots, -a_m\rangle\rangle$. In particular the isometry class of this Pfister form is independent of the basis chosen for q.

(2) Suppose $\beta \simeq \langle b_1, \ldots, b_m\rangle$ and define $P(\beta) = \langle\langle b_1, \ldots, b_m\rangle\rangle$, the associated Pfister form.

Lemma. *If $\beta \simeq \gamma$ then $P(\beta) \simeq P(\gamma)$.*

This follows from part (1). Also prove it using Witt's Chain-Equivalence Theorem (Exercise 2.8), without mentioning Clifford algebras.

(3) Define $P_i(\beta)$ to be the "degree i" part of the Pfister form $P(\beta)$, so that $\dim P_i(\beta) = \binom{m}{i}$. For example, $P_0(\beta) = \langle 1\rangle$, $P_1(\beta) = \beta$ and $P_2(\beta) = \langle b_1b_2, b_1b_3, \ldots, b_{m-1}b_m\rangle$. The lemma generalizes: If $\beta \simeq \gamma$ then $P_i(\beta) \simeq P_i(\gamma)$ for each i.

(4) If $C = C(-\alpha \perp \beta)$ and $J = J_{A,B}$ is the involution extending $(-1) \perp (1)$ on $-\alpha \perp \beta$, define the trace form B as before. Then $(C, B) \simeq P(\alpha \perp \beta)$.

15. **More trace forms.** Let $C = C(V, q)$ with the associated trace form $B_0 : C \times C \to F$ defined in Exercise 14.

(1) Let $\mathcal{L}$ and $\mathcal{R} : C \to \mathrm{End}_F(C)$ be the left and right regular representations. If $c \in C$ then $\mathcal{L}(c)$ is a similarity of (C, B_0) if and only if $\bar{c}c \in F$. Consequently $\mathcal{L}(F + V) \subseteq \mathrm{Sim}(C, B_0)$ is a subspace of dimension $m + 1$. Similarly for $\mathcal{R}(F+V)$. These two subspaces can be combined to provide an $(m+1, m+1)$-family $(\mathcal{L}(F + V), \mathcal{R}(F + V) \circ \alpha)$ where α is the canonical automorphism of C. How does this compare to the Construction Lemma 2.7?

(2) **Clifford and Cayley.** Let $C = C(\langle a_1, a_2, a_3\rangle)$ be an 8-dimensional Clifford algebra. Let $U = \mathrm{span}\{1, e_1, e_2, e_3\}$ so that $C = U + Uz$. Shift the $(4, 4)$-family constructed in (1) to an $(8, 0)$-family and identify it with C as in (1.9). This provides

a new multiplication $\diamond$ on C given by: $(x+y)\diamond c = xc + \alpha(c)y$, for $x \in U$, $y \in Uz$ and $c \in C$. Using $N_0(c) = B_0(c,c)$ we have $N_0(ab) = N_0(a)N_0(b)$. This $\diamond$ defines an octonion algebra. Compare the multiplication tables of the two algebras to see that they differ only by a few $\pm$ signs.

(3) Let $W \subseteq C$ be a linear subspace spanned by elements of degree $\equiv 2, 3 \pmod 4$. If $\bar{w}w = w\bar{w} \in F$ for every $w \in W$ then $\mathcal{L}(W) + \mathcal{R}(W) \circ \alpha \subseteq \mathrm{Sim}(C, B_0)$. For example we find $\langle\langle a_1\rangle\rangle \otimes \langle 1, a_2, \ldots, a_m\rangle < \mathrm{Sim}(\langle\langle a_1, \ldots, a_m\rangle\rangle)$.

16. **Clifford division algebras.** Let $\alpha = \langle 1\rangle \perp \alpha_1$ where $\dim\alpha = m+1$, and let $C = C(-\alpha_1)$. Then $\dim C = 2^m$. Note that $d\alpha = d(-\alpha_1)$.

(1) Here are necessary and sufficient conditions for C to be a division algebra:

$m = 1$: α is anisotropic.

$m = 2$: α is anisotropic.

$m = 3$: α and $\langle 1, -d\alpha\rangle$ are anisotropic.

$m = 4$: $\alpha \perp \langle -d\alpha\rangle$ is anisotropic.

$m = 5$: $\langle 1, -d\alpha\rangle$ is anisotropic and $\alpha \otimes F(\sqrt{da})$ is anisotropic.

No similar result is known for $m = 6$.

(2) Let q be a form over F and t an indeterminate. Then $C(q \perp \langle t\rangle)$ is a division algebra over $F(t)$ if and only if $C(q)$ is a division algebra over F.

(Hint. (1) For $m = 4$ use Exercise 10(5). (2) If $A = C(q)$ over F, let $A(t) = A \otimes F(t)$. Then $C = C(q \perp \langle t\rangle) = A(t) \oplus A(t)e$ where $e^2 = t$ and $e^{-1}xe = \alpha(x)$ for $x \in A(t)$. Suppose A is a division algebra and C is not, and choose $c = x(t) + y(t)e$ with $c^2 = 0$. Relative to a fixed basis of A assume that $x(t)$ and $y(t)$ have polynomial coefficients of minimal degree. From $x^2 + y\alpha(y)t = 0$ argue that t divides everything, contrary to the minimality.)

17. **Albert forms.** (1) Suppose q is a form with $\dim q = 6$ and $dq = \langle 1\rangle$. Then $q \perp \mathbb{H} \simeq \varphi_1 \perp -\varphi_2$, where φ_1 and φ_2 are 2-fold Pfister forms, and $c(q)$ is a tensor product of two quaternion algebras.

(2) **Lemma.** *Suppose α and β are forms with $\dim\alpha = \dim\beta = 6$, $d\alpha = d\beta$ and $c(\alpha) = c(\beta)$. Then α and β are similar.*

(3) Suppose $A = Q_1 \otimes Q_2$ is a tensor product of two quaternion algebras whose norm forms are φ_1 and φ_2. Define the *Albert form* $\alpha = \alpha_A = \varphi_1' \perp -\varphi_2'$. Then $\dim\alpha = 6$, $d\alpha = \langle 1\rangle$, $c(\alpha) = [A]$. Also: A is a division algebra if and only if α_A is anisotropic (by Exercise 10(5)).

Proposition. *The similarity class of α_A depends only on the algebra A and not on Q_1 and Q_2.*

(4) If $A = C(q)$ where $\dim q = 4$ then $\alpha_A = q \perp \langle -1, dq\rangle$.

(Hint. (2) Given $\alpha \equiv \beta \pmod{J_3(F)}$, we may assume $\alpha \simeq \langle 1\rangle \perp \alpha_1$ and $\beta \simeq \langle 1\rangle \perp \beta_1$. By (3.12), $\alpha_1 \perp -\beta_1$ is isotropic, so there exists d such that $\alpha_1 \simeq \langle d\rangle \perp \alpha_2$ and $\beta_1 \simeq \langle d\rangle \perp \beta_2$, where α_2 and β_2 are 4-dimensional. Apply Exercise 12(4).)

18. **Generalizing Albert forms.** (1) If $\dim q = 2m$ then $C(q)$ is isomorphic to a tensor product of m quaternion algebras. Conversely, if A is a tensor product of m quaternion algebras then $A \cong C(q)$ for some form q with $\dim q = 2m$. Possibly $C(q)$ is similar to a product of fewer than m quaternion algebras (e.g. if q is isotropic).

(2) An F-algebra A is similar to a tensor product of $m-1$ quaternion algebras if and only if $[A] = c(\varphi)$ for some form φ with $\dim \varphi = 2m$ and $d\varphi = \langle 1\rangle$. Such a form φ is called an *Albert form* for A. Compare Exercise 17.

(3) Suppose A is a tensor product of quaternion algebras. If A is a division algebra then every Albert form for A is anisotropic.

(4) There exists some A having two Albert forms which are not similar. There exists some A which is not a division algebra but every Albert form of A is anisotropic.

(Hint. (2) ($\Longleftarrow$) Express $\varphi \simeq \langle a\rangle \perp \alpha$, note that $d\alpha = \langle -a\rangle$ and compute $c(\varphi) = c(\alpha) = [C_0(\alpha)]$. ($\Longrightarrow$) Express $A \cong C(q)$ where $\dim q = 2m-2$. Let $\varphi = q \perp \langle -1, dq\rangle$.

(4) For the second statement let D be the example of Amitsur, Rowen and Tignol (1979) mentioned in Theorem 6.15(2) below. Then $A = \mathbb{M}_2(D)$ is a product of 4 quaternion algebras but D contains no quaternion subalgebras. If φ is an isotropic Albert form for A then $[D] = [A] = c(\varphi)$ is a product of 3 quaternion algebras in $\mathrm{Br}(F)$.)

19. **The signs in $C(V, q)$.** Let $\{e_1, \dots, e_n\}$ be a basis of (V, q) corresponding to $q \simeq \langle a_1, \dots, a_n\rangle$, and with $\{e^\Delta\}$ the derived basis of $C = C(V, q)$. Then $e^\Delta e^\Gamma = \pm a_{\Delta\Gamma} e^{\Delta+\Gamma}$ where $a_\Delta = a_1^{\delta_1} \dots a_n^{\delta_n} \in F^\bullet$, as in Exercise 1.11.

(1) This $\pm$ sign is $(-1)^{\beta(\Delta,\Gamma)}$ where $\beta : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ is a bilinear form. In fact, if $\{\varepsilon_1, \dots, \varepsilon_n\}$ is the standard basis for $\mathbb{F}_2^n$ then $\beta(\varepsilon_i, \varepsilon_j) = 1$ if $i > j$ and 0 otherwise.

(2) Conversely, given a bilinear form β on $\mathbb{F}_2^n$ define an F-algebra $A(\beta)$ of dimension 2^n with basis $\{e^\Delta\}$ using the formula above. Then $A(\beta)$ is an associative algebra with 1. (For the β specified above, this observation leads to a proof of the existence of the Clifford algebra.)

(3) Let Q_β be the quadratic form on $\mathbb{F}_n^2$ defined by β, that is, $Q_\beta(x) = \beta(x, x)$. If β' is another form and $Q_\beta = Q_{\beta'}$ then $A(\beta) \cong A(\beta')$. Our algebra $A(\beta)$ could be called $A(Q)$.

(4) If Q is a regular form (i.e. the bilinear form $Q(x+y) - Q(x) - Q(y)$ is regular) then the algebra $A(Q)$ is central simple over F. (For the simplicity, suppose I is an ideal and choose $0 \neq c \in I$ with $c = \sum c_\Delta e^\Delta$ of minimal length. Compare Proposition 1.11.)

(5) If $Q \simeq Q_1 \perp Q_2$ then $A(Q) \cong A(Q_1) \otimes A(Q_2)$. Therefore if Q is regular, $A(Q)$ is a tensor product of quaternion algebras.

20. **Singular forms.** (1) Suppose q is a quadratic form on V and define the *radical* of V to be $V^\perp = \{v \in V : B(v, x) = 0 \text{ for every } x \in V\}$. Then q induces a quadratic form $\bar{q}$ on the quotient space $\bar{V} = V/V^\perp$ and $\bar{q}$ is regular. If W is any complement

of $V^\perp$ in V (i.e. $V = V^\perp \oplus W$ as vector spaces) the restriction $(W, q|W)$ is isometric to $(\bar{V}, \bar{q})$. Then $q \simeq r\langle 0\rangle \perp q_1$ for a regular form q_1, unique up to isometry.

(2) For q as above there exists an isometry $(V, q) \to (V', q')$ where q' is a regular form. In fact we can use $q' = r\mathbb{H} \perp q_1$. (Note: isometries are injective by definition.) What is the minimal value for $\dim V'$ here? Is that minimal form q' unique?

(3) Complete the proof of (3.7).

(4) If $q = r\langle 0\rangle \perp q_1$ for a regular form q_1, what is the center of $C(q)$? In particular what is the center of the exterior algebra $\Lambda(V)$?

Notes on Chapter 3

In 1878 W. K. Clifford defined his algebras using generators and relations. He expressed such an algebra as a tensor product of quaternion algebras and the center (but using different terminology). Clifford's algebras were used by R. Lipschitz in his study of orthogonal groups in 1884. These algebras were rediscovered in the case $n = 4$ by the physicist P. A. M. Dirac, who used them in his theory of electron spin. The algebraic theory of Clifford algebras was presented in a more general form by Brauer and Weyl (1935), by E. Cartan (1938) and by C. Chevalley (1954). Also compare Lee (1945) and Kawada and Iwahori (1950). Most of the algebraic information about Clifford algebras that we need appears in various texts, including: Bourbaki (1959), Lam (1973), Jacobson (1980), Scharlau (1985) and Knus (1988).

Terminologies and notations often vary with the author, and sometimes the notations are inconsistent within one book. For example we used A° for the "pure" part of the Cayley–Dickson algebra in Exercise 1.25 (3) and we used C_0 for the even Clifford algebra in (3.8). (Some authors use A^+ and C^+ for these objects.) Moreover, a quaternion algebra A is both a Cayley–Dickson algebra and a Clifford algebra, but we sometimes write A_0 for the set of pure quaternions.

Here are some further examples of confusing notations in this subject. As mentioned earlier, the Pfister form $\langle\langle a_1, \ldots, a_n\rangle\rangle$ in this book (and in Lam (1973) and Scharlau (1985)) is written as $\langle\langle -a_1, \ldots, -a_n\rangle\rangle$ in Knus et al. (1998). For a quadratic form q, Lam uses dq for our determinant $\det(q)$ and $d_\pm q$ for the discriminant. In Clifford algebra theory, the names for the canonical automorphism α, and for the involutions $x^\top = J_0(x)$ and $\bar{x} = J_1(x)$ are even less standard. Their names and notations vary widely in the literature.

The quaternion algebra decompositions in (3.14) follow Dubisch (1940). Similar explicit formulas were given by Clifford (1878).

Proofs of (3.18) also appear in Lam (1973), p. 121 or implicitly in Scharlau (1985), p. 81, Theorem 12.9.

The ideal $J_3(F)$ coincides with the ideal defined by Arason and Knebusch using the "degree" of a quadratic form. See Scharlau (1985), p. 164.

The proof of Theorem 3.21 first appeared in Satz 14 of Pfister (1966). It is also given in Scharlau (1985), pp. 90–91. Some work has been done recently on 14-dimensional forms with trivial invariants. See the remarks before (9.12) below.

Exercise 2. There is a more abstract treatment of the subspaces $V_{(k)}$. It uses the canonical bijection $\Lambda(V) \to C(V,q)$, and the exterior power $\Lambda^k(V)$ corresponds to $V_{(k)}$. In the usual product on $C(V,q)$, if $x \in V_{(r)}$ and $y \in V_{(s)}$ then $xy \in V_{(r+s)} + V_{(r+s-2)} + \cdots$. Using that bijection to transfer the exterior product "$\wedge$" to $C(V,q)$, it turns out that $x \wedge y$ is exactly the $V_{(r+s)}$-component of xy. See Bourbaki (1959), Wonenburger (1962a) or Marcus (1975).

