and $\hat{w}_2 = ycv_2 - xw_2$. The matrix of g (relative to the original basis) becomes: $g = \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} x & cy \\ y & -x \end{pmatrix}$. It is now easy to see that $fg = gf$. □

Exercises for Chapter 5

1. Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an unsplittable (s,t)-family where σ represents 1 and $\dim q \leq 8$. If $(s,t) \neq (2,2)$ then q must be similar to a Pfister form.

2. Complete Proposition 5.7 by listing all q such that $(\sigma, \tau) < \mathrm{Sim}(q)$, where (σ, τ) equals:

(i) $(\langle 1, a\rangle, \langle x, y\rangle)$ with $\langle axy\rangle \simeq \langle 1\rangle$.

(ii) $(\langle 1\rangle, \langle x, y\rangle)$.

(iii) $(\langle 1\rangle, \langle x, y, z\rangle)$.

3. (i) Give a simple direct proof that if $(\langle 1, a, b\rangle, \langle x\rangle) < \mathrm{Sim}(q)$ then $\langle 1, abx\rangle < \mathrm{Sim}(q)$.

(ii) Find some a, b, x, q such that $\langle\langle a, b\rangle\rangle \mid q$ and $x \in G_F(q)$ but $(\langle 1, a, b\rangle, \langle x\rangle)$ is not realizable in $\mathrm{Sim}(q)$.

4. **Round forms.** (1) **Lemma.** *A quadratic space (V, φ) is round iff the group* $\mathrm{Sim}^\bullet(V, \varphi)$ *acts transitively on the set $V^\bullet$ of anisotropic vectors.*

(2) Recall that any (regular) quadratic form q has a *Witt decomposition* $q \simeq q_a \perp q_h$ where q_a is anisotropic and q_h is hyperbolic. These components are unique up to isometry. An isotropic form φ is round iff φ_a is round and universal.

5. **Level of a field.** If $d \in F$ define $\mathrm{length}_F(d)$ to be the smallest n such that d is a sum of n squares in F. That is, $n = \mathrm{length}_F(d) \iff d \in D_F(n) - D_F(n-1)$. If d is not a sum of squares then $\mathrm{length}_F(d) = \infty$. The *level* (or Stufe) of F is: $s(F) = \mathrm{length}_F(-1)$.

(1) **Proposition.** *If $s(F)$ is finite then $s(F) = 2^m$ for some m.*

(2) Suppose $K = F(\sqrt{-d})$. Then $s(K)$ is finite $\iff \mathrm{length}_F(d)$ is finite. It is each to check that $s(K) \leq \mathrm{length}_F(d)$.

Proposition. *Suppose $K = F(\sqrt{-d})$ and define m by:* $2^m \leq \mathrm{length}_F(d) < 2^{m+1}$. *Then $s(K) = 2^m$.*

(Hint. (1) Suppose $-1 = a_1^2 + \cdots + a_s^2$ and suppose $2^m \leq s < 2^{m+1}$. To prove: $-1 \in D_F(2^m)$. If $n = 2^m$ then $-(1 + a_{n+1}^2 + \cdots + a_s^2) = (a_1^2 + \cdots + a_n^2)$. By (5.2) or Exercise 0.5, $D_F(2^m)$ is a group.

(2) $s(K) \leq \mathrm{length}_F(d)$ implies $s(K) \leq 2^m$ by (1). If $s(K) = n$ then $-1 = \sum_{i=1}^n (a_i + b_i\sqrt{-d})^2$ so that $d \cdot \sum_{i=1}^n b_i^2 = 1 + \sum_{i=1}^n a_i^2$ and $\sum_{i=1}^n a_i b_i = 0$. Then

$d = \left(\sum_{i=1}^{n} b_i^2\right)^{-1} + \left(\sum_{i=1}^{n} a_i^2\right) \cdot \left(\sum_{i=1}^{n} b_i^2\right)^{-1}$, and the first term of a sum of n squares. Since n is a 2-power the second term is a sum of $n-1$ squares, using Exercise 0.5(4). Therefore $n \le \text{length}_F(d) < 2n$ implying $n = 2^m$.)

6. $\mathcal{M}$**-indecomposables.** Suppose $\mathcal{M} = \mathcal{M}(\varphi_1, \dots, \varphi_k, \langle b_1\rangle, \dots, \langle b_n\rangle)$ for some $b_i \in F^\bullet$ and some round forms φ_j, following the notations used before (5.5).

(1) Every $\mathcal{M}$-indecomposable which is isotropic must actually be hyperbolic.

(2) There is a unique hyperbolic $\mathcal{M}$-indecomposable form $m\mathbb{H}$.

(3) When can there exist an $\mathcal{M}$-indecomposable with dimension $< 2m$?

7. (1) **Lemma.** *If* $\langle\langle x\rangle\rangle$ *is anisotropic and* $\langle\langle x\rangle\rangle \otimes q$ *is isotropic then there exists* $\beta \subset q$ *such that* $\dim \beta = 2$ *and* $\langle\langle x\rangle\rangle \otimes \beta$ *is hyperbolic.*

(2) **Corollary.** *If* $\langle a\rangle q \simeq q$ *then* $q \simeq q_1 \perp \cdots \perp q_n$ *for subforms* q_i *with* $\dim q_i = 2$ *and* $\langle a\rangle q_i \simeq q_i$.

(3) If $\langle\langle x, y\rangle\rangle \otimes q$ is isotropic, does the analog of (1) hold?

(Hint. (1) Mimic the argument in (5.5).)

8. (1) If $(\langle 1, a, b\rangle, \tau) < \text{Sim}(\langle\langle a, b\rangle\rangle)$, then $\tau \subset \langle 1, a, b\rangle$.

(2) List all pairs (σ, τ) having an unsplittable module of dimension ≤ 4.

(3) If $(\langle 1, a, b, c\rangle, \tau) < \text{Sim}(\langle\langle a, b, c\rangle\rangle)$, then $\tau \subset \langle 1, a, b, c\rangle$. Characterize the forms τ such that $(\langle 1, a, b, c\rangle, \tau) < \text{Sim}(\langle\langle a, b, w\rangle\rangle)$. Here $abc \in G_F(\langle\langle w\rangle\rangle)$ as in (5.3).

(Hint. (1) Show $\dim \tau \le 3$ and use (5.7)(7) if $\dim \tau = 1$. By Expansion we may assume $\dim \tau = 3$. Then $\det \tau = \langle ab\rangle$ since the Clifford algebra is not simple.)

9. **When σ does not represent 1.** Recall Exercise 2.2(1).

(1) Let $\mathcal{M} = \mathcal{M}(a, b) = \{q : a, b \in G_F(q)\}$. Then $q \in \mathcal{M}(a, b)$ iff $(\langle a\rangle, \langle b\rangle) < \text{Sim}(q)$. If $\langle a\rangle \not\simeq \langle 1\rangle$ then the hyperbolic plane is a 2-dimensional $\mathcal{M}$-indecomposable.

(2) Over the rational field $\mathbb{Q}$ the forms $\mathbb{H}$, $\langle\langle 1\rangle\rangle$ and $\langle\langle 2, 5\rangle\rangle$ are $\mathcal{M}(2, 5)$-indecomposables. Find an $\mathcal{M}(2, 5)$-indecomposable which is not similar to a Pfister form. (Note. These proofs involve the Hasse–Minkowski Theorem over $\mathbb{Q}$.)

(3) **Open question.** What are the possible dimensions of $\mathcal{M}(a, b)$-indecomposables?

10. The following are equivalent:

(i) $\langle x, y\rangle < \text{Sim}(q)$.

(ii) $(\langle 1\rangle, \langle x, y\rangle) < \text{Sim}(q)$.

(iii) $(\langle 1, xy\rangle, \langle x\rangle) < \text{Sim}(q)$.

(iv) $\langle\langle xy\rangle\rangle \mid q$ and $x \in G_F(q)$.

11. (1) The following are equivalent:

(i) $(\langle 1,a\rangle,\langle 1,x\rangle) < \mathrm{Sim}(q)$.

(ii) $\langle\langle a\rangle\rangle \mid q$ and $\langle\langle x\rangle\rangle \mid q$.

(iii) $q \simeq \langle\langle a\rangle\rangle \otimes \beta$ for some form β such that $ax \in G_F(\beta)$.

(2) Find a direct proof of (ii) $\iff$ (iii), not using results on similarities.

(Hint. (1) To see (i) $\iff$ (iii) scale by a and use the Eigenspace Lemma 2.10.)

12. **Proposition.** $(\langle 1,a,b\rangle,\langle 1,x\rangle) < \mathrm{Sim}(q)$ *if and only if* $\langle\langle a,b\rangle\rangle \mid q$ *and* $\langle\langle ab,x\rangle\rangle \mid q$.

The proof is outlined below, following the same steps as (5.7).

(1) $(\langle 1,a,b\rangle,\langle 1,x\rangle) < \mathrm{Sim}(q)$ if and only if $(\langle 1,a,b\rangle,\langle 1,ab,abx\rangle) < \mathrm{Sim}(q)$. The "only if" part of the proposition follows.

(2) For the "if" we may assume $\langle a,b\rangle$ does not represent x, so that $\langle\langle a,b\rangle\rangle \not\simeq \langle\langle ab,x\rangle\rangle$.

(3) (8-dim case.) Suppose $q \simeq \langle\langle a,b,w\rangle\rangle$ and $\langle\langle ab,x\rangle\rangle \mid q$. Then $\langle a,b\rangle \perp \langle w\rangle\langle\langle a,b\rangle\rangle$ represents x, so that $x = ar^2 + bs^2 + u$ where $u \in D_F(\langle w\rangle\langle\langle a,b\rangle\rangle)$. Then $q \simeq \langle\langle a,b,u\rangle\rangle$ and $(\langle 1,a,b\rangle,\langle 1,x\rangle) \subset (\langle 1,a,b,u\rangle,\langle 1,a,b,u\rangle) < \mathrm{Sim}(q)$.

(4) If $\varphi = \langle\langle a,b\rangle\rangle$ and $\psi = \langle\langle ab,x\rangle\rangle$, the $\mathcal{M}(\varphi,\psi)$-indecomposables are all 8-dimensional. More generally suppose $\varphi = \alpha\otimes\langle\langle b\rangle\rangle$ and $\psi = \alpha\otimes\langle\langle c_1,\dots,c_k\rangle\rangle$ where α is an r-fold Pfister form and $\varphi \nmid \psi$. Then the $\mathcal{M}(\varphi,\psi)$-indecomposables all have dimension 2^{r+k+1}.

(5) If $\langle 1,a,b,-x,-y\rangle$ is isotropic, for what q is $(\langle 1,a,b\rangle,\langle x,y\rangle) < \mathrm{Sim}(q)$?

(Hint. (1) Use the generators f_2, f_3, g_1, g_2.)

13. The following are equivalent:

(i) $\langle\langle a,b\rangle\rangle \mid q$ and $\langle\langle ab,x\rangle\rangle \mid q$.

(ii) $q \simeq \langle\langle a\rangle\rangle \otimes \gamma$ for some form γ where $\langle\langle ab\rangle\rangle \mid \gamma$ and $ax \in G_F(\gamma)$.

(Hint. Use (5.7), Exercise 11 and the Eigenspace Lemma 2.10.)

Open question. Is there some generalization which includes the Pfister factor results of Exercises 11, 12 and 13 ?

14. Suppose that the trace map ℓ used in (5.9) is replaced by $\ell' : E \to F$ where $\ell'(1) = 1$ and $\ell'(\sqrt{axy}) = 0$. If $\theta = r + s\sqrt{axy}$ determine the form $\ell'(\langle\theta\rangle_E)$.

15. Suppose (K,J) is a field with non-trivial involution, where we write $\bar{\alpha}$ for $J(\alpha)$. Suppose V is a K-vector space and $f : V \to V$ is (K,J)-semilinear.

(1) Let $\{v_1,\dots,v_n\}$ be a K-basis of V and express $f(v_j) = \sum_{i=1}^n a_{ij}v_i$. Then $A = (a_{ij})$ is the matrix associated to f. A vector $v = \sum_{i=1}^n x_iv_i$ is represented by the column vector $X = (x_1,\dots,x_n)^\top$ so that $f(v) = \sum_{i=1}^n x_i'v_i$ is represented by the column vector $X' = A\bar{X}$.

(2) If f and g are (K,J)-semilinear maps on V represented by matrices A and B, then $f\circ g$ is K-linear and is represented by the matrix $A\bar{B}$.

(3) Suppose $h : V \times V \to K$ is a regular hermitian form. Let $M = (h(v_i, v_j))$ be the matrix of h, so that $M^\top = \bar{M}$. If $v, w \in V$ correspond to the column vectors X, Y then $h(v, w) = X^\top M \bar{Y}$. To define the adjoint involution $\sim$ applied to a (K, J)-semilinear map f the usual formula makes no sense: $h(f(v), w) = h(v, \tilde{f}(w))$. (Why?) It is replaced by the definition:

$$\overline{h(f(v), w)} = h(v, \tilde{f}(w)).$$

Then $\tilde{f}$ is also (K, J)-semilinear and $\sim$ is a K-linear involution on the space of all (K, J)-semilinear maps of V. (I.e. $(\widetilde{\alpha f}) = \alpha \tilde{f}$, $(\widetilde{f + g}) = \tilde{f} + \tilde{g}$ and $\tilde{\tilde{f}} = f$ when f is (K, J)-semilinear and $\alpha \in K$.)

(4) If $\tilde{A}$ is the matrix corresponding to $\tilde{f}$ then $\tilde{A} = M^{-\top} A^\top M$. Consequently, $\tilde{f} = f$ if and only if the matrix $M^\top A$ is symmetric.

(5) Does any of this become easier if we use the other definition of "hermitian", where $h(v, w)$ is (K, J)-semilinear in v and K-linear in w?

16. Suppose F, E, K are as described before (5.9) and the involution trace $\ell \circ \mathrm{tr} : K \to F$ is given. Suppose V is a K-vector space and $b_q : V \times V \to F$ is a symmetric bilinear form which admits (K, J). Then there exists a unique hermitian form $h : V \times V \to K$ such that $\ell \circ \mathrm{tr} \circ h = b_q$. Find an explicit formula for h.

(Hint. Say $b : V \times V \to E$ is the corresponding form over E. For $v, w \in V$ show that $b(v, w) = b_q(\sqrt{axy} \cdot v, w) + b_q(v, w) \cdot \sqrt{axy}$. Now build b up to h.)

17. **Norm principle.** Suppose $K = F(\sqrt{d})$ is a quadratic extension of F and define $s : K \to F$ by $s(x + y\sqrt{d}) = y$. If α is a quadratic form over K let $s_*(\alpha)$ denote the transfer to F. (See Lam (1973), p. 201 or Scharlau (1985), p. 50 for discussions of this s_*.)

Lemma. *$s_*(\alpha)$ is isotropic iff α represents some element of $F^\bullet$.*

We also need the following analog of "Frobenius reciprocity":

If φ is a form over F and α is a form over K then $s_*(\varphi_E \otimes \alpha) \simeq \varphi \otimes s_*(\alpha)$.

(1) **Norm Principle.** Let φ be a form over F and $x \in K$. Then $N(x) \in D_F(\varphi) \cdot D_F(\varphi)$ if and only if $x \in F^\bullet \cdot D_K(\varphi_K)$.

(2) Deduce Lemma 5.12.

(Hint. (1) $\varphi \perp \langle -Nx \rangle \varphi$ is F-isotropic iff $s_*(\langle x \rangle \varphi)$ is F-isotropic.)

18. **Examples.** (1) Give an example of an unsplittable $\sigma < \mathrm{Sim}(q)$ where q is anisotropic but is not similar to a Pfister form.

(2) Give an example of an unsplittable $\sigma < \mathrm{Sim}(8\mathbb{H} \perp 16\langle 1 \rangle)$ over $\mathbb{Q}$ where $\dim \sigma = 8$.

19. **Common slot.** Suppose $\alpha \simeq \langle\langle a, a' \rangle\rangle$ and $\beta \simeq \langle\langle b, b' \rangle\rangle$ are 2-fold Pfister forms. If $\alpha \simeq \beta$ then there exists $x \in F^\bullet$ such that $\alpha \simeq \langle\langle a, x \rangle\rangle$ and $\beta \simeq \langle\langle b, x \rangle\rangle$.

20. **Contradiction? Conjecture.** Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an (s, t)-family and q represents $a \in F^\bullet$. Then there is a decomposition $q = q_1 \perp \cdots \perp q_n$ such that for every i, $(\sigma, \tau) < \mathrm{Sim}(q_i)$ is unsplittable, and such that q_1 represents a.

(1) If q is a Pfister form the Conjecture is true. Suppose there is a Pfister form φ such that: $(\sigma, \tau) < \mathrm{Sim}(q)$ iff $\varphi \mid q$. Then the Conjecture is true.

(2) Consider the set-up of (C, J)-modules and suppose $V = U \perp U'$ where U is an irreducible submodule. If $W \subseteq V$ is irreducible with $W \not\subseteq U'$, then $W = U[f] = \{u + f(u) : u \in U\}$ is the graph of some C-homomorphism $f : U \to U'$. Now specialize to the case that $\mathrm{End}_C(U) = F$ and $U' \cong U$. Then any value represented by an irreducible submodule W must lie in $(1+\lambda^2) \cdot D_F(U)$ for some $\lambda \in F$. For a specific case let $(\sigma, \tau) = (\langle 1, 1\rangle, \langle 1\rangle)$ and $V \simeq \langle\langle 1, 1\rangle\rangle$. Then any irreducible submodule of V represents only values in $D_F(\langle\langle 1\rangle\rangle)$, and the Conjecture is false.

(3) Resolve the apparent contradiction between parts (1) and (2).

(Hint. (1) For the first statement, choose any unsplittable decomposition and let $b \in D_F(q_1)$. Then $q \simeq \langle ab\rangle q$.)

21. **Transfer ideals.** Suppose (K, J) is a field with involution, F is a subfield fixed by J and $t : K \to F$ is an involution trace (that is, t is F-linear and $t(\bar{a}) = t(a)$). If (V, h) is a (K, J)-hermitian space then the transfer $t_*(V, h) = (V, t \circ h)$ is a quadratic space over F. Let $\mathcal{I}((K, J)/F)$ be the set of (isometry classes of) all such transferred spaces. Then $\mathcal{I}((K, J)/F)$ does not depend on the choice of t and its image in the Witt ring $W(F)$ is an ideal.

Suppose $a, b \in F^\bullet$ and $K = F(\sqrt{-a}, \sqrt{-b})$ is an extension field of degree 4. Let J be the involution on K which induces non-trivial involutions J_a and J_b on the subfields $A = F(\sqrt{-a})$ and $B = F(\sqrt{-b}$ respectively. Let $t : K \to F$ be an involution trace which induces the (unique) involution traces $t_a : A \to F$ and $t_b : B \to F$.

Proposition. $\mathcal{I}((K, J)/F) = \mathcal{I}((A, J_a)/F) \cap \mathcal{I}((B, J_b)/F)$.

(Hint. This is a restatement of Proposition 5.16. First check that $\mathcal{I}((A, J_a)/F) = \mathcal{M}(\langle\langle a\rangle\rangle)$ and similarly for b.)

22. **Forms of odd dimension.** Assume the following result, due originally to Pfister (1966).

Proposition. *If* $\dim \delta$ *is odd then* δ *is not a zero-divisor in the Witt ring* $W(F)$.

(1) If α is not hyperbolic then $\alpha \mid m\mathbb{H}$ if and only if $\dim \alpha \mid m$. (Generalizing (5.5) (3).)

(2) If $a \in G_F(\alpha \otimes \delta)$ where $\dim \delta$ is odd, then $a \in G_F(\alpha)$.

(3) If φ is a Pfister form and $\varphi \mid \alpha \otimes \delta$ where $\dim \delta$ is odd, then $\varphi \mid \alpha$.

(4) If (σ, τ) has unsplittables of dimension ≤ 4, the answer to the following question is "yes".

Odd Factor Question. If $(\sigma, \tau) < \mathrm{Sim}(\alpha \otimes \delta)$ where $\dim \delta$ is odd, does it follow that $(\sigma, \tau) < \mathrm{Sim}(\alpha)$?

(Hint. (3) This seems to require the theory of function fields described in the appendix to Chapter 9. Express $\alpha = \alpha_0 \perp k\mathbb{H}$ where α_0 is anisotropic. Apply (9.A.6) and (5.5).)

23. **Pfister factors.** (1) If φ is a Pfister form and $\langle 1, b\rangle \subset \varphi$ then $\varphi \simeq \langle\langle b, c_2, \dots, c\rangle\rangle$ for some $c_j \in F^\bullet$. This was proved in (5.2) (1).

Lemma. *If φ is a 3-fold Pfister form and $\langle 1, a, b\rangle \subset \varphi$ then $\varphi \simeq \langle\langle a, b, w\rangle\rangle$ for some w.*

(2) If $\dim \alpha = \dim \beta = 4$, $d\alpha = d\beta$ and $c(\alpha) = c(\beta) = 1$ then α and β are similar.

(Hint. (1) Given $\varphi \simeq \langle\langle a, x, y\rangle\rangle$ such that $\langle x\rangle\langle\langle a\rangle\rangle \perp \langle y\rangle\langle\langle a, x\rangle\rangle$ represents b. We may assume $b = xu + yv$ for some $u \in D_F(\langle\langle a\rangle\rangle)$ and $v \in D_F(\langle\langle a, x\rangle\rangle)$. Then $\varphi \simeq \langle\langle a, xu, yv\rangle\rangle$.

(2) Let $d\alpha = \langle d\rangle$ and let $\varphi = \alpha \perp \langle d\rangle\beta$. Then $\dim \varphi = 8$, $d\varphi = \langle 1\rangle$ and $c(\varphi) = 1$ so that φ is similar to a Pfister form, by (3.20) (2). We may assume $\alpha = \langle 1, a, b, abd\rangle$ and find $\varphi \simeq \langle\langle a, b, w\rangle\rangle$ for some w. Then d is represented by $\langle 1\rangle \perp \langle w\rangle\langle\langle a, b\rangle\rangle$ so that $d = t^2 + u$ for some $t, u \in F^\bullet$ such that $\varphi \simeq \langle\langle a, b, u\rangle\rangle$. Then $\varphi \simeq \langle 1, a, b, ab\rangle \otimes \langle\langle u\rangle\rangle \simeq \alpha \otimes \langle\langle u\rangle\rangle$. Cancel α to finish the proof.)

Notes on Chapter 5

In the proof of Lemma 5.2 we assumed that $x, y \neq 0$, leaving the other cases to the reader. Actually that non-zero case is sufficient if we invoke the Transversality Lemma of Exercise 1.15

Lemma 5.5 and Proposition 5.6 follow Wadsworth and Shapiro (1977b). Lemma 5.5 is also treated in Szymiczek (1977). More recent results on round forms appear in Alpers (1991) and Hornix (1992).

Exercise 5. These results on the level $s(F)$, due to Pfister, helped to motivate the investigation of the multiplicative properties of quadratic forms. The second result leads to examples of fields which have prescribed level 2^m. See Exercise 9.11 below.

Exercise 7. See Elman and Lam (1973b), pp. 288–289. Compare Exercise 2.9.

Exercise 9. The different dimensions possible for unsplittable $(\langle a\rangle, \langle b\rangle)$-modules contrast with the Decomposition Theorem 4.1. The image of $\mathcal{M}(a, b)$ in $W(F)$ is the ideal $\mathcal{A} = \mathrm{ann}(\langle\langle -a\rangle\rangle) \cup \mathrm{ann}(\langle\langle -b\rangle\rangle)$. It is known that $\mathcal{A}$ is generated by 1-fold and 2-fold Pfister forms. See Elman, Lam and Wadsworth (1979). For the case of global fields see Exercise 11.6.

Exercise 12 (4) follows Wadsworth and Shapiro (1977b).

Exercise 17. The Norm Principle appears in Elman and Lam (1976), 2.13.

Exercise 19. Compare Exercise 3.10.

Exercise 21. If $E = F(\sqrt{ab})$ with trivial involution then $\mathcal{I}(E/F) = \mathcal{M}(ab)$ is contained in $\mathcal{M}(\langle\langle a\rangle\rangle, \langle\langle b\rangle\rangle)$. The analog of this proposition for biquadratic extensions with trivial involution is proved in Leep and Wadsworth (1990).

Exercise 22. Proofs of the proposition appear in Lam (1973) on pp. 250 and 310, in Scharlau (1985), p. 54, and in D. W. Lewis (1989).

Exercise 23. Compare Exercise 3.12(4) and the references given in Chapter 3. The lemma here is a special case of Exercise 9.15.

Chapter 6

Involutions

If (C, J) is an algebra with involution, when does a given C-module V possess a λ-form admitting C? A regular λ-form on V induces an adjoint involution on $\mathrm{End}(V)$, and every involution on $\mathrm{End}(V)$ arises from some λ-form. This sign λ is called the "type" of the involution. The question posed above is then equivalent to asking whether there is an involution on $\mathrm{End}(V)$ which is compatible with (C, J). If C is central simple it splits off as a tensor factor: $\mathrm{End}(V) \cong C \otimes A$, for some central simple algebra A. The involutions on $\mathrm{End}(V)$ compatible with (C, J) are then exactly the maps $J \otimes K$, where K is an involution on A. The focus of our work has then moved to an analysis of this algebra A and its involutions.