Exercise 6. This first appeared in Satz 9 of Witt (1937).

Exercise 8. These are old results going back at least to Albert (1939). The simple proof of part (1) appears in Lam (1973), p. 200 and Scharlau (1985), p. 45.

Exercise 10. (5) Albert (1931) first discovered when a tensor product of two quaternion algebras is a division algebra. If $Q_1 \otimes Q_2$ is not a division algebra then α is isotropic and Q_1 and Q_2 have a common maximal subfield (as in 10(1)). A more direct proof of this was given by Albert (1972). A different approach appears in Knus et al. (1998) in Corollary 16.29.

Exercise 11. Further information on such graded algebras appears in Lam (1973), Chapter 4 and in Knus (1988), Chapter 4.

Exercise 12 follows Wadsworth (1975). See Exercise 5.23 below for another proof. A different method and related results appear in Knus (1988), pp. 76–78. Tignol has found a proof involving the corestriction of algebras.

Exercise 14. Some trace forms in the split case are considered in Exercise 1.13. See also Exercise 7.14.

Exercise 16. (1) Compare Edwards (1978).

(2) A more general result is stated in Mammone and Tignol (1986).

Exercise 17. Albert forms were introduced by Albert (1931) in order to characterize when a tensor product of two quaternion algebras is a division algebra. The proposition about the similarity class of α_A was first proved by Jacobson (1983) using Jordan structures. The quadratic form proof here was extended to characteristic 2 in Mammone and Shapiro (1989). The Albert form arises more naturally as the form on the alternating elements of A induced by a "Pfaffian" as mentioned in Chapter 9 below. This application of Pfaffians originated with Knus, Parimala and Sridharan (1989). This whole theory is also presented in Knus et al. (1998), §16.

Exercise 18 is part of the preliminary results for Merkurjev's construction of a non-formally real field F having $u(F) = 2n$. See Lam (1989) and Merkurjev (1991).

Exercise 19 follows ideas told to me by F. Rodriguez-Villegas.

Chapter 4

C-Modules and the Decomposition Theorem

An (s, t)-family on (V, q) provides V with the structure of a C-module, for a certain Clifford algebra C. Moreover, the adjoint involution I_q on $\mathrm{End}(V)$ is compatible with an involution J on C. We examine a more general sort of (C, J)-module, discuss hyperbolic modules and derive the basic Decomposition Theorem for (s, t)-families.

Before pursuing these general ideas let us state the main result. If (σ, τ) is a pair of quadratic forms over F we say that a quadratic space (V, q) is a (σ, τ)-*module* if $(\sigma, \tau) < \mathrm{Sim}(V, q)$. A (σ, τ)-module (V, q) is *unsplittable* if there is no decomposition $(V, q) \simeq (V_1, q_1) \perp (V_2, q_2)$ where each (V_i, q_i) is a non-zero (σ, τ)-module. Clearly every (σ, τ)-module is isometric to an orthogonal sum of unsplittables.

4.1 Decomposition Theorem. *Let (σ, τ) be a pair of quadratic forms where σ represents* 1. *All unsplittable (σ, τ)-modules have the same dimension 2^k, for some k.*

Without the condition that σ represents 1 the result fails. Examples appear in Exercise 5.9.

The proof of this theorem involves the development of the theory of quadratic (C, J)-modules, where C is a Clifford algebra with an involution J. In order to pinpoint the properties of the Clifford algebras used in the proof, we will develop the theory of quadratic modules over a semisimple F-algebra with involution. But before introducing those ideas we point out some simple consequences of (4.1).

First of all, this theorem explains why the Hurwitz–Radon function $\rho(n)$ depends only on the 2-power part: if $n = 2^m n_0$ where n_0 is odd, then $\rho(n) = \rho(2^m)$. In fact, suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ where $\dim q = n$. By the theorem, an unsplittable (σ, τ)-module (W, φ) must have dimension 2^k dividing n. Then $k \leq m$ and $(\sigma, \tau) < \mathrm{Sim}(q')$ for some form q' of dimension 2^m. Here q' can be taken to be $2^{m-k}\varphi$.

The theorem also provides a more conceptual proof of Proposition 1.10. Suppose (W, α) is unsplittable for $\langle 1, a\rangle$. (I.e., it is an unsplittable $(\langle 1, a\rangle, 0)$-module.) By (1.9) we know that $\langle x\rangle\langle\langle a\rangle\rangle \subset \alpha$ for some $x \in F^\bullet$, and in particular $\dim \alpha \geq 2$. By explicit construction, $\langle 1, a\rangle < \mathrm{Sim}(\langle\langle a\rangle\rangle)$, so $\langle\langle a\rangle\rangle$ is an unsplittable module for $\langle 1, a\rangle$. The Decomposition Theorem then implies that $\dim \alpha = 2$, so that $\alpha \simeq \langle x\rangle\langle\langle a\rangle\rangle$. It quickly follows that if $\langle 1, a\rangle < \mathrm{Sim}(q)$ then q is a sum of unsplittables, or equivalently $q \simeq \langle\langle a\rangle\rangle \otimes \varphi$ for some form φ.

Several small (s,t)-families can be analyzed in this way. These arguments are presented in Chapter 5, and the interested reader can skip there directly. For the rest of this Chapter we discuss quadratic modules.

Suppose $(S,T) \subseteq \mathrm{Sim}(V,q)$ is an (s,t)-family and σ and τ are the quadratic forms induced on S and T. Then $1_V \in S$ and we define $S_1 = (1_V)^\perp$. If $f \in S_1$ and $g \in T$ then:

$$I_q(f+g) = -f+g$$
$$(f+g)^2 = f^2+g^2 = (-\sigma(f)+\tau(g))1_V.$$

Therefore the inclusion map $S_1 \perp T \to \mathrm{End}(V)$ is compatible with the quadratic form on $-\sigma_1 \perp \tau$ on $S_1 \perp T$. By the definition of Clifford algebras, there is an induced F-algebra homomorphism

$$\pi : C \to \mathrm{End}(V),$$

where $C = C(-\sigma_1 \perp \tau)$ is the Clifford algebra of dimension 2^{s+t-1}. This π provides an action of C on V, making V into a C-module.

To be a little more careful let us define the space $\breve{S}_1 \perp \breve{T}$ to be the generating space of C , so that $S_1 = \pi(\breve{S}_1)$ and $T = \pi(\breve{T})$. Setting $\breve{S} = F \cdot 1 + \breve{S}_1 \subseteq C$, we have $S = \pi(\breve{S})$. For example, suppose $\sigma \simeq \langle 1, a_2, \ldots, a_s\rangle$ and $\tau \simeq \langle b_1, \ldots, b_t\rangle$, and let $f_2, \ldots, f_s, g_1, \ldots, g_t$ be given as in (2.1). The algebra $C = C(-\sigma_1 \perp \tau)$ has generators $e_2, \ldots, e_s, d_1, \ldots, d_t$ corresponding to the given diagonalization of $-\sigma_1 \perp \tau$. Then $\breve{S} = \mathrm{span}\{1, e_2, \ldots, e_s\}$, $\breve{T} = \mathrm{span}\{d_1, \ldots, d_t\}$ and $\pi(e_i) = f_i$, $\pi(d_j) = g_j$. We often identify S with $\breve{S}$ and T with $\breve{T}$ to simplify notations. We do this even though the identification of S and T with subspaces of C is sometimes misleading, since this embedding depends on the representation π.

4.2 Proposition. *Let (V,q) be a quadratic space of dimension $n = 2^m n_0$, where n_0 is odd. Then any (s,t)-family on (V,q) must have $s+t \leq 2m+2$.*

Proof. Suppose $(\sigma,\tau) < \mathrm{Sim}(V,q)$ and let $C = C(-\sigma_1 \perp \tau)$ be the associated Clifford algebra with representation $\pi : C \to \mathrm{End}(V)$. By the Structure Theorem 3.6 either $\pi(C)$ or $\pi(C_0)$ is a central simple subalgebra of $\mathrm{End}(V)$. The double centralizer theorem implies that the dimension of this subalgebra must divide $\dim(\mathrm{End}(V)) = n^2$. Then 2^{s+t-2} divides $n^2 = 2^{2m}n_0^2$ so that $s+t-2 \leq 2m$. □

The original 1, 2, 4, 8 Theorem is an immediate consequence of this inequality. (Compare Exercise 1.1.) The proof of this proposition uses only the information that V is a C-module. To get sharper information we will take the involutions into account and analyze the "unsplittable components" of (V,q).

4.3 Definition. Define $J_S = J_{\breve{S}_1,\breve{T}}$ to be the involution on C as in Definition 3.15. Then J_S acts as -1 on $\breve{S}_1$ and as 1 on $\breve{T}$.

This involution is chosen to match the behavior of the involution I_q on $\mathrm{End}(V)$. That is, the action of I_q on the maps f_i, g_j in $\mathrm{End}(V)$ matches the action of J_S on the generators e_i, d_j in C. Therefore, for every $c \in C$, $\pi(J_S(c)) = I_q(\pi(c))$. Hence, π is a homomorphism of algebras-with-involution:

$$\pi : (C, J_S) \to (\mathrm{End}(V), I_q).$$

Such a map π is sometimes called a *similarity representation* or a *spin representation*.

The map π is usually not written explicitly. We write the action of an element $c \in C$ as a multiplication: $cv = \pi(c)(v)$, for $v \in V$. Then the compatibility of the involutions says exactly that:

$$B_q(cv, w) = B_q(v, J_S(c)w), \qquad (*)$$

for every $c \in C$ and $v, w \in V$. Conversely, if V is a C-module and q is a quadratic form on V satisfying the compatibility condition $(*)$, then $(\sigma, \tau) < \mathrm{Sim}(V, q)$. Therefore (V, q) is a (σ, τ)-module if and only if V is a C-module and the form q satisfies the compatibility condition $(*)$ above.

Different C-module structures on V can arise from the same family (S, T) in $\mathrm{Sim}(V, q)$. To see this let δ be an automorphism of C which preserves the subspaces $\check{S}_1$ and $\check{T}$. If π is a similarity representation coming from (S, T), define $\pi' = \pi \circ \delta$. Then π' is another similarity representation associated to (S, T). This ambiguity should cause little trouble, since we usually fix one representation.

Let us now set up the theory of quadratic modules. To see where the special properties of Clifford algebras are used, we describe the theory for a wider class of algebras.

Notation. Let C be a finite dimensional semisimple F-algebra with involution J. The involution is often written simply as "bar". Unless explicitly stated otherwise, every module is a left C-module which is finite dimensional over F.

It is useful to consider alternating spaces in parallel with quadratic spaces. To handle these cases together, let $\lambda = \pm 1$ and define a λ-*form* B on a vector space V to be a bilinear form $B : V \times V \to F$ which is λ-symmetric, that is: $B(y, x) = \lambda B(x, y)$ for every $x, y \in V$. The λ-form B is *regular* if $V^{\perp} = 0$, (or equivalently if the induced map θ_B from V to its dual is a bijection). Then a λ-*space* (V, B) is a vector space V with a regular λ-form B.

Since $2 \neq 0$ in F, a quadratic space is the same as a 1-space. That is, a quadratic form q is determined by its associated symmetric bilinear form B_q. An *alternating* space is another name for a (-1)-space. For any λ-space (V, B) there is an associated adjoint involution I_B as in (1.2).

It is well known that alternating spaces over the field F must have even dimension, and any two alternating spaces of the same dimension are isometric. However in the category of alternating spaces admitting C, such an easy characterization no longer applies.

4.4 Definition. Let C be an algebra with involution as above. Suppose B is a regular λ-form on a C-module V. Then B *admits* C if

$$B(cu, v) = B(u, \bar{c}v)$$

for every $u, v \in V$ and $c \in C$. In this case (V, B) is called a λ-*space admitting* C, or a λ-*symmetric* (C, J)-*module*. If V, V' are λ-spaces admitting C, then they are C-*isometric* (written $V \approx V'$) if there is a C-module isomorphism $V \to V'$ which is also an isometry.

We will extend the standard definitions and techniques of the theory of quadratic forms over F to this wider context. Much of this theory can be done more generally, allowing F to be a commutative ring having $2 \in F^\bullet$ and considering λ-hermitian modules. For example see Fröhlich and McEvett (1969), Shapiro (1976), or for more generality, Quebbemann et al. (1979). The category of λ-spaces admitting C is equivalent to the category of λ-hermitian C-modules. This equivalence is proved in the appendix to this chapter.

If $U \subseteq V$ then $U^\perp$ is the "orthogonal complement" in the usual sense: $U^\perp = \{x \in V : B(x, U) = 0\}$. Then a subspace $U \subseteq V$ is regular if and only if $U \cap U^\perp = 0$, and is totally isotropic iff $U \subseteq U^\perp$.

4.5 Lemma. *Let (V, B) be a λ-space admitting C, and let $T \subseteq V$ be a C-submodule.*

(1) *Then $T^\perp$ is also a C-submodule.*

(2) *If T is a regular subspace of V then $V \approx T \perp T^\perp$.*

(3) *If T is an irreducible submodule then either T is regular or T is totally isotropic.*

Proof. The same argument as in the classical cases. For (3) consider $T \cap T^\perp$. □

We can consider these bilinear forms in terms of dual spaces. Let $\hat{V} = \mathrm{Hom}_F(V, F)$ be the dual vector space. The dual pairing is written

$$\langle\ |\ \rangle : V \times \hat{V} \to F.$$

The space $\hat{V}$ has a natural structure as a right C-module, defined by: $\langle v|\hat{v}c\rangle = \langle cv|\hat{v}\rangle$. We will use the involution to change hands and make $\hat{V}$ into a left C-module.

4.6 Definition. Let V be a left C-module. For $\hat{v} \in \hat{V}$ and $c \in C$ define $c\hat{v}$ by:

$$\langle v|c\hat{v}\rangle = \langle \bar{c}v|\hat{v}\rangle \quad \text{for all } v \in V.$$

A λ-form B on V induces a linear map $\theta_B : V \to \hat{V}$ by defining $\theta_B(v) = B(-, v)$. That is, $\langle u|\theta_B(v)\rangle = B(u, v)$. By definition, B is regular if and only if θ_B is bijective. Furthermore the definitions imply that: B admits C if and only if θ_B is a C-module isomorphism.

Consequently if (V, B) is a λ-space admitting C then $\hat{V} \cong V$ as C-modules. Conversely, if $\hat{V} \cong V$ must there exist such a λ-form? Here is one special case when a form always exists.