In this short chapter we describe the basic results about involutions on central simple algebras, postponing the applications to later chapters. Those results on involutions have appeared in various textbooks. In fact, most of the ideas we use go back at least to the 1930s and are summarized in Albert's book *Structure of Algebras* (1939). We assume the reader is familiar with the general theory of central simple algebras, including the Wedderburn Theorems, the Double Centralizer Theorem, the existence of splitting fields, and the Skolem–Noether Theorem. However it seems worthwhile to derive the tools we need concerning involutions. Further information about algebras and involutions is available in the books by Rowen (1980), Scharlau (1985), Knus (1988), and Knus et al. (1998).

If A is a ring we let $A^\bullet$ denote the group of units, and if $S \subseteq A$ we write $S^\bullet$ for the subset $S \cap A^\bullet$. However, following standard practice we write $\mathrm{GL}(V)$ rather than $\mathrm{End}^\bullet(V)$. If A is an F-algebra an *involution* J on A is defined to be an anti-automorphism such that J^2 is the identity map. When F is the center of A then J preserves F and the restriction is an involution on the field F. The involution is said to be of the first kind or second kind, depending on whether or not it fixes F.

> *Unless explicitly stated otherwise, involutions in this book are F-linear. That is, we assume they are of the "first kind", inducing the identity map on the ground field.*

6.1 Definition. Let A be an F-algebra with involution J. If $a \in A^\bullet$ define the map $J^a : A \to A$ by

$$J^a(x) = a^{-1}J(x)a \quad \text{for } x \in A.$$

6.2 Lemma. *Let A, J and a be given as above and suppose A has center F. Then J^a is an involution if and only if $J(a) = \pm a$. The element a is uniquely determined, up to non-zero scalar multiple, by J and J^a.*

Proof. If J^a is an involution then $x = J^a J^a(x) = a^{-1}J(a)xJ(a^{-1})a$ for every $x \in A$. Then $a^{-1}J(a)$ is central so that $J(a) = \varepsilon a$ for some $\varepsilon \in F^\bullet$. Applying J again we find that $\varepsilon^2 = 1$. The converse follows from the same formula. If $J^b = J^a$ for some $b \in A^\bullet$ then $a^{-1}b$ is central and $b \in aF^\bullet$. □

We now make a key observation: every involution on the split algebra $\mathrm{End}(V)$ comes from a regular λ-form on V.

6.3 Lemma. *Let V be an F-vector space.*

(1) *If B is a regular λ-form on V and $f \in \mathrm{GL}(V)$, define the bilinear form $B^f : V \times V \to F$ by*

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

for $x, y \in V$. If $I_B(f) = \varepsilon f$ where $\varepsilon = \pm 1$, then B^f is a regular $\varepsilon\lambda$-form and $I_{B^f} = I_B^f$. Every regular $\varepsilon\lambda$-form on V arises from B in this way.

(2) *If J is an involution on $\mathrm{End}(V)$ then $J = I_B$ for some regular λ-form B on V. This form B is uniquely determined, up to non-zero scalar multiple.*

Proof. (1) It is easy to see that B^f is a regular $\varepsilon\lambda$-form. To prove the formula for the involutions note that $B^f(x, h(y)) = B(I_B(h)f(x), y) = B^f(f^{-1}I_B(h)f(x), y)$. Recall that the map $\theta_B : V \to \hat{V}$ is defined by $\langle x|\theta_B(y)\rangle = B(x, y)$. If B' is any regular $\varepsilon\lambda$-form on V, let $f = (\theta_{B'} \circ \theta_B^{-1})^\top$. Then $B' = B^f$.

(2) Let B_0 be a regular 1-form on V with adjoint involution I_0. By the Skolem–Noether Theorem and (6.2) we have $J = I_0^f$ for some $f \in \mathrm{GL}(V)$ with $I_0(f) = \lambda f$ for some $\lambda = \pm 1$. Then $B = B_0^f$ is a λ-form on V having $I_B = J$. If B' is another regular form having $I_{B'} = J$, then (1) implies that $B' = B^g$ for some $g \in \mathrm{GL}(V)$ and $J = I_B^g = J^g$. Then g is in the center of $\mathrm{End}(V)$, and B' is a scalar multiple of B. □

An involution J is the adjoint involution of some λ-form on V. We define the *type* of J to be this sign λ, and say that J is a λ-*involution*. Some authors say that J has *orthogonal type* if its type is 1 and J has *symplectic type* if its type is -1.

The notion of type can be generalized by considering the behavior of involutions under extension of scalars. If L/F is a field extension and J is an involution of the F-algebra A, then $J \otimes 1_L$ is an involution of the L-algebra $A \otimes L$. If A is a central simple F-algebra then there are “splitting fields” L such that $A \otimes L \cong \mathrm{End}_L(V)$, for some L-vector space V. One well-known consequence is that $\dim A$ is a square. The algebra A is said to have *degree* n if $\dim A = n^2$ (and $\dim_L V = n$).

6.4 Definition. Suppose (A, J) is a central simple F-algebra with involution and L is a splitting field for A. Then the involution $J \otimes 1_L$ on $A \otimes L \cong \mathrm{End}_L(V)$ is the adjoint involution of some λ-form B on V. The *type* of J is this sign λ, and J is called a *λ-involution*.

For a given splitting field L Lemma 6.3 implies that this sign λ is uniquely determined. Since any two splitting fields can be embedded in a larger field extension, it follows that the type λ is independent of the choice of L. This independence is also clear from the next lemma.

6.5 Lemma. *Let A be a central simple F-algebra of degree n, so that* $\dim A = n^2$.

(1) *If J and J' are involutions on A then $J' = J^a$ for some $a \in A^\bullet$ with $J(a) = \pm a$. Furthermore, J and J' have the same type if and only if $J(a) = a$.*

(2) *If J is an involution on A define $\mathcal{S}^\varepsilon(A, J) = \{x \in A : J(x) = \varepsilon x\}$, the subspace of elements which are ε-symmetric for J. If J has type λ then* $\dim \mathcal{S}^\varepsilon(A, J) = \frac{n(n+\varepsilon\lambda)}{2}$.

Proof. (1) The existence and uniqueness (up to scalar multiple) of the element a follow as in (6.3)(2) and (6.2). We may extend scalars to assume $A \cong \mathrm{End}(V)$ for some vector space V. If $J(a) = \varepsilon a$ then by (6.3) $J = I_B$ for some λ-form B on V and $J' = I_{B'}$ where $B' = B^a$ is an $\varepsilon\lambda$-form on V.

(2) We may assume that $A = \mathrm{End}(V)$. The quadratic form $n\langle 1\rangle$ on V has adjoint involution I which is just the transpose map on matrices. The dimensions are easily found: $\dim \mathcal{S}^\varepsilon(A, J) = \frac{n(n+\varepsilon)}{2}$. By (1) $J = I^a$ for some $a \in A^\bullet$ with $I(a) = \lambda a$. The claim follows from the general observation that

$$\mathcal{S}^\varepsilon(A, I^a) = \mathcal{S}^{\lambda\varepsilon}(A, I) \cdot a. \qquad \square$$

We are working here in the category of "central simple F-algebras with involution." If (A_1, J_1) and (A_2, J_2) are in that category we write $\varphi : (A_1, J_1) \to (A_2, J_2)$ to indicate an F-algebra homomorphism $\varphi : A_1 \to A_2$ which preserves the involutions: $J_2 \circ \varphi = \varphi \circ J_1$. Similarity representations (as in Chapter 4) are examples of such homomorphisms. Let us analyze some special cases of isomorphisms in this category.

6.6 Proposition. *Suppose (V_i, B_i) is a regular λ_i-space for $i = 1, 2$. Let I_i denote the involution I_{B_i} on* $\mathrm{End}(V_i)$. *Then* $(\mathrm{End}(V_1), I_1) \cong (\mathrm{End}(V_2), I_2)$ *if and only if* (V_1, B_1) *and* (V_2, B_2) *are similar spaces.*

Proof. Suppose $h : (V_1, B_1) \to (V_2, B_2)$ is a bijective similarity. Define the map $\varphi : \mathrm{End}(V_1) \to \mathrm{End}(V_2)$ by: $\varphi(f) = hfh^{-1}$. To show that $I_2 \circ \varphi = \varphi \circ I_1$ we check that for $x, y \in V$ the expressions $B_2(I_2(\varphi(f))(h(x)), h(y))$ and $B_2(\varphi(I_1(f))(h(x)), h(y))$ both reduce to the same value $\mu(h)B_1(x, f(y))$. Conversely suppose $\varphi : (\mathrm{End}(V_1), I_1) \to (\mathrm{End}(V_2), I_2)$ is an isomorphism. Since the dimensions are equal there is some linear bijection $g : V_1 \to V_2$. By Skolem–Noether, the map $f \mapsto g^{-1}\varphi(f)g$ is an inner automorphism of $\mathrm{End}(V_1)$, so there is a linear bijection $h : V_1 \to V_2$ with $\varphi(f) = hfh^{-1}$. Define B' on V by setting $B'(x, y) = B_2(h(x), h(y))$. Then h is an isometry $(V_1, B') \to (V_2, B_2)$ and the calculation above shows that $I_{B'} = \varphi^{-1} \circ I_2 \circ \varphi = I_1$. Therefore $B' = aB_1$ for some $a \in F^\bullet$, and $(V_2, B_2) \simeq (V_1, aB_1)$. □

When considering isomorphisms of two algebras with involution we often identify the algebras and concentrate on the involutions.

6.7 Lemma. *Let (A, J) be a central simple F-algebra with involution, and let $a, b \in A^\bullet$. Then $(A, J^a) \cong (A, J^b)$ if and only if $b = rJ(u)au$ for some $r \in F^\bullet$ and $u \in A^\bullet$.*

Proof. If $\alpha : (A, J^a) \to (A, J^b)$ is the given isomorphism then α is an F-algebra isomorphism and $J^b = \alpha \circ J^a \circ \alpha^{-1}$. By Skolem–Noether there exists $u \in A^\bullet$ such that $\alpha(x) = u^{-1}xu$ and the claim follows. The converse is similar. □

For quaternion algebras we get a complete characterization of the involutions.

6.8 Lemma. *Let A be a quaternion algebra with bar involution J_0. Express $A = F + A_0$ where A_0 is the set of pure quaternions.*

(1) *J_0 is the only (-1)-involution on A.*

(2) *If J is a 1-involution then $J = J_0^e$ for some $e \in A_0^\bullet$. For any $e \in A_0^\bullet$, the only involutions sending $e \mapsto -e$ are J_0 and J_0^e.*

(3) *For J as above the value Ne is uniquely determined up to a square factor. Define $\det(J) = \langle Ne\rangle$ in $F^\bullet/F^{\bullet 2}$. Suppose J_1, J_2 are 1-involutions on A. Then $(A, J_1) \cong (A, J_2)$ if and only if $\det(J_1) = \det(J_2)$.*

Proof. (1) By (6.5) J_0 has type -1. Any involution J on A must equal J_0^e for some $e \in A^\bullet$ with $J_0(e) = \pm e$. If J has type -1 then $J_0(e) = e$ so that $e \in F^\bullet$ and $J = J_0$.

(2) If J has type 1 then $e \in A_0^\bullet$ and $J(e) = -e$. The uniqueness follows since $\dim \mathcal{S}^-(A, J) = 1$.

(3) If $J = J_0^e$, the element e is determined up to a factor in $F^\bullet$. Hence the norm Ne is determined up to a factor in $F^{\bullet 2}$, and $\det(J)$ is well defined. Suppose $J_1 = J_0^a$ and $J_2 = J_0^b$ for some $a, b \in A_0^\bullet$. If $J_1 \cong J_2$ use (6.7). Conversely suppose $\det(J_1) = \det(J_2)$. Altering b by a scalar we may assume that $Na = Nb$. Standard facts about quaternion algebras (see Exercise 2) imply that there exists $u \in A^\bullet$ such that $b = u^{-1}au = (Nu)^{-1}J(u)au$ and (6.7) applies. □

Our next task is to show that the type behaves well under tensor products.

6.9 Proposition. *Let A_i be a central simple F-algebra with λ_i-involution J_i, for $i = 1, 2$. Then $J_1 \otimes J_2$ is a $\lambda_1\lambda_2$-involution on $A_1 \otimes A_2$.*

Proof. We may replace the field F by a splitting field to assume that $A_i \cong \mathrm{End}(V_i)$ and that J_i is the adjoint involution of a λ_i-form B_i on V_i. Suppose ψ is the natural isomorphism

$$\psi : \mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(V_1 \otimes V_2).$$

To complete the proof we must verify that ψ carries $I_{B_1} \otimes I_{B_2}$ to $I_{B_1 \otimes B_2}$. To see this recall that by definition, $\psi(f_1 \otimes f_2)(x_1 \otimes x_2) = f_1(x_1) \otimes f_2(x_2)$ whenever $f_i \in \mathrm{End}(V_i)$ and $x_i \in V_i$. One can then check directly that $\psi(I_{B_1}(f_1) \otimes I_{B_2}(f_2))$ does act as the adjoint of $\psi(f_1 \otimes f_2)$ relative to the form $B_1 \otimes B_2$. □

6.10 Corollary. *Suppose (V_i, B_i) is a regular λ_i-space for $i = 1, 2$. Let I_i denote the involution I_{B_i} on $\mathrm{End}(V_i)$.*

(1) *(V, B) is similar to $(V_1 \otimes V_2, B_1 \otimes B_2)$ if and only if*

$$(\mathrm{End}(V), I_B) \cong (\mathrm{End}(V_1), I_1) \otimes (\mathrm{End}(V_2), I_2).$$

(2) *There is a homomorphism $(\mathrm{End}(V_1), I_1) \to (\mathrm{End}(V_2), I_2)$ if and only if (V_1, B_1) "divides" (V_2, B_2) in the sense that $(V_2, B_2) \simeq (V_1, B_1) \otimes (W, B)$ for some $\lambda_1\lambda_2$-space (W, B).*

Proof. For (1) apply (6.6) and (6.9). We prove a sharper version of (2) in the next corollary. □

6.11 Corollary. *Suppose (C, J) is a central simple algebra with involution and $A \subseteq C$ is a central simple subalgebra preserved by J. Then $(C, J) \cong (A, J|_A) \otimes (C', J')$ for some central simple subalgebra C' with involution J'.*

Suppose further that A is split so that $(A, J|_A) \cong (\mathrm{End}(U), I_B)$ for some λ-form B on U. If (V, q) is a quadratic (C, J)-module, one then obtains:

$(V, q) \simeq (U, B) \otimes (U', B')$ where (U', B') is some λ-space admitting (C', J').

Proof. The algebra C' is the centralizer of A in C and the Double Centralizer Theorem implies that C' is central simple and $A \otimes C' \cong C$. Since J preserves A it also preserves C' and induces some involution J' there. Since C is simple the given homomorphism $(C, J) \to (\mathrm{End}(V), I_q)$ is injective and we view C as a subalgebra of $\mathrm{End}(V)$. Then as above there is a decomposition $(C, J) \otimes (C'', J'') \cong (\mathrm{End}(V), I_q)$. Therefore $A \otimes C' \otimes C'' \cong \mathrm{End}(V)$ and since A is split Wedderburn's Theorem implies that $C' \otimes C'' \cong \mathrm{End}(U')$ for some U'. The involution $J' \otimes J''$ then induces an involution $I_{B'}$ for some form B' on U'. Therefore $(\mathrm{End}(U), I_B) \otimes (\mathrm{End}(U'), I_{B'}) \cong (A, J|_A) \otimes (C' \otimes C'', J' \otimes J'') \cong (\mathrm{End}(V), I_q)$ and (6.10)(1) implies that (V, q) is similar to $(U, B) \otimes (U', B')$. We may alter B' by a scalar to assume this is an isometry.

Since q is quadratic and B is λ-symmetric, (6.9) implies that B' is λ-symmetric. By construction (U', B') admits (C', J'). □

This corollary gives another proof of the Eigenspace Lemma 2.10. See Exercise 4(3) below. It also provides an interpretation of "Pfister factors" entirely in terms of algebras, as follows.

6.12 Corollary. *Suppose (V, q) is a quadratic space and $a_1, \dots, a_m \in F^\bullet$. Then $\langle\langle a_1, \dots, a_m\rangle\rangle$ is a tensor factor of q if and only if there is a homomorphism $(Q_1, J_1) \otimes \cdots \otimes (Q_m, J_m) \to (\mathrm{End}(V), I_q)$ where each (Q_k, J_k) is a split quaternion algebra with involution of type 1 such that there exists $f_k \in Q_k$ such that $J_k(f_k) = -f_k$ and $f_k^2 = -a_k$.*

Proof. Note that $(Q_k, J_k) \cong (\mathrm{End}(F^2), I_{\varphi_k})$ where $\varphi_k \simeq \langle\langle a_k\rangle\rangle$. The equivalence follows from (6.11). □

Suppose C is a central simple F-algebra with an ε-involution J, and V is a C-module. The relevant question is:

When is there a regular λ-form B on V admitting C?

The C-module structure provides a homomorphism $\pi : C \to \mathrm{End}(V)$ which is injective since C is simple. We may view π as an inclusion $C \subseteq \mathrm{End}(V)$ and let A be the centralizer of C, that is, $A = \mathrm{End}_C(V)$. By the Double Centralizer Theorem, A is also a central simple F-algebra and

$$C \otimes A \cong \mathrm{End}(V).$$

In particular, the dimension of A can be found from $\dim C$ and $\dim V$.

If V possesses a regular λ-form B admitting C then there is an involution I_B on $\mathrm{End}(V)$ which is compatible with the involution J on C. That is, I_B extends J and in particular it preserves the subspace $C \subseteq \mathrm{End}(V)$. Therefore I_B preserves the centralizer A and induces an involution K on A. Then $J \otimes K = I_B$, and by (6.9) the involution K has type $\varepsilon\lambda$. Conversely if A possesses an $\varepsilon\lambda$-involution K then $J \otimes K$ on $C \otimes A \cong \mathrm{End}(V)$ provides an involution on $\mathrm{End}(V)$. Then by (6.3) and (6.9) this involution must be I_B for some regular λ-form B on V. This form B does admit C since I_B is compatible with J. Therefore, the existence of a λ-form B admitting C is equivalent to the existence of an $\varepsilon\lambda$-involution on A.

We can use these methods to prove that A must possess an involution.

6.13 Proposition. *Suppose A and C are central simple algebras which are equivalent in the Brauer group. If C has an involution then so does A.*

Proof. By Wedderburn, $C \cong D \otimes \mathrm{End}(U)$ and $A \cong D \otimes \mathrm{End}(W)$ where D is some F-central division algebra and U, W are F-vector spaces. Since $\mathrm{End}(W)$ always has a 1-involution it suffices to prove that D possesses an involution. Since J is an anti-automorphism, we know C is isomorphic to its opposite algebra C^{op}, so that $C \otimes C \cong C \otimes C^{\mathrm{op}}$ is split. Therefore $C \otimes D$ is also split, say $C \otimes D \cong \mathrm{End}(V)$. Since D is a division algebra, V is an irreducible C-module. The dual $\hat{V}$ is also a C-module (as defined in Chapter 4) and has the same dimension as V. Therefore $\hat{V} \cong V$ and Lemma 4.11 implies that V has some regular λ-form B admitting (C, J), for some $\lambda = \pm 1$. The adjoint involution I_B on $\mathrm{End}(V)$ preserves the subalgebra C, so it must also preserve D, the centralizer of C. The restriction of I_B to D is an involution. □

Actually (6.13) is part of a famous theorem of Albert (1939). If A is a central simple algebra admitting an involution then it certainly has an anti-automorphism. If A has an anti-automorphism then there is an isomorphism $A \cong A^{\mathrm{op}}$, and therefore $[A]^2 = 1$ in the Brauer group $\mathrm{Br}(F)$. Albert proved the converse.

6.14 Theorem. *If A is a central simple algebra with $[A]^2 = 1$ then A has an involution.*

We refer the reader to the beautiful proof appearing as Theorem 8.8.4 in Scharlau (1985). Several proofs have appeared in the literature. For example see Knus et al. (1998), §3. The original version, given as Theorem 10.19 of Albert (1939), was proved using the theory of crossed products.

6.15 Corollary. *Let A be a central simple algebra with involution. There exist involutions of both types on A unless A is a split algebra of odd degree.*

Proof. Let D be the "division algebra part" of A. Then $A \cong D \otimes \mathrm{End}(U)$ for some vector space U. By (6.14) the algebra D has an involution and there is always a 1-involution on $\mathrm{End}(U)$. Therefore there is an involution J on A which preserves the subalgebras D and $\mathrm{End}(U)$. If there exists $c \in A^\bullet$ with $J(c) = -c$ then J and J^c have opposite type. If $D \neq F$ there exists $d \in D$ with $J(d) \neq d$, and we use $c = J(d) - d$. If $\dim U$ is even then there exists a regular (-1)-form on U so there must exist $c \in \mathrm{GL}(U)$ with $J(c) = -c$. The only exception is when $D = F$ and $\dim U$ is odd. □

We noted in Chapter 4 that unsplittable (C, J)-modules are usually irreducible. For a central simple algebra C the exceptions are now easy to describe.

6.16 Corollary. *Let C be a central simple algebra with an ε-involution J and let V be a C-module. The hyperbolic module $H_\lambda(V)$ is (C, J)-unsplittable if and only if $C \cong \mathrm{End}(V)$ and $\lambda \neq \varepsilon$. In this case all λ-symmetric (C, J)-modules are hyperbolic.*

Proof. By Theorem 4.10 we know that $H_\lambda(V)$ is unsplittable if and only if V is irreducible and possesses no regular λ-form admitting C. The "if" part is clear. Conversely, we know that $C \otimes A \cong \mathrm{End}(V)$ where $A = \mathrm{End}_C(V)$. Then (6.9) implies that A has no $\varepsilon\lambda$-involution. Since V is irreducible Schur's Lemma implies A is a division algebra and (6.15) implies that $A = F$. □

The standard examples of central simple algebras with involution are quaternion algebras and matrix algebras. So if $A \cong \mathbb{M}_n(D)$ where D is a tensor product of quaternion algebras, then A has an involution. In the 1930s Albert considered the following converse question:

If D is an F-central division algebra with involution then must D be isomorphic to a tensor product of quaternions?

There has been considerable work on this question since then. The next theorem summarizes some major results in this area.

6.17 Theorem. *Suppose D is an F-central division algebra with involution.*

(1) *D has degree 2^m for some m. If $m = 1$ then D is a quaternion algebra. If $m = 2$ then D is a tensor product of two quaternion algebras.*

(2) *There exists a division algebra D of degree 8 over its center F such that D has an involution but has no quaternion subalgebras. For any such D the algebra $\mathbb{M}_2(D)$ is isomorphic to a tensor product of 4 quaternion algebras.*

(3) *$[D]$ is a product of quaternion algebras in the Brauer group.*

Here are references where the proofs of these statements can be found.

If $\deg(D) = n$, Albert showed that $[D]^n = 1$ in $\mathrm{Br}(F)$, and that $\deg(D)$ and the order of [D] involve the same prime factors. (See Albert (1939), Theorem 5.17, p. 76, or Draxl (1983), Theorem 11, p. 66.) Consequently if D has an involution then $[D]^2 = 1$ and $\deg(D)$ must be a 2-power. The stronger result when $m = 2$ is due to Albert (1932), with various different proofs given by Racine (1974), Jančevskiĭ (1974) and Rowen (1978). Several proof are presented by Knus et al. (1998), §16. We prove it in (10.21) below following Rowen's method.

(2) Such examples were found by Amitsur, Rowen and Tignol (1979), where the center is a purely transcendental extension of $\mathbb{Q}$ of degree 4. The criteria involved in constructing this counterexample were generalized by Elman, Lam, Tignol and Wadsworth (1982) and further counterexamples were found (all of characteristic 0). The second statement was proved by Tignol (1978).

(3) This is part of an important theorem of Merkurjev (1981) which states that the quaternion symbol map $k_2F \to \mathrm{Br}_2(F)$ is an isomorphism. This implies that some matrix algebra over D is isomorphic to a tensor product of quaternion algebras.

Exercises for Chapter 6

1. **The type of J_S.** Let $\sigma \cong \langle 1\rangle \perp \sigma_1$ be a quadratic form of dimension $s = 2m+1$. Then $C = C(-\sigma_1)$ is central simple of degree 2^m and has the involution J_S.

Lemma. *J_S has type* 1 *if and only if* $s \equiv \pm 1 \pmod 8$.

(1) Proof #1. Apply (6.5) directly by computing $\dim \mathcal{S}^+(C, J_S)$ to be the sum of all $\binom{n}{j}$ where $j \equiv 0, 3 \pmod 4$. Such sums can be evaluated using the binomial theorem with appropriate roots of unity. (See Knuth (1968), 1.2.6, Exercise 38.)