4.7 Definition. Let T be a C-module and $\lambda = \pm 1$. Define $H_\lambda(T)$ to be the C-module $T \oplus \hat{T}$ together with the λ-form B_H defined by: $B_H(s + \hat{s}, t + \hat{t}) = \langle s|\hat{t}\rangle + \lambda\langle t|\hat{s}\rangle$, for $s, t \in T$ and $\hat{s}, \hat{t} \in \hat{T}$. A λ-space admitting C is *C-hyperbolic* if it is C-isometric to some $H_\lambda(T)$.

One easily checks that B_H is regular, λ-symmetric and admits C. If $T \cong T'$ as C-modules then $H_\lambda(T) \approx H_\lambda(T')$. Also $H_\lambda(S \oplus T) \approx H_\lambda(S) \perp H_\lambda(T)$.

4.8 Lemma. *Let (V, B) be a λ-space admitting C.*

(1) *V is C-hyperbolic iff $V = T_1 + T_2$ where T_1 and T_2 are totally isotropic submodules.*

(2) *$V \perp \langle -1\rangle V \approx H_\lambda(V)$ is C-hyperbolic.*

Proof. (1) If $V = H_\lambda(T)$ let $T_1 = T \oplus 0$ and $T_2 = 0 \oplus \hat{T}$. Conversely, suppose $V = T_1 + T_2$. Then $T_i \subseteq T_i^\perp$, and since $V^\perp = 0$ we have $T_1^\perp \cap T_2^\perp = 0$. The map $\psi : T_2 \to \hat{T}_1$, defined by $\psi(x) = B(-, x)$, is a C-homomorphism and $\ker \psi = 0$. The surjectivity of ψ follows from the surjectivity of θ_B (or by comparing dimensions). Then ψ is a C-isomorphism and $1 \oplus \psi$ is a C-isometry $V \to H_\lambda(T_1)$.

(2) We are given a space $U = V \oplus V'$ and a C-isomorphism $f : V \to V'$ which is also a (-1)-similarity. Let $T_+ = \{x + f(x) : x \in V\} \subseteq U$ be the graph of f, and similarly let T_- be the graph of $-f$. It is easy to check that T_+ and T_- are totally isotropic submodules and $U = T_+ + T_-$ so part (1) applies. □

4.9 Proposition. *Let (V, B) be a λ-space admitting C and $T \subseteq V$ a totally isotropic submodule. Then there is another totally isotropic submodule $T' \subseteq V$ with $T + T' \approx H_\lambda(T)$, a regular submodule of V.*

Proof. Since C is semisimple there exists a submodule W of V complementary to the submodule $T^\perp$. Then the induced pairing $B_0 : W \times T \to F$ induces a C-isomorphism $W \cong \hat{T}$. If W is totally isotropic then $T + W \approx H_\lambda(T)$ by Lemma 4.8. Therefore the proposition is proved once we find a totally isotropic complement to $T^\perp$.

Given W, all other complements to $T^\perp$ appear as graphs of C-homomorphisms $f : W \to T^\perp$. Define the homomorphism $f : W \to T \subseteq T^\perp$ by the equation:

$$B_0(w_1, f(w_2)) = -\tfrac{1}{2}B(w_1, w_2),$$

for $w_1, w_2 \in W$. The nonsingularity of the induced pairing B_0 above shows that f is well-defined and C-linear. The graph of this f provides the complement we need. □

This proposition gives information about the structure of unsplittables. We define a λ-space V admitting C to be *C-unsplittable* if there is no expression $V \approx V_1 \perp V_2$ where V_1 and V_2 are non-zero submodules. Equivalently, V is C-unsplittable if and only if V has no regular proper submodules. The following result contains most of the information needed to prove the Decomposition Theorem 4.1.

4.10 Theorem. *Let (V, B) be an unsplittable λ-space admitting C. Then either V is irreducible or $V \approx H_\lambda(T)$ for an irreducible module T. Moreover, $H_\lambda(T)$ is unsplittable if and only if T is irreducible and possesses no regular λ-form admitting C.*

Proof. If V is reducible let $T \subseteq V$ be an irreducible submodule. Since V is unsplittable T must be singular, and hence totally isotropic by (4.5)(3). Then by (4.9) we have $T \subseteq H \subseteq V$, where $H \approx H_\lambda(T)$. Since V is unsplittable, $V = H$.

Now suppose T is an irreducible C-module. If T possesses a regular λ-form admitting C, then by (4.8)(2) we have $H_\lambda(T) \approx T \perp \langle -1 \rangle T$ is splittable. □

Let (V, B) be any λ-space admitting C. Then there is a decomposition

$$V = H_u \perp H_s \perp V_a,$$

where H_u is an orthogonal sum of unsplittable C-hyperbolic subspaces, and H_s is an orthogonal sum of splittable hyperbolic subspaces, and V_a is C-anisotropic. Here we define a λ-space to be C-anisotropic if it has no totally isotropic irreducible submodules. From (4.10) we conclude that no irreducible submodule of H_u can be isomorphic to a submodule of $H_s \perp V_a$. Therefore H_u and $H_s \perp V_a$ are uniquely determined submodules of V.

Moreover, as in the classical case, the submodules H_s and V_a are unique up to isometry because there is a Cancellation Theorem:

If U, V and W are λ-spaces admitting C and $U \perp V \approx U \perp W$ then $V \approx W$.

We omit the proof of this theorem because it does not seem to have a direct application to the study of (s, t)-families. Proofs of more general results appear in McEvett (1969), Shapiro (1976), and Quebbemann et al. (1979). Knowing the Cancellation Theorem it is natural to investigate the Witt ring $W^\lambda(C, J)$ of λ-spaces admitting (C, J). We will not pursue this investigation here.

When does an irreducible C-module W possess a regular λ-form admitting C? If such a form exists then certainly $\hat{W} \cong W$ as C-modules.

4.11 Lemma. *If W is an irreducible C-module with $\hat{W} \cong W$, then W has a regular λ-form admitting C, for some sign λ.*

Proof. If $g : U \to V$ is a C-module homomorphism, the transpose $g^\top : \hat{V} \to \hat{U}$ is defined by the equation $\langle u | g^\top(\hat{v}) \rangle = \langle g(u) | \hat{v} \rangle$. Any C-isomorphism $\theta : W \to \hat{W}$

induces a regular bilinear form B on W by setting $B(x, y) = \langle x|\theta(y)\rangle$. After identifying W with its double dual, we see that B is a regular λ-form if and only if $\theta^\top = \lambda\theta$. Now from the given C-isomorphism θ, define $\theta_\lambda = \frac{1}{2}(\theta + \lambda\theta^\top)$. These two maps are C-homomorphisms and $\theta_\lambda^\top = \lambda \cdot \theta_\lambda$. They are not both zero since $\theta = \theta_+ + \theta_-$, so at least one of them must be an isomorphism, by the irreducibility. The corresponding form B is then a regular λ-form admitting C. □

We now return to the original situation of Clifford algebras. Let (σ, τ) be a pair of forms as usual and $C = C(-\sigma_1 \perp \tau)$ with the involution J_S. For a λ-space (V, B) we see that $(\sigma, \tau) < \mathrm{Sim}(V, B)$ if and only if V can be expressed as a C-module where B admits (C, J_S). If C is simple then up to isomorphism there is only one irreducible module, and the ideas above are easy to apply. The non-simple case requires an additional remark.

Suppose C is not simple. Then $s + t$ is even, $d(-\sigma_1 \perp \tau) = \langle 1\rangle$ and C_0 is simple. We can choose $z = z(S_1 \perp T)$ with $z^2 = 1$. Then $Z = F + Fz$ is the center of C and the non-trivial central idempotents are $e_\varepsilon = \frac{1}{2}(1 + \varepsilon z)$ for $\varepsilon = \pm 1$. Then $C = Ce_+ \times Ce_- \cong C_0 \times C_0$ and there are two natural projection maps $p_+, p_- : C \to C_0$. Let V be an irreducible C_0-module with associated representation $\pi : C_0 \to V$. Define V_ε to be the C-module associated to the representation $\pi_\varepsilon = \pi \circ p_\varepsilon$. It follows that every irreducible C-module is isomorphic to either V_+ or V_-. These two module structures differ only by an automorphism of C.

4.12 Lemma. *Let C, J_S be as above. Let $\lambda = \pm 1$ be a fixed sign.*

(1) *Suppose C is not simple. If $s \equiv t \pmod 4$ then $\hat{V}_+ \cong V_+$ and $\hat{V}_- \cong V_-$. If $s \equiv t + 2 \pmod 4$ then $\hat{V}_+ \cong V_-$.*

(2) *If one irreducible C-module possesses a regular λ-form admitting C, then they all do.*

Proof. (1) By the definition of $\hat{W}$ as a left C-module, z acts on $\hat{W}$ as $J_S(z)$ acts on W. Therefore if $J_S(z) = z$ then $\hat{V}_\varepsilon \cong V_\varepsilon$. If $J_S(z) = -z$ then $\hat{V}_\varepsilon \cong V_\varepsilon$. A sign calculation completes the proof.

(2) If C is simple the claim is trivial. Suppose C is not simple and V_ε possesses a regular λ-form B admitting C. The module $V_{-\varepsilon}$ can be viewed as the same vector space V with a twisted representation: $\pi_{-\varepsilon}(c) = \pi_\varepsilon(\alpha(c))$ where α is the canonical automorphism of C. It follows that the form B admits this twisted representation (since α and J_S commute), so $V_{-\varepsilon}$ also has a regular λ-form admitting C. □

4.13 Corollary. *Let (C, J_S) be the Clifford algebra with involution as above. Let $\lambda = \pm 1$ be a fixed sign. Then all the C-unsplittable λ-spaces have the same dimension 2^k, for some k.*

Proof. By the remarks above, all irreducible C-modules have the same dimension 2^m, for some m. It is a power of 2 since C is a direct sum of irreducibles and $\dim C = 2^{r+s-1}$. If one irreducible module possesses a regular λ-form admitting C, then they all do and by (4.10) every unsplittable is irreducible of dimension 2^m. Otherwise (4.10) implies that every unsplittable is isometric to $H_\lambda(T)$ for some irreducible T, so that the unsplittables all have dimension 2^{m+1}. □

Finally we can complete the proof of the original Decomposition Theorem 4.1. The only remaining step is to show that the two notions of "unsplittable" coincide. The problem is that the definition of unsplittable (σ, τ)-module involves isometry of quadratic spaces over F (written $\simeq$) while the definition of unsplittable quadratic space admitting C involves C-isometry (written $\approx$). If a space is (σ, τ)-unsplittable it certainly must be C-unsplittable. Conversely suppose (V, q) is C-unsplittable, but $V \simeq V_1 \perp V_2$ for some non-zero (σ, τ)-modules V_i. Then V_i is a quadratic space admitting C, so it is C-isometric to a sum of C-unsplittables. Comparing dimensions we get a contradiction to (4.13). This completes the proof. □

4.14 Definition. An (s, t)-pair (σ, τ) is of *regular type* if an unsplittable quadratic (σ, τ)-module is irreducible. Otherwise it is of *hyperbolic type*. In working with alternating forms we say that (σ, τ) is of (-1)-*hyperbolic type* or of (-1)-*regular type*.

By (4.12) this condition does not depend on the choice of unsplittable module. If (σ, τ) is of hyperbolic type then (4.10) implies that every unsplittable (σ, τ)-module is $H_\lambda(T)$ for some irreducible C-module T. Consequently, every (σ, τ)-module is C-hyperbolic and (σ, τ)-modules are easy to classify. For example, if $s \equiv t + 2 (\mathrm{mod}\ 4)$ then (4.12) implies that (σ, τ) is of hyperbolic type (and of (-1)-hyperbolic type). The other cases are not as easy to classify. Further information about these types is obtained in Chapter 7.

When C is a division algebra with involution the irreducible module is just C itself. In this case it is sometimes useful to analyze all the λ-forms on C which admit C. This can be done by comparing everything to a given trace form.

4.15 Definition. Let C be an F-algebra with involution. An F-linear map $\ell : C \to F$ is an *involution trace* if

(1) $\ell(\bar{c}) = \ell(c)$ for every $c \in C$;

(2) $\ell(c_1 c_2) = \ell(c_2 c_1)$ for every $c_1, c_2 \in C$;

(3) The F-bilinear form $L : C \times C \to F$, defined $L(c_1, c_2) = \ell(c_1 c_2)$, is regular.

For example if $C = \mathrm{End}(V)$ and J is any involution on C, then the ordinary trace is an involution trace. Suppose $C = C(-\sigma_1 \perp \tau)$ is a Clifford algebra as above and

$J = J_S$. Then the usual trace is an involution trace. Generally every semisimple F-algebra with involution does possess an involution trace. (See Exercise 14 below.)

4.16 Proposition. *Let C be an F-algebra with involution J and with an involution trace ℓ. If B is a regular λ-form on C such that (C, B) admits C then there exists $d \in C^\bullet$ such that $J(d) = \lambda d$ and $B(x, y) = \ell(xdJ(y))$ for all $x, y \in C$.*

Proof. Let $B_1(x, y) = \ell(xJ(y))$. Since ℓ is an involution trace, B_1 is a regular 1-form on C. It is easy to check that (C, B_1) admits C. Since B_1 is regular, the given bilinear form B can be described in terms of B_1: there exists $f \in \mathrm{End}_F(C)$ such that $B(x, y) = B_1(f(x), y)$ for all $x, y \in C$. Since B is regular this f is invertible. The condition that B admits C becomes $B_1(f(cx), y) = B(cx, y) = B(x, J(c)y) = B_1(f(x), J(c)y) = B_1(cf(x), y)$. Therefore $f(cx) = cf(x)$, and f is determined by its value $d = f(1)$. Therefore $B(x, y) = B_1(xd, y) = \ell(xdJ(y))$. Since B is a λ-form we find $J(d) = \lambda d$. □

For example, one such trace form was considered in Exercise 3.14. In the case that $C = \left(\frac{-a,-b}{F}\right)$ is a quaternion division algebra with the usual involution $J =$ "bar" there is a *unique* unsplittable quadratic (C, J)-module. This follows since the only J-symmetric elements of C are the scalars. The "uniqueness" here is up to a C-similarity. In terms of the quadratic forms over F this says that if $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ is unsplittable then q is similar to $\langle\langle a, b\rangle\rangle$. This re-proves Proposition 1.10.

Appendix to Chapter 4. λ-Hermitian forms over C

In this appendix we return to the more general set-up where C is a semisimple F-algebra with involution J and describe the one-to-one correspondence between the λ-spaces admitting C and the λ-hermitian forms over C. This equivalence of categories provides a different viewpoint for this whole theory. Since these ideas are not heavily used later we just sketch them in this appendix.

We could allow the involutions here to be non-trivial on the base ring F. In that case there can be λ-hermitian forms for any $\lambda \in F$ with $\bar{\lambda}\lambda = 1$. The details were worked out by Fröhlich and McEvett (1969), and the reader is referred there for further information.

A.1 Definition. Let V be a C-module and $\lambda = \pm 1$. A λ-*hermitian* form on V (over C) is a mapping $h : V \times V \to C$ satisfying

(1) h is additive in each slot,

(2) $h(cx, y) = ch(x, y)$ for every $x, y \in V$ and $c \in C$,

(3) $h(y, x) = \lambda\overline{h(x, y)}$ for every $x, y \in V$.

It follows that $h(x, cy) = h(x, y)\bar{c}$. For a simple example let $V = C$ and for $a \in C$ define $h_a : C \times C \to C$ by $h_a(x, y) = xa\bar{y}$. If $\bar{a} = \lambda a$ then h_a is a λ-hermitian form.

Define the C-dual module $\tilde{V} = \mathrm{Hom}_C(V, C)$. For fixed $x \in V$ the map $\theta_h(v) = h(-, v)$ is in $\tilde{V}$. This map $\theta_h : V \to \tilde{V}$ is F-linear. The form h is said to be *regular* if θ_h is bijective. Define a λ-*hermitian space* over C to be a C-module V equipped with a regular λ-hermitian form h. One can now define isometries, similarities, orthogonal sums and tensor products in the category of λ-hermitian spaces.

In analogy with our treatment of the F-dual, we write the dual pairing as

$$[\ |\ ] : V \times \tilde{V} \to C.$$

Then $[\ |\ ]$ is F-bilinear, and by definition $[cx|\tilde{x}] = c[x|\tilde{x}]$. With this notation we have: $[u|\theta_h(v)] = h(u, v)$.

As before we use the involution on C to change hands and make $\tilde{V}$ a left C-module: for $\tilde{x} \in \tilde{V}$ and $c \in C$ define $c\tilde{x}$ by

$$[x|c\tilde{x}] = [x|\tilde{x}]\bar{c}$$

for all $x \in V$. Therefore if h is a λ-hermitian form then $\theta_h : V \to \tilde{V}$ is a homomorphism of left C-modules.

The hyperbolic functor H_λ can be introduced in this new context, in analogy with the discussion for λ-spaces admitting C. All the results proved above for λ-spaces admitting C can be done for λ-hermitian modules. In fact, when there is an involution trace map on C, these two contexts are equivalent. This equivalence arises because the two notions of "dual" module, $\tilde{V}$ and $\hat{V}$, actually coincide.

A.2 Proposition. *Let C be a semisimple F-algebra with involution J and possessing an involution trace ℓ.*

(1) *Let (V, h) be a λ-hermitian space over C and define $B = \ell \circ h$. Then (V, B) is a λ-space admitting C, denoted by $\ell_*(V, h)$.*

(2) *Let (V, B) be a λ-space admitting C. Then there is a unique regular λ-hermitian form h on V having $\ell_*(V, h) = (V, B)$.*

(3) *This correspondence ℓ_* preserves isometries, orthogonal sums and the H_λ construction.*

Proof sketch. (This is Theorem 7.11 of Fröhlich and McEvett.) (1) It is easy to see that B is F-bilinear, λ-symmetric and admits C. Composition with ℓ induces a map on the dual spaces $\ell_0 : \tilde{V} \to \hat{V}$, that is: $\langle x|\ell_0(\tilde{x})\rangle = \ell([x|\tilde{x}])$. The properties of ℓ imply that this ℓ_0 is an isomorphism of left C-modules. Furthermore $\ell_0 \circ \theta_h = \theta_B$, and we conclude that B is regular.

(2) Given B we can construct θ_h as $\ell_0^{-1} \circ \theta_B$. It then follows that h is λ-hermitian and $\ell \circ h = B$.

(3) Checking these properties is routine. □

By using hermitian forms over C we sometimes obtain a better insight into a problem. For instance the simplest hermitian spaces over C are the "1-dimensional" forms obtained from the left C-module C itself. If $a \in C^\bullet$ satisfies $\bar{a} = \lambda a$ then the form

$$h_a : C \times C \to C \quad \text{defined by} \quad h_a(x, y) = xa\bar{y},$$

is a regular λ-hermitian form on C. Let $\langle a \rangle_C$ denote this λ-hermitian space (C, h_a). In this notation, the trace form considered in Proposition 4.16 is just $\ell_*(\langle d \rangle_C)$. This transfer result (A.2) quickly yields another proof of (4.16).

A.3 Lemma. *Let C be an F-algebra with involution and $a, b \in C^\bullet$ with $\bar{a} = \lambda a$ and $\bar{b} = \lambda b$. Then $\langle a \rangle_C \simeq \langle b \rangle_C$ if and only if $b = ca\bar{c}$ for some $c \in C^\bullet$.*

Proof. Suppose $\varphi : (C, h_b) \to (C, h_a)$ is an isometry. Then φ is an isomorphism of left C-modules, so that $\varphi(x) = xc$ where $c = \varphi(1) \in C^\bullet$. Since $h_a(\varphi(x), \varphi(y)) = h_b(x, y)$ the claim follows. The converse is similar. □

A.4 Corollary. *Suppose D is an F-division algebra with involution.*

(1) *Every hermitian space over D has an orthogonal basis.*

(2) *If the involution is non-trivial then every (-1)-hermitian space over D has an orthogonal basis.*

Proof. (1) The irreducible left D-module D admits a regular hermitian form (e.g. $\langle 1 \rangle_D$). Then by (A.2) and (4.10) we conclude that every hermitian space over D is an orthogonal sum of unsplittable submodules, each of which is 1-dimensional over D. These provide an orthogonal basis.

(2) There exists $a \in D^\bullet$ such that $\bar{a} = -a$. Then $\langle a \rangle_D$ is a regular (-1)-hermitian form on D. The conclusion follows as before. □

Of course this corollary can be proved more directly, without transferring to the theory of λ-spaces admitting D.

Exercises for Chapter 4

1. **Group rings.** Suppose G be a finite group with order n and the characteristic of F does not divide n. Then the group algebra $C = F[G]$ is semisimple (Maschke's theorem). Define the involution J on C by sending $g \mapsto g^{-1}$ for every $g \in G$. There is a one-to-one correspondence between orthogonal representations $G \to \mathrm{O}(V, q)$ and quadratic (C, J)-modules. These algebras provide examples where unsplittable (C, J)-modules may have different dimensions.

2. **Proposition.** *Suppose V, W are C-anisotropic λ-spaces admitting C. If $V \perp W$ is C-hyperbolic then $V \approx \langle -1 \rangle W$. This is a converse of* (4.8) (2).

(Hint. Let $V \perp W = H$ and suppose $T \subseteq H$ is a totally isotropic submodule with $2 \cdot \dim T = \dim H$. Examine the projections to V and W to see that T is the graph of some $f : V \to W$. This f must be a (-1)-similarity.)

3. **Averaging Process.** (1) Let F be an ordered field and suppose σ, τ are positive definite forms over F with $\sigma \simeq \langle 1 \rangle \perp \sigma_1$ as usual. Let $C = C(-\sigma_1 \perp \tau)$ and let V be a C-module. Then there exists a positive definite quadratic form q on V making $(\sigma, \tau) < \mathrm{Sim}(q)$.

(2) Let $\mathbb{R}$ be the real field, and $C = C((r-1)\langle -1 \rangle)$. Then $r\langle 1 \rangle < \mathrm{Sim}(n\langle 1 \rangle)$ over $\mathbb{R}$ if and only if there is a C-module of dimension n. This explains why the Hurwitz–Radon Theorem can be done over $\mathbb{R}$ without considering the involutions.

(Hint. (1) Let φ be a positive definite form on V and define q by averaging. For instance if $\sigma \simeq \langle 1, a_2, \ldots, a_n \rangle$ and $\tau = 0$, define $q(x) = \sum a_\Delta^{-1} \varphi(e^\Delta x)$.)

4. **Commuting similarities.** What are the possible dimensions of two subspaces of $\mathrm{Sim}(V, q)$ which commute elementwise?

Definition. $\kappa_r(n) = \max\{s$: there exist commuting subspaces of dimensions r and s in $\mathrm{Sim}(V, q)$ for some n-dimensional quadratic space $(V, q)\}$.

Let $R, S \subseteq \mathrm{Sim}(V, q)$ be commuting subspaces which we may assume contain 1_V. Let D be the Clifford algebra corresponding to R so that V is a left D-module. Define $\mathrm{Sim}_D(V, q)$ and note that $S \subseteq \mathrm{Sim}_D(V, q)$. If C is the Clifford algebra for S then this occurs if and only if there is a homomorphism $C \otimes D \to \mathrm{End}(V)$ which preserves the involutions.

(1) If $n = 2^m \cdot$ (odd) then $\kappa_r(n) = \kappa_r(2^m)$.

(2) Define (s, t)-families in $\mathrm{Sim}_D(V, q)$ and prove the Expansion, Shift and Construction Lemmas.

(3) Define $\kappa'_r(n)$ analogously for alternating forms (V, B).

(i) $\kappa'_r(4n) \geq 4 + \kappa_r(n)$ and $\kappa_r(4n) \geq 4 + \kappa'_r(n)$.

(ii) If $r \equiv 2 \pmod 4$ then $\kappa'_r(n) = \kappa_r(n)$.

(4) $\kappa_2(2^m) = 2m$.

(5) **Proposition.** *Suppose $\kappa_r(n) > 0$ where $n = 2^m \cdot$ (odd). Then*

$$\kappa_r(n) = \begin{cases} \rho(n) + 1 - r & \text{if } r \equiv 1 \pmod 4 \\ 2m + 2 - r & \text{if } r \equiv 2 \pmod 4 \\ 1 + \rho_r(n) & \text{if } r \equiv 3 \pmod 4. \end{cases}$$

(Hint. (3) (i) If $\sigma < \mathrm{Sim}_D(q)$ then $(\sigma \perp \langle 1, 1 \rangle, \langle 1, 1 \rangle) < \mathrm{Sim}(\langle\langle 1, 1 \rangle\rangle \otimes q)$. Shift by 2 as in Exercise 2.6(1). (ii) Let $R, S \subseteq \mathrm{Sim}(V, q)$. Then $z = z(R_1)$ commutes with R and S, $\tilde{z} = -z$ and $R, S \subseteq \mathrm{Sim}(V, B')$ where $B'(u, v) = B(u, zv)$. In fact an (s, t)-family in this case is equivalent to an $(s + t, 0)$-family.

(4) $\kappa_2(2^m) \leq 2m$ for otherwise the representation $C \to \mathrm{End}_F(V)$ is surjective and there is no room for D. Check $\kappa_2(1) = 0$ and $\kappa_2(2) = 2$, then apply (3), (4) and induction.

(5) When r is odd, consider commuting $R, S \subseteq \mathrm{Sim}(V)$ and examine $z(R_1) \circ S$. For the even case use (3) to see $\kappa_r(n) \leq \min\{\kappa_{r-1}(n), \kappa'_{r-1}(n)\} = 2m + 2 - r$. Equality follows as in (4).)

5. **More commuting similarities.** Let $D = C(\langle -1\rangle\alpha_1)$ where $\alpha = \langle 1\rangle \perp \alpha_1$ is a given form with $\dim \alpha = r$. We examine subspaces $S \subseteq \mathrm{Sim}_D(V, q)$.

Definition. $\kappa(\alpha; n) = \max\{s$: there exists a subspace of dimension s in $\mathrm{Sim}_D(V, q)$ for some n-dimensional quadratic space for which $\alpha < \mathrm{Sim}(V, q)\}$.

Then certainly $\kappa(\alpha; n) \leq \kappa_r(n)$ with equality if F is algebraically closed.

(1) If $n = 2^m \cdot$ (odd) then $\kappa(\alpha; n) = \kappa(\alpha; 2^m)$. Also $\kappa^{-\lambda}(\alpha; 4n) \geq 4 + \kappa^{\lambda}(\alpha; n)$.

(2) If $\alpha \simeq \langle 1, a\rangle$ then $\kappa(\alpha; n) = \kappa_2(n)$. If $\alpha \simeq \langle 1, a, b\rangle$ or $\alpha \simeq \langle 1, a, b, ab\rangle$ then $\kappa(\alpha; n) = \kappa_3(n)$.

(3) Suppose K is a field with a non-trivial involution and F is the fixed field of that involution, so that $K = F(\sqrt{-a})$. If (V, h) is a hermitian space over K define $\mathrm{Sim}_K(V, h)$ and note that comparable similarities span F-quadratic spaces. Define the corresponding Hurwitz–Radon function $\rho^{\mathrm{herm}}(n)$, where $n = \dim_K(V)$.

Let $B = \ell \circ h$ be the underlying F-bilinear form and let g be the action of $\sqrt{-a}$ on V. Then $\{1_V, g\}$ spans a subspace $R \subseteq \mathrm{Sim}(V, B)$ with $R \simeq \langle 1, a\rangle$. Then $S \subseteq \mathrm{Sim}_K(V, h)$ if and only if $S \subseteq \mathrm{Sim}_F(V, B)$ and S commutes with R. Consequently, if $n = 2^m \cdot$ (odd) then

$$\rho^{\mathrm{herm}}(n) = \kappa(\langle 1, a\rangle; 2n) = \kappa_2(2n) = 2m + 2.$$

(4) How does this analysis generalize to hermitian forms over a quaternion algebra?

(Hint. (2) The equalities for small values follow by considering the quadratic and quaternion algebras with prescribed norm forms.)

6. **More Hurwitz–Radon functions.** (1) Define $\rho^+(n) = \max\{k : C((k-1)\langle 1\rangle)$ has an n-dimensional module over $\mathbb{R}\}$. Let $n = 2^{4a+b}n_0$ where n_0 is odd and $0 \leq b \leq 3$. According to Lam (1973), p. 132, Theorem 4.8′, $\rho^+(n) = 8a+b+[b/3]+2$. (Here $[x]$ denotes the greatest integer function.) In our notation, $\rho^+(n) = 1 + \rho_1(n)$. "Explain" this result as in Exercise 3.

(2) Let D be the quaternion division algebra over $\mathbb{R}$. Let $\rho^D(n) = \max\{r$: $C((r-1)\langle -1\rangle)$ has an n-dimensional module over $D\}$. Then $\rho^D(n) = 8a + 2b + \frac{1}{2}(b+2)(3-b)$, according to Wolf (1963a), p. 437. Modify Exercise 3 to see that $\rho^D(n) = \max\{r : r\langle 1\rangle < \mathrm{Sim}_D(n\langle 1\rangle)\}$. Use Exercises 3, 4, 5 to show $\rho^D(n) = \kappa(3\langle 1\rangle; n) = \kappa_3(4n) = 1 + \rho_3(4n)$, which coincides with Wolf's formula.

7. **Hermitian compositions again.** Suppose $n = 2^m \cdot$ (odd).

(1) Recall the compositions (over $\mathbb{C}$) considered in Exercise 2.15. The formula has type 2 if each z_k if bilinear in $(X, \bar{X})$ and Y.