(2) Proof #2. An explicit decomposition of C as a product of quaternions is given in (3.14). Note that J_S preserves each quaternion algebra, compute the type and apply (6.9).

A third proof appears in (7.5) below.

2. **Quaternion conjugates.** Let A be a quaternion algebra over F and recall the usual definitions of the norm and trace of an element a: $Na = a\bar{a}$ and $Ta = a + \bar{a}$. If $a, b \in A$ we write $a \sim b$ to mean that a and b are conjugate, i.e. $b = cac^{-1}$ for some $c \in A^\bullet$.

Lemma. *If $a, b \in A$ then $a \sim b$ if and only if $Na = Nb$ and $Ta = Tb$.*

(Hint. See Exercise 4.10(2).)

3. **Two Quaternions.** Suppose (A, J) is a central simple F-algebra with involution and with $\dim A = 16$. Suppose J is "decomposable", in the sense that there exists a J-invariant quaternion subalgebra $Q_1 \subseteq A$. For every such subalgebra there is a decomposition

$$(A, J) \simeq (Q_1, J_1) \otimes (Q_2, J_2).$$

(1) If J_1 and J_2 both have type 1, then $(A, J) \cong (A_1, K_1) \otimes (A_2, K_2)$ where each A_j is a quaternion algebra and each K_j is the "bar" involution, of type -1.

(2) Suppose J_1 and J_2 both have type -1. Then those quaternion subalgebras Q_1, Q_2 are unique in a strong sense: If B is any J-invariant quaternion subalgebra on which the induced involution has type -1, then either $B = Q_1$ or $B = Q_2$.

(Hint. (1) Re-arrange the generators $i_1 \otimes i_2$, $i_1 \otimes j_2$, etc.

(2) Compare Exercise 1.4.)

4. **Explicit quaternions.** Suppose (σ, τ) is an (s, t)-pair where $s + t = 2m + 1$. Let (C, J) be the associated Clifford algebra with involution. Let $\{e_1, \dots, e_{2m}\}$ be an orthogonal basis of the generating subspace such that $J(e_j) = \pm e_j$. Then $\{e^\Delta : \Delta \in \mathbb{F}_2^{2m}\}$ forms the derived basis of C. If e^Γ and e^Δ anticommute then they generate a quaternion subalgebra Q preserved by J and $C \cong Q \otimes C'$ where C' is the centralizer of Q. Then J induces an involution J' on C'.

(1) (C', J') is the Clifford algebra with involution associated to some (s', t')-family (σ', τ') where $s' + t' = 2m - 1$.

(2) Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ and Q is split. If $J|_Q$ has type -1 then q is hyperbolic (but not necessarily (C, J)-hyperbolic). If $J|_Q$ has type 1 then $(Q, J|_Q)$ is the Clifford algebra associated to some (2, 2)-family $(\langle 1, a\rangle, \langle 1, a\rangle)$ and $q \simeq \langle\langle a\rangle\rangle \otimes q'$ for some q' such that $(\sigma', \tau') < \mathrm{Sim}(q')$. Moreover in this case we may assume $(s', t') = (s-1, t-1)$.

(3) The Eigenspace Lemma 2.10 follows by these methods.

(4) Suppose $\sigma < \mathrm{Sim}(q)$ where $\sigma = \langle 1, a_1, \dots, a_{2m}\rangle$. Decompose the associated (C, J) into quaternion subalgebras with involution:
$(C, J) \cong (Q_1, J_1) \otimes \cdots \otimes (Q_m, J_m)$ as in (3.14). Then $[Q_k] = [d\alpha_k, -a_{2k-1}a_{2k}]$ where $\alpha_k = \langle 1, a_1, \dots, a_{2k-1}\rangle$ and J_k has type $(-1)^k$. Deduce some consequences of (2). For instance: If $\alpha \subset \sigma < \mathrm{Sim}(q)$ where $\dim \alpha \equiv 2 \pmod 4$, $\alpha \neq \sigma$ and $d\alpha = \langle 1\rangle$, then q is hyperbolic. (Compare Yuzvinsky (1985).) Many results of this nature follow more easily from Exercise 2.5.

(5) Suppose C is split and J has type 1 so that $(C, J) \cong (\mathrm{End}(V), I_q)$ where (V, q) is a quadratic space of dimension 2^m. Further suppose $C \cong Q_1 \otimes \cdots \otimes Q_m$ where each Q_k is a split quaternion algebra preserved by the involution J. Then q is similar to a Pfister form.

5. **Trace forms once more.** (1) Let A be a central simple F-algebra with involution. There is an algebra isomorphism $\varphi : A \otimes A \xrightarrow{\cong} \mathrm{End}_F(A)$ defined as follows, using an anti-autormophism ι of A: $\varphi(a \otimes b)(x) = ax\iota(b)$ for every $a, b, x \in A$. Let J_1 and J_2 be involutions of the same type on A so that $J_1 \otimes J_2$ is a 1-involution on $A \otimes A$, inducing an involution I_B on $\mathrm{End}_F(A)$. The isometry class of this symmetric bilinear form B on A depends only on the isomorphism classes of the involutions J_1, J_2, and is independent of the choice of ι.

(2) The form $B : A \times A \to F$ can be chosen to satisfy:
$B(axb, y) = B(x, J_1(a)yJ_2(b))$ for every $a, b, x \in A$. Express B as a trace form.

(3) Suppose $A = C(-\sigma_1 \perp \tau)$ is the Clifford algebra for an (s, t)-pair (σ, τ) such that $s + t$ is odd. Let $J_1 = J_2$ be the corresponding (s, t)-involution. Then B is a Pfister form.

(4) Let $A = \left(\frac{-a, x}{F}\right) \cong \left(\frac{-b, y}{F}\right)$ be a quaternion algebra, so that $\langle\langle a, -x\rangle\rangle \simeq \langle\langle b, -y\rangle\rangle$. Let J_1 be the involution corresponding to $(\langle 1, a\rangle, \langle x\rangle)$, and J_2 the involution for $(\langle 1, b\rangle, \langle y\rangle)$. Then $J_1 \otimes J_2$ yields I_B on $\mathrm{End}_F(A)$. Then $(A, B) \simeq \langle\langle a, xb\rangle\rangle \simeq \langle\langle b, ya\rangle\rangle$.

(Hint. (2) Let $J_1 = J_2^w$ for $w \in A^\bullet$ with $J_1(w) = w$. Then $B(x, y) = \mathrm{tr}(wJ_1(x)y) = \mathrm{tr}(wyJ_2(x))$.

(3) Use Exercise 3.14.)

6. **$\otimes$ of irreducibles.** (1) Suppose A_1 and A_2 are central simple F-algebras with irreducible modules V_1, V_2, respectively. Then $V_1 \otimes V_2$ becomes an $A_1 \otimes A_2$-module where the action is defined "diagonally": $(a_1 \otimes a_2)(v_1 \otimes v_2) = (a_1v_1) \otimes (a_2v_2)$. Let D_i be the "division algebra part" of A_i. That is $A_i \cong \mathbb{M}_{n_i}(D_i)$.

Lemma. *$V_1 \otimes V_2$ is an irreducible $A_1 \otimes A_2$-module if and only if $D_1 \otimes D_2$ is a division algebra.*

(2) Here is an analog to Corollary 6.11: Suppose $(C, J) \cong (A_1, J_1) \otimes (A_2, J_2)$ in the category of central simple algebras with involution. Suppose V_k is an A_k-module so that $V = V_1 \otimes V_2$ is a C-module. If q is a quadratic form on V which admits (C, J) does it follow that $(V, q) \cong (U_1, q_1) \otimes (U_2, q_2)$ for some quadratic spaces (U_k, q_k) admitting A_k?

(Hint. (1) Count the dimensions. Suppose D_i has degree d_i over F. Then $\dim V_i = n_i d_i^2$. If $D_1 \otimes D_2 \cong \mathbb{M}_r(D)$ for a division algebra D of degree d over F then $d_1 d_2 = rd$. Compute that an irreducible $A_1 \otimes A_2$-module has dimension $n_1 n_2 r d^2$. Then $V_1 \otimes V_2$ is irreducible if and only if $\dim V_1 \otimes V_2 = n_1 n_2 r d^2$.)

7. **Uniqueness of the forms.** Suppose q and q' are regular quadratic forms on the vector space V where $\dim V = n$.

(1) Suppose $S \subseteq \mathrm{End}(V)$ is a linear subspace which is a (regular) subspace of similarities for both forms q and q'. Must the induced forms σ, σ' on S coincide?

(2) Suppose $S, T \subseteq \mathrm{End}(V)$ are linear subspaces and that (S, T) is an (s, t)-family relative to both q and q'. Then the induced forms (σ, τ) and (σ', τ') coincide. Express $n = 2^m n_0$ where n_0 is odd and suppose further that $s + t \geq 2m + 1$. Then $J = J'$ and $q' = c \cdot q$ for some $c \in F^{\bullet}$.

(Hint. (1) Let J, J' be the involutions and express $J' = J^g$. For each $f \in S$, $\sigma'(f) = \zeta \cdot \sigma(f)$ for some $\zeta \in F$ with $\zeta^n = 1$. This ζ is independent of f. Are there examples where $\zeta \neq 1$?

(2) Let C be the associated Clifford algebra and note that the similarity representation $C \to \mathrm{End}(V)$ is surjective. In fact this uniqueness holds true whenever the given family is “minimal” as defined in the next chapter.)

Notes on Chapter 6

The analysis of central simple algebras with involution was covered in some depth by Albert (1939), who used somewhat different terminology. Most of the results in this chapter have appeared in other books. See especially Knus et al. (1998), §3.

The invariant $\det(J)$ in (6.8) is generalized in (10.24) below.

The ideas for (6.11), Exercise 4 and Exercise 6 follow Yuzvinsky (1985).

Exercise 1. The computation of the type of the standard involution of a central simple Clifford algebra was done by Chevalley (1954) using a different technique. The dimension counting method is mentioned in Jacobson (1964).

Chapter 7

Unsplittable (σ, τ)-Modules

Given (σ, τ), what is the dimension of an unsplittable (σ, τ)-module? We present a complete answer when the associated Clifford algebra C is split or reduces to a quaternion algebra. We also characterize the (s, t)-pairs (σ, τ) which have unsplittables of minimal dimension.

Notations. Let (σ, τ) be a pair of quadratic forms where $\dim \sigma = s$, $\dim \tau = t$. Assume σ represents 1 and define σ_1 by $\sigma = \langle 1 \rangle \perp \sigma_1$. Define $\beta = \sigma \perp -\tau$ and $\beta_1 = \sigma_1 \perp -\tau$. Let $C = C(-\beta_1)$ be the associated Clifford algebra with involution $J = J_S$. Then $\dim C = 2^{s+t-1}$. Let z be an "element of highest degree" in C and $Z = F + Fz$.

The Basic Sign Calculation (2.4) says: $J(z) = z$ if and only if $s \equiv t$ or $t + 1 \pmod 4$. A direct calculation shows that $d\beta = d(-\beta_1)$ and $c(\beta) = c(-\beta_1)$. As noted in (4.2) an unsplittable (σ, τ)-module has dimension 2^k for some k where $s + t \leq 2k + 2$. When can equality hold?

7.1 Lemma. *Suppose $s + t = 2m + 2$. Then $(\sigma, \tau) < \mathrm{Sim}(V, B)$ for some 2^m-dimensional λ-space (V, B) (for some $\lambda = \pm 1$) if and only if $d\beta = \langle 1 \rangle$, $c(\beta) = 1$ and $s \equiv t \pmod 4$.*

Proof. If such (V, B) exists let $\pi : C \to \mathrm{End}(V)$ be the representation. By comparing dimensions we must have $C \cong C_0 \times C_0$ and $\pi(C_0) = \mathrm{End}(V)$. Therefore $d\beta = \langle 1 \rangle$ and $c(\beta) = [C_0] = 1$. Furthermore $\pi(z)$ must be a scalar, so that $J(z) = z$ since the involutions are compatible. The Basic Sign Calculation (2.4) then implies that $s \equiv t \pmod 4$.

Conversely since $s + t - 1$ is odd and $c(\beta) = 1$ we find $[C_0] = 1$ so that $C_0 \cong \mathrm{End}(V)$ for some V with $\dim V = 2^m$. Since $d\beta = \langle 1 \rangle$ the Structure Theorem implies that $C \cong C_0 \times C_0$ and the restriction of J to C_0 induces an involution I on $\mathrm{End}(V)$, corresponding to a λ-form B on V by (6.3). From $s \equiv t \pmod 4$ we find $J(z) = z$, so the composite map $C \to C_0 \cong \mathrm{End}(V)$ is compatible with the involutions and (V, B) becomes a (C, J)-module. □

Note. The conditions $\dim \beta =$ even, $d\beta = \langle 1 \rangle$ and $c(\beta) = 1$ are equivalent to: $\beta \in J_3(F)$. (Recall that $J_3(F)$ is the ideal of the Witt ring introduced at the end of

Chapter 3, and that $J_3(F) = I^3F$ by Merkurjev's Theorem.) Since $\beta = \sigma \perp -\tau$, those conditions say: $\sigma \equiv \tau \pmod{J_3(F)}$, or equivalently: $\dim \sigma \equiv \dim \tau \pmod 2$, $d\sigma = d\tau$ and $c(\sigma) = c(\tau)$.

7.2 Lemma. *Let (V, B) be a λ-symmetric (C, J)-module where $\dim V = 2^m$ and $s + t = 2m + 1$. Then I_B is the unique involution on $\operatorname{End}(V)$ compatible with (C, J). Consequently every (C, J)-module of dimension 2^m is C-similar to (V, B).*

Proof. The uniqueness of the involution is clear since the representation $C \to \operatorname{End}(V)$ is bijective. If (V', B') is another (C, J)-module of dimension 2^m then $V' \cong V$ as C-modules. Let $h : V \to V'$ be a C-isomorphism and define the form B_1 on V by: $B_1(x, y) = B'(h(x), h(y))$. Then h is a C-isometry $(V, B_1) \to (V', B')$ and the forms here admit (C, J). By the uniqueness of the involution, $I_{B_1} = I_B$ so that $B_1 = aB$ for some $a \in F^\bullet$. Then h is an a-similarity $(V, B) \to (V', B')$. (Compare the proof of (6.6).) □

This result is also true if $s + t = 2m + 2$, except that the C-module may have to be "twisted" by the main automorphism of C to ensure that $V' \cong V$. (There are two irreducible C-modules as described in (4.12).)

The next step is to separate the types of the involutions used above. This refinement of (7.1) is equivalent to computing the type of the involution J_S.

7.3 Proposition. *Suppose $s + t = 2m + 2$. Then $(\sigma, \tau) < \operatorname{Sim}(V, q)$ where (V, q) is a quadratic space of dimension 2^m if and only if $d\beta = \langle 1 \rangle$, $c(\beta) = 1$ and $s \equiv t \pmod 8$. For the case of alternating forms the congruence changes to $s \equiv t + 4 \pmod 8$.*

Proof. Suppose that $d\beta = \langle 1 \rangle$, $c(\beta) = 1$ and $s \equiv t \pmod 4$. Then $(\sigma, \tau) < \operatorname{Sim}(V, B)$ for some 2^m-dimensional λ-space (V, B). If $s \equiv t \pmod 8$ we will show $\lambda = 1$. By (2.8) we have an example of an $(m+1, m+1)$-family $(\alpha, \alpha) < \operatorname{Sim}(W, \varphi)$ where $\dim W = 2^m$. Since $s \equiv t \pmod 8$ the Shift Lemma (2.6) produces $(\sigma', \tau') < \operatorname{Sim}(W, \varphi)$ where $\dim \sigma' = s$ and $\dim \tau' = t$. Extending scalars to an algebraic closure K of F we see that $\sigma \simeq \sigma'$ and $\tau \simeq \tau'$ over K, and Lemma 7.2 implies that (V, B) and (W, φ) are similar over K and we conclude that $\lambda = 1$. Analogously if $s \equiv t + 4 \pmod 8$ then $\lambda = -1$.

Conversely, suppose $(\sigma, \tau) < \operatorname{Sim}(V, q)$ where $\dim V = 2^m$. Then $d\beta = \langle 1 \rangle$, $c(\beta) = 1$ and $s \equiv t \pmod 4$, by (7.1). If $s \equiv t + 4 \pmod 8$ we obtain a contradiction from the proof above. Therefore $s \equiv t \pmod 8$. A similar argument works when $\lambda = -1$. □

7.4 Corollary. (1) *If $s + t$ is odd then C is central simple, and J_S has type* 1 *iff $s \equiv t \pm 1 \pmod 8$.*

(2) *If $s + t$ is even then C_0 is central simple, and the restriction J^+ of J_S has type* 1 *iff $s \equiv t$ or $t + 2 \pmod 8$.*

Proof. (1) Suppose $s + t = 2m + 1$. Extending to a splitting field we may assume $C \cong \text{End}(V)$ where $\dim V = 2^m$. If J_S has type λ there is an induced λ-form B on V so that $(\sigma, \tau) < \text{Sim}(V, B)$. By the Expansion Lemma 2.5, (σ, τ) expands to either an $(s + 1, t)$-family or an $(s, t + 1)$-family in $\text{Sim}(V, B)$. Apply (7.3).

(2) As in (3.9) C_0 becomes a Clifford algebra and J^+ is the involution corresponding to an $(s-1, t)$-family. Now apply part (1) to compute the type. A similar argument works in the case $t \geq 1$, viewing C_0 as the algebra for a $(t, s - 1)$-family. □

So far in this chapter we have analyzed cases where $c(\beta) = 1$. We push these ideas one step further by allowing $c(\beta) =$ quaternion. This means that $c(\beta)$ is represented by a (possibly split) quaternion algebra in the Brauer group.

7.5 Corollary. (1) *Suppose* $(\sigma, \tau) < \text{Sim}(V, B)$ *where* $\dim V = 2^m$. *If* $s+t \geq 2m-1$ *then* $c(\beta) =$ quaternion.

(2) *If* $c(\beta) =$ quaternion *and* $s + t \leq 2m - 1$ *then there are* λ*-symmetric* (σ, τ)*-modules of dimension* 2^m*, for both values of* λ.

Proof. (1) Generally $s + t \leq 2m + 2$. We have seen that if $s + 1 \geq 2m + 1$ then $c(\beta) = 1$. If $s + t = 2m$ then C_0 is central simple and we have $C_0 \otimes A \cong \text{End}(V)$ where A is the centralizer of C_0. Counting dimensions we find $\dim A = 4$ so that A is a quaternion algebra and $c(\beta) = [C_0] = [A] =$ quaternion. If $s + t = 2m - 1$ a similar argument works.

(2) Suppose $s+t$ is odd. It suffices to settle the case $s+t = 2m-1$. If $c(\beta) = [A]$ where A is a quaternion algebra, then $[C \otimes A] = 1$ so that $C \otimes A \cong \text{End}(V)$ where $\dim V = 2^m$. Since involutions of both types exist on A there are regular λ-forms on V which admit C, for both values of λ. Suppose $s + t$ is even. Then $s + t + 1 \leq 2m - 1$ and we can apply the odd case to $(\sigma, \tau \perp \langle 1 \rangle)$ after noticing that $c(\beta \perp \langle -1 \rangle) = c(\beta) =$ quaternion. □

Next we consider expansions of a given (s, t)-family, generalizing the Expansion Lemma 2.5. Recall that when $s + t$ is odd we can "adjoin z" to $(S, T) \subseteq \text{Sim}(V, q)$ to form a family (S_0, T_0) which is one dimension larger. This larger family has $s_0 \equiv t_0 \pmod 4$ and $d\beta_0 = \langle 1 \rangle$. Furthermore the module V is not a faithful $C_{(0)}$-module, for the larger Clifford algebra $C_{(0)}$. This means that $C_{(0)} \to \text{End}(V)$ is not injective, so that the element "z" for the larger family acts as a scalar. Conversely every non-faithful family arises this way from a smaller family.

7.6 Expansion Proposition. *Suppose* $(S, T) \subseteq \text{Sim}(V, q)$ *is an* (s, t)*-family where* $\dim V = 2^m$ *and* $s+t = 2m-1$. *Then* (S, T) *expands to an* (s', t')*-family* $(S', T') \subseteq \text{Sim}(V, q)$ *where* $s'+t' = 2m+2$. *Moreover, any expansion of* (S, T) *either is inside* (S', T') *or is obtained from* (S, T) *by adjoining* z.

Proof. The Clifford algebra C is central simple of dimension 2^{2m-2}. The representation $C \to \mathrm{End}(V)$ is then injective and we view C as the subalgebra of $\mathrm{End}(V)$ generated by S and T. By the Double Centralizer Theorem, $C \otimes A \cong \mathrm{End}(V)$ where $A = \mathrm{End}_C(V)$ is the centralizer of C. Then $\dim A = 4$ so that A must be a quaternion algebra, and I_q preserves C so it induces an involution K on A.

The element $z \in C$ anti-commutes with every element of $S_1 \cup T$ and $J(z) = \pm z$. If $a \in A$ and $K(a) = \pm a$ then az can be adjoined to S or T, depending on whether $I_q(za) = K(a)J(z)$ equals $-za$ or za. When $a = 1$ we have the situation of the Expansion Lemma 2.5. To adjoin more than one dimension to (S, T) we need anticommuting elements of A, so let us stick to the pure quaternions A_0. Define the eigenspaces $A_0 = A_+ \oplus A_-$ where $K(x) = \lambda x$ for $x \in A_\lambda$. Then either $(S + zA_+, T + zA_-)$ or $(S + zA_-, T + zA_+)$ forms an (s', t')-family in $\mathrm{Sim}(V, q)$. Since $\dim A_+ + \dim A_- = 3$ we see that $s' + t' = s + t + 3 = 2m + 2$.

For the uniqueness suppose $(S", T")$ is some expansion of (S, T), say $(S", T") = (S \perp R_-, T \perp R_+)$. Then $R_- + R_+ \subseteq zA$ since every element of $R_- + R_+$ anticommutes with $S_1 \cup T$. If $R_- + R_+ = Fz$ then the family $(S", T")$ was obtained just by adjoining z. Otherwise $R_- + R_+ \subseteq zA_0$. Furthermore if $f \in R_\varepsilon$ then $K(f) = \pm f$, and it follows that R_- and R_+ are contained in A_+ and A_-, in some order. Therefore $(S", T")$ is contained in (S', T'). □

Of course the exact dimension of A_+ (either 0 or 2 as in (6.8)), and whether zA_+ is adjoined to S or to T, depend on the values of s and t. We do not need to keep careful track of this in the proof above because we know from (7.3) that $s' \equiv t' \pmod 8$.

Exactly when does a given pair (σ, τ) possess a quadratic module of dimension 2^m? We can now refine Theorem 2.11 and answer this question, provided the Witt invariant is quaternion.

7.7 Theorem. *Suppose* $c(\beta) =$ quaternion. *Then there is a quadratic* (σ, τ)*-module of dimension* 2^m *if and only if one of the following holds:*

(1) $s + t \le 2m - 1$.

(2) $s + t = 2m$ *and either:* $d\beta = \langle 1 \rangle$ *and* $s \equiv t \pmod 4$, *or:* $c(\beta)$ *is split by* $F(\sqrt{d\beta})$ *and* $s \equiv t - 2, t$ *or* $t + 2 \pmod 8$.

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

(4) $s + t = 2m + 2$, $d\beta = \langle 1 \rangle$, $c(\beta) = 1$ *and* $s \equiv t \pmod 8$.

Proof. Suppose $(\sigma, \tau) < \mathrm{Sim}(V, q)$ where $\dim V = 2^m$. Then we know that $s + t \le 2m + 2$. If $s + t \le 2m - 1$ then (7.5) applies and if $s + t = 2m + 2$ we use (7.3). If $s + t = 2m + 1$, then by the Expansion Lemma 2.5 we can expand (σ, τ) to a larger family (σ', τ'). By (7.3) we know that $d\beta' = \langle 1 \rangle$, $c(\beta') = 1$ and $s' \equiv t' \pmod 8$. Since $\beta' = \beta \perp \langle d \rangle$ for some $d \in F^\bullet$, it follows that $c(\beta) = c(\beta' \perp \langle -d \rangle) = c(\beta')[d\beta', d] = 1$ and either $s \equiv t + 1$ or $s + 1 \equiv t \pmod 8$.

Now suppose that $s+t = 2m$. Choose a subfamily (σ_0, τ_0) where $s_0+t_0 = 2m-1$. If the original family is non-faithful then it must be obtained from (σ_0, τ_0) by adjoining z and we conclude from the Expansion Lemma that $d\beta = \langle 1 \rangle$ and $s \equiv t \pmod 4$. Otherwise by (7.6) the family (σ, τ) lies within a full expansion (σ', τ') where $s'+t' = 2m+2$. Then (s', t') must equal $(s+2, t)$, $(s+1, t+1)$ or $(s, t+2)$, and we know that $s \equiv t-2$, t or $t+2 \pmod 8$. Also $\beta' = \beta \perp \langle x, y \rangle$ for some $x, y \in F^\bullet$. Then $d\beta = d(\beta' \perp \langle -x, -y \rangle) = \langle -xy \rangle$ and $c(\beta) = c(\beta' \perp \langle -x, -y \rangle) = [-x, -y]$ which is split by the field $F(\sqrt{-xy}) = F(\sqrt{d\beta})$.

For the converse suppose (σ, τ) is given satisfying one of those conditions. If $s+t = 2m-1$ we are done by (7.5) and if $s+t = 2m+2$ we apply (7.3). Suppose $s+t = 2m+1$. Letting $d = -d\beta$ we find that $c(\beta \perp \langle d \rangle) = c(\beta)[d\beta, d] = 1$ since $c(\beta) = 1$. Let (σ', τ') equal either $(\sigma \perp \langle d \rangle, \tau)$ or $(\sigma, \tau \perp \langle -d \rangle)$, according as $s \equiv t-1$ or $t+1 \pmod 8$. Then by (7.3) we have $(\sigma, \tau) \subset (\sigma', \tau') < \mathrm{Sim}(V, q)$ where $\dim V = 2^m$.

Suppose $s+t = 2m$. In the case $d\beta = \langle 1 \rangle$ and $s \equiv t \pmod 8$ we can remove one dimension from σ or τ to get a subfamily (σ_0, τ_0) having $s_0 + t_0 = 2m-1$ and $c(\beta_0) = c(\beta) =$ quaternion. Then there is a quadratic (σ_0, τ_0)-module of dimension 2^m, and the Expansion Lemma makes it a (σ, τ)-module. In the final case suppose $d\beta = \langle d \rangle$ and $c(\beta) = [d, x]$ for some $x \in F^\bullet$. Define $\beta' = \beta \perp \langle -x, xd \rangle$ and note that $d\beta' = \langle 1 \rangle$ and $c(\beta') = c(\beta)[-x, xd][d, d] = 1$. Define a pair (σ', τ') by enlarging (σ, τ) appropriately to make $\beta' \simeq \sigma' \perp -\tau'$ and $s' \equiv t' \pmod 8$. Then again by (7.2) we get $(\sigma, \tau) \subset (\sigma', \tau') < \mathrm{Sim}(V, q)$ where $\dim V = 2^m$. □

The information in this theorem can be restated to provide the dimension of an unsplittable (σ, τ)-module whenever $c(\beta) =$ quaternion. We do this now, choosing the notation so that in each case the smallest possible unsplittable dimension is 2^m. That is, $m = \delta(s, t)$ in the sense of (2.15).

7.8 Theorem. *Let (σ, τ) be a pair of quadratic forms where σ represents* 1 *and* $\dim \sigma = s$ *and* $\dim \tau = t$. *Define $\beta = \sigma \perp -\tau$ and suppose $c(\beta) =$* quaternion. *Let ψ be an unsplittable quadratic (σ, τ)-module.*

If $\boxed{s \equiv t \pmod 8}$ *let $s+t = 2m+2$. Then $m \equiv t-1 \pmod 4$ and:*

$\dim \psi = 2^m$ *iff $d\beta = \langle 1 \rangle$ and $c(\beta) = 1$.*

$\dim \psi = 2^{m+1}$ *iff the first case fails and either $d\beta = \langle 1 \rangle$* or *$c(\beta)$ is split by $F(\sqrt{d\beta})$.*

$\dim \psi = 2^{m+2}$ *otherwise.*

If $\boxed{s \equiv t \pm 1 \pmod 8}$ *let $s+t = 2m+1$. Then $m \equiv t$ or $t-1 \pmod 4$ and:*

$\dim \psi = 2^m$ *iff $c(\beta) = 1$.*

$\dim \psi = 2^{m+1}$ *otherwise.*

If $\boxed{s \equiv t \pm 2 \pmod 8}$ *let $s+t = 2m$. Then $m \equiv t \pm 1 \pmod 4$ and:*

$\dim \psi = 2^m$ *iff* $c(\beta)$ *is split by* $F(\sqrt{d\beta})$.

$\dim \psi = 2^{m+1}$ *otherwise.*

If $\boxed{s \equiv t + 4 \pmod 8}$ *let* $s + t = 2m$. *Then* $m \equiv t + 2 \pmod 4$ *and:*

$\dim \psi = 2^m$ *iff* $d\beta = \langle 1 \rangle$.

$\dim \psi = 2^{m+1}$ *otherwise.*

If $\boxed{s \equiv t \pm 3 \pmod 8}$ *let* $s + t = 2m - 1$. *Then* $m \equiv t + 2$ *or* $t + 3 \pmod 4$ *and:*

$\dim \psi = 2^m$.

Proof. These criteria can be read off directly from (7.7). □

The pairs (σ, τ) whose unsplittable quadratic modules are as small as possible are the nicest kind. Recall from (2.15) that for given (s, t) the smallest unsplittable module that an (s, t)-family can have is $2^{\delta(s,t)}$. We define an (s, t) pair (σ, τ) to be a *minimal* pair if its unsplittable quadratic modules have this smallest possible dimension $2^{\delta(s,t)}$. Then (σ, τ) is minimal if and only if $c(\beta) =$ quaternion and (σ, τ) satisfies the conditions for $\dim \psi = 2^m$ given in (7.8).

Remark. The dimensions of unsplittables for alternating (σ, τ)-modules can be found by altering in (7.8) each of the congruences for s and t by 4 (mod 8). (See Exercise 2.6.) We can also define (σ, τ) to be a (-1)-*minimal pair* if its unsplittable alternating modules have the smallest possible dimension.

7.9 Proposition. *Suppose* (σ, τ) *is an* (s, t)*-pair where* $s \geq 1$, $t \geq 0$ *and where the dimension of a quadratic unsplittable is* 2^m. *Then* (σ, τ) *is minimal if and only if one of the following equivalent conditions holds:*

(1) $m = \delta(s, t)$.

(2) *Each unsplittable quadratic* (σ, τ)*-module remains unsplittable after any scalar extension.*

(3) $s > \rho_t(2^{m-1})$.

(4) $$s + t = \begin{cases} 2m + 1 & \text{if } m \equiv t \\ 2m & \text{if } m \equiv t + 1 \\ 2m - 1 \mathit{or}\ 2m & \text{if } m \equiv t + 2 \\ 2m - 1, 2m, 2m + 1 \text{ } \mathit{or} \text{ } 2m + 2 & \text{if } m \equiv t + 3 \end{cases} \pmod 4.$$

Proof. (1) $\iff$ (2) follows from the definition of "minimal".

(3) $\iff$ (4): Use the formulas in (2.13). The lower bounds in (4) come from condition (3). For the upper bounds note that there exists a (σ, τ)-module of dimension 2^m so that $s \leq \rho_t(2^m)$.

(2) $\Longrightarrow$ (3): Suppose (σ, τ) is a minimal (s, t)-pair with an unsplittable module (V, q) of dimension 2^m. If $s \leq \rho_t(2^{m-1})$ then there is some (s, t)-pair (σ', τ')

having a module of dimension 2^{m-1}. Passing to an extension field K we may assume $(\sigma', \tau') \simeq (\sigma, \tau)$. But then (V_K, q_K) is not unsplittable, contrary to hypothesis.

(3) $\implies$ (2): If $s > \rho_t(2^{m-1})$ then (σ, τ) must be minimal since no (s, t)-pair can have a module of dimension 2^{m-1}. □

For example the possible sizes of minimal (s, t) pairs with $s \geq t$ and having unsplittables of dimension 8 are: $(4, 1)$, $(4, 2)$, $(4, 3)$, $(4, 4)$, $(5, 0)$, $(5, 1)$, $(6, 0)$, $(7, 0)$, $(8, 0)$. Every pair $(s\langle 1\rangle, t\langle 1\rangle)$ is minimal (see Exercise 4). The minimal pairs are characterized by a strong uniqueness property for their unsplittable modules. Compare Lemma 7.2.

7.10 Proposition. *An (s, t)-pair (σ, τ) is minimal if and only if there exists a (σ, τ)-module (V, q) such that I_q is the unique* 1*-involution on* $\mathrm{End}(V)$ *compatible with* (C, J_S).

Proof. Let $(\sigma, \tau) < \mathrm{Sim}(V, q)$, view V as a C-module and recall that I_q is a 1-involution on $\mathrm{End}(V)$ compatible with (C, J_S). Let $A = \mathrm{End}_C(V)$ and K the involution on A induced by I_q. Then the 1-involutions on $\mathrm{End}(V)$ compatible with (C, J_S) are exactly the involutions I_q^a where $a \in A^\bullet$ and $K(a) = a$. The unique involution property is equivalent to requiring that $\mathcal{S}^+(A, K)$ have dimension 1. Since this condition is independent of scalar extension we may assume F is algebraically closed.

If $s \leq \rho_t(2^{m-1})$ then there is a quadratic (C, J_S)-module (W, φ) of dimension 2^{m-1}. Let $V = W \oplus W$ and consider the forms $\varphi \perp \langle b\rangle\varphi$ on V for $b \in F^\bullet$. For different values of b these forms provide unequal 1-involutions on $\mathrm{End}(V)$ compatible with (C, J_S).

Conversely suppose $(\sigma, \tau) < \mathrm{Sim}(V, q)$ where $\dim V = 2^m$ and $s > \rho_t(2^{m-1})$. We will show that I_q is unique. If $s + t \geq 2m + 1$ the uniqueness is clear since C maps surjectively onto $\mathrm{End}(V)$. Suppose $s + t = 2m - 1$ so that $A = \mathrm{End}_C(V)$ is a quaternion algebra with $C \otimes A \cong \mathrm{End}(V)$. Then I_q is unique iff K is the bar involution on A, which occurs iff K has type -1. By (6.7) this is equivalent to saying that J_S has type -1 and by (7.4) it occurs iff $s \equiv t \pm 3 \pmod 8$. Since $s + t = 2m - 1$, this congruence is the same as $m \equiv t + 2$ or $t + 3 \pmod 4$.

The remaining case is when $m \equiv t + 1 \pmod 4$ and $s + t = 2m$. Then $s \equiv t + 2 \pmod 8$. As before we have $C_0 \otimes A' \cong \mathrm{End}(V)$ for a quaternion algebra A' having an induced involution K'. Then $A = \mathrm{End}_C(V)$ is the centralizer of $z' = \pi(z)$ in A'. (Here π is the corresponding representation of C.) Since $s \equiv t + 2 \pmod 8$, the sign computation says that $J_S(z) = -z$ so that $K(z') = -z'$. Then z' is a pure quaternion and $A = F + Fz'$. Therefore $\mathcal{S}^+(A, K) = F$ so that I_q is unique. □

The uniqueness of the involution I_q for a minimal pair (σ, τ) implies that all (σ, τ)-unsplittables are C-similar (with the standard exception when C is not simple).

7.11 Corollary. *Suppose (σ, τ) is a minimal (s, t)-pair with unsplittable quadratic module (V, ψ). Then every unsplittable (σ, τ)-module is C-similar to (V, ψ), (up to a twist by the main automorphism when C is not simple). Consequently, $(\sigma, \tau) < \mathrm{Sim}(\alpha)$ if and only if $\psi \mid \alpha$.*

Proof. Suppose (V', ψ') is another (σ, τ)-unsplittable. Then V and V' are C-modules, $\dim V = \dim V' = 2^m$ and $s > \rho_t(2^{m-1})$.

Claim. We may assume $V' \cong V$ as C-modules. For if C is simple the modules are certainly isomorphic. Otherwise s + t is even and we know $s + t \geq 2m - 1$. If $s+t = 2m+2$ the two module structures differ only by the usual "twist" as described in (4.12), so we can arrange $V' \cong V$. Suppose $s + t = 2m$. If there exist two different C-module structures then both cases in Theorem 7.7 (2) hold true. Therefore $s \equiv t \pmod 8$, $d\beta = \langle 1 \rangle$ and $c(\beta) = 1$. But then there exists an (s, t)-family on some quadratic space of dimension 2^{m-1} contrary to the hypothesis $s > \rho_t(2^{m-1})$. This proves the claim.

The argument is completed as in the proof of (7.2). □

Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an (s, t)-family with $s + t \geq 2m - 1$. If $\dim q = 2^m$ then the Expansion Proposition 7.6 implies that there exists an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$. This statement can fail if we allow $\dim q = 2^m n_0$, as seen in Exercise 10. However the assertion does generalize in some cases.

7.12 Corollary. *Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an (s, t)-family and $\dim q = n = 2^m n_0$ where n_0 is odd. If $s = \rho_t(n)$ is the maximal value, then (σ, τ) is minimal pair and there exists an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$.*

Proof. Since $s = \rho_t(2^m) > \rho_t(2^{m-1})$ the pair is minimal. Let $(\sigma, \tau) < \mathrm{Sim}(\psi)$ be the unique unsplittable, so that $\dim \psi = 2^m$ and $q \simeq \psi \otimes \gamma$ where $\dim \gamma$ is odd. Since $s + t \geq 2m - 1$ the Expansion Proposition 7.6 implies that $\mathrm{Sim}(\psi)$ admits an (s', t')-family where $s' + t' = 2m + 2$. Then $s' \equiv t' \pmod 8$ and shifting produces an $(m + 1, m + 1)$-family. □

From Theorem 7.8 we can read off the criteria for an (s, t)-pair (σ, τ) to be minimal. It is interesting to display this calculation explicitly in the case of a single form σ over the real field $\mathbb{R}$.

7.13 Proposition. *Let $\sigma = p\langle 1 \rangle \perp r\langle -1 \rangle$ over $\mathbb{R}$. Then σ is not minimal if and only if there is a dot (•) in the corresponding entry of the following table, indexed by the values of p and r* (mod 8).

$p \diagdown r$	0	1	2	3	4	5	6	7
0								
1				●		●	●	●
2						●	●	●
3		●				●	●	●
4								
5		●	●	●				●
6		●	●	●				
7		●	●	●		●		

Proof. Using calculations of $d\sigma$ and $c(\sigma)$ in Exercises 3.5 and 3.6 we can translate the criteria in (7.8) to congruence conditions on $\dim \sigma$ and $\operatorname{sgn} \sigma$. These yield the table.□

Remark. The proof also shows that σ is (-1)-minimal if and only if $\sigma \perp 2\mathbb{H}$ is minimal. Some of the symmetries in this table are explored in Exercise 4.

At this point we can complete the classification of (s, t)-pairs which have hyperbolic type, as defined in (4.14) and discussed in (6.16). Recall that these are the pairs (σ, τ) such that the unsplittables are not irreducible. With our usual notations, this says that an irreducible C-module does not have a symmetric bilinear form admitting (C, J). Some of the details of the proof below are left to the reader.

7.14 Proposition. *Let (σ, τ) be an (s, t)-pair such that σ represents* 1, *and $\beta = \sigma \perp -\tau$. Then (σ, τ) is of hyperbolic type if and only if one of the following conditions holds:*

$s \equiv t \pm 3 \pmod 8$ *and* $c(\beta) = 1$.

$s \equiv t \pm 2 \pmod 8$ *and* $d\beta = \langle 1 \rangle$.

$s \equiv t + 4 \pmod 8$ *and $c(\beta)$ is split by $F(\sqrt{d\beta})$.*

Proof. Let $C = C(-\sigma_1 \perp \tau)$ with involution $J = J_S$ as usual, and let V be an irreducible C-module. Then (σ, τ) has hyperbolic type iff there is no symmetric bilinear form on V which admits (C, J). Equivalently, there does not exist a 1-involution on $\operatorname{End}(V)$ compatible with (C, J).

Suppose $s + t$ is odd so that C is central simple. Then $A = \operatorname{End}_C(V)$ is a central division algebra and $C \otimes A \cong \operatorname{End}_F(V)$. By (6.13) there exists an involution K on A, and $J \otimes K$ induces an involution I on $\operatorname{End}(V)$. If $A \neq F$ then by (6.15) A has involutions of both types and one of them yields a 1-involution I. If $A = F$ then $\operatorname{type}(I) = \operatorname{type}(J)$. Then by (7.4) we see that (σ, τ) has hyperbolic type iff $c(\beta) = [A] = 1$ and $s \equiv t \pm 3 \pmod 8$.

Suppose $s+t$ is even so that $C = C_0 \otimes Z$ where $Z = F \otimes Fz$. Let $A = \operatorname{End}_{C_0}(V)$, so that A is central simple and $C_0 \otimes A \cong \operatorname{End}_F(V)$. First assume that $d\beta = \langle d \rangle \neq \langle 1 \rangle$. Then $Z \cong F(\sqrt{d})$ is a field and we may view $Z \subseteq A$.

Claim. There exist involutions K_+, K_- on A such that $K_\varepsilon(z) = \varepsilon z$.

This follows from an extension theorem for involutions due to Kneser, (see Scharlau (1985), Theorem 8.10.1). The claim is also proved below in Exercise 10.13.

Let $K = K_\varepsilon$ with ε chosen to make $K(z) = J(z)$. Define $B = \operatorname{Cent}_A(Z) = \operatorname{End}_C(V)$ so that B is a division algebra with center Z. If there exists $x \in B^\bullet$ with $K(x) = -x$ then K and K^x are involutions of both types on A and compatible with (C, J). Therefore if our 1-involution on $\operatorname{End}(V)$ fails to exist then no such x exists, and we see that $K(z) = z$ and $B = Z$. From the dimensions of centralizers we see that A must be a quaternion algebra containing the subfield Z. Furthermore, $J^+ \otimes K$ must have type -1. Since $K(z) = z$ we know that $s \equiv t \pmod 4$ and K has type 1. Then J^+ must have type -1 and $s \equiv t + 4 \pmod 8$ by (7.4). Thus in this case when $s + t$ is even and $d\beta \neq \langle 1 \rangle$, we see that (σ, τ) is of hyperbolic type iff $c(\beta) = [A]$ is split by $F(\sqrt{d})$ and $s \equiv t + 4 \pmod 8$.

Finally suppose $d\beta = \langle 1 \rangle$ so that $z^2 = 1$ and z acts as ± 1 on the irreducible module V. Then V is an irreducible C_0-module and A is a division algebra. If $J(z) = -z$ there can be no compatible involutions at all. This is the case $s \equiv t+2 \pmod 4$ already noted after (4.14). Otherwise $s \equiv t \pmod 4$ so that $J(z) = z$ and any involution K on A is compatible with (C, J). As before if $A \neq F$ there exist involutions of both types on A. Then (σ, τ) has hyperbolic type iff $A = F$ and the induced involution J^+ on C_0 has type -1. By (7.4) this occurs iff $c(\beta) = 1$ and $s \equiv t + 4 \pmod 8$. □

Remark. The criteria for (σ, τ) to be of (-1)-hyperbolic type are obtained by cycling the congruences above by 4 (mod 8).

7.15 Corollary. *Let $\sigma = p\langle 1 \rangle \perp r\langle -1 \rangle$ over $\mathbb{R}$. Then σ is of hyperbolic type if and only if there is a dot (•) in the corresponding entry of the following table, indexed by the values of p and r* (mod 8).

$p \backslash r$	0	1	2	3	4	5	6	7
0								
1		•	•	•		•		
2		•	•	•				
3		•	•	•				•
4								
5		•				•	•	•
6						•	•	•
7				•		•	•	•

Proof. Apply the proposition and the calculations of $d\sigma$ and $c(\sigma)$. □

Remark. From the symmetries of the tables we see that σ has hyperbolic type if and only if $\sigma \perp 4\mathbb{H}$ does as well. Analysis of the proof shows that σ has (-1)-hyperbolic type if and only if $\sigma \perp 4\langle 1\rangle$ has hyperbolic type.

If $(S, T) \subseteq \mathrm{Sim}(V, q)$ is a pair of amicable subspaces, then so is $(S', T') = (fSg, fTg)$ for any $f, g \in \mathrm{Sim}^\bullet(V, q)$. Conversely if (S, T) and (S', T') are pairs of amicable subspaces in $\mathrm{Sim}(V, q)$, how can we tell whether they are equivalent in this way? One obvious necessary condition is that the induced pairs of quadratic forms (σ, τ) and (σ', τ') be similar. For minimal pairs that condition suffices.

7.16 Corollary. *Suppose (S, T) and (S', T') are pairs of amicable subspaces of $\mathrm{Sim}(V, q)$ which are similar as quadratic spaces: $S' \simeq \langle c\rangle S$ and $T' \simeq \langle c\rangle T$ for some $c \in F^\bullet$. If $\dim V = 2^m$ and $s > \rho_t(2^{m-1})$, then there exist $f, g \in \mathrm{Sim}^\bullet(V, q)$ such that $(S', T') = (fSg, fTg)$.*

Proof. We may assume $1_V \in S$. Then there exists $f \in S'$ with $\mu(f) = c$. We compose with f^{-1} to assume $S' \simeq S$ and $T' \simeq T$. The Clifford algebra $C = C(-\sigma_1 \perp \tau)$ with the involution $J = J_S$ then has two representations π and π' on (V, q) corresponding to these two (s, t)-families. That is, (V, q) becomes a (C, J)-module in two ways. In the notation used at the start of Chapter 4, the subspaces $\breve{S}, \breve{T} \subseteq C$ satisfy: $S = \pi(\breve{S})$, $T = \pi(\breve{T})$, and $S' = \pi'(\breve{S})$, $T' = \pi'(\breve{T})$.

Since $s > \rho_t(2^{m-1})$ the (C, J)-module structures on V must be unsplittable. By (7.11) these two unsplittables are C-similar (possibly after twisting π in the non-simple case). Let $h : V \to V$ be a C-similarity carrying the π-structure to the π'-structure. Then $h(\pi(c)x) = \pi'(c)h(x)$ for all $c \in C$ and $x \in V$. That is, $\pi'(c) = h \circ \pi(c) \circ h^{-1}$. Therefore $S' = hSh^{-1}$ and $T' = hTh^{-1}$. □

In some cases we can eliminate the restriction on dimensions in (7.16). We are given (C, J) and two quadratic (C, J)-modules (V, q) and (V', q') which are F-similar, and hope to conclude that they are C-similar. First suppose C is simple, so that V and V' are isomorphic as C-modules. They break into unsplittables

$$V = V_1 \perp \cdots \perp V_k \quad \text{and} \quad V' = V'_1 \perp \cdots \perp V'_k.$$

Assuming (σ, τ) is minimal we see from (7.11) that all V_i and V'_j are C-similar. In order to glue these similarities we must find the unsplittables together with C-similarities $g_j : V_j \to V'_j$ such that the norms $\mu(g_j)$ are all equal. For example suppose $F = \mathbb{R}$ and (V, q) is positive definite. Then any C-similarity between the unsplittable components has positive norm so it can be scaled to yield a C-isometry, and the "gluing" works. The same idea goes through in a few more cases over $\mathbb{R}$ (see Exercise 8).

Suppose now that C is not simple, so that $s + t$ is even and $d\sigma = d\tau$. In order to ensure that the two C-module structures on V are isomorphic, we require that the two (s, t)-families have the same "character". Let $z = z(S_1 \perp T)$ be an element of highest degree with $z^2 = 1$. As mentioned before (4.12) there are exactly two irreducible C-modules V_+ and V_-, chosen so that z acts as $\varepsilon 1_{V_\varepsilon}$ on V_ε. Any C-module V is isomorphic to a direct sum of n_+ of copies of V_+ and n_- copies of V_-, for some integers $n_+, n_- \geq 0$. Then

$$\dim V = (n_+ + n_-) \cdot 2^m \quad \text{and} \quad \operatorname{trace}(\pi(z)) = (n_+ - n_-) \cdot 2^m,$$

where $2^m = \dim V_+ = \dim V_-$. Therefore two C-modules are isomorphic iff they have the same dimension and the same value for $\operatorname{trace}(\pi(z))$.

Since we are interested only in the spaces S, T and not in the representation π, we may "twist" π by replacing it by $\pi \circ \alpha$ where α is the canonical automorphism of C. This operation leaves the subspaces S and T unchanged but it alters the sign of $\operatorname{trace}(\pi(z))$. Therefore the non-negative integer $|\operatorname{trace}(\pi(z))|$ depends only on the given family (S, T), and not on the choice of the representation π.

7.17 Definition. If $(S, T) \subseteq \operatorname{Sim}(V, q)$ is an (s, t)-family, let z be an element of highest degree in the Clifford algebra C, chosen so that if C is not simple then $z^2 = 1$. Define $\chi(S, T) = |\operatorname{trace}(\pi(z))|$, the *character* of the family.