Proposition. *A type* 2 *composition of size* (r, n, n) *exists if and only if* $r \leq m+1$.
(2) $s \leq \rho^{\text{herm}}(n) = 2m+2$ if and only if there is a formula

$$(x_1^2 + x_2^2 + \cdots + x_s^2) \cdot (|y_1|^2 + \cdots + |y_n|^2) = |z_1|^2 + \cdots + |z_n|^2$$

where $X = (x_1, \ldots, x_s)$ is a system of real variables, $Y = (y_1, \ldots, y_n)$ is a system of complex variables and each z_k is $\mathbb{C}$-bilinear in X, Y. Write out some examples of such formulas.

(Hint. (1) From Exercise 2.15 such a composition exists iff there is an (r, r)-family in $\text{Sim}^{\text{herm}}(V, h)$ where $V = \mathbb{C}^n$ and h is the standard hermitian form. Clifford algebra representations imply $2r - 2 \leq 2m$. Conversely constructions over $\mathbb{R}$ provide an $(m+1, m+1)$-family in $\text{Sim}^{\text{herm}}(V, h)$.)

8. **Matrix factorizations.** Suppose $\sigma(X) = \sigma(x_1, \ldots, x_r)$ is a quadratic form. Recall that: $\sigma < \text{Sim}(n\langle 1\rangle)$ if and only if there exists an $n \times n$ matrix A whose entries are linear forms in X satisfying: $A^\top \cdot A = \sigma(X) \cdot I_n$. (Compare (1.9).) Define a somewhat weaker property: σ admits a *matrix factorization in order n* if there exist $n \times n$ matrices A, B whose entries are linear forms in X satisfying: $A \cdot B = \sigma(X) \cdot I_n$. If σ has such a factorization over F then so does every quadratic form similar to σ.

(1) **Proposition.** *Let* σ *be a quadratic form over* F. *Then* σ *admits a matrix factorization in order n if and only if there is a* $C_0(\sigma)$*-module of dimension n.*

In fact, any regular quadratic form σ possesses "essentially" just one matrix factorization.

(2) If $\sigma = \langle 1\rangle \perp \sigma_1$ represents 1 then $C_0(\sigma) \cong C(-\sigma_1)$ as ungraded F-algebras. Suppose F is an ordered field and σ is a positive definite form over F. Then σ admits a matrix factorization in order n over F if and only if $\sigma < \text{Sim}(q)$ for some n-dimensional positive definite form q over F.

(Hint. (1) ($\Longrightarrow$): Let (S, σ) be the given space. View A, B as linear maps $\alpha, \beta : S \to \text{End}(V)$, where $\dim V = n$. Define $\lambda : S \to \text{End}(V \oplus V)$ by: $\lambda = \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix}$. Then $\lambda(f)^2 = \sigma(f) \cdot 1_{V \oplus V}$ for every $f \in S$ so that $V \oplus V$ becomes $C(S, \sigma)$-module. It is a graded module as in Exercise 3.10(3), determined by the $C_0(\sigma)$-module V.

(2) See Exercise 3.)

9. **Conjugate families.** Let C and J_S be as usual. Suppose (V, q) and (V', q') are quadratic spaces admitting (C, J_S), with associated (s, t)-families $(S, T) \subseteq \text{Sim}(V, q)$ and $(S', T') \subseteq \text{Sim}(V', q')$. Then V and V' are C-similar if and only if $(S', T') = (fSf^{-1}, fTf^{-1})$ for some invertible $f \in \text{Sim}(V, V')$.

10. **Quaternion algebras.** Let A be a quaternion algebra over F, with the usual bar-involution. Recall that the norm and trace on A are defined by: $N(a) = a \cdot \bar{a}$ and $T(a) = a + \bar{a}$. Let φ be the norm form of A, so that $D_F(\varphi) = \{N(d) : d \in A^\bullet\}$ is the group of all norms. Let A_0 be the subspace of "pure" quaternions.

(1) If $a, b \in F^\bullet$ then $\langle a\rangle_A \simeq \langle b\rangle_A$ if and only if the classes of a, b coincide in $F^\bullet/D_F(\varphi)$.

(2) Two λ-hermitian spaces (V_i, h_i) are *similar* if $(V_2, h_2) \simeq (V_1, r \cdot h_1)$ for some $r \in F^\bullet$.

Lemma. *Let $a, b \in A_0^\bullet$. The following statements are equivalent.*

(i) *$\langle a\rangle_A$ and $\langle b\rangle_A$ are similar as skew-hermitian spaces.*

(ii) *$b = t \cdot da\bar{d}$ for some $t \in F^\bullet$ and some $d \in A^\bullet$.*

(iii) *$\langle N(a)\rangle = \langle N(b)\rangle$ in $F^\bullet/F^{\bullet 2}$.*

(3) It is harder to characterize isometry. The lemma above reduces the question to determining the "similarity factors" of the space $\langle a\rangle_A$. Suppose $a \in A_0^\bullet$ is given and let $x = N(a)$, so that the norm form is $\varphi \simeq \langle\langle x, y\rangle\rangle$ for some $y \in F^\bullet$.

If $t \in F^\bullet$ then: $\langle t \cdot a\rangle_A \simeq \langle a\rangle_A$ if and only if $t \in D_F(\langle\langle x\rangle\rangle) \cup -y \cdot D_F(\langle\langle x\rangle\rangle)$.

In particular: $\langle t \cdot a\rangle_A \simeq \langle a\rangle_A$ for every $t \in F^\bullet$ if and only if $D_F(\langle\langle x\rangle\rangle)$ is a subgroup of index 1 or 2 in $F^\bullet$.

(4) Let D be the quaternion division algebra over $\mathbb{R}$ with the "bar" involution. Isometry of hermitian spaces over D is determined by the dimension and the signature. Isometry of skew-hermitian spaces over D is determined by the dimension.

(Hint. (2) (iii) $\Longrightarrow$ (ii). Given $N(b) = s^2 \cdot N(a)$ for $s \in F^\bullet$, alter a to assume $N(b) = N(a)$.

Claim. There exists $u \in A^\bullet$ such that $b = uau^{-1}$. (If A is split this is standard linear algebra. Suppose A is a division algebra. If $b = -a$ choose $u \in F(a)^\perp$, otherwise let $u = a + b$.)

(3) Choose $b \in A_0$ with $ab = -ba$ and $N(b) = y$. From the isometry we have $t \cdot a = da\bar{d}$ for some $d \in A^\bullet$. Then $t = \lambda N(d)$ where $\lambda = \pm 1$, so that $\lambda ad = da$. If $\lambda = 1$ then $d \in F(a)$ while if $\lambda = -1$ then $d \in b \cdot F(a)$.)

11. **Associated Hermitian Forms.** Suppose $\sigma \simeq \langle 1, a_2, \ldots, a_s\rangle$ and let $C = C(-\sigma_1)$ and $J = J_S$ as usual. Let ℓ be the trace map with $\ell(1) = 1$ (as in Exercise 3.14). Then $J(e^\Delta)e^\Delta = a_\Delta$ where $\{e^\Delta\}$ is the derived basis. If (V, h) is a λ-hermitian space over C, the associated bilinear form $B = \ell \circ h$ is defined on V as in Proposition A.2 above. Given B we can reconstruct the hermitian form h explicitly as: $h(x, y) = \sum B((e^\Delta)^{-1}x, y)e^\Delta = \sum B(x, e^\Delta y)J(e^\Delta)^{-1}$.

12. Let (V, B) be a regular λ-symmetric bilinear space over F. Then the ring $E = \mathrm{End}(V)$ acts on V as well, and the form B admits $(\mathrm{End}(V), I_B)$. Use Proposition A.2 (with the usual trace map on $\mathrm{End}(V)$) to lift the form $B : V \times V \to F$ to a unique λ-hermitian form $h : V \times V \to \mathrm{End}(V)$. Exactly what is this form h?

(*Answer*: $h(u, v)(x) = B(x, v)u$ for all $x, u, v \in V$. Compare Exercise 1.13.)

13. Let C be semisimple F-algebra with involution. Then $C \cong A_1 \times \cdots \times A_k$ where the A_j are the simple ideals of C. Let e_j be the identity element of A_j and let V_j be an irreducible A_j-module, viewed as a C-module by setting $A_i V_j = 0$ if $i \neq j$.

(1) Every C-module is isomorphic to a direct sum of some of these V_j.

(2) Any involution J on C permutes $\{e_1, \ldots, e_k\}$. If $J(e_i) = e_j$ then $\hat{V}_i \cong V_j$.

(3) Under what conditions do all the unsplittable λ-spaces admitting (C, J) have the same dimension?

14. **Existence of an involution trace.** Generalize Definition 4.15, allowing K to be a field with involution ("bar"), requiring the involution on the algebra C to be compatible ($\overline{rc} = \bar{r} \cdot \bar{c}$), and replacing condition (4.15) (1) by: $\ell(\bar{c}) = \overline{\ell(c)}$

Proposition. *Every semisimple K-algebra C with involution has an involution trace $C \to K$.*

The proof is done in several steps:

(1) Every central simple K-algebra C with involution has an involution trace $C \to K$.

(2) If E/K is a finite extension of fields with involution, there is an involution trace $E \to K$. Consequently, if C is an E-algebra with involution having an involution trace $C \to E$ then there is an involution trace $C \to K$.

(3) The proposition follows by considering the simple components.

(Hint. (1) The reduced trace Trd always works. Every K-linear map $\ell : C \to K$ with $\ell(xy) = \ell(yx)$ must be a scalar multiple of Trd. (For $[C, C] = \text{span}\{xy - yx\}$ has codimension 1.)

15. **Homometric elements.** Let A be a ring with involution $J =$ "bar". Elements $a, b \in A$ are called *homometric* if $\bar{a}a = \bar{b}b$. If $u \in A$ is a "spectral unit", that is if $\bar{u}u = 1$, then a and ua are homometric. We say that (A, J) has the *homometric property* if the converse holds: if $\bar{a}a = \bar{b}b$ then a and b differ by a spectral unit.

(1) If A is a division ring then (A, J) has the homometric property.

(2) Suppose (A, J) has the homometric property and $a \in A$. If $\bar{a}a$ is nilpotent, then $a = 0$. Consequently A has no non-trivial nil ideals.

(3) Let $A = \text{End}(V)$ and $J = I_h$, where (V, h) is an anisotropic hermitian space over a field F with involution. (For example, $A \cong \mathbb{M}_n(\mathbb{C})$ with $J =$ conjugate-transpose.) Then (A, J) has the homometric property.

(4) What other semisimple rings with involution have the homometric property?

(Hint. (3) Given $f, g \in \text{End}(V)$. Then $\ker(\tilde{f}f) = \ker(f)$ and hence $\tilde{f}f(V) = \tilde{f}(V)$. If $\tilde{f}f = \tilde{g}g$ then $\tilde{f}(V) = \tilde{g}(V)$. Construct an isometry $\sigma : f(V) \to g(V)$. By Witt Cancellation, σ extends to an isometry $\varphi : V \to V$. Then $\bar{\varphi}\varphi = 1$ and $\varphi f = g$.)

Notes on Chapter 4

The proof of Proposition 4.9 follows Knebusch (1970), especially (3.2.1) and (3.3.2).

Exercises 4 and 5 are derived from §6 of Shapiro (1977a).

Exercise 8. Matrix factorizations of quadratic forms are investigated in Buchweitz, Eisenbud and Herzog (1987), where they are related to graded Cohen–Macauley modules over certain rings. A similar situation was studied by Eichhorn (1969), (1970). Matrix factorizations of forms of higher degrees are analyzed using generalized Clifford algebras by Backelin, Herzog and Sanders (1988).

Exercise 14. This follows Shapiro (1976), Proposition 4.4.

Exercise 15. See Rosenblatt and Shapiro (1989).

Chapter 5

Small (s, t)-Families

As a break from the general theory of algebras with involution we present some explicit examples of (σ, τ)-modules for small (s, t)-pairs. Since we are concerned with these (σ, τ)-modules up to F-similarity, we will work only with quadratic forms over F.

Good information is obtained for (σ, τ)-modules when the unsplittables have dimension at most 4. In these cases we can classify the (σ, τ)-modules in terms of certain Pfister factors. The smallest case where non-Pfister behavior can occur is for $(2, 2)$-families. The unsplittable $(\langle 1, a\rangle, \langle x, y\rangle)$-modules are analyzed using a new "trace" method. We obtain concrete examples where the unsplittable module is not similar to a Pfister form.

As a convenience to the reader we provide the proofs of the basic properties of Pfister forms, even though this theory appears in a number of texts. If q is a quadratic form recall that the *value set* and the *norm group* are:

$$D_F(q) = \{c \in F^\bullet : q \text{ represents } c\} \quad \text{and} \quad G_F(q) = \{c \in F^\bullet : \langle c\rangle q \simeq q\}.$$

One easily checks that $G_F(q) \cdot D_F(q) \subseteq D_F(q)$. A (regular) quadratic form φ is defined to be *round* if $G_F(\varphi) = D_F(\varphi)$. In particular this implies that the value set $D_F(n)$ is a multiplicative group. We will prove below that every Pfister form is round.

We need the notion of "divisibility" of quadratic forms:

$$\alpha \mid \beta \text{ means that } \beta \simeq \alpha \otimes \delta, \text{ for some quadratic form } \delta.$$

For anisotropic forms, we have seen in (3.20) that divisibility by a binary form $\langle 1, b\rangle = \langle\langle b\rangle\rangle$ is determined by behavior under a quadratic extension. We restate that result here since it is so important for motivating some of the later work.

5.1 Lemma. *Let q be an anisotropic quadratic form over F. If $q \otimes F(\sqrt{-b})$ is isotropic then $q \simeq \langle x\rangle\langle 1, b\rangle \perp q_1$ for some $x \in F^\bullet$ and some form q_1 over F. Consequently, $q \otimes F(\sqrt{-b})$ is hyperbolic iff $\langle\langle b\rangle\rangle \mid q$.*

Proof. See Lemma 3.20. □

5.2 Proposition. *Let ψ be a round form over F, and $\varphi = \langle\langle a\rangle\rangle \otimes \psi$ for some $a \in F^\bullet$.*

(1) *Then φ is also round. Consequently, every Pfister form is round.*

(2) *If φ is isotropic then it is hyperbolic.*

(3) *Suppose φ is a Pfister form and define the pure subform φ' by $\varphi \simeq \langle 1\rangle \perp \varphi'$. If $b \in D_F(\varphi')$ then $\langle\langle b\rangle\rangle \mid \varphi$.*

Proof. (1) Suppose φ represents c, say $c = x + ay$ where $x, y \in D_F(\psi) \cup \{0\}$. Suppose $x, y \neq 0$. (The other cases are easier and are left to the reader.) Comparing determinants we see that $\langle x, ay\rangle \simeq \langle c, caxy\rangle$. Since ψ is round $D_F(\psi) = G_F(\psi)$ is a group so that x, y and xy lie in $G_F(\psi)$. Then $\varphi \simeq \langle\langle a\rangle\rangle \otimes \psi \simeq \langle x, ay\rangle \otimes \psi \simeq \langle c\rangle\langle 1, axy\rangle \otimes \psi \simeq \langle c\rangle\langle\langle a\rangle\rangle \otimes \psi \simeq \langle c\rangle\varphi$ and consequently φ is round. An induction proof now shows that a Pfister form φ is round, for if $\dim \varphi = 2^m > 1$ then $\varphi \cong \langle\langle a\rangle\rangle \otimes \psi$ where ψ is another Pfister form.