7.18 Lemma. *If* $\chi(S, T) \neq 0$ *then* $s \equiv t \pmod 4$, $d\sigma = d\tau$ *and* (S, T) *is maximal.*

Proof. If (S, T) can be expanded in $\operatorname{Sim}(V, q)$ then there exists $f \in \operatorname{Sim}^\bullet(V, q)$ which anticommutes with $\pi(z)$, so that $\operatorname{trace}(\pi(z)) = 0$. If $s + t$ is odd then (S, T) can be expanded. If $s \equiv t + 2 \pmod 4$ then $J(z) = -z$ so that $\operatorname{trace}(\pi(z)) = 0$. Finally suppose $s \equiv t \pmod 4$ but $d\sigma \neq d\tau$. Then $Z = F + Fz \cong F(\sqrt{d})$ is a field and the minimal polynomial for $\pi(z)$ is $x^2 - d$, which is irreducible. Then $\operatorname{trace}(\pi(z)) = 0$ since the characteristic polynomial must be a power of $x^2 - d$. □

7.19 Proposition. *Suppose* (V, q) *is positive definite over the real field* $\mathbb{R}$. *Suppose* (S, T) *and* (S', T') *are* (s, t)*-families in* $\operatorname{Sim}(V, q)$ *such that* $\chi(S, T) = \chi(S', T')$. *Then* $(S', T') = (hSh^{-1}, hTh^{-1})$ *for some* $h \in \mathrm{O}(V, q)$.

Proof. Since the forms are positive definite over $\mathbb{R}$ we have $S \simeq S' \simeq s\langle 1\rangle$ and $T \simeq T' \simeq t\langle 1\rangle$ as quadratic spaces. For C and J as usual, we see that (V, q) becomes a quadratic (C, J)-module in two ways. We may twist the representation π by α, if necessary, to assume that $\operatorname{trace}(\pi(z)) = \operatorname{trace}(\pi'(z))$. Then these two C-module structures are isomorphic. The two (C, J)-modules can then be broken into unsplittables

$$V = V_1 \perp \cdots \perp V_k \quad \text{and} \quad V' = V_1' \perp \cdots \perp V_k'$$

in such a way that V_i and V_i' are isomorphic C-modules. Since $(s\langle 1\rangle, t\langle 1\rangle)$ is a minimal pair we know as in (7.11) that V_i and V_i' are C-similar. The norm of such a similarity must be positive in $\mathbb{R}$ so we may scale it to find a C-isometry $h_i : V_i \to V_i'$. Glue these h_i's together to obtain an isometry $h : (V, q) \to (V, q)$ carrying the π-structure to the π'-structure. This completes the proof, as in (7.16). □

7.20 Corollary. (1) *Suppose* $(S, T) \subseteq \mathrm{Sim}(V, n\langle 1\rangle)$ *over* $\mathbb{R}$. *If* $\chi(S, T) = 0$ *then* (S, T) *can be enlarged to a family of maximal size. That trace condition always holds if* $s \not\equiv t \pmod 4$.

(2) *Every sum of squares formula of size* $[r, n, n]$ *over* $\mathbb{R}$ *is equivalent to one over* $\mathbb{Z}$.

Exercises for Chapter 7

1. **Maximal families.** Suppose $(S, T) \subseteq \mathrm{Sim}(V, B)$ is an (s, t)-family with associated representation $\pi : C \to \mathrm{End}(V)$.

(1) If π is non-faithful then (S, T) is maximal. More generally if $\chi(S, T) \neq 0$ (as defined in (7.17)) then (S, T) is maximal.

(2) Find examples of faithful maximal families. If $(S, T) \subseteq \mathrm{Sim}(V, B)$ is maximal and faithful, what can be said about the algebra $A = \mathrm{End}_{C_0}(V)$?

(Hint. (1) If $f \in \mathrm{Sim}^\bullet(V)$ anticommutes with $S_1 + T$ then f must anticommute with $\pi(z)$.)

2. **Why is $c(\beta)$ split by $F(\sqrt{\beta})$?** In the situation of Theorem 7.7 suppose $s + t = 2m$ and there is a quadratic module (V, q) of dimension 2^m. Let $Z \cong F(\sqrt{\beta})$ be the center of the Clifford algebra C and suppose Z is a field. Then C is a central simple Z-algebra and there is an induced Z-action on V. Then $\dim_Z C = 2^{2m-2}$, $\dim_Z V = 2^{m-1}$ and $C \cong \mathrm{End}_Z(V)$. Therefore $1 = [C]_Z = [C_0 \otimes Z]$ and $c(\beta) = [C_0]$ is split by $F(\sqrt{\beta})$. If $s \equiv t \pmod 4$ then $J(z) = z$. Compute type(J) as a Z-involution to see $s \equiv t \pmod 8$. Is there a similar argument when $d\beta = \langle 1\rangle$?

3. The following can be proved by methods of Chapter 2 or by applying (7.8).

(1) If the dimension of an unsplittable (σ, τ)-module is 2^m then the dimension of an unsplittable $(\sigma \perp \langle a\rangle, \tau \perp \langle a\rangle)$-module is 2^{m+1}.

(2) If (σ, τ) is a minimal pair and α is any quadratic form, then $(\sigma \perp \alpha, \tau \perp \alpha)$ is also minimal. If α represents 1 then (α, α) is minimal. If $(\sigma, \tau) < \mathrm{Sim}(\varphi)$ is unsplittable, what is the unsplittable quadratic module for $(\sigma \perp \alpha, \tau \perp \alpha)$?

(3) For any $s \geq 1, t \geq 0$ the pair $(s\langle 1\rangle, t\langle 1\rangle)$ is minimal with (unique) unsplittable module $2^m\langle 1\rangle$, where $m = \delta(s, t)$.

4. (1) If (σ, τ) is minimal and $\varphi = \langle\langle a, b, c\rangle\rangle$ then $(\sigma \perp \varphi, \tau)$ is also minimal.

(2) If (σ, τ) is minimal and $a \in D_F(\sigma)$ then $(\langle a\rangle\sigma, \langle a\rangle\tau)$ is also minimal.

(3) If σ is minimal then $\sigma \perp 8\langle 1\rangle$, $\sigma \perp 8\langle -1\rangle$ and $\sigma \perp \mathbb{H}$ are minimal. If σ is also isotropic then $\langle -1\rangle\sigma$ is minimal. Interpret these in terms of the symmetry of the table in (7.13).

(4) Repeat the observations above using "hyperbolic type" rather than "minimal". Observe from (7.13) and (7.15) that the entry (p, r) is marked in one chart iff $(p, -r)$ is marked in the other. Is there any deeper explanation of this coincidence?

(Hint. (1) Express $\varphi = \alpha \perp (d\alpha)\alpha$ where $\alpha = \langle 1, a, b, c\rangle$ and shift.)

5. Suppose (σ, τ) has the property that every unsplittable (σ, τ)-module is similar to a Pfister form. Then $(\sigma \perp \alpha, \tau \perp \alpha)$ has the same property.

6. Suppose (σ, τ) is a pair where σ represents 1 with unsplittables of dimension 2^m. Then there exist subforms $\sigma' \subset \sigma$ and $\tau' \subset \tau$ such that σ' represents 1 and (σ', τ')-unsplittables have dimension 2^{m-1}.

7. (1) Given an (s, t)-pair (σ, τ) where $\sigma = \langle 1\rangle \perp \sigma_1$, let $\beta = \sigma \perp -\tau$. For which $a \in F^\bullet$ is the $(s + 1, t)$-pair $(\sigma \perp \langle a\rangle, \tau)$ minimal? This occurs if and only if one of the following conditions holds:

$s \equiv t$ or $t - 2 \pmod 8$ and $c(\beta) = [d\beta, -a]$.

$s \equiv t + 1$ or $t - 3 \pmod 8$ and $c(\beta)$ is split by $F(\sqrt{-a \cdot d\beta})$.

$s \equiv t + 2$ or $t + 4 \pmod 8$ and $c(\beta)[d\beta, -a] =$ quaternion.

$s \equiv t + 3 \pmod 8$ and $d\beta = \langle -a\rangle$ and $c(\beta) =$ quaternion.

$s \equiv t - 1 \pmod 8$ and $d\beta = \langle -a\rangle$ and $c(\beta) = 1$.

(2) For what (s, t) is it possible that a non-minimal (s, t)-pair can be expanded to a minimal $(s + 1, t)$-pair?

(3) Similarly analyze the cases where $(\sigma, \tau \perp \langle b\rangle)$ is minimal.

(Hint. (2) $\delta(s + 1, t) = 1 + \delta(s, t)$ if and only if $s - t \equiv 0, 1, 2, 4 \pmod 8$.)

8. **Conjugate subspaces.** (1) Suppose $\{1_V, f_2, \dots, f_t\}$ is an orthogonal basis of some subspace of $\mathrm{Sim}(V, q)$. Define

$$S = \mathrm{span}\{1_V, f_2, f_3, f_4\} \quad \text{and} \quad S' = \mathrm{span}\{1_V, f_2, f_3, f_2 f_3\}.$$

Then S' cannot be expressed as fSg for any $f, g \in \mathrm{GL}(V)$.

(2) Explain Exercise 1.16 using the more abstract notions of (7.16). The strong conjugacy in that exercise seems to require a Clifford algebra C such that $\bar{c} \cdot c \in F$ for every $c \in C$.

(3) Suppose σ, q are forms over $\mathbb{R}$ such that σ is minimal and both forms represent 1. Suppose $S, S' \subseteq \mathrm{Sim}(V, q)$ with $1_V \in S \cap S'$, $S \simeq S' \simeq \sigma$, and $\chi(S) = \chi(S')$.

Question. For which σ, q does it follow that $S' = hSh^{-1}$ for some $h \in \mathrm{O}(V, q)$?

From (7.19) we know it is true when σ, q are positive definite. The same argument proves the statement when σ is positive definite and $\dim \sigma \not\equiv 0 \pmod 4$, (in those cases the algebra C is simple). If σ is of hyperbolic type the statement is certainly true. It fails in all other cases.

(Hint. If σ is definite and C is not simple let $(V_\varepsilon, \psi_\varepsilon)$ be the positive definite irreducible (C, J)-modules. Let $V = \psi_1 \perp \langle -1\rangle\psi_1 \perp \psi_{-1} \perp \langle -1\rangle\psi_{-1}$ and $V' = \psi_1 \perp \psi_1 \perp \langle -1\rangle\psi_{-1} \perp \langle -1\rangle\psi_{-1}$ to get a counterexample. If σ is indefinite and regular type, an irreducible (C, J)-module (W, ψ) admits no C-similarity of norm -1. Then $\psi \perp \psi$ and $\psi \perp \langle -1\rangle\psi$ are C-isomorphic and F-isometric, but are not (C, J)-similar. (Use the Cancellation Theorem mentioned after (4.10).)

9. **Spaces not containing 1.** Suppose $S \subseteq \mathrm{Sim}(V, q)$, choose $g \in S^\bullet$ and define the character $\chi(S) = \chi(g^{-1}S)$ following (7.17) for spaces containing 1_V.

(1) This value is independent of the choice of g.

(2) Generalize the definition and (7.19) to amicable pairs $(S, T) \subseteq \mathrm{Sim}(V, q)$.

(Hint. Recall $z(S)$ defined in Exercise 2.8. Suppose $\dim S \equiv 0 \pmod 4$ and $dS = \langle 1\rangle$. If we choose $z(S)^2 = 1$ then $\chi(S) = |\,\mathrm{trace}(z(S))|$.)

10. **Non-minimal behavior.** There exists an example where $(\langle 1, a\rangle, \langle x\rangle) < \mathrm{Sim}(V, q)$ where $\dim q = 12$ but such that $\mathrm{Sim}(q)$ does not admit any $(3, 3)$-family. Compare this with the assertion in (7.12). Find an explicit example over $\mathbb{R}$.

(Hint. Recall (5.7) (4) and find q such that $\langle\langle a\rangle\rangle \mid q$, $x \in G_F(q)$ but q does not have a 2-fold Pfister factor.)

11. **Unique unsplittables.** A pair (σ, τ) is defined to have *unique unsplittables* if all unsplittable quadratic (σ, τ)-modules are (C, J)-similar, possibly after twisting the associated representation in the non-simple case.

(1) If $(\sigma, \tau) < \mathrm{Sim}(\varphi)$ is unsplittable and (σ, τ) has unique unsplittables, then: $(\sigma, \tau) < \mathrm{Sim}(q)$ if and only if $\varphi \mid q$.

(2) Suppose (σ, τ) is an (s, t)-pair where $s + t$ is odd, and suppose $(\sigma, \tau) < \mathrm{Sim}(V, q)$ is unsplittable. Let C be the associated Clifford algebra with centralizer A, so that $C \otimes A \cong \mathrm{End}(V)$ and $J \otimes K \cong I_q$ as usual. Then (σ, τ) has unique unsplittables iff every $f \in A$ with $K(f) = f$ can be expressed as $f = r \cdot K(g)g$ for some $g \in A$ and $r \in F$.

12. Let (σ, τ) be an (s, t)-pair and suppose $c(\beta) = [-x, -y] \neq 1$.

If $s \equiv t \pm 3 \pmod 8$ then (σ, τ) has unique unsplittables, as defined in Exercise 11.

If $s \equiv t \pm 1 \pmod 8$ then the (C, J)-similarity classes of unsplittables are in one-to-one correspondence with $D_F(\langle x, y, xy\rangle)/F^{\bullet 2}$.

(Hint. Let (V, q) be unsplittable so that $C \otimes A \cong \mathrm{End}(V)$ where $A = (-x, -y/F)$ with induced involution K. If $s \equiv t \pm 3$ then $K = \mathrm{bar}$. Otherwise every (C, J)-unsplittable arises from a 1-involution on A. These are the involutions K_0^e where $K_0 = \mathrm{bar}$ and $e \in A_0^\bullet$. Apply (6.8) (3).)

13. By Exercise 3.15(3) we know that $\langle\langle a_1\rangle\rangle \otimes \langle 1, a_2, \dots, a_m\rangle < \mathrm{Sim}(\langle\langle a_1, \dots, a_m\rangle\rangle)$. This module is unsplittable iff m is odd. That space of dimension $2m$ is minimal

iff $m \not\equiv 0 \pmod 4$. From Corollary 7.11 we find that: If $m \not\equiv 0 \pmod 4$ and if the forms $\langle\langle a_1\rangle\rangle \otimes \langle 1, a_2, \dots, a_m\rangle$ and $\langle\langle b_1\rangle\rangle \otimes \langle 1, b_2, \dots, b_m\rangle$ are similar, then $\langle\langle a_1, \dots, a_m\rangle\rangle \simeq \langle\langle b_1, \dots, b_m\rangle\rangle$.

14. **More on trace forms.** (1) **Lemma.** *Let $C = C(-\alpha \perp \tau)$ where $\dim \alpha = a$, $\dim \tau = t$ and $a + t = 2m$ is even. Let $J = J_{A,T}$ be the involution extending the map $(-1) \perp (1)$ on $-\alpha \perp \tau$. Then J has type 1 iff $a - t \equiv 0$ or $6 \pmod 8$.*

Recall the notation $P(\alpha)$ from Exercise 3.14.

(2) Suppose α and τ are forms as above and $c(-\alpha \perp \tau) = 1$.

If $a - t \equiv 2$ or $4 \pmod 8$, the Pfister form $P(\alpha \perp \tau)$ is hyperbolic.

If $a - t \equiv 0$ or $6 \pmod 8$, then $P(\alpha \perp \tau) \simeq q \otimes q$ for some form q.

(3) If $\dim q = 2^m$ and there is an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$ then $q \otimes q$ is a Pfister form.

(4) **Corollary.** *If $\dim \sigma = 2m$ and $\sigma \in I^3F$ then*

$$P(\sigma) \simeq \begin{cases} 2^m\langle 1\rangle \otimes \psi & \textit{if } m \equiv 0 \\ \textit{hyperbolic} & \textit{if } m \not\equiv 0 \end{cases} \pmod 4.$$

(Hint. (2) For C and J as above define the trace form B_J on C by $B_J(x, y) = \ell(J(x)y)$. By Exercise 3.14, $(C, B_J) \simeq P(\alpha \perp \beta)$ as quadratic spaces. Also $C \cong \mathrm{End}(V)$ where $\dim V = 2^m$ and J induces an involution I_B on $\mathrm{End}(V)$ for some λ-form B. The induced map $\ell : \mathrm{End}(V) \to F$ is the scalar multiple of the trace map having $\ell(1_V) = 1$. By Exercise 1.13 it follows that $(C, B_J) \simeq (V \otimes V, B \otimes B)$. If $a - t \equiv 2 \pmod 8$ then B is an alternating form by (1), and $B \otimes B$ is hyperbolic. Otherwise B corresponds to a quadratic form q.

(4) Let φ be a $2m$-fold Pfister form. Then $\varphi \simeq q \otimes q$ iff $\varphi \simeq 2^m\langle 1\rangle \otimes \psi$ for some m-fold Pfister form ψ. This can be proved using:

Lemma. *If φ and γ are Pfister forms and $\gamma \subset \varphi$ then $\varphi \simeq \gamma \otimes \delta$ where δ is a Pfister form.*

See Exercise 9.15 or Lam (1973), Chapter 10, Exer. 8.)

Notes on Chapter 7

The idea of using a chart as in (7.13) follows Gauchman and Toth (1994), §2.

The equivalence and expansion results in (7.18) and (7.19) were done over $\mathbb{R}$ by Y. C. Wong (1961) using purely matrix methods.

Exercise 13. Wadsworth and Shapiro (1977b) used a different method to prove that if φ is a round form and if $\varphi \otimes (\langle 1\rangle \perp \alpha)$ and $\varphi \otimes (\langle 1\rangle \perp \beta)$ are similar then $\varphi \otimes P(\alpha) \simeq \varphi \otimes P(\alpha)$. The main tool for this proof is Lemma 5.5 above.

Chapter 8

The Space of All Compositions

The topological space $\mathrm{Comp}(s, n)$ of all composition formulas of type $\mathbb{R}^s \times \mathbb{R}^n \to \mathbb{R}^n$ turns out to be a smooth compact real manifold. After deriving general properties of $\mathrm{Comp}(s, n)$, we focus on the spaces of real composition algebras. For example the space $\mathrm{Comp}(8, 8)$ has 8 connected components, each of dimension 56. Since these algebras have such a rich structure we compute the dimensions by another method, by considering autotopies, monotopies and the associated Triality Theorem.

The spaces $\mathrm{Comp}(s, n)$ are accessible since they are orbits of certain group actions. This analysis requires the reader to have some familiarity with basic results from the theory of algebraic groups. For instance we use properties of orbits and stabilzers, and we assume some facts about the the orthogonal group $\mathrm{O}(n)$ and the symplectic group $\mathrm{Sp}(n)$ (e.g. their dimensions and number of components).

We begin with the general situation, specializing to the real case later. Let (S, σ) and (V, q) be quadratic spaces over the field F, with dimensions s, n respectively. To avoid trivialities, assume $s > 1$ so that n is even. Define the sets

$$\mathrm{Bil}(S, V) = \{m \colon S \times V \to V : m \text{ is bilinear}\}$$
$$\mathrm{Comp}(\sigma, q) = \{m \in \mathrm{Bil}(S, V) : q(m(x, y)) = \sigma(x) \cdot q(y) \text{ for every } x \in S, y \in V\}$$

Then $\mathrm{Bil}(S, V)$ is an F-vector space of dimension sn^2 and $\mathrm{Comp}(\sigma, q)$ is an affine algebraic set (since it is the solution set of the Hurwitz Matrix Equations). If the base field needs some emphasis we may write $\mathrm{Comp}_F(\sigma, q)$, etc.

The product of orthogonal groups $\mathrm{O}(\sigma) \times \mathrm{O}(q) \times \mathrm{O}(q)$ acts on $\mathrm{Comp}(\sigma, q)$ by:

$$((\alpha, \beta, \gamma) \bullet m)(x, y) = \gamma(m(\alpha^{-1}(x), \beta^{-1}(y))) \quad \text{for } x \in S \text{ and } y \in V.$$

This definition can be recast using the notation of similarities. If $m \in \mathrm{Comp}(\sigma, q)$ define

$$\hat{m} : S \to \mathrm{Sim}(V, q) \quad \text{by} \quad \hat{m}(x)(y) = m(x, y).$$

Then $\hat{m}$ is a linear isometry from (S, σ) to the subspace $S_m = \mathrm{image}(\hat{m}) \subseteq \mathrm{Sim}(V, q)$. This $\hat{m}$ determines the composition m and we think of $\hat{m}$ as an element of $\mathrm{Comp}(\sigma, q)$. The group action becomes:

$$((\alpha, \beta, \gamma) \bullet \hat{m})(x) = \gamma \circ \hat{m}(\alpha^{-1}(x)) \circ \beta^{-1} \quad \text{for } x \in S.$$

The subspace S_m is carried to $\gamma \circ S_m \circ \beta^{-1}$ by this action.

8.1 Lemma. *If* $\langle a\rangle q \simeq q$ *then* $\mathrm{Comp}(\sigma, q) \cong \mathrm{Comp}(\langle a\rangle\sigma, q)$.

Proof. Given $h \in \mathrm{Sim}^\bullet(q)$ with $\mu(h) = a$. If $m \in \mathrm{Comp}(\sigma, q)$ then sending m to $h \circ m$ provides the isomorphism. □

We view (S, σ) as a quadratic space *with a given orthogonal basis* $\{e_1, e_2, \dots, e_s\}$. In the applications it will be $\mathbb{R}^s$ or $\mathbb{C}^s$ with the standard orthonormal basis. We may assume that σ represents 1. For if $\mathrm{Comp}(\sigma, q) \neq \emptyset$, choose $a \in D_F(\sigma) \subseteq G_F(q)$ and apply (8.1). Then we may assume that the given basis was chosen so that $\sigma(e_1) = 1$.

8.2 Definition. $\mathrm{Comp}^1(\sigma, q) = \{m \in \mathrm{Comp}(\sigma, q) : \hat{m}(e_1) = 1_V\}$.

We define $\mathrm{Bil}^1(S, V)$ similarly and note that it is a coset of a linear subspace of dimension $(s-1)n^2$ in the vector space $\mathrm{Bil}(S, V)$.

8.3 Lemma. $\mathrm{Comp}(\sigma, q) \cong \mathrm{O}(q) \times \mathrm{Comp}^1(\sigma, q)$*, an isomorphism of algebraic sets.*

Proof. Define $\varphi : \mathrm{O}(q) \times \mathrm{Comp}^1(\sigma, q) \to \mathrm{Comp}(\sigma, q)$ by $\varphi(g, m_0) = g \circ m_0$. The inverse map is given by $\varphi^{-1}(m) = (\hat{m}(e_1), \hat{m}(e_1)^{-1} \circ m)$. Note that φ and φ^{-1} are polynomial maps since $\hat{m}(e_1)^{-1} = I_q(\hat{m}(e_1))$. □

The action of $\mathrm{O}(q) \times \mathrm{O}(q)$ on $\mathrm{Comp}(\sigma, q)$ becomes the following action on $\mathrm{O}(q) \times \mathrm{Comp}^1(\sigma, q)$:

$$(\beta, \gamma) \bullet (g, \hat{m}_0) = (\gamma g \beta^{-1}, \beta \diamond \hat{m}),$$

where $\beta \diamond \hat{m}$ denotes the conjugation action of $\mathrm{O}(q)$ on $\mathrm{Comp}^1(\sigma, q)$ given by:

$$(\beta \diamond \hat{m})(x) = \beta \circ \hat{m} \circ \beta^{-1} \quad \text{for } x \in S.$$

To analyze this conjugation action we introduce the "character" of $m \in \mathrm{Comp}^1(\sigma, q)$, as mentioned in the discussion before (7.17).

The map $\hat{m} : S \to \mathrm{Sim}(V)$ sends $e_1 \mapsto 1_V$. The associated Clifford algebra $C = C(-\sigma_1)$ is generated by $\{e_2, \dots, e_s\}$, and $\hat{m}$ induces a similarity representation $\pi_m : C \to \mathrm{End}(V)$ where $\pi_m(e_i) = \hat{m}(e_i)$. This makes V into a C-module which we denote by V_m. Define the element $z = e_2 \dots e_s \in C$ as usual. When $s \equiv 0 \pmod 4$ and $d\sigma = \langle 1\rangle$ then C is not simple and admits an irreducible unsplittable module. In that case we normalize our choice of basis to ensure that $z^2 = 1$. That normalization is automatic if $\sigma \simeq s\langle 1\rangle$ and an orthonormal basis is chosen.

8.4 Definition. If $m \in \mathrm{Comp}^1(\sigma, q)$ define the character $\chi(m) = \mathrm{trace}(\pi_m(z))$. Define

$$\mathrm{Comp}^1(\sigma, q; k) = \{m \in \mathrm{Comp}^1(\sigma, q) : \chi(m) = k\}.$$

If $s \not\equiv 0 \pmod 4$ or if $d\sigma \neq \langle 1\rangle$ we know that $\chi(m) = 0$. Generally, $\chi(m)$ is an even integer between $-n$ and n. As we mentioned in the discussion before (7.17):

$$\chi(m) = \chi(m') \text{ if and only if } V_m \cong V_{m'} \text{ as C-modules.}$$

It easily follows that $\chi(m) = \chi(\beta \diamond m)$, so that the $\mathrm{O}(q)$-orbit of m is inside $\mathrm{Comp}^1(\sigma, q; \chi(m))$.

This character can be extended to the whole set $\mathrm{Comp}(\sigma, q)$ by using the isomorphism φ in (8.3). Then the $\mathrm{O}(q) \times \mathrm{O}(q)$-orbit of m is contained in $\mathrm{Comp}(\sigma, q; \chi(m))$. See Exercise 1 for more details.

8.5 Lemma. *Suppose $\sigma = s\langle 1\rangle$, $q = n\langle 1\rangle$ and F is $\mathbb{R}$ or $\mathbb{C}$. Then $\mathrm{O}(q)$ acts transitively on $\mathrm{Comp}^1(\sigma, q; k)$, and $\mathrm{O}(q) \times \mathrm{O}(q)$ acts transitively on $\mathrm{Comp}(\sigma, q; k)$.*

Proof. If $m, m' \in \mathrm{Comp}^1(\sigma, q; k)$ then $V_m \cong V_{m'}$ as C-modules. As in (7.19), these two structures are C-isometric, so there exists $\beta \in \mathrm{O}(V, q)$ such that $\beta \circ \pi(c) = \pi'(c) \circ \beta$ for every $c \in C$. Then $\beta \circ \hat{m}(x) = \hat{m}'(x) \circ \beta$ for every $x \in F^s$ and hence $\beta \diamond \hat{m} = \hat{m}'$. The second transitivity follows using (8.3). □

To analyze the $\mathrm{O}(q)$-orbit $\mathrm{Comp}^1(\sigma, q; k)$ we gather information about the stabilizer subgroup. Let us return briefly to the more general situation with $\sigma = \langle 1\rangle \perp \sigma_1$ and q over F. For $m \in \mathrm{Comp}^1(\sigma, q)$, define an automorphism group

$$\begin{aligned}\mathrm{Aut}(m) &= \{\beta \in \mathrm{O}(q) : \beta \diamond m = m\}\\ &= \{\beta \in \mathrm{O}(q) : \beta \circ f \circ \beta^{-1} = f \text{ for every } f \in S_m\}.\end{aligned}$$

Since the C-module structure V_m is determined by the elements of S_m,

$$\mathrm{Aut}(m) = \mathrm{O}(V, q) \cap \mathrm{End}_C(V).$$

8.6 Lemma. (1) *Suppose s is odd and let $A = \mathrm{End}_C(V)$. Then A is central simple, $C \otimes A \cong \mathrm{End}(V)$, and I_q induces an involution "$\sim$" on A, which has type 1 if and only if $s \equiv \pm 1 \pmod 8$. Then*

$$\mathrm{Aut}(m) \cong \{a \in A : \tilde{a} \cdot a = 1\}.$$

(2) *Suppose s is even and let $A = \mathrm{End}_{C_0}(V)$. Then A is central simple, $C_0 \otimes A \cong \mathrm{End}(V)$, and I_q induces an involution "$\sim$" on A, which has type 1 if and only if $s \equiv 0, 2 \pmod 8$. Let $y = \pi_m(z) \in A$, where $z = z(S) \in C$. Then $y^2 \in F^\bullet$, $\tilde{y} = (-1)^{s/2} \cdot y$ and*

$$\mathrm{Aut}(m) \cong \{a \in A : ay = ya \text{ and } \tilde{a} \cdot a = 1\}.$$

Proof. The properties of A have been mentioned earlier, the type calculation follows from (7.4) and (6.9), and the description of $\mathrm{Aut}(m)$ is a restatement of the definition. □

The group $\mathrm{Aut}(m)$ is an algebraic group (it is an algebraic set defined over F and the multiplication and inverse maps are defined by polynomials). We can determine the dimension of $\mathrm{Aut}(m)$ by extending scalars and computing that dimension in the case F is algebraically closed.

Since we are primarily concerned with the sums-of-squares forms over $\mathbb{R}$ and $\mathbb{C}$, let us simplify the notations a little and define:

$$\mathrm{Comp}^1(s,n) = \mathrm{Comp}^1(s\langle 1\rangle, n\langle 1\rangle),$$

and similarly for $\mathrm{Comp}^1(s,n;k)$, $\mathrm{Bil}(s,n)$, etc. We also use the standard notation $\mathrm{O}(n)$ in place of $\mathrm{O}(n\langle 1\rangle)$. The stabilizer $\mathrm{Aut}(m) \subseteq \mathrm{O}(n)$ changes only by conjugation in $\mathrm{O}(n)$ as m varies in the orbit $\mathrm{Comp}^1(s,n;k)$. Then as an abstract algebraic group, $\mathrm{Aut}(m)$ depends only on s, n and k and we sometimes write it as $\mathrm{Aut}(s,n;k)$.

8.7 Proposition. *Let* $m \in \mathrm{Comp}^1(s,n;k)$.

(1) *If s is odd let* $\varepsilon = \mathrm{type}(\sim) = (-1)^{(s^2-1)/8}$. *Then:* $\dim \mathrm{Aut}(s,n;k) = \frac{n^2}{2^s} - \frac{\varepsilon n}{2^{(s+1)/2}}$.

(2) *If* $s \equiv 2 \pmod 4$ *then:* $\dim \mathrm{Aut}(s,n;k) = \frac{n^2}{2^s}$.

(3) *If* $s \equiv 0 \pmod 4$ *let* $\varepsilon = \mathrm{type}(\sim) = (-1)^{s/4}$. *Then:* $\dim \mathrm{Aut}(s,n;k) = \frac{n^2+k^2}{2^s} - \frac{\varepsilon n}{2^{s/2}}$.

Proof. We may assume F is algebraically closed. Choose $m \in \mathrm{Comp}(s,n;k)$.

(1) From (8.6) we know that $A \cong \mathbb{M}_r(F)$ where: $r \cdot 2^{(s-1)/2} = n$. If $\varepsilon = 1$ then $\mathrm{Aut}(m) \cong \mathrm{O}(r)$ has dimension $\frac{1}{2}\cdot r(r-1)$. If $\varepsilon = -1$ then $\mathrm{Aut}(m) \cong \mathrm{Sp}(r)$ has dimension $\frac{1}{2}\cdot r(r+1)$.

(2) We have $A \cong \mathbb{M}_r(F)$ where: $r \cdot 2^{\frac{s}{2}-1} = n$, and we may assume $y \in A$ satisfies $y^2 = 1$ and $\tilde{y} = -y$. Let W be an irreducible A-module so that $\dim W = r$, $A \cong \mathrm{End}(W)$, and tilde induces an ε-symmetric form $b : W \times W \to F$. The (± 1)-eigenspaces of y are then totally isotropic subspaces of W, each of dimension $r/2$. Using dual bases for these eigenspaces the Gram matrix of b is $\begin{pmatrix} 0 & 1 \\ \varepsilon 1 & 0 \end{pmatrix}$. Representing $a \in A$ as a block matrix $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ we have $\tilde{a} = \begin{pmatrix} a_4^\top & \varepsilon a_2^\top \\ \varepsilon a_3^\top & a_1^\top \end{pmatrix}$. If $a \in \mathrm{Aut}(m)$ then $ay = ya$ implies that $a = \begin{pmatrix} a_1 & 0 \\ 0 & a_4 \end{pmatrix}$. Therefore $\mathrm{Aut}(m) \cong \left\{ \begin{pmatrix} c & 0 \\ 0 & c^{-\top} \end{pmatrix} : c \in \mathrm{GL}_{r/2}(F) \right\}$ and the dimension result follows.

(3) We have A and r as above, and $y \in A$ satisfies $y^2 = 1$ and $\tilde{y} = y$. Then V is a direct sum of r (isomorphic) irreducible C_0-modules

$$V = V_1 \oplus \cdots \oplus V_r \quad \text{where } \dim V_i = 2^{\frac{s}{2}-1} = \frac{n}{r}.$$

Therefore $A = \mathrm{End}_{C_o}(V) \cong \mathbb{M}_r(F)$, since the only C_0-linear maps from V_i to V_j are scalars. Each V_i is an irreducible C-module, and these come in two non-isomorphic versions: V_+ and V_-, depending on the action of $\pi(z)$. Suppose there are p_ε copies of V_ε, so that $p_+ + p_- = r$. We may replace z by $-z$ if necessary (adjusting via the automorphism α of C) to assume $p_+ \geq p_-$. Then $k = \chi(m) = \mathrm{trace}(\pi(z)) = (p_+ - p_-) \cdot \frac{n}{r}$. In the representation $A \cong \mathbb{M}_r(F)$ the element $y = \pi(z) \in A$ has matrix $\begin{pmatrix} 1_{p_+} & 0 \\ 0 & -1_{p_-} \end{pmatrix}$. If $a \in A$ commutes with y then $a = \begin{pmatrix} a_+ & 0 \\ 0 & a_- \end{pmatrix}$ where $a_\varepsilon \in \mathbb{M}_{p_\varepsilon}(F)$. As before $(A, \sim) \cong (\mathrm{End}(W), I_b)$ for some ε-symmetric space (W, b). Since $\tilde{y} = y$ the eigenspaces of y are orthogonal, and b induces regular forms on them. If $\varepsilon = 1$ then $\mathrm{Aut}(m) \cong \mathrm{O}(p_+) \times \mathrm{O}(p_-)$ while if $\varepsilon = -1$ then $\mathrm{Aut}(m) \cong \mathrm{Sp}(p_+) \times \mathrm{Sp}(p_-)$. Therefore $\dim \mathrm{Aut}(m) = \frac{1}{2} \cdot (p_+(p_+ - \varepsilon) + p_-(p_- - \varepsilon)) = \frac{1}{4} \cdot ((p_+ + p_- - \varepsilon)^2 + (p_+ - p_-)^2 - 1)$ and a calculation completes the proof. □

Let us review some of the properties of group actions. If G is a group acting on a set W and $x \in W$ we write $G \cdot x = \{gx : g \in G\}$ for the orbit of x and $G_x = \{g \in G : gx = x\}$ for the stabilizer (isotropy subgroup) of x. The map $G \to G \cdot x$ induces a bijection between the left cosets of G_x and the orbit $G \cdot x$:

$$G/G_x \leftrightarrow G \cdot x.$$

At this point we assume that the reader knows some of the basic theory of algebraic groups as presented, for example, in Humphreys (1975). Suppose that G is an algebraic group, W is a (nonempty) algebraic variety over $\mathbb{C}$ and G acts morphically on W (i.e. the map $G \times W \to W$ is a morphism of varieties). In general an orbit $G \cdot x$ might be embedded in W in some complicated way, but it can still be viewed as a variety.

8.8 Lemma. *Suppose H is a closed subgroup of an algebraic group G. Then G/H is a nonsingular variety with* $\dim(G/H) = \dim(G) - \dim(H)$, *and with all irreducible components of this dimension. If G acts morphically on a variety W, then G_x is a closed subgroup of G, the orbit $G \cdot x$ is a nonsingular, locally closed subset of W, and the boundary of $G \cdot x$ is a union of orbits of strictly lower dimension. Furthermore,*

$$\dim G \cdot x = \dim G - \dim G_x.$$

Proof. See Humphreys (1975), §8, §4.3, and §12. □

A set Y is "locally closed" if it is the intersection of an open set and a closed set, in the Zariski topology. Equivalently, Y is an open subset of its closure $\bar{Y}$. The boundary of Y is the closed set $\bar{Y} - Y$. As one consequence, the closure $\overline{G \cdot x}$ is a subvariety of W with the same dimension as the orbit $G \cdot x$.

These ideas from algebraic geometry require the base field to be algebraically closed. In some cases we can extract geometric information about the *real* part of a complex variety.

8.9 Lemma. *Suppose W is a nonsingular algebraic variety over $\mathbb{C}$, which is defined over $\mathbb{R}$. If the set of real points $W(\mathbb{R})$ is nonempty then it is a smooth real manifold and* $\dim W(\mathbb{R})$ *as a manifold coincides with* $\dim W$ *as a variety.*

Proof outline. These statements about $W(\mathbb{R})$ are well-known to the experts, but I found no convenient reference. The ideal of W is $\mathcal{I}(W) = \{f \in \mathbb{C}[X] : f(\zeta) = 0 \text{ for every } \zeta \text{ in } W\}$. Here $X = (x_1, \dots, x_n)$ is the set of indeterminates. Let $f_1, \dots, f_t$ be a set of generators for $\mathcal{I}(W)$ and consider the $t \times n$ Jacobian matrix $J = \left(\frac{\partial f_i}{\partial x_j}\right)$. Recall the classical Jacobian criterion for nonsingularity: W is nonsingular if and only if for every $\zeta \in W$, $\operatorname{rank}(J(\zeta)) = n - \dim W$. (See e.g. Hartshorne (1977), p. 31.)

Since W is defined over $\mathbb{R}$ we can arrange $f_i \in \mathbb{R}[X]$, (see Exercise 2). Now view f_i as a real valued C^∞-function on $\mathbb{R}^n$ and $W(\mathbb{R})$ as a "level surface" of $\{f_1, \dots, f_t\}$. By the Implicit Function Theorem the constant rank of the Jacobian matrix J at points $\zeta \in W(\mathbb{R})$ implies that $W(\mathbb{R})$ is a smooth real manifold whose dimension equals $\dim W$. □

8.10 Proposition. *Suppose $1 < s \le \rho(n)$. Then $\operatorname{Comp}^1_{\mathbb{C}}(s, n)$ is a nonempty, nonsingular algebraic variety. Each nonempty $\operatorname{Comp}^1_{\mathbb{C}}(s, n; k)$ is a variety with two irreducible components both of dimension equal to*

$$\frac{1}{2}n(n-1) - \dim \operatorname{Aut}(s, n; k).$$

Moreover each nonempty $\operatorname{Comp}^1_{\mathbb{R}}(s, n; k)$ is a smooth compact, real manifold with two connected components. The dimension of each component equals the value displayed above. Similar statements hold for $\operatorname{Comp}_{\mathbb{C}}(s, n; k)$ and $\operatorname{Comp}_{\mathbb{R}}(s, n; k)$.

Proof. The set is nonempty by the basic Hurwitz–Radon Theorem, and it is certainly an affine algebraic set, hence a closed subvariety of $\operatorname{Bil}(s, n)$. Most of the remaining statements follow using (8.3), (8.5), (8.8) and (8.9). Since $\mathrm{O}(n)$ has two components given by the cosets of $\mathrm{O}^+(n)$, the statement that there are two components is equivalent to:

$$\text{If } m \in \operatorname{Comp}^1(s, n; k) \text{ then } \operatorname{Aut}(m) \text{is contained in } \mathrm{O}^+(n).$$

Since $\operatorname{Aut}(m) = \mathrm{O}(n) \cap \operatorname{End}_C(V)$, every $f \in \operatorname{Aut}(m)$ centralizes the algebra C and hence commutes with every element of the subspace $S_m \subseteq \operatorname{Sim}(V, n\langle 1 \rangle)$. This implies $f \in \mathrm{O}^+(n)$, by the result of Wonenburger (1962b) mentioned in Exercise 1.17(4). The compactness follows since $\mathrm{O}(n, \mathbb{R})$ is a compact group acting transitively on the set of real points, as in (8.5). □

Here is a list of these dimensions in a few small cases. If $s \equiv 0 \pmod 4$ the maximality of s forces the representation to be non-faithful so that $\chi(m) = \pm n$. In those cases $\mathrm{Comp}^1(s, n) = \mathrm{Comp}^1(s, n; n) \cup \mathrm{Comp}^1(s, n; -n)$.

(s, n)	$\dim \mathrm{Aut}(s, n)$	$\dim \mathrm{Comp}^1(s, n)$	$\dim \mathrm{Bil}^1(s, n)$
$(2, 2)$	1	0	4
$(4, 4)$	3	3	48
$(8, 8)$	0	28	448
$(9, 16)$	0	120	2048

The values in the first two columns follow from (8.7) and (8.10).

The dimension of $\mathrm{Comp}(s, n)$ can be determined using (8.3) (see Exercise 4). For example

$$\dim \mathrm{Comp}(4, 4) = 9 \quad \text{and} \quad \dim \mathrm{Comp}(8, 8) = 56.$$

The proposition also determines the number of connected components. For example $\mathrm{Comp}_{\mathbb{R}}(4, 4) = \mathrm{O}(4) \times \mathrm{Comp}^1_{\mathbb{R}}(4, 4)$ and $\mathrm{Comp}^1_{\mathbb{R}}(4, 4) = \mathrm{Comp}^1_{\mathbb{R}}(4, 4; 4) \cup \mathrm{Comp}^1_{\mathbb{R}}(4, 4; -4)$. Since $\mathrm{O}(4)$ and $\mathrm{Comp}^1(4, 4; \pm 4)$ each have two components, $\mathrm{Comp}_{\mathbb{R}}(4, 4)$ has eight connected components, each of dimension 9. Similarly $\mathrm{Comp}_{\mathbb{R}}(8, 8)$ has eight components each of dimension 56.

Let us now consider the set of all subspaces of similarities, as a subset of the Grassmann variety of all s-planes in n-space. Recall that the character $\chi(S)$ was defined in (7.17) and if $S' = \gamma \cdot S \cdot \beta^{-1}$ then $\chi(S') = \chi(S)$. Some information is lost in passing from $\chi(m)$ to $\chi(S)$. In fact, if $S = S_m$, then $\chi(S) = |\chi(m)|$.

8.11 Definition. $\mathrm{Sub}(s, n)$ is the set of all linear subspaces $S \subseteq \mathrm{Sim}(n\langle 1\rangle)$ such that $\dim S = s$ and the induced quadratic form on S is regular.

$$\mathrm{Sub}(s, n; k) = \{S \in \mathrm{Sub}(s, n) : \chi(S) = k\},$$
$$\mathrm{Sub}^1(s, n) = \{S \in \mathrm{Sub}(s, n) : 1_V \in S\}$$

and $\mathrm{Sub}^1(s, n; k)$ is defined similarly.

As usual, $\mathrm{Sub}(s, n) = \mathrm{Sub}(s, n; 0)$ when $s \not\equiv 0 \pmod 4$. If $F = \mathbb{R}$ the regularity condition on the induced quadratic form is automatic. We may view $\mathrm{Sub}(s, n; k)$ and $\mathrm{Sub}^1(s, n; k)$ as nonsingular algebraic varieties, since they are orbits of algebraic group actions. Note that sending m to $S_m = \mathrm{image}(\hat{m})$ provides a surjection

$$\varphi : \mathrm{Comp}(s, n; k) \to \mathrm{Sub}(s, n; |k|).$$

The action of $\mathrm{O}(n) \times \mathrm{O}(n)$ on $\mathrm{Comp}(s, n; k)$ descends to the action $(\beta, \gamma) \bullet S = \gamma S \beta^{-1}$ on $\mathrm{Sub}(s, n; |k|)$.

8.12 Lemma. *Suppose $k \geq 0$ and* $\operatorname{Comp}(s, n, k)$ *is nonempty.*

$$\dim \operatorname{Sub}(s, n; k) = \dim \operatorname{Comp}(s, n; k) - \frac{s(s-1)}{2},$$
$$\dim \operatorname{Sub}^1(s, n; k) = \dim \operatorname{Comp}^1(s, n; k) - \frac{(s-1)(s-2)}{2}.$$

Proof. Given $S \in \operatorname{Sub}(s, n; k)$, the fiber $\varphi^{-1}(S) = \{m \in \operatorname{Comp}(s, n; k) : S_m = S\} \cong \{\hat{m} : \mathbb{R}^s \to S \text{ an isometry}\} \cong \mathrm{O}(s)$, and the first dimension formula follows. For the second formula, restrict φ to $\varphi_1 : \operatorname{Comp}^1 \to \operatorname{Sub}^1$ and compute the fiber $\varphi_1^{-1}(S) \cong \{\hat{m} : \mathbb{R}^s \to S \text{ an isometry with } \hat{m}(e_1) = 1_V\} \cong \mathrm{O}(s-1)$. □

For example, $\dim \operatorname{Sub}^1(4, 4) = 0$. In fact we have already seen (in Exercise 1.4) that $\operatorname{Sub}^1(4, 4)$ contains exactly two elements.

8.13 Proposition. $\operatorname{Sub}^1_{\mathbb{R}}(s, n; k)$ *and* $\operatorname{Sub}_{\mathbb{R}}(s, n; k)$ *are smooth real manifolds. If* $\operatorname{Sub}^1_{\mathbb{R}}(s, n; k)$ *is nonempty, then it has two connected components and* $\operatorname{Sub}_{\mathbb{R}}(s, n; k)$ *has four connected components.*

Proof. The fact that these spaces are manifolds follows from the general theory as before. Since the components of $\mathrm{O}(n)$ are the cosets of $\mathrm{O}^+(n)$, the $\mathrm{O}(n) \times \mathrm{O}(n)$ orbit $\operatorname{Sub}_{\mathbb{R}}(s, n; k)$ breaks into four $\mathrm{O}^+(n) \times \mathrm{O}^+(n)$ orbits, each of which is connected. Given $S \in \operatorname{Sub}^1_{\mathbb{R}}(s, n; k)$, these four orbits are represented by:

$$\begin{array}{ll} S & \beta S \beta^{-1} \\ \beta S & S\beta \end{array}$$

where $\beta \in \mathrm{O}^-(n)$, i.e. $\det(\beta) = -1$. We must show that these four orbits are disjoint. For if that is done certainly $\operatorname{Sub}_{\mathbb{R}}(s, n; k)$ has those four components. Moreover the two orbits of $\mathrm{O}^+(n)$ acting (by conjugation) on $\operatorname{Sub}^1_{\mathbb{R}}(s, n; k)$ are contained in the larger orbits represented by the first row above, and hence are also disjoint.

Recall from Exercise 1.17 that if $f \in S$ or if $f \in \beta S \beta^{-1}$ then f is proper, and hence if $f \in \beta S$ or $f \in S\beta$ then f is not proper. Therefore the orbits in the top row above are disjoint from the orbits in the bottom row. To complete the argument we invoke the following lemma, whose proof is surprisingly tricky. □

8.14 Lemma. *Suppose $1_V \in S \subseteq \operatorname{Sim}(V, q)$ and $s = \dim S > 2$. If $\beta, \gamma \in \operatorname{Sim}^\bullet(V, q)$ and $\gamma S \beta^{-1} = S$ then β and γ are proper.*

See Exercise 12 for an outline of the proof.

Finally we turn to a case of particular interest: real division algebras. Recall that a *real division algebra* is defined to be a finite dimensional $\mathbb{R}$-vector space D together with an $\mathbb{R}$-bilinear mapping $m : D \times D \to D$ such that: $m(x, y) = 0$ only when

$x = 0$ or $y = 0$. No associativity or commutativity is assumed; an identity element is not assumed to exist. Each of the classical composition algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ is a real division algebra satisfying many algebraic properties. There are several classification results, each assuming that the division algebra satisfies some algebraic property and then listing all the possibilities up to isomorphism. Here are some classical examples when A is a real division algebra with 1:

- If A is associative then $A \cong \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ (Frobenius 1877).
- If A is a composition algebra then $A \cong \mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ or $\mathbb{O}$ (Hurwitz 1898).
- If A is alternative then $A \cong \mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ or $\mathbb{O}$ (Zorn 1933).
- If A is commutative then $A \cong \mathbb{R}$ or $\mathbb{C}$ (Hopf 1940).

Actually in 1898 Hurwitz proved that $\dim A = 1, 2, 4, 8$ and only stated the uniqueness of the solutions. This uniqueness was worked out by his student E. Robert (1912). The classification results mentioned above are described further in Koecher and Remmert (1991), §8.2, §8.3, §9.3. The Hopf theorem was proved using topology, as outlined in Exercise 12.12.

More recent work in this direction has been done with quadratic division algebras, with flexible ones (satisfying the flexible law: $xy \cdot x = x \cdot yx$), with algebras having a large derivation algebra, and with various other types. Flexible real division algebras were classified by Benkart, Britten and Osborn (1982). A survey of such results appears in Benkart and Osborn (1981).

Can general real division algebras be classified is some reasonable way? Even determining the possible dimensions for such algebras is a deep question. In 1940 Stiefel and Hopf used algebraic topology to prove that if D is an n-dimensional real division algebra then $n = 2^m$ for some m. (See (12.4) below.) Finally in 1958 Bott's Periodicity Theorem was used to prove that n must be 1, 2, 4 or 8. This theorem later became an corollary of topological K-theory. (See Exercise 0.8 and (12.20).)

Let $\mathrm{Div}(n)$ be the set of n-dimensional real division algebras. Then $\mathrm{Div}(n)$ is nonempty only when $n = 1, 2, 4$ or 8. It is fairly easy to describe $\mathrm{Div}(1)$ and $\mathrm{Div}(2)$ explicitly. The challenge is to describe the sets $\mathrm{Div}(4)$ and $\mathrm{Div}(8)$, and possibly to find some general algebraic classifications. Useful results in this direction remain elusive. Let us consider four algebraic methods for constructing examples of division algebras.