(2) Since φ is isotropic there exist $x, y \in D_F(\psi)$ such that $x + ay = 0$. Then $-a = xy^{-1} \in G_F(\psi)$ so that $\varphi \simeq \langle\langle -xy^{-1}\rangle\rangle \otimes \psi \simeq \langle\langle -1\rangle\rangle \otimes \psi$ is hyperbolic.

(3) We are given $\varphi \simeq \langle\langle a\rangle\rangle \otimes \psi$ for a Pfister form ψ. Note that ψ remains round under any field extension. By hypothesis, $\varphi \simeq \langle 1, b, \ldots\rangle$. If φ is isotropic then by (2) it is hyperbolic and the conclusion is clear. Otherwise φ is anisotropic but $\varphi \otimes F(\sqrt{-b})$ is isotropic. But then $\varphi \otimes F(\sqrt{-b})$ is hyperbolic by (2) applied over this larger field, and (5.1) implies $\langle\langle b\rangle\rangle \mid \varphi$. □

The fundamental fact here is that Pfister forms are round. That is, a Pfister form φ has multiplicative behavior:

$$D_F(\varphi) \text{ is a subgroup of } F^\bullet.$$

Applying this to the form $2^m\langle 1\rangle$ we see that the set $D_F(2^m)$ of all non-zero sums of 2^m squares in F is closed under multiplication. (See Exercise 0.5 for another proof of this fact.)

If φ is any m-fold Pfister form over F, the element $\varphi(X)$ in $F(X) = F(x_1, \ldots, x_{2^m})$ is represented by the form $\varphi \otimes F(X)$, and the proposition implies that $\varphi(X)$ lies in $G_{F(X)}(\varphi \otimes F(X))$. Writing V for the underlying space of $\varphi \otimes F(X)$, this says that there exists a linear mapping $f : V \to V$ with $\varphi(f(v)) = \varphi(X)\varphi(v)$ for every $v \in V$. Writing this out in terms of matrices as done in Chapter 0, we obtain a multiplication formula

$$\varphi(X) \cdot \varphi(Y) = \varphi(Z),$$

where each entry z_k is linear in Y with coefficients in $F(X)$. Further information appears in the texts by Lam and Scharlau.

When the unsplittable (σ, τ)-modules have dimension ≤ 4 we characterize the unsplittables in terms of certain Pfister forms. In the discussion below we use the quadratic forms over F rather than working directly with modules over the Clifford algebras. The module approach provides more information but the proofs tend to be longer.

5.3 Proposition. *In the following table, every unsplittable (σ,τ)-module is F-similar to one of the forms q listed.*

(σ,τ)	q
$(\langle 1\rangle, \langle x\rangle)$ *where* $\langle x\rangle \not\simeq \langle 1\rangle$	$q \simeq \langle\langle w\rangle\rangle$ *where* $x \in G_F(q)$
$(\langle 1, a\rangle, 0)$	$q \simeq \langle\langle a\rangle\rangle$
$(\langle 1, a, b\rangle, 0)$	$q \simeq \langle\langle a, b\rangle\rangle$
$(\langle 1, a\rangle, \langle x\rangle)$ *where* $\langle 1, a, -x\rangle$ *is anisotropic*	$q \simeq \langle\langle a, w\rangle\rangle$ *where* $x \in G_F(q)$
$(\langle 1, a\rangle, \langle x, y\rangle)$ *where* $\langle axy\rangle \not\simeq \langle 1\rangle$ *and* $\langle 1, a, -x, -y\rangle$ *is isotropic*	$q \simeq \langle\langle a, w\rangle\rangle$ *where* $\langle\langle xy\rangle\rangle \mid q$
$(\langle 1, a, b, c\rangle, 0)$ *where* $\langle abc\rangle \not\simeq \langle 1\rangle$	$q \simeq \langle\langle a, b, w\rangle\rangle$ *where* $abc \in G_F(\langle\langle w\rangle\rangle)$
$(\langle 1, a, b\rangle, \langle x\rangle)$ *where* $\langle 1, a, b, -x\rangle$ *is anisotropic*	$q \simeq \langle\langle a, b, w\rangle\rangle$ *where* $\langle\langle abx\rangle\rangle \mid q$

Proof. We will do a few of these cases in detail, leaving the rest to the reader. First suppose $(\sigma,\tau) \simeq (\langle 1, a, b\rangle, 0)$, and $\sigma < \mathrm{Sim}(q)$ is unsplittable where q represents 1. Then (1.9) implies $\sigma \subset q$ so that $\dim q \geq 3$. Since $\sigma < \mathrm{Sim}(\langle\langle a, b\rangle\rangle)$, the Decomposition Theorem shows that $\dim q = 4$. Therefore $q \simeq \langle 1, a, b, d\rangle$ for some $d \in F^\bullet$. Since $\langle 1, a\rangle < \mathrm{Sim}(q)$ we know from an earlier case (or from (1.10)) that $\langle\langle a\rangle\rangle \mid q$, so that $\det q = \langle 1\rangle$. Then $\langle d\rangle = \langle ab\rangle$ and $q \simeq \langle\langle a, b\rangle\rangle$.

Suppose $(\sigma,\tau) = (\langle 1, a\rangle, \langle x, y\rangle)$ where $\langle axy\rangle \not\simeq \langle 1\rangle$ and $\langle 1, a, -x, -y\rangle$ is isotropic. Then $\langle 1, a\rangle$ and $\langle x, y\rangle$ represent some common value e. Scaling by e we get an equivalent pair of forms $(\langle e\rangle\langle 1, a\rangle, \langle e\rangle\langle x, y\rangle) \simeq (\langle 1, a\rangle, \langle 1, xy\rangle)$. There exist 4-dimensional (σ,τ)-modules, for example $\langle\langle a, xy\rangle\rangle$. Since $\langle axy\rangle \not\simeq \langle 1\rangle$ the unsplittables cannot have dimension 2, and the Decomposition Theorem implies that every unsplittable q has $\dim q = 4$. Since $\langle 1, a\rangle < \mathrm{Sim}(q)$ we know $q \simeq \langle\langle a, w\rangle\rangle$ for some w. Also since $\langle 1, xy\rangle < \mathrm{Sim}(q)$ we have $\langle\langle xy\rangle\rangle \mid q$. Conversely suppose $q \simeq \langle\langle a, w\rangle\rangle$ and $\langle\langle xy\rangle\rangle \mid q$. Then the form $\langle a, w, aw\rangle$ represents xy, so we can express $xy = ar^2 + wd$, for some $r \in F$ and $d \in D_F(\langle\langle a\rangle\rangle) \cup \{0\}$. Then $d \neq 0$, since $\langle axy\rangle \not\simeq \langle 1\rangle$, so that $q \simeq \langle\langle a, wd\rangle\rangle$ and $\langle a, wd\rangle$ represents xy. Therefore $(\langle 1, a\rangle, \langle 1, xy\rangle) \subset (\langle 1, a, wd\rangle, \langle 1, a, wd\rangle) < \mathrm{Sim}(q)$, and the result follows.

Suppose $(\sigma,\tau) \simeq (\langle 1, a, b, c\rangle, 0)$ where $\langle abc\rangle \not\simeq \langle 1\rangle$. There exist (σ,τ)-modules of dimension 8, for instance $\langle\langle a, b, c\rangle\rangle$. If q is an unsplittable module which represents 1, then $\langle 1, a, b, c\rangle \subset q$ and since $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ we also have $\langle\langle a, b\rangle\rangle \mid q$. If $\dim q = 4$ we contradict the hypothesis $\langle abc\rangle \not\simeq \langle 1\rangle$. Therefore $\dim q = 8$ and $q \simeq \langle\langle a, b, u\rangle\rangle$ for some u. Since $\langle 1, a, b, c\rangle \subset q$ we find $\langle ab\rangle \perp \langle u\rangle\langle\langle a, b\rangle\rangle$ represents c and therefore $\langle 1\rangle \perp \langle u\rangle\langle\langle a, b\rangle\rangle$ represents abc. Express $abc = r^2 + ue$ where $r \in F$ and $e \in D_F(\langle\langle a, b\rangle\rangle) \cup \{0\}$. Since $\langle abc\rangle \not\simeq \langle 1\rangle$ we find $e \neq 0$ and therefore $q \simeq \langle\langle a, b, ue\rangle\rangle$ and $\langle 1, ue\rangle$ represents abc. The desired shape for q follows when we set $w = ue$. The converse follows as before. □

In the small cases analyzed above we can go on to characterize *arbitrary* (σ, τ)-modules. For instance it immediately follows from (5.2) that $\langle 1, a\rangle < \mathrm{Sim}(q)$ if and only if $\langle\langle a\rangle\rangle \,|\, q$, and that $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ if and only if $\langle\langle a, b\rangle\rangle \,|\, q$. For the other cases we need a decomposition theorem for Pfister factors analogous to the Decomposition Theorem 4.1.

5.4 Definition. Let $\mathcal{M}$ be a set of (isometry classes of) quadratic forms over F. A quadratic form $q \in \mathcal{M}$ is *$\mathcal{M}$-indecomposable* if there is no non-trivial decomposition $q \simeq q_1 \perp q_2$ where $q_i \in \mathcal{M}$.

Certainly any form q in $\mathcal{M}$ can be expressed as $q \simeq q_1 \perp \cdots \perp q_k$ where each q_j is $\mathcal{M}$-indecomposable. We will get some results about the $\mathcal{M}$-indecomposables for some special classes $\mathcal{M}$. Generally if the φ_i are round forms and $b_j \in F^\bullet$ we consider the classes of the type

$$\mathcal{M} = \mathcal{M}(\varphi_1, \ldots, \varphi_k, b_1, \ldots, b_n) = \{q : \varphi_i \mid q \text{ and } b_j \in G_F(q) \text{ for every } i, j\}.$$

The $\mathcal{M}$-indecomposables are easily determined in a few small cases. For instance, for a single round form φ we see that q is $\mathcal{M}(\varphi)$-indecomposable if and only if q is similar to φ. For a single scalar $b \in F^\bullet$ where $\langle b\rangle \not\simeq \langle 1\rangle$, every $\mathcal{M}(b)$-indecomposable has dimension 2. (This is Dieudonné's Lemma of Exercise 2.9; also see Exercise 7.) The Proposition 5.6 below generalizes these two cases.

We first prove a lemma about "division" by round forms which is of some interest in its own right. Recall that $\mathbb{H} = \langle 1, -1\rangle$ is the hyperbolic plane and that any quadratic form q has a unique "Witt decomposition" $q = q_a \perp q_h$ where q_a is anisotropic and $q_h \simeq m\mathbb{H}$ is hyperbolic.

5.5 Lemma. *Suppose φ is a round form.*

(1) *If $\varphi \mid q$ and $a \in D_F(q)$ then $q \simeq \varphi \otimes \alpha$ for some form α which represents a. If $\varphi \mid q$ and q is isotropic with $\dim q > \dim \varphi$ then $q \simeq \varphi \otimes \alpha$ for some isotropic form α.*

(2) *If $\varphi \mid \alpha \perp \beta$ and $\varphi \mid \alpha$ then $\varphi \mid \beta$.*

(3) *Suppose φ is anisotropic. Then: $\varphi \mid m\mathbb{H}$ if and only if $\dim \varphi \mid m$. If $\varphi \mid q$ then $\varphi \mid q_a$ and $\varphi \mid q_h$, where $q = q_a \perp q_h$ is the Witt decomposition.*

Proof. (1) If $q \simeq \varphi \otimes \langle b_1, \ldots, b_n\rangle$ represents a then $a = b_1x_1 + \cdots + b_nx_n$ for some $x_j \in D_F(\varphi) \cup \{0\}$. Define $y_j = x_j$ if $x_j \neq 0$ and $y_j = 1$ if $x_j = 0$ and set $\alpha = \langle b_1y_1, \ldots, b_ny_n\rangle$. Then α represents a and since $\varphi \otimes \langle y_j\rangle \simeq \varphi$ we have $q \simeq \varphi \otimes \alpha$. If q is isotropic we use a non-trivial representation of $a = 0$. If the terms x_i above are not all 0 the previous argument works. Otherwise the non-triviality of the representation implies that φ must be isotropic and hence universal. Since φ is round this implies that $\langle c\rangle\varphi \simeq \varphi$ for every $c \in F^\bullet$. In particular, $\varphi \otimes \langle b_1, b_2\rangle \simeq \varphi \otimes \langle 1, -1\rangle$ and the result follows.

(2) Apply induction on $\dim \alpha$. If $a \in D_F(\alpha)$ then part (1) implies that $\alpha \perp \beta \simeq \langle a \rangle \varphi \perp \delta$ and $\alpha \simeq \langle a \rangle \varphi \perp \alpha_0$ for some forms δ and α_0 such that $\varphi \mid \delta$ and $\varphi \mid \alpha_0$. Cancelling we find that $\delta \simeq \alpha_0 \perp \beta$ and the induction hypothesis applies.

(3) Let $k = \dim \varphi$. The "if" part is clear since $\varphi \otimes \mathbb{H} \simeq k\mathbb{H}$. For the "only if" part we use induction on m, assuming $\varphi \mid m\mathbb{H}$. Since φ is anisotropic we know $k \leq m$. Part (1) implies that $m\mathbb{H} \simeq \varphi \otimes \alpha$ where α is isotropic. Expressing $\alpha \simeq \mathbb{H} \perp \alpha'$ we have $m\mathbb{H} \simeq k\mathbb{H} \perp (\varphi \otimes \alpha')$. If $k = m$ we are done. Otherwise, $\varphi \mid (m-k)\mathbb{H}$ and the induction hypothesis applies.

For the last statement let $q_h \simeq m\mathbb{H}$ and use induction on m. We may assume $m > 0$. Then q is isotropic and $\dim q > \dim \varphi$ (since φ is anisotropic). Part (1) implies that $q \simeq \varphi \otimes \alpha$ for some isotropic α. Expressing $\alpha \simeq \alpha' \perp \mathbb{H}$ we have $q_a \perp m\mathbb{H} \simeq q \simeq (\varphi \otimes \alpha') \perp k\mathbb{H}$ where $k = \dim \varphi$. Therefore $k \leq m$ and cancellation implies $\varphi \mid (q_a \perp (m-k)\mathbb{H})$. The result follows using the induction hypothesis. □

5.6 Proposition. *Suppose φ is a Pfister form and $b \in F^\bullet$. Then all $\mathcal{M}(\varphi, b)$-indecomposables have the same dimension and all $\mathcal{M}(\varphi, \langle\langle b \rangle\rangle)$-indecomposables have the same dimension.*

Proof. We will consider the case $\mathcal{M} = \mathcal{M}(\varphi, \langle\langle b \rangle\rangle)$ here, leaving the other to the reader. Suppose q is an $\mathcal{M}$-indecomposable which represents 1. If $\langle\langle b \rangle\rangle \mid \varphi$ it is clear that $q \simeq \varphi$.

Suppose $\langle\langle b \rangle\rangle \nmid \varphi$. By (5.5), $q \simeq \varphi \perp q_1$ and $\langle\langle b \rangle\rangle \subset q$. Then $b \in D_F(\varphi' \perp q_1)$ so that $b = x + y$ where $x \in D_F(\varphi') \cup \{0\}$ and $y \in D_F(q_1) \cup \{0\}$. If $y = 0$ then $b = x \in D_F(\varphi')$ and (5.2) (3) implies that $\langle\langle b \rangle\rangle \mid \varphi$, contrary to hypothesis. Then $y \neq 0$ and by (5.5) again we have $q_1 \simeq \langle y \rangle \varphi \perp q_2$ where $\varphi \mid q_2$, and therefore $q \simeq \varphi \otimes \langle\langle y \rangle\rangle \perp q_2$. Since $\alpha = \varphi \otimes \langle\langle y \rangle\rangle$ is a Pfister form and $\alpha' = \varphi' \perp \langle y \rangle \varphi$ represents b we know that $\langle\langle b \rangle\rangle \mid \alpha$ so that $\alpha \in \mathcal{M}$. By (5.5) (2) we also have $q_2 \in \mathcal{M}$. Since q is $\mathcal{M}$-indecomposable, q_2 must be 0 and $\dim q = 2 \cdot \dim \varphi$. □

Since φ is a Pfister form here we see that every $\mathcal{M}$-indecomposable is also a Pfister form.

5.7 Proposition. (1) $(\langle 1 \rangle, \langle x \rangle) < \mathrm{Sim}(q)$ *iff* $x \in G(q)$.

(2) $\langle 1, a \rangle < \mathrm{Sim}(q)$ *iff* $\langle\langle a \rangle\rangle \mid q$.

(3) $\langle 1, a, b \rangle < \mathrm{Sim}(q)$ *iff* $\langle\langle a, b \rangle\rangle \mid q$.

(4) $(\langle 1, a \rangle, \langle x \rangle) < \mathrm{Sim}(q)$ *iff* $\langle\langle a \rangle\rangle \mid q$ *and* $x \in G(q)$.

(5) *If* $\langle 1, a, -x, -y \rangle$ *is isotropic, then* $(\langle 1, a \rangle, \langle x, y \rangle) < \mathrm{Sim}(q)$ *iff* $\langle\langle a \rangle\rangle \mid q$ *and* $\langle\langle xy \rangle\rangle \mid q$.

(6) $\langle 1, a, b, c \rangle < \mathrm{Sim}(q)$ *iff* $q \simeq \langle\langle a, b \rangle\rangle \otimes \gamma$ *where* $abc \in G_F(\gamma)$.

(7) $(\langle 1, a, b \rangle, \langle x \rangle) < \mathrm{Sim}(q)$ *iff* $\langle\langle a, b \rangle\rangle \mid q$ *and* $\langle\langle abx \rangle\rangle \mid q$.

Proof. We will prove the last two, omitting the others. Suppose $\langle 1, a, b, c\rangle < \mathrm{Sim}(q)$. If $\langle abc\rangle \simeq \langle 1\rangle$ the result is easy, so suppose $\langle abc\rangle \not\simeq \langle 1\rangle$. If $\langle 1, a, b, c\rangle < \mathrm{Sim}(q)$ then q is a sum of unsplittables of the type listed in (5.3), and it follows that $q \simeq \langle\langle a, b\rangle\rangle \otimes \gamma$ where $abc \in G_F(\gamma)$. Conversely suppose q is given in this way. Since $\langle abc\rangle \not\simeq \langle 1\rangle$, Proposition 5.6 implies that the $\mathcal{M}(abc)$-indecomposables all have dimension 2. Therefore $\gamma \simeq \gamma_1 \perp \cdots \perp \gamma_r$ where $\dim \gamma_j = 2$ and $\gamma_j \in \mathcal{M}(abc)$. Then $\gamma_j \simeq \langle u_j\rangle\langle\langle w_j\rangle\rangle$ where $abc \in G_F(\langle\langle w_j\rangle\rangle)$ and we get $q \simeq q_1 \perp \cdots \perp q_r$ where $q_j \simeq \langle u_j\rangle\langle\langle a, b, w_j\rangle\rangle$. Again by Proposition 5.3 we conclude that $\langle 1, a, b, c\rangle < \mathrm{Sim}(q)$.

Now consider the case $(\langle 1, a, b\rangle, \langle x\rangle)$. If $\langle 1, a, b\rangle$ represents x then $\langle\langle abx\rangle\rangle \,|\, \langle\langle a, b\rangle\rangle$ and $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ if and only if $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q)$. Therefore we may assume $\langle 1, a, b, -x\rangle$ is anisotropic. If $(\langle 1, a, b\rangle\langle x\rangle) < \mathrm{Sim}(q)$ then $q \simeq q_1 \perp \cdots \perp q_r$ where each $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q_j)$ is unsplittable. By Proposition 5.3 we have $\langle\langle a, b\rangle\rangle \mid q_j$ and $\langle\langle abx\rangle\rangle \mid q_j$, and the claim follows. Conversely suppose that $q \in \mathcal{M} = \mathcal{M}(\langle\langle a, b\rangle\rangle, \langle\langle abx\rangle\rangle)$. Then $q \simeq q_1 \perp \cdots \perp q_r$ where each q_j is $\mathcal{M}$-indecomposable. Since $\langle 1, a, b, -x\rangle$ is anisotropic we see that $\langle\langle abx\rangle\rangle \nmid \langle\langle a, b\rangle\rangle$ and Proposition 5.6 implies that $\dim q_j = 8$. Therefore $q_j \simeq \langle u_j\rangle\langle\langle a, b, w_j\rangle\rangle$ where $\langle\langle abx\rangle\rangle \mid q_j$. Apply (5.3) again to conclude that $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q_j)$ for each j and therefore $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q)$. □

The rest of this chapter is concerned with the more difficult case of (2, 2)-families. Let $(\sigma, \tau) = (\langle 1, a\rangle, \langle x, y\rangle)$. The case when $\langle 1, a, -x, -y\rangle$ is isotropic is included in Proposition 5.7. If $\langle axy\rangle \simeq \langle 1\rangle$ then $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(q)$ iff $(\langle 1, a\rangle, \langle x\rangle) < \mathrm{Sim}(q)$, by the Expansion Lemma. This case is also included in (5.7). Therefore let us assume that

$$\langle 1, a, -x, -y\rangle \text{ is anisotropic and } \langle axy\rangle \not\simeq \langle 1\rangle.$$

Let $C = C(\langle -a, x, y\rangle)$ be the associated Clifford algebra. Then the center of C is isomorphic to the field $E = F(\sqrt{axy})$ and C is a quaternion algebra over E. It follows that C is a division algebra (this is part of Exercise 3.16) and every unsplittable (σ, τ)-module has dimension 8. Let J_S denote the usual involution on C.

If $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(V, q)$ then we have $\langle\langle a\rangle\rangle \mid q$, $\langle\langle xy\rangle\rangle \mid q$ and $x \in G_F(q)$. It is not so clear whether the converse holds: do those "divisibility" conditions on q always imply the existence of the (2, 2)-family? Those conditions do provide some motivation for the following approach.

To say that $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(V, q)$ is equivalent to saying that (V, q) is a quadratic (C, J_S)-module. In this case we have $f_2, g_1, g_2 \in \mathrm{End}(V)$ which satisfy the familiar rules listed in Lemma 2.3. Then $f = f_2$ satisfies $\tilde{f} = -f$ and $f^2 = -a \cdot 1$ so it corresponds to the subspace $\langle 1, a\rangle < \mathrm{Sim}(q)$. Similarly $g = g_1 g_2$ satisfies $\tilde{g} = -g$ and $g^2 = -xy \cdot 1$ so that g corresponds to $\langle 1, xy\rangle < \mathrm{Sim}(q)$. Since f and g commute, they induce an action of the field $K = F(\sqrt{-a}, \sqrt{-xy})$ on the vector space V. Let J be the involution of K sending $\sqrt{-a}$ and $\sqrt{-xy}$ to their negatives. Then (V, q) becomes a quadratic (K, J)-module. Naturally we may view K as a subfield of C

where J is the restriction of J_S to K. Note that $E = F(\sqrt{axy})$ is the subfield of K which is fixed by J. We often write "bar" for J when there is no ambiguity.

Conversely, if (V, q) is a quadratic (K, J)-module, what further information is needed to make it a (C, J_S)-module?

5.8 Lemma. *Suppose (K, J) is the field with involution described above and (V, q) is a quadratic (K, J)-module. This structure extends to make (V, q) into a (C, J_S)-module if and only if there exists $k \in \mathrm{End}_F(V)$ such that k is (K, J)-semilinear, $\tilde{k} = k$, and $k^2 = x \cdot 1$.*

Proof. The (K, J)-semilinearity of k means that $k(\alpha v) = \bar{\alpha} k(v)$ for every $\alpha \in K$ and $v \in V$. This is equivalent to saying that k anticommutes with f and g. If the (C, J_S)-module structure is given, just define $k = g_1$. Conversely, given the (K, J)-module structure and given k, define $f_2 = f$, $g_1 = k$, $g_2 = k^{-1}g$ and verify that they provide the desired (2, 2)-family. □

Suppose (V, q) is a (K, J)-module. Then the symmetric bilinear form $b_q : V \times V \to F$ is the "transfer" of a hermitian form over K. This is a special case of Proposition A.2 of Chapter 4, applied to the algebra $C = K$. In fact if $s : K \to F$ is an involution trace then there exists a unique hermitian form $h : V \times V \to K$ such that $b_q = s \circ h$. (See Exercise 16.) This hermitian space (V, h) is an orthogonal sum of some 1-dimensional spaces over K:

$$(V, h) \simeq \langle \theta_1, \theta_2, \ldots, \theta_m \rangle_K \quad \text{for some } \theta_i \in E^\bullet.$$

These diagonal entries θ_i lie in E since they must be symmetric: $\bar{\theta}_i = \theta_i$.

To do calculations we must choose an involution trace. First note that $K = E(\sqrt{-a})$ and define $\mathrm{tr} : K \to E$ by setting $\mathrm{tr}(1) = 1$ and $\mathrm{tr}(\sqrt{-a}) = 0$. (This is the unique involution trace from K to E, up to scalar multiple.) Since the involution on $E = F(\sqrt{axy})$ is trivial there are many involution traces from E to F. We will use the standard one employed in quadratic form theory, namely $\ell : E \to F$ defined by setting $\ell(1) = 0$ and $\ell(\sqrt{axy}) = 1$. If $\theta \in E^\bullet$ then the 1-dimensional hermitian space $\langle \theta \rangle_K$ over K transfers down to a 4-dimensional quadratic space $\ell \circ \mathrm{tr}(\langle \theta \rangle_K)$ over F.

5.9 Lemma. *Suppose $\theta \in E^\bullet$. Then $\ell \circ \mathrm{tr}(\langle \theta \rangle_K) \simeq \langle s \rangle \langle\langle a, -N\theta \rangle\rangle$ over F.*

Proof. Here N is the field norm $N_{E/F}$. If $\theta = r + s\sqrt{axy}$ then $N(\theta) = r^2 - axys^2$. The 1-dimensional hermitian space $\langle \theta \rangle_K$ can be viewed as the K-vector space K with the form $h : K \times K \to K$ given by $h(x, y) = \theta x \bar{y}$. If $b = \mathrm{tr} \circ h$ then $b(u, v) = \theta \cdot \mathrm{tr}(u\bar{v})$. If $u = u_1 + u_2\sqrt{-a}$ and $v = v_1 + v_2\sqrt{-a}$ we find that $\mathrm{tr}(u\bar{v}) = u_1v_1 + au_2v_2$, so that $\mathrm{tr}(\langle \theta \rangle_K) \simeq \langle \theta, a\theta \rangle_E$ as quadratic forms over E. To transfer the quadratic form $\langle \theta \rangle_E$ from $E = F(\sqrt{axy})$ down to F, we compute the inner products (relative to this form) of the basis elements $\{1, \sqrt{axy}\}$ to find the

Gram matrix $\begin{pmatrix} s & r \\ r & axys \end{pmatrix}$. Since it represents s and has determinant $-N(\theta)$, we have $\ell(\langle\theta\rangle_E) \simeq \langle s\rangle\langle\langle -N\theta\rangle\rangle$, provided $s \neq 0$. If $s = 0$ that form is isotropic, hence is $\mathbb{H}$. The result now follows since $\ell \circ \mathrm{tr}(\langle\theta\rangle_K) = \ell(\langle\theta\rangle_E) \perp \langle a\rangle\ell(\langle\theta\rangle_E)$. □

Remark. If $\theta, \theta' \in E^\bullet$ then $\langle\theta\rangle_K \simeq \langle\theta'\rangle_K$ as hermitian spaces over K if and only if $\theta' = \alpha\bar{\alpha}\theta$ for some $\alpha \in K^\bullet$. (For a K-linear map $K \to K$ must be multiplication by some $\alpha \in K$.) If such α exists then the transferred quadratic forms over F must also be isometric.

Our goal is to construct unsplittable modules (V, q) for the (2, 2)-pair $(\langle 1, a\rangle, \langle x, y\rangle)$. Then $\dim_F V = 8$ and $\dim_K V = 2$ using the induced (K, J)-action, and we view (V, q) as the transfer of a hermitian space $(V, h) = \langle\theta_1, \theta_2\rangle_K$. Given such a hermitian space over K, we will find conditions on θ_1 and θ_2 which imply that this (K, J)-action can be extended to an action of (C, J_S).