(1) *Isotopes*. Two F-algebras D, D' are isotopic if there exist bijective linear maps $f, g, h : D \to D'$ such that

$$f(xy) = g(x) \cdot h(y) \quad \text{for every } x, y \in D.$$

If D is a division algebra then any isotope of D is also a division algebra. Then isotopy is an equivalence relation on $\mathrm{Div}(n)$. This concept was introduced in Steenrod's work on homotopy groups and was formalized by Albert (1942b). Every division algebra is isotopic to one with an identity element (see Exercise 0.8). Then $\mathrm{Div}(1)$ and $\mathrm{Div}(2)$ each have only one isotopy class, but $\mathrm{Div}(4)$ and $\mathrm{Div}(8)$ are much more complicated. The concept of isotopy (or isotopism) arises naturally in several contexts. For example, two division rings are isotopic if and only if they coordinatize isomorphic projective planes. See Hughes and Piper (1973), p. 177.

(2) *Mutations*. A mutation of an F-algebra D with parameters $r, s \in F$ is given by altering the multiplication of D to $m_{r,s} : D \times D \to D$ defined by

$$m_{r,s}(x, y) = rxy + syx.$$

If D is a composition division algebra over $\mathbb{R}$ then this mutation is also a division algebra with identity, provided $r \neq \pm s$. The "bar" map is still an involution for the mutation and if $r + s = 1$ the elements of the mutation have the same inverses as they do in D. (Compare Lex (1973).)

(3) *Bilinear perturbations*. Suppose D is a composition algebra over $\mathbb{R}$ and $\beta : D \times D \to \mathbb{R}$ is a bilinear form. Define $m_\beta : D \times D \to D$ by $m_\beta(x, y) = xy + \beta(x, y) \cdot 1$. This furnishes a division algebra if and only if the quadratic form $Q(x) = x \cdot \bar{x} + \beta(x, \bar{x})$ is anisotropic. For example let $\ell : D \to \mathbb{R}$ be the trace map $\ell(x) = \frac{1}{2} \cdot (x + \bar{x})$. If D is a division algebra, then $\beta(x, y) = \ell(xy)$ or $\ell(x)\ell(y)$ yield division algebras. We also get division algebras from $\beta(x, y) = t_1 \cdot \ell(xy) + t_2 \cdot \ell(x\bar{y}) + t_3 \cdot \ell(x)\ell(y)$ for certain values of the real parameters t_1, t_2, t_3. The examples in Hähl (1975) are of this type.

(4) *Twisted quaternions*. Choosing $b \in \mathbb{C}$, define an algebra $\mathbb{H}_b = \mathbb{C} \oplus \mathbb{C}j$, with multiplication given as follows. For $r, s, u, v \in \mathbb{C}$ define

$$(r + sj) \cdot (u + vj) = (ru + bs\bar{v}) + (rv + s\bar{u})j.$$

Then $\mathbb{H}_b$ is a 4-dimensional $\mathbb{R}$-vector space with basis $\{1, i, j, ij\}$, $1 \in \mathbb{C}$ is the identity element, $jx = \bar{x}j$ for every $x \in \mathbb{C}$ and $j^2 = b$. If $b < 0$ then $\mathbb{H}_b \cong \mathbb{H}$, the associative quaternion algebra. If $b \notin \mathbb{R}$ then $\mathbb{H}_b$ is a division algebra (use the formula to analyze zero-divisors) and $\mathbb{H}_b$ is not associative: in fact, $j \cdot j^2 \neq j^2 \cdot j$. Even though every non-zero element of $\mathbb{H}_b$ has a left inverse and a right inverse, those inverses can differ. For example, $(b^{-1}j) \cdot j = 1$ but $j \cdot (b^{-1}j) \neq 1$. The twisted quaternion algebras discussed by Bruck (1944) are of this type. Such algebras are studied more generally by Waterhouse (1987).

If the entries of the multiplication table of a real division algebra are altered by small amounts then the result yields another division algebra. That is, the collection $\mathrm{Div}(n)$ of n-dimensional real division algebras is an open set. Generally, let $\mathrm{Bil}(r, s, n)$ be the set of all bilinear maps $f : \mathbb{R}^r \times \mathbb{R}^s \to \mathbb{R}^n$. It is a vector space of dimension rsn. Such a map f is defined to be *nonsingular* if $f(x, y) \neq 0$ whenever $x \neq 0$ in $\mathbb{R}^r$ and $y \neq 0$ in $\mathbb{R}^s$. Let $\mathrm{Nsing}(r, s, n)$ be the set of all nonsingular elements in $\mathrm{Bil}(r, s, n)$. Then $\mathrm{Div}(n) = \mathrm{Nsing}(n, n, n)$.

8.15 Lemma. $\mathrm{Nsing}(r, s, n) \subseteq \mathrm{Bil}(r, s, n)$ *is an open set.*

Proof. If $f \in \mathrm{Bil}(r, s, n)$ then $f(S^{r-1}, S^{s-1}) \subseteq \mathbb{R}^n$ is a compact subset, since the spheres S^k are compact. Define $\omega(f)$ to be the distance between 0 and this compact subset. The map $\omega : \mathrm{Bil}(r, s, n) \to [0, \infty)$ is continuous and $\mathrm{Nsing}(r, s, n)$ is the complement of $\omega^{-1}(0)$. □

It is usually difficult to determine whether $\mathrm{Nsing}(r, s, n)$ is nonempty. (See Chapter 12.) But if it is nonempty, then $\mathrm{Nsing}(r, s, n)$ is an open set of dimension rsn. For the classical cases of $\mathrm{Div}(n)$ we obtain:

$$\begin{array}{ll} \dim \mathrm{Comp}(4, 4) = 9 & \dim \mathrm{Div}(4) = 64 \\ \dim \mathrm{Comp}(8, 8) = 56 & \dim \mathrm{Div}(8) = 512. \end{array}$$

Therefore the algebraic constructions of division algebras (e.g. by isotopy or mutation) cannot produce all the possible division algebras of dimension 4 or 8. For example the set of algebra multiplications which are isotopic to a fixed octonion algebra forms one orbit of an action of $\mathrm{GL}(8) \times \mathrm{GL}(8) \times \mathrm{GL}(8)$. This orbit has dimension at most $3 \cdot 8^2 = 192$ inside $\mathrm{Div}(8)$. Compare Exercise 18.

Let us now consider real division algebras with a (2-sided) identity element. To facilitate the discussion we simplify and extend some of the notations. As before let $e = e_1 = (1, 0, \dots, 0)$ be the first element of the standard basis of $\mathbb{R}^n$. Define:

$$\begin{aligned} \mathrm{Bil}(n) &= \{m : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n \text{ such that } m \text{ is bilinear}\}; \\ \mathrm{Bil}^1(n) &= \{m \in \mathrm{Bil}(n) : e \text{ is a left identity element for } m\}; \\ \mathrm{Bil}^{11}(n) &= \{m \in \mathrm{Bil}(n) : e \text{ is a 2-sided identity element for } m\}. \end{aligned}$$

Then $m \in \mathrm{Bil}(n)$ is a multiplication on $\mathbb{R}^n$ (setting $x * y = m(x, y)$). It is a *division algebra* if: $m(x, y) = 0$ implies $x = 0$ or $y = 0$. It is a *composition algebra* if it satisfies the norm property: $|m(x, y)| = |x| \cdot |y|$ for every $x, y \in \mathbb{R}^n$. Let us use similar notations for the sets of division algebras and composition algebras:

$$\begin{array}{lll} \mathrm{Div}(n) & \mathrm{Div}^1(n) & \mathrm{Div}^{11}(n) \\ \mathrm{Comp}(n) & \mathrm{Comp}^1(n) & \mathrm{Comp}^{11}(n). \end{array}$$

Of course these are nonempty only when $n = 1, 2, 4$ or 8. Note that $\mathrm{Bil}(n)$ is a vector space of dimension n^3; $\mathrm{Bil}^1(n)$ is a coset of a linear subspace with dimension $(n-1)n^2$; and $\mathrm{Bil}^{11}(n)$ is a coset of a linear subspace of dimension $(n-1)^2 n$. We know that $\mathrm{Div}(n)$ is an open subset of $\mathrm{Bil}(n)$. Similarly, $\mathrm{Div}^1(n) \subseteq \mathrm{Bil}^1(n)$ and $\mathrm{Div}^{11}(n) \subseteq \mathrm{Bil}^{11}(n)$ are open subsets.

What is the dimension of $\mathrm{Comp}^{11}(n)$ and how many connected components does it have? We present the answer to this question twice, using different methods. The first uses the direct group action ideas mentioned above. The second approach employs the Triality Theorem.

8.16 Propositon. $\mathrm{Comp}^{11}(4)$ *is a set of two points.*

$\mathrm{Comp}^{11}(8)$ *is a nonsingular algebraic variety with two components each isomorphic to* 7*-dimensional projective space.*

Proof. Let $\mathbb{R}$ be the base field (although more general fields F will work here as well). Suppose $m \in \text{Comp}^{11}(4)$. Then $xy = m(x, y)$ makes $\mathbb{R}^4$ into a composition algebra with identity element $e = e_1$. The mapping m is determined by the values e_ie_j where $\{e_1, \dots, e_4\}$ is the given orthonormal basis. We know that $e_2^2 = e_3^2 = e_4^2 = -1$ and $e_2e_3 = \pm e_4$. The other values e_ie_j are determined by that choice of sign since m is associative. Then either m is the standard quaternion multiplication, $m(x, y) = xy$, or else m comes from the opposite algebra: $m(x, y) = yx$. These are the two points in $\text{Comp}^{11}(4)$. (Exercise 1.4 is relevant here.)

If $m \in \text{Comp}^{11}(8) \subseteq \text{Comp}^1(8, 8)$ we defined the character $\chi(m)$ as $\text{trace}(\pi(z))$, using the associated representation $\pi : C \to \text{End}(V)$ and the central element z satisfying $z^2 = 1$. Then $\pi(z) = \pm 1$ and $\chi(m) = \pm 8$. Then $\text{Comp}^{11}(8)$ is a union of two disjoint components $\text{Comp}^{11}(8, +) \subseteq \text{Comp}^1(8, 8; 8)$ and $\text{Comp}^{11}(8, -) \subseteq \text{Comp}^1(8, 8; -8)$. Any $m \in \text{Comp}^{11}(8)$ has an associated operation m' defined: $m'(x, y) = m(y, x)$. Since $\chi(m') = -\chi(m)$, those two spaces are isomorphic.

Recall that O(8) acts transitively on the space $\text{Comp}^1(8, 8; 8)$ as in (8.5). Let $m_0(x, y) = x \cdot y = xy$ be the standard octonion multiplication. If $m(x, y) = x * y$ lies in $\text{Comp}^1(8, 8; 8)$ then m arises from m_0 by the action of some $\beta \in \text{O}(8)$. Working through the defnitions, we find:

$$\beta(x * y) = x \cdot \beta(y) \quad \text{for every } x, y.$$

Certainly this operation $*$ admits e as a left-identity element. If m lies in $\text{Comp}^{11}(8, +)$ then e is also a right-identity: $x * e = x$. This occurs if and only if $\beta(x) = x \cdot \beta(e)$ for every x. Thus $\beta = \mathcal{R}_b$ is a right multiplication map on the octonions, for some $b = \beta(e)$ with $|b| = 1$. This provides a surjective map from the sphere S^7 of unit octonions to the space $\text{Comp}^{11}(8, +)$, sending b to the operation $*$ determined by:

$$(x * y) \cdot b = x \cdot (y \cdot b).$$

To examine the fibers of this map, suppose $b, c \in S^7$ both go to the same operation. Then

$$(x \cdot yb)b^{-1} = (x \cdot yc)c^{-1} \quad \text{for every } x, y.$$

Setting $x = b$ and using the Moufang identity (as in (1.A.10)) we find: $by = (byb)b^{-1} = (b \cdot yc)c^{-1}$ so that $by \cdot c = b \cdot yc$. Exercise 1.27 implies that $1, b, c$ must be linearly dependent. Interchanging b and c if necessary we may write $c = r + sb$ for some $r, s \in \mathbb{R}$. The alternative law then implies that $(w \cdot b^{-1}) \cdot c = w \cdot (b^{-1} \cdot c)$. In particular $x \cdot yc = (x \cdot yb)(b^{-1}c)$ and plugging in $c = r + sb$ yields: $rxy = r(x \cdot yb)b^{-1}$. Suppose c is not a scalar multiple of b, so that b is not scalar and $r \neq 0$. Then $xy \cdot b = x \cdot yb$ for every x, y and Exercise 1.27 implies b is a scalar, a contradiction. Hence $c = \pm b$.

Consequently $\text{Comp}^{11}(8, +)$ is exactly the sphere S^7 with antipodal points identified, so it is 7-dimensional projective space. □

We can also analyze the space Comp(8) by using the action of the full group O(8) × O(8) × O(8). This approach yields another proof of (8.16) but more importantly it leads to a consideration of the interesting phenomenon of "triality".

The group O(8) × O(8) × O(8) acts transitively on Comp(8). This fact follows from the Clifford algebra theory (see (8.5)), but more direct proofs can be given for this case. What is the stabilizer of the standard octonion algebra D ? From the definition of the action, this stabilizer is related to the group of autotopies defined below. The next results are valid over general fields F (where $2 \neq 0$), provided D is a division algebra.

The results here are well known but the terminology follows ideas of J. H. Conway. As in the appendix of Chapter 1, we use $[x] = \bar{x}x$ to denote the norm form in the octonion algebra and we write $\mathrm{O}(D)$ for the orthogonal group of this norm form. For the usual case over $\mathbb{R}$ this group becomes O(8).

8.17 Definition. Let D be an octonion division algebra over F. If $\alpha, \beta, \gamma \in \mathrm{GL}(D)$ the triple (α, β, γ) is an *autotopy* of D if $\gamma(xy) = \alpha(x) \cdot \beta(y)$ for every $x, y \in D$. If (α, β, γ) is an autotopy define γ to be a *monotopy*. Let $\mathrm{Autot}(D)$ and $\mathrm{Mon}(D)$ the groups of all autotopies and monotopies of D, respectively. Define $\mathrm{Autot}^{\mathrm{o}}(D)$ and $\mathrm{Mon}^{\mathrm{o}}(D)$ to be the corresponding groups of isometries (restricting to the case $\alpha, \beta, \gamma \in \mathrm{O}(D)$).

It is easy to see that $\mathrm{Autot}(D)$ is a group under componentwise composition and $\mathrm{Mon}(D)$ is the image of the projection $\pi : \mathrm{Autot}(D) \to \mathrm{GL}(D)$ sending (α, β, γ) to γ. Similarly $\mathrm{Mon}^{\mathrm{o}}(D)$ is the image of $\mathrm{Autot}^{\mathrm{o}}(D)$. If $\varphi \in \mathrm{Aut}(D)$ is an algebra automorphism then $(\varphi, \varphi, \varphi)$ is an autotopy and φ is an isometry. Hence $\mathrm{Aut}(D) \subseteq \mathrm{Mon}^{\mathrm{o}}(D)$.

8.18 Lemma. $\ker(\mathrm{Autot}^{\mathrm{o}}(D) \to \mathrm{Mon}^{\mathrm{o}}(D)) \cong \{\pm 1\}$.

Proof. An element of the kernel is $(\alpha, \beta, 1)$ where $\alpha(x)\beta(y) = xy$. Then $\alpha(x) = xa$ and $\beta(y) = by$ for every x, y (where $a = \beta(1)^{-1}$ and $b = \alpha(1)^{-1}$). Then $xa \cdot by = xy$ and consequently $xa \cdot z = x \cdot az$ for every x, z. This says that a is in the nucleus $\mathcal{N}(D) = F$ (as in Exercise 1.27). □

If (α, β, γ) is an autotopy then each of α, β, γ is a monotopy. To see this suppose $z = xy$ and consider the resulting "braiding sequence": $xy = z$, $x = zy^{-1}$, $z^{-1}x = y^{-1}$, $z^{-1} = y^{-1}x^{-1}$, $yz^{-1} = x^{-1}$, $y = x^{-1}z$. Each of these six expressions leads to another autotopy. For example from $x = zy^{-1}$ we find $\alpha(zy^{-1}) = \alpha(x) = \gamma(z)\beta(y)^{-1}$ so that $(\gamma, \iota\beta\iota, \alpha)$ is also an autotopy. (Here ι denotes the inverse map:

$\iota(x) = x^{-1}$). The six associated autotopies are best displayed in a hexagon:

$$\begin{array}{ccc} & (\alpha, \beta, \gamma) & \\ (\iota\alpha\iota, \gamma, \beta) & & (\gamma, \iota\beta\iota, \alpha) \\ (\beta, \iota\gamma\iota, \iota\alpha\iota) & & (\iota\gamma\iota, \alpha, \iota\beta\iota) \\ & (\iota\beta\iota, \iota\alpha\iota, \iota\gamma\iota) & \end{array}$$

Therefore α, β, γ are monotopies.

Recall from (1.A.10) that D satisfies various weak forms of associativity, including:

$a \cdot ab = a^2b$ and $ba \cdot a = ba^2$	(the alternative laws)
$ax \cdot a = a \cdot xa$	(flexible law)
$a(xy)a = ax \cdot ya$	(Moufang identity)

Setting $L_a(x) = ax$, $R_a(x) = xa$ and $B_a(x) = axa$, Moufang says that (L_a, R_a, B_a) is an autotopy for every $a \in D^{\bullet}$. Therefore each L_a, R_a and B_a is a monotopy. It is clear that these maps are similarities, relative to the norm form. In fact, $L_a, R_a, B_a \in \mathrm{Sim}^+(D)$ by Exercise 1.17.

The bi-multiplication map B_a is closely related to the hyperplane reflection τ_a on D, relative to the norm form $[x] = \bar{x}x$. Recall that $\tau_a(x) = x - \frac{2[x,a]}{[a]} \cdot a$. Since $x\bar{a} + a\bar{x} = 2[x, a]$ we find $\tau_a(x) = -[a]^{-1} \cdot a\bar{x}a$. Then $\tau_1(x) = -\bar{x}$ and

$$B_a = [a] \cdot \tau_a\tau_1.$$

This proves again that $B_a \in F^{\bullet}\,\mathrm{O}^+(D) \subseteq \mathrm{Sim}^+(D)$.

8.19 Triality Theorem. $\mathrm{Mon}(D) = \mathrm{Sim}^+(D)$ *and* $\mathrm{Mon}^{\mathrm{o}}(D) = \mathrm{O}^+(D)$

Consequently every $\gamma \in \mathrm{O}^+(D)$ has associated maps $\alpha, \beta \in \mathrm{O}^+(D)$ making (α, β, γ) an autotopy, and these α, β are unique up to sign. This three-fold symmetry among α, β, γ is a version of the Triality Principle studied in Lie theory and elsewhere.

For the usual cases over $\mathbb{R}$ we find that $\mathrm{Mon}(8) = \mathrm{Sim}^+(8) = \mathbb{R}^{\bullet} \cdot \mathrm{O}^+(8)$ has dimension 29, and using (8.18): $\dim \mathrm{Autot}(8) = 30$. Similarly $\dim \mathrm{Mon}^{\mathrm{o}}(8) = \dim \mathrm{Autot}^{\mathrm{o}}(8) = 28$.

As a step toward the proof of this theorem we show that monotopies are similarities.

8.20 Lemma. $\mathrm{Mon}(D) \subseteq \mathrm{Sim}^{\bullet}(D)$.

Proof. If (α, β, γ) is an autotopy, $\gamma(xy) = \alpha(x) \cdot \beta(y)$. Then $\gamma(x) = \alpha(x) \cdot \beta(1)$. Since $\alpha, \gamma \in \mathrm{GL}(D)$, $\beta(1)$ must be invertible and we may set $a = \beta(1)^{-1}$ and conclude: $\alpha(x) = \gamma(x) \cdot a$. Similarly $\beta(y) = b \cdot \gamma(y)$ where $b = \alpha(1)^{-1}$ and

$$\gamma(xy) = \gamma(x)a \cdot b\gamma(y) \quad \text{for every } x, y \in D.$$

The elements a, b are called the "companions" of γ. Take norms to find $[\gamma(xy)] = r \cdot [\gamma(x)] \cdot [\gamma(y)]$, where $r = [ab]$. Then the form $q(x) = r \cdot [\gamma(x)]$ satisfies

$q(xy) = q(x)q(y)$ and D is a composition algebra relative to q. It follows (Exercise 13) that the forms $q(x)$ and $[x]$ coincide, and γ is a similarity. $\square$

Proof of the Triality Theorem. The "bar" map $J(x) = \bar{x}$ is an anti-monotopy and an improper similarity. (Define (α, β, γ) to be an anti-autotopy if $\gamma(xy) = \alpha(y)\beta(x)$, etc.) If $g \in \mathrm{Sim}^\bullet(D)$ then $g = L_{g(1)} \circ h$ where $h \in \mathrm{O}(D)$. This h can be expressed as a product of hyperplane reflections τ_a (by a weak form of the Cartan–Dieudonné Theorem). As mentioned before (8.19), each τ_a is a scalar multiple of $B_a \circ J$ so it is an anti-monotopy. Therefore g is in the group generated by maps L_u, B_a and J so that g is a monotopy or an anti-monotopy. Moreover, g is a monotopy if and only if an even number of τ_a's are involved, if and only if g is a proper similarity. Conversely if $g \in \mathrm{Mon}(D)$ then $g \in \mathrm{Sim}^\bullet(D)$ and the same parity argument shows that g is proper. $\square$

We can use this theorem to analyze the spaces of composition algebras over $\mathbb{R}$ or $\mathbb{C}$. These numbers, summarized in the next corollary, agree with the earlier computations.

8.21 Corollary. *The table below lists the number of components and the dimensions of the spaces under discussion.*

	# of components	dimension
Comp(8)	8	56
$\mathrm{Comp}^1(8)$	4	28
$\mathrm{Comp}^{11}(8)$	2	7

Proof. The group $\mathrm{O}(8)^3$ has 8 components and acts transitively on Comp(8). Since $\mathrm{Comp}(8) \cong \mathrm{O}(D)^3/\,\mathrm{Autot}^{\mathrm{o}}(D)$ we find $\dim \mathrm{Comp}(8) = 3 \cdot 28 - 28 = 56$. Since $\mathrm{Autot}^{\mathrm{o}}(D) \subseteq \mathrm{O}^+(D)^3$, which is one component of $\mathrm{O}(D)^3$, there are still 8 components in Comp(8).

Using (8.5) we know that O(8) acting on $\mathrm{Comp}^1(8)$ has two orbits and $\mathrm{Stab}(D) = \{\beta \in \mathrm{O}(8) : \beta(xy) = x\beta(y) \text{ for every } x, y \in D\}$. If $\beta \in \mathrm{Stab}(D)$ then $\beta = R_b$ where $b = \beta(1)$ and $xy \cdot b = x \cdot yb$ (compare the proof of (8.16)). Then b is scalar (as in Exercise 1.27) and $\mathrm{Stab}(D) = \{\pm 1\}$, so that $\mathrm{Comp}^1(8) \cong \mathrm{O}(8)/\{\pm 1\}$ has 4 components and dimension 28.

Finally if $*$ is in $\mathrm{Comp}^1(8)$ define a new multiplication $\heartsuit$ by: $x \heartsuit y = R_e^{-1}(x) * y$. That is, $\heartsuit$ is defined by the formula: $(x * e) \heartsuit y = x * y$. Then e is a 2-sided identity element for $\heartsuit$ (see Exercise 0.8). The projection map $\pi : \mathrm{Comp}^1(8) \to \mathrm{Comp}^{11}(8)$, defined by $\pi(*) = \heartsuit$, acts as the identity map on $\mathrm{Comp}^{11}(8)$. O(8) acts on Comp(8) by: $(\alpha \bullet m)(x, y) = m(\alpha(x), y)$, and the subgroup $\mathrm{O}(7) = \{\alpha \in \mathrm{O}(8) : \alpha(e) = e\}$ acts on $\mathrm{Comp}^1(8)$. The point is that every O(7)-orbit in $\mathrm{Comp}^1(8)$ contains exactly one element in $\mathrm{Comp}^{11}(8)$. The uniqueness is easy and the existence follows since $\pi(m) = R_e^{-1} \bullet m$. Then $\mathrm{Comp}^{11}(8)$ becomes the orbit space $\mathrm{Comp}^1(8)/\,\mathrm{O}(7)$. Therefore $\mathrm{Comp}^{11}(8)$ has half as many components as $\mathrm{Comp}^{1}(8)$ and $\dim \mathrm{Comp}^{11}(8) = \dim \mathrm{Comp}^{1}(8) - \dim \mathrm{O}(7) = 28 - 21 = 7$. □

For $n = 4$ or 8, the eight components of $\mathrm{Comp}(n, n)$ are represented by the eight standard multiplications:

$$\begin{array}{cc} xy & yx \\ \bar{x}y & y\bar{x} \\ x\bar{y} & \bar{y}x \\ \bar{x}\bar{y} & \bar{y}\bar{x} \end{array}$$

Since $e * y = y$ for every multiplication in $\mathrm{Comp}^1(n)$, all the $\bar{y}$ terms are eliminated and the four components of $\mathrm{Comp}^1(n)$ are represented by the top four multiplications in the list. Similarly the two components of $\mathrm{Comp}^{11}(n)$ are represented by the first two cases: xy and yx.

We compared the dimensions of $\mathrm{Comp}(n)$ and $\mathrm{Div}(n)$ in the table after (8.10). For algebras with identity we see that $\mathrm{Comp}^{11}(8)$ is a compact 7-dimensional space inside $\mathrm{Div}^{11}(8)$ which is an open subset of the flat space $\mathrm{Bil}^{11}(8)$ of dimension 392. Actually the set of composition algebras inside $\mathrm{Div}^{11}(8)$ is a little larger, because $\mathrm{Comp}^{11}(8)$ uses a fixed norm form on $\mathbb{R}^8$. See Exercise 20.

Exercises for Chapter 8

1. **Defining $\chi(m)$.** Suppose $m \in \mathrm{Comp}(\sigma, q)$. Then $\hat{m} : S \to \mathrm{End}(V)$ and the space (S, σ) has a given orthogonal basis $\{e_1, \dots, e_s\}$. In the case $s \equiv 0 \pmod 4$ and $d\sigma = \langle 1 \rangle$ we also assume that $\sigma(e_1) \dots \sigma(e_s) = 1$. We defined $\chi(m)$ to equal $\chi(m_0)$ where $m_0 = \varphi^{-1}(m)$ as in (8.3).

(1) Setting $f_i = \hat{m}(e_i) \in S_m$ we have $\chi(m) = \mathrm{trace}(\tilde{f}_1 f_2 \tilde{f}_3 f_4 \dots)$.

(2) If $s \not\equiv 0 \pmod 4$ or if $d\sigma \neq \langle 1 \rangle$ then $\chi(m) = 0$. In any case, $\chi(m)$ is an even integer between $-n$ and n. (See (7.18).)

(3) If $(\alpha, \beta, \gamma) \in \mathrm{O}(\sigma) \times \mathrm{O}(q) \times \mathrm{O}(q)$ then $\chi((\alpha, \beta, \gamma) \bullet m) = (\det \alpha) \cdot \chi(m)$.

(Hint. (1) $\mathrm{image}(\hat{m}_0)$ has orthogonal basis $1_V, \tilde{f}_1 f_2, \dots, \tilde{f}_1 f_s$ so the element "z" equals $(\tilde{f}_1 f_2)(\tilde{f}_1 f_3) \dots (\tilde{f}_1 f_s)$. Then $z = \tilde{f}_1 f_2 \tilde{f}_3 f_4 \dots$, at least up to some scale factor. If $s \equiv 0 \pmod 4$ and $d\sigma = \langle 1 \rangle$ then $\tilde{z} = z$ and $z^2 = \mu(z) = 1$, and the scale factor needed was 1. Compare Exercise 2.8.

(3) See Exercise 2.8 (3), (4).)

2. **Generation of radical ideals.** In (8.9) the variety W is defined over $\mathbb{R}$. This means that $W = \mathcal{Z}(g_1, \dots, g_k)$, the zero set for a list of polynomials $g_j \in \mathbb{R}[X]$. The Jacobian criterion might not work directly for these g_i. (Provide an example where it fails.) In the proof of (8.9) we need to know that $\mathcal{I}(W)$ is generated by elements of $\mathbb{R}[X]$. If $\mathcal{A} = (g_1, \dots, g_k)\mathbb{C}[X]$ the Nullstellensatz says that $\mathcal{I}(W) = \sqrt{\mathcal{A}}$, the radical of the ideal $\mathcal{A}$. Our claim follows from a more general result:

Lemma. *Suppose K/F is a separable algebraic extension of fields. If $\mathcal{B} \subseteq F[X]$ is an ideal, then $\sqrt{\mathcal{B} \otimes K} = \sqrt{\mathcal{B}} \otimes K$.*

(Hint. It is enough to show that the ring $K[X]/(\sqrt{\mathcal{B}} \otimes K)$ is reduced (i.e. has no non-zero nilpotent elements). Since $\sqrt{\mathcal{B}}$ is an intersection of primes, $F[X]/\sqrt{\mathcal{B}}$ embeds into some direct product of fields. It suffices to show: if L/F is a field extension then $L \otimes K$ is reduced. We may assume here that K/F is finite and separable.)

3. Suppose W is an algebraic variety and G is an algebraic group which acts morphically on W, all defined over $\mathbb{C}$. If $G(\mathbb{C})$ acts transitively on $W(\mathbb{C})$ then W is a nonsingular variety and all the irreducible components of W have the same dimension. Moreover if G, W and the G-action are defined over $\mathbb{R}$ then $W(\mathbb{R})$ is a smooth real manifold. Does it follow that $G(\mathbb{R})$ acts transitively on $W(\mathbb{R})$?

(Hint. Let $G = W = \mathbb{C}^\bullet$ (an affine variety embedded in $\mathbb{C}^2$), with action $g \bullet w = g^2 w$.)

4. **Connected components.** $\text{Comp}^1_{\mathbb{R}}(s, n)$ has $2c$ components and $\text{Comp}_{\mathbb{R}}(s, n)$ has $4c$ components, where c is the number of k for which $\text{Comp}^1_{\mathbb{R}}(s, n; k) \neq \emptyset$. If $C = C((s-1)\langle -1 \rangle)$ then c is the number of non-isomorphic n-dimensional C-modules. Hence

$$c = \begin{cases} 1 & \text{if } s \not\equiv 0 \pmod 4 \\ 1 + \frac{n}{2^m} & \text{otherwise.} \end{cases}$$

The irreducible dimension 2^m can be computed directly from the structure of C.

5. **Characters.** Let D be a quaternion or octonion algebra with left representation $\mathcal{L} : D \to \text{Sim}(D)$ and compute the character of $\mathcal{L}$. Similarly compute the character of the right representation. Are the left and right characters equal?

6. **More division algebras.** Let D be a real composition algebra with $n = \dim D = 2$, 4 or 8. Suppose $b : D \times D \to D$ is an $\mathbb{R}$-bilinear map with the property that $|b(x, y)| < 1$ whenever $|x| = |y| = 1$. Define

$$m_b : D \times D \to D \quad \text{by} \quad m_b(x, y) = xy + b(x, y).$$

Then (D, m_b) is a division algebra. If we assume only $|b(x, y)| \leq 1$ what further conditions are needed to ensure that m_b is a division algebra? This construction provides a space of division algebras of dimension n^3. Does it equal the whole space $\text{Div}(n) = \text{Nsing}(n, n)$?

7. **Inverses.** Suppose A is an F-algebra, where F is a field.

(1) If A is an alternative division algebra and $\dim A$ is finite then A must have an identity element.

(2) Suppose A has an identity element and every non-zero element of A has an inverse (that is: if $0 \neq a \in A$, there exists $b \in A$ with $ab = ba = 1$). Does it follow that A is a division algebra? Find a counterexample where $F = \mathbb{R}$, $\dim A = 3$.

(3) A *strong inverse* for $a \in A$ is $a^{-1} \in A$ such that $a^{-1} \cdot ax = x = xa \cdot a^{-1}$ for every $x \in A$. Suppose every non-zero element of A has a strong inverse. Check that $(a^{-1})^{-1} = a$ and deduce that A is a division algebra. In a composition algebra every a with $[a] \neq 0$ has a strong inverse.

Theorem. *Suppose A is a ring with* 1. *Then: every non-zero element of A has a strong inverse if and only if A is an alternative division ring.*

(Hint. (1) If $a \neq 0$, find e with $ae = a$. Prove $e^2 = e$.

(2) Let $A = \mathbb{R}^3$ with basis $\{1, i, j\}$, choose $\delta \in A$ and define $i^2 = j^2 = -1$ and $ij = -ji = \delta$. Then every non-zero element has an inverse. (Define "bar" and compute $u \cdot \bar{u} = \bar{u} \cdot u$.) Moreover, if $\delta \neq 0$ then $uv = vu = 0$ implies $u = 0$ or $v = 0$. Hence inverses are unique, but clearly A cannot be a division algebra.

(3) The proof of the theorem is elementary but not easy. See Hughes and Piper (1973), pp. 137–138 and p. 151, or see Mal'cev (1973), pp. 91–94.)

8. **Components.** $\mathrm{Div}(n)$ is a nonempty open subset of $\mathrm{Bil}(n)$, provided $n = 1$, 2, 4, 8.

(1) Describe the topological spaces $\mathrm{Div}^{11}(2)$ and $\mathrm{Div}(2)$ explicitly. Check that $\mathrm{Div}^{11}(2)$ is the "interior" of a certain parabola in $\mathrm{Bil}^{11}(2) \cong \mathbb{R}^2$. Then $\mathrm{Div}(2)$ is 8-dimensional with 4 components. Everything in $\mathrm{Div}(2)$ is isotopic to $\mathbb{C}$ and $\mathrm{Autot}(\mathbb{C}) \cong \mathbb{C}^* \times \mathbb{C}^* \times \{1, -1\}$.

(2) If $m \in \mathrm{Div}(n)$ and $0 \neq x \in \mathbb{R}^n$, define $\lambda(m) = \mathrm{sgn}(\det(m_x))$, where m_x is the left multiplication map. This $\lambda(m)$ is independent of x. Let $\rho(m)$ be the sign for the right multiplications. For signs ε, η let $\mathrm{Div}^{\varepsilon\eta} = \{m \in \mathrm{Div}(n) : \lambda(m) = \varepsilon \text{ and } \rho(m) = \eta\}$. These four subsets are represented by xy, $\bar{x}y$, $x\bar{y}$, $\overline{xy}$.

(3) If $m \in \mathrm{Div}^{++}(n)$ there is a path in $\mathrm{Div}^{++}(n)$ from m to some $m_1 \in \mathrm{Div}^{11}(n)$.

(4) Buchanan (1979) used homotopy theory to prove:

Theorem. *If $n = 4$ or 8 then $\mathrm{Div}^{11}(n)$ has two connected components, represented by the multiplications xy and yx.*

Corollary. $\mathrm{Div}(4)$ *and* $\mathrm{Div}(8)$ *each have* 8 *connected components, represented by the eight standard multiplications.*

(Hint. (3) By Exercise 0.8, there exist $f, g \in \mathrm{GL}^+(n)$ with $(f, g) * m \in \mathrm{Div}^{11}(n)$. Choose paths in $\mathrm{GL}^+(n)$ from 1_n to f and from 1_n to g.)

9. **$\mathrm{Sub}(s, n; k)$.** Define $\varphi : \mathrm{O}(n) \times \mathrm{Sub}^1(s, n; k) \to \mathrm{Sub}(s, n; k)$ by: $\varphi(g, T) = gT$. Then φ is surjective with fiber $\varphi^{-1}(S) \cong S \cap \mathrm{O}(n)$, which is the unit sphere in S. Hence $\dim \mathrm{Sub}(s, n; k) = \frac{n(n-1)}{2} + \dim \mathrm{Sub}^1(s, n; k) - (s - 1)$. Is this consistent with (8.12)?

10. How does the $\mathrm{O}(s)$ action relate to the $\mathrm{O}(n) \times \mathrm{O}(n)$ action?

(1) Let $\alpha \in \mathrm{O}(s)$ and $m \in \mathrm{Comp}^1(s, n)$. Then $\chi(\alpha \bullet m) = (\det \alpha) \cdot \chi(m)$. Each orbit of the group $\mathrm{O}(s) \times \mathrm{O}(n)$ equals $\mathrm{Comp}^1(s, n; k) \cup \mathrm{Comp}^1(s, n; -k)$ for some k.

(2) Let $S \in \mathrm{Sub}^1(s, n; k)$. Define $\mathrm{Aut}^{\&}(S) = \{(\beta, \gamma) \in \mathrm{O}(n) \times \mathrm{O}(n) : \gamma S \beta^{-1} = S\}$ and consider the induced group homomorphism $\mathrm{Aut}^{\&}(S) \to \mathrm{O}(S)$. The image is $\mathrm{O}^+(n)$ if $\chi(S) \neq 0$, and it is $\mathrm{O}(n)$ if $\chi(S) = 0$.

(3) There is an exact sequence

$$1 \to \mathrm{Aut}(m) \to \mathrm{Aut}^{\&}(S) \to \left\{ \begin{matrix} \mathrm{O}(S) & \text{if } \chi(S) = 0 \\ \mathrm{O}^+(S) & \text{if } \chi(S) \neq 0 \end{matrix} \right\} \to 1.$$

Compute $\dim \mathrm{Aut}^{\&}(S)$ and use this to give another computation of $\dim \mathrm{Sub}(s, n)$.

(4) Similarly analyze $\mathrm{Aut}(S) = \{\beta \in \mathrm{O}(n) : \beta S \beta^{-1} = S\}$.

(Hint. (2) If $\alpha \in \mathrm{O}^+(S)$ then α is in the image, using C-isometries as in (8.5) or (7.19). Conversely suppose α is in that image. If $\chi(m) \neq 0$ apply part (1).)

11. **Automorphism groups.** There are several reasonable definitions for “the” automorphism group of a composition $m \in \mathrm{Comp}(s, n)$. For example,

$$\mathrm{Aut}(m) = \{\beta \in \mathrm{O}(n) : \beta \diamond m = m\} = \{\beta \in \mathrm{O}(n) : (1, \beta, \beta) \bullet m = m\},$$

as defined above.

$$\mathrm{Aut}^{\&}(m) = \{(\beta, \gamma) \in \mathrm{O}(n) \times \mathrm{O}(n) : (1, \beta, \gamma) \bullet m = m\}.$$

$$\mathrm{Aut}^{\%}(m) = \{(\alpha, \beta) \in \mathrm{O}(s) \times \mathrm{O}(n) : (\alpha, \beta, \beta) \bullet m = m\}.$$

$$\mathrm{Autot}(m) = \{(\alpha, \beta, \gamma) : (\alpha, \beta, \gamma) \bullet m = m\}.$$

These are related to the groups $\mathrm{Aut}(S)$ and $\mathrm{Aut}^{\&}(S)$ defined in Exercise 10. What are the dimensions of these algebraic groups?

12. **Proper similarities.** Here is a sketch of the proof of (8.14). Suppose $1_V \in S \subseteq \mathrm{Sim}(V, q)$ and $s = \dim S > 2$.

First Step. If $g \in \mathrm{Sim}^\bullet(V, q)$ and $gSg^{-1} = S$ then g is proper.

(1) Find a counterexample when $\dim S = \dim V = 2$. If $\dim S = 2$ and $4 \mid \dim V$ then g is proper.

(2) Suppose $C = C(W, \varphi)$ is a Clifford algebra with center Z. If $x \in W$ is anisotropic then $xWx^{-1} = W$. (In fact the map $w \mapsto xwx^{-1}$ is the reflection through the line Fx.)

Lemma. *If $u \in C^\bullet$ and $uWu^{-1} = W$ then $u = y \cdot x_1 \cdot x_2 \dots x_k$ for some $y \in Z$ and $x_i \in W$.*

(3) *Proof of First Step when s is odd.* $C = C(-S_1)$ is central simple, and $C \otimes A = \mathrm{End}(V)$ where $A = \mathrm{End}_C(V)$. The involution $I_q =$ “$\sim$” preserves C and A. Then $gCg^{-1} = C$ so there exists $u \in C^\bullet$ such that $a = u^{-1}g \in A$. Since $\tilde{g}g = \mu(g)$ conclude that $\tilde{a}a$ and $\tilde{u}u$ are scalars. Since a commutes with elements of S it is proper, by Exercise 1.17. Since $uS_1u^{-1} = S_1$ and $Z = F$, the lemma implies $u = x_1 \cdot x_2 \dots x_k$ for some $x_i \in S_1$. Hence $g = ua$ is proper.

(4) *Proof of First Step when s is even.* C_0 is central simple, and $C_0 \otimes A = \mathrm{End}(V)$ where $A = \mathrm{End}_{C_0}(V)$. As before, there exists $u \in C_0^\bullet$ such that $a = u^{-1}g \in A$

and $\tilde{a}a$ and $\tilde{u}u = \beta$ are scalars. Then a is proper since it commutes with f_2f_3. Since $Z = F \oplus Fz$ is the center of C, $gzg^{-1} = \varepsilon z$ for some $\varepsilon = \pm 1$. Then $aza^{-1} = u^{-1}gzg^{-1}u = \varepsilon z$ and hence $aS_1a^{-1} = S_1$ since $S_1 \subseteq zC_0$. Therefore $uS_1u^{-1} = S_1$ and the lemma applies as before to show that u and $g = ua$ are proper.

(5) $h \in S$ implies $hSh \subseteq S$.

(6) Suppose F is algebraically closed. If $f \in S$ there exists $h \in S$ with $h^2 = f$.

(7) Suppose $\gamma S\beta^{-1} = S$ as in (8.14). Assume F is algebraically closed and use (6) to find $h \in S$ such that $h^2 = \gamma^{-1}\beta$. Let $g = \gamma h$ so that $g^{-1} = h\beta^{-1}$. By (5), $gSg^{-1} = \gamma hSh\beta^{-1} = S$ and the First Step implies that g is proper. Since h is proper conclude that both β and γ are proper.

(Hint. (1) Exercise 1.17.

(2) The map $w \mapsto uwu^{-1}$ is in $\mathrm{O}(W)$, and hence is a product of hyperplane reflections. Compare Cassels (1978), pp. 175–177 or Scharlau (1985), pp. 334–336.

(5) Choose the basis of S so that $h = a + bf_2$ and compute hf_jh.

(6) If $f = r + sf_2$ let $h = x + yf_2$ and solve for x and y.)

13. **Norm form uniqueness.** Suppose D is a composition algebra (with identity) relative to two quadratic forms $q(x)$ and $q'(x)$. These forms must coincide.

(Hint. The theory in Chapter 1 provides associated involutions $\bar{x}$ and $\tilde{x}$ so that $q(x) = x \cdot \bar{x}$ and $q'(x) = x \cdot \tilde{x}$. Show that these involutions coincide.)

14. **Trilinear map.** (1) For euclidean spaces U, V, W the following are equivalent:

(a) There is a bilinear $f : U \times V \to W$ with the norm property $|f(u, v)| = |u| \cdot |v|$.

(b) There is a trilinear map $g : U \times V \times W \to \mathbb{R}$ such that $|g(u, v, w)| \le |u| \cdot |v| \cdot |w|$ and moreover for every u, v there exists a non-zero w such that equality holds.

(2) If $\dim U = \dim V = \dim W$ then condition (b) is symmetric in U, V, W.

(Hint. (2) f, g are related by $g(u, v, w) = \langle f(u, v) | w \rangle$, where $\langle x|y \rangle$ is the dot product.)

15. The Triality Theorem implies that for every $\gamma \in \mathrm{O}^+(8)$, there exist $\alpha, \beta \in \mathrm{O}^+(8)$ such that (α, β, γ) is an autotopy, relative to the standard octonion multiplication. Moreover α, β are uniquely determined up to sign.

(1) Every $\gamma \in \mathrm{O}^+(8)$ equals $B_{\bar{a}}B_bB_{\bar{c}} \dots B_{\bar{g}}$, a product of (at most) 7 bi-multiplication maps.

(2) Then $\alpha = L_{\bar{a}}L_bL_{\bar{c}} \dots L_{\bar{g}}$ and $\beta = R_{\bar{a}}R_bR_{\bar{c}} \dots R_{\bar{g}}$, up to sign.

(3) Every $\alpha \in \mathrm{O}^+(8)$ can be expressed as a product of 7 of the maps L_a and also as a product of 7 of the maps R_a.

(4) If $(\alpha, \beta, \gamma) \in \mathrm{Autot}(D)$ then: $\alpha = \beta = \gamma$ is an automorphism $\iff \alpha(1) = \beta(1) = 1$. Compare Exercise 1.24.

(5) How much of this theory goes through for octonion algebras over a general field?

(Hint. (1) The Cartan–Dieudonné Theorem (proved in Artin (1957) or Lam (1973)) implies that $\gamma = \tau_1 \cdot \tau_a \dots \tau_g$ for some 7 unit vectors $a, \dots, g \in \mathbb{R}^8 = D$. Then $\gamma = B_{\bar{a}} B_b B_{\bar{c}} \dots B_{\bar{g}}$.

(2) Use the explicit autotopies (L_u, R_u, B_u) and the uniqueness of α, β.

(5) There are some difficulties with scalars over a general field F. For instance the group $\mathcal{B}$ generated by the B_a's consists of all $\theta(\sigma) \cdot \sigma$ where $\sigma \in \mathrm{O}^+(D)$ and $\theta(\sigma)$ denotes the spinor norm of σ. The group $F^\bullet \cdot \mathcal{B}$ can be a proper subgroup of $\mathrm{Sim}^+(D)$. Does the group generated by the L_a's equal $\mathrm{Sim}^+(D)$?)

16. **Automorphism and autotopy.** (1) If D is the octonion division algebra over $\mathbb{R}$ determine $\dim \mathrm{Aut}(D)$.

(2) The "companion" map $\mathrm{Autot}^{\mathrm{o}}(8) \to S^7 \times S^7$ sends $(\alpha, \beta, \gamma) \in \mathrm{Autot}^{\mathrm{o}}(8)$ to $(a, b) = (\beta(1)^{-1}, \alpha(1)^{-1})$. Then $\alpha = R_a \circ \gamma$ and $\beta = L_b \circ \gamma$. The nonempty fibers of this companion map are the cosets $(\alpha, \beta, \gamma) \cdot \mathrm{Aut}(D)$.

(3) $\mathrm{Autot}^{\mathrm{o}}(8)$ is a connected 2-fold covering group of $\mathrm{Mon}^{\mathrm{o}}(8) = \mathrm{O}^+(8)$.

(4) The companion map is surjective.

How does composition of autotopies corresponding to an operation on the associated companion pairs in $S^7 \times S^7$?

(Hint. (1) $\dim \mathrm{Aut}(D) = 14$. For D is generated by unit vectors i, j, v such that $D = H \perp Hv$ where H is the quaternion algebra generated by i, j. If $\varphi \in \mathrm{Aut}(D)$ then $\varphi(i)$ can be any unit vector in $\{1\}^\perp$, a choice in S^6. Given $\varphi(i)$, then $\varphi(j)$ can be any unit vector in $\{1, i\}^\perp$, etc.

(3) $\pi : \mathrm{Autot}^{\mathrm{o}}(8) \to \mathrm{Mon}^{\mathrm{o}}(8)$ is a homomorphism with kernel $\{(1, 1, 1), (-1, -1, 1)\}$. Find a path between those two points in $\mathrm{Autot}^{\mathrm{o}}(8)$ by using autotopies (L_a, R_a, B_a).

(4) Compute dimensions.)

17. **Dimension 1, 2, 4.** (1) Analyze the spaces $\mathrm{Comp}^{11}(1)$ and $\mathrm{Comp}^{11}(2)$.

(2) Work out the parallels of (8.17) through (8.21) for quaternion algebras. Deduce that $\dim \mathrm{Autot}(4) = 11$ and $\dim \mathrm{Autot}^{\mathrm{o}}(4) = 9$. What is the analog of the companion map of Exercise 16?

18. **Isotopy and isomorphism.** Let D be a quaternion or octonion division algebra over $\mathbb{R}$.

(1) If $n = 4$ or 8 let Isotop(n) be the set of all multiplications on $\mathbb{R}^n$ which are isotopic to the multiplication of D. (Why is this independent of the choice of D?) Then Isotop(n) can be viewed as an algebraic variety. What is its dimension?

(2) Similarly analyze $\mathrm{Isomor}(n)$, the set of algebras isomorphic to D.

(Hint. (1) Isotop(n) is an orbit of $\mathrm{GL}(n)^3$ with stabilizer $\mathrm{Autot}(D)$.

(2) $\mathrm{Isomor}(n)$ is an orbit of $\mathrm{GL}(n)$ with stabilizer $\mathrm{Aut}(D)$.)

19. **Loops.** An *inverse loop* is a set G with a binary operation such that (i) there is an identity element $1 \in G$; and (ii) for every $x \in G$ there exists $x^{-1} \in G$ satisfying: $x^{-1} \cdot xy = y = yx \cdot x^{-1}$ for every $y \in G$. An *autotopy* on G is a triple (α, β, γ) of invertible maps on G such that: $\gamma(xy) = \alpha(x)\beta(y)$ for every x, y.

(1) If $xy = z$ then $x = zy^{-1}$, $z^{-1}x = y^{-1}, \dots$, and we get the associated hexagon of six autotopies of G. Define a monotopy and deduce that α, β, γ are monotopies.

(2) γ is a monotopy if and only if there exist $a, b \in G$ such that $\gamma(xy) = \gamma(x)a \cdot b\gamma(y)$ for every x, y. The elements a, b are the *companions* of γ. Note that $\alpha = R_a \circ \gamma$ and $\beta = L_b \circ \gamma$ provide the autotopy, and $a = \beta(1)^{-1}$ and $b = \alpha(1)^{-1}$.

(3) For a as above, $B_a(x) = axa$ is unambiguously defined and (L_a, R_a, B_a) is an autotopy. Similarly we find autotopies (B_a, L_a^{-1}, L_a), (R_a^{-1}, B_a, R_a) etc. These