5.10 Lemma. *Suppose (V, q) is the transfer of the hermitian space $(V, h) = \langle\theta_1, \theta_2\rangle_K$. The following statements are equivalent, where $\theta = \theta_1\theta_2$.*

(1) *(V, q) is a (C, J_S)-module in a way compatible with the given (K, J)-action.*

(2) *$\langle 1, \theta\rangle_K$ represents x, that is, $\alpha\bar{\alpha} + \theta\beta\bar{\beta} = x$ for some $\alpha, \beta \in K^\bullet$.*

(3) *$\langle 1, a, \theta, a\theta\rangle$ represents x over E.*

(4) *$-\theta \in D_E(\langle\langle a, -x\rangle\rangle)$.*

Proof. We use a matrix formulation of (1) to show its equivalence with (2). By (5.8), condition (1) holds if and only if there exists $k \in \mathrm{End}_F(V)$ which is (K, J)-semilinear, $\tilde{k} = k$ and $k^2 = x \cdot 1$. We are given a K-basis $\{v_1, v_2\}$ of V such that $h(v_i, v_i) = \theta_i$ and $h(v_1, v_2) = 0$. Representing a vector $v = x_1v_1 + x_2v_2$ in V as a column vector $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, the (K, J)-semilinear map k is represented by a matrix $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ where $\alpha, \beta, \gamma, \delta \in K$. This is done so that $k(v) = x_1'v_1 + x_2'v_2$ is represented by the column vector $X' = A\bar{X}$.

The adjoint map $\tilde{k}$ is also (K, J)-semilinear and has matrix $\tilde{A} = M^{-\top}A^\top M$ where $M = \begin{pmatrix} \theta_1 & 0 \\ 0 & \theta_2 \end{pmatrix}$ is the matrix of the hermitian form. (See Exercise 15 for more details.) The symmetry condition $\tilde{k} = k$ is equivalent to the symmetry of the matrix $MA = \begin{pmatrix} \theta_1\alpha & \theta_1\gamma \\ \theta_2\beta & \theta_2\delta \end{pmatrix}$. This condition holds if and only if $\theta_2\beta = \theta_1\gamma$. Define $\theta = \theta_2/\theta_1$ (which has the same square class in $E^\bullet$ as $\theta_1\theta_2$). Then the symmetry condition becomes: $\gamma = \theta\beta$.

The condition $k^2 = x \cdot 1$ becomes the matrix equation $A\bar{A} = xI$ (see Exercise 15). On multiplying this out when $A = \begin{pmatrix} \alpha & \theta\beta \\ \beta & \delta \end{pmatrix}$ we find it to be equivalent to the

following equations:

$$\alpha\bar{\beta} = -\beta\bar{\delta}, \quad \alpha\bar{\alpha} = \delta\bar{\delta}, \quad \alpha\bar{\alpha} + \theta\beta\bar{\beta} = x.$$

If $\beta = 0$ then $\alpha\bar{\alpha} = x$ so that $x \in D_E(\langle 1, a\rangle)$ and $\langle 1, a, -x\rangle_E$ is isotropic over E. We know that $C = \left(\frac{-a,x}{E}\right)$ is a quaternion division algebra, so its norm form $\langle\langle a, -x\rangle\rangle_E$ is anisotropic over E. This is a contradiction.

Therefore $\beta \neq 0$ and $\delta = -\bar{\alpha}\beta\bar{\beta}^{-1}$. With this formula for δ the first two equations above are automatic. Therefore statement (1) holds if and only if there exist $\alpha, \beta \in K$ such that $\alpha\bar{\alpha} + \theta\beta\bar{\beta} = x$. This is statement (2).

The equivalence of statements (2) and (3) is clear since $\{\alpha\bar{\alpha} : \alpha \in K\} = D_E(\langle 1, a\rangle)$. Finally note that (3) holds if and only if $\langle\langle a, -x, \theta\rangle\rangle$ is hyperbolic over E, if and only if $\langle\langle a, -x\rangle\rangle$ represents $-\theta$ over E. Therefore (3) and (4) are equivalent. □

In the statement of Lemma 5.10 the symmetry between x and y is not apparent. However, since $\langle axy\rangle_E \simeq \langle 1\rangle_E$ we may note that $\langle 1, a, -x, -y\rangle_E \simeq \langle\langle a, -x\rangle\rangle_E \simeq \langle\langle a, -y\rangle\rangle_E$.

The payoff of these calculations can now be summarized.

5.11 Proposition. *Suppose $a, x, y \in F^\bullet$ such that $\langle axy\rangle \not\simeq \langle 1\rangle$ and $\langle 1, a, -x, -y\rangle$ is anisotropic. Let $E = F(\sqrt{axy})$ and let $N = N_{E/F}$ be the norm. If q is a quadratic form over F with $\dim q = 8$, then the following statements are equivalent:*

(1) $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(q)$.

(2) *There exist $\theta_i = r_i + s_i\sqrt{axy}$ in $E^\bullet$ such that $q \simeq \langle s_1\rangle\langle\langle a, -N\theta_1\rangle\rangle \perp \langle s_2\rangle\langle\langle a, -N\theta_2\rangle\rangle$ and such that $-\theta_1\theta_2 \in D_E(\langle\langle a, -x\rangle\rangle)$.*

Proof. Here, as before, if $s_i = 0$ the corresponding term in the expression for q is interpreted as $2\mathbb{H}$. This equivalence is obtained by combining (5.9) and (5.10). □

As one immediate consequence we see that $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(4\mathbb{H})$ for every a, x, y. To prove the next corollary we use the following "Norm Principle".

5.12 Lemma. *Let $E = F(\sqrt{d})$ be a quadratic extension, let φ be a Pfister form over F and let $\theta \in E^\bullet$. Then $\theta \in F^\bullet \cdot D_E(\varphi_E)$ if and only if $N\theta \in D_F(\varphi)$.*

Proof. See Elman and Lam (1976). The proof is outlined in Exercise 17. □

5.13 Corollary. *Suppose $a, x, y \in F^\bullet$ as above and suppose φ is a 2-fold Pfister form. The following are equivalent.*

(1) $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(\varphi \perp 2\mathbb{H})$.

(2) $\varphi \cong \langle\langle a, -c\rangle\rangle$ *for some* $c \in D_F(\langle\langle -axy\rangle\rangle) \cap D_F(\langle\langle a, -x\rangle\rangle)$.

Proof. (1) $\Longrightarrow$ (2). By (5.5) $\langle\langle a\rangle\rangle \mid \varphi$ so that $\varphi \simeq \langle\langle a, w\rangle\rangle$ for some w. Furthermore $\varphi \perp 2\mathbb{H} \simeq \langle s_1\rangle\langle\langle a, -N\theta_1\rangle\rangle \perp \langle s_2\rangle\langle\langle a, -N\theta_2\rangle\rangle$ for θ_i as in (5.11). Computing Witt invariants we find that $\varphi \simeq \langle\langle a, -c\rangle\rangle$ where $c = N(\theta_1\theta_2) \in D_F(\langle\langle -axy\rangle\rangle)$. Since $-\theta_1\theta_2 \in D_E(\langle\langle a, -x\rangle\rangle)$ the lemma implies that $c \in D_F(\langle\langle a, -x\rangle\rangle)$.

(2) $\Longrightarrow$ (1). We may express $c = N\theta \in D_F(\langle\langle a, -x\rangle\rangle)$. If $\langle c\rangle \simeq \langle 1\rangle$ the claim is vacuous, so we may assume that $\theta \notin F$. By the lemma we find that $\theta = t \cdot \theta_1$ where $t \in F^\bullet$ and $-\theta_1 \in D_E(\langle\langle a, -x\rangle\rangle)$. Let $\theta_2 = 1$ and apply (5.11) to conclude that $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(q)$ where $q \simeq \langle s_1\rangle\langle\langle a, -N\theta_1\rangle\rangle \perp 2\mathbb{H}$. Then $\langle s_1\rangle q \simeq \langle\langle a, -c\rangle\rangle \perp 2\mathbb{H}$ and the result follows. □

Example 1. Let $a = 1$, $x = -1$ and $y = -2$ over the rational field $\mathbb{Q}$. Then $\langle 1, a, -x, -y\rangle \simeq \langle 1, 1, 1, 2\rangle$ is anisotropic and $\langle axy\rangle \simeq \langle 2\rangle \not\simeq \langle 1\rangle$. If φ is a 2-fold Pfister form then (5.13) says: $(\langle 1, 1\rangle, \langle -1, -2\rangle) < \mathrm{Sim}(\varphi \perp 2\mathbb{H})$ if and only if $\varphi \simeq \langle\langle 1, -c\rangle\rangle$ for some $c \in D_{\mathbb{Q}}(\langle\langle -2\rangle\rangle) \cap D_{\mathbb{Q}}(\langle\langle 1, 1\rangle\rangle)$. For example

$$(\langle 1, 1\rangle, \langle -1, -2\rangle) < \mathrm{Sim}(q) \quad \text{where } q = \langle\langle 1, -7\rangle\rangle \perp 2\mathbb{H}.$$

To get anisotropic examples we use the criterion in (5.11). To deduce that a form $\langle 1, a, -x, -ax, \theta\rangle_E$ is isotropic over an algebraic number field we need only check (by the Hasse–Minkowski Theorem) that it is indefinite relative to every ordering of E.

Example 2. Let $a = 1$, $x = 7$ and $y = 14$ over $\mathbb{Q}$. Then $\langle axy\rangle \simeq \langle 2\rangle \not\simeq \langle 1\rangle$ and $\langle 1, a, -x, -y\rangle \simeq \langle 1, 1, -7, -14\rangle$ is anisotropic. (In fact it is anisotropic over the field $\mathbb{Q}_7$.) Furthermore $E = \mathbb{Q}(\sqrt{2})$, and $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-2})$. For any $\theta \in E^\bullet$ the form $\langle\langle a, -x\rangle\rangle \perp \langle -\theta\rangle = \langle 1, 1, -7, -7, \theta\rangle$ is isotropic over $E = \mathbb{Q}(\sqrt{2})$ since it is indefinite at both orderings. Using $\theta_1 = 1 + \sqrt{2}$ and $\theta_2 = 1 + 2\sqrt{2}$ we find:

$$(\langle 1, 1\rangle, \langle 7, 14\rangle) < \mathrm{Sim}(q) \quad \text{where } q = \langle\langle 1, 1\rangle\rangle \perp \langle\langle 1, 7\rangle\rangle \simeq \langle\langle 1\rangle\rangle \otimes \langle 1, 1, 1, 7\rangle.$$

This form q is anisotropic but is not similar to a Pfister form.

Many further examples can be constructed along these lines. Non-Pfister unsplittables for larger (s, t)-families can be found using the Construction and Shift Lemmas. The smaller families considered earlier in this chapter were all characterized by certain "division" properties of quadratic forms. If $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(q)$ then certainly $\langle\langle a\rangle\rangle \mid q$, $\langle\langle xy\rangle\rangle \mid q$ and $x \in G_F(q)$. Is it possible that these three independent conditions suffice? Certainly this converse fails for simple reasons of dimensions: the 4-dimensional form $2\mathbb{H}$ always satisfies these divisibility conditions, but the dimensions of the unsplittables may be 8. We modify the conjecture as follows:

5.14 Question. If $\dim q = 8$ and $\langle\langle a\rangle\rangle \mid q$, $\langle\langle xy\rangle\rangle \mid q$ and $x \in G_F(q)$ does it follow that $(\langle 1, a\rangle, \langle x, y\rangle) < \mathrm{Sim}(q)$?

We may assume that $\langle 1, a, -x, -y\rangle$ is anisotropic and $\langle axy\rangle \not\simeq \langle 1\rangle$ since the other cases are settled by Proposition 5.7. The answer is unknown in general. In Chapter 10 we succeed in proving the answer to be "yes" when F is a global field. As the ideas used to prove (5.7) indicate, the following question is relevant.

5.15 Question. If $\mathcal{M} = \mathcal{M}(\langle\langle a\rangle\rangle, \langle\langle xy\rangle\rangle, x)$ what are the dimensions of the $\mathcal{M}$-indecomposables?

We will see in Chapter 10 that over a global field the indecomposables must have dimension 2 or 4. It is unknown what dimensions are possible over arbitrary fields.

The following observation is interesting (and perhaps surprising) in light of the $F \subseteq E \subseteq K$ set-up used above. To simplify notations we use b in place of xy here.

5.16 Proposition. *Suppose $\langle a\rangle \not\simeq \langle b\rangle$ over F. Let $K = F(\sqrt{-a}, \sqrt{-b})$ with involution J as above. The following statements are equivalent for a quadratic space (V, q) over F.*

(1) *$\langle\langle a\rangle\rangle \mid q$ and $\langle\langle b\rangle\rangle \mid q$.*

(2) *(V, q) can be made into a (K, J)-module.*

Proof. (2) $\Longrightarrow$ (1). Given the (K, J)-module (V, q) let $f = \mathcal{L}(\sqrt{-a})$ be the multiplication map on V. Then $f \in \mathrm{End}(V)$ and $f^2 = -a \cdot 1$. Since q admits (K, J) and $J(\sqrt{-a}) = -\sqrt{-a}$ we know that $\tilde{f} = -f$. Therefore $\{1_V, f\}$ span a space of similarities $\langle 1, a\rangle < \mathrm{Sim}(V, q)$ and we conclude that $\langle\langle a\rangle\rangle \mid q$ by (1.10). Similarly using $g = \mathcal{L}(\sqrt{-b})$ we find $\langle\langle b\rangle\rangle \mid q$.

(1) $\Longrightarrow$ (2). It suffices to settle the case $\dim q = 4$. This follows from (5.6) since the $\mathcal{M}(\langle\langle a\rangle\rangle, \langle\langle b\rangle\rangle)$-indecomposables are 4-dimensional. Given $\dim q = 4$ and $\langle\langle a\rangle\rangle \mid q$ we know there exists $f \in \mathrm{End}(V)$ with $\tilde{f} = -f$ and $f^2 = -a \cdot 1$. Similarly since $\langle\langle b\rangle\rangle \mid q$ there exists $g \in \mathrm{End}(V)$ with $\tilde{g} = -g$ and $g^2 = -b \cdot 1$. The difficulty is to find such f, g which commute.

We may assume q represents 1. By hypothesis, $q \simeq \langle\langle a, c\rangle\rangle \simeq \langle\langle b, d\rangle\rangle$ for some $c, d \in F^\bullet$. In fact we may assume $c = d$, (see Exercise 19) so that

$$q \simeq \langle\langle c, a\rangle\rangle \simeq \langle\langle c, b\rangle\rangle \text{ and } \langle a, ac\rangle \text{ represents } b.$$

Let $\{v_1, w_1, v_2, w_2\}$ be the orthogonal basis corresponding to $q \simeq \langle 1, c, a, ac\rangle$ and define f by setting $f(v_1) = v_2$, $f(v_2) = -av_1$ and similarly for the w_i's. Then $\tilde{f} = -f$ and $f^2 = -a \cdot 1$. The matrix of f can be expressed as a Kronecker product: $f = \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $\{v_1, w_1, \hat{v}_2, \hat{w}_2\}$ be a basis corresponding to $q \simeq \langle 1, c, b, bc\rangle$ and define g analogously using this new basis, so that $\tilde{g} = -g$ and $g^2 = -b \cdot 1$. To compute g explicitly, express $b = ax^2 + acy^2$ for some $x, y \in F$, and use $\hat{v}_2 = xv_2 + yw_2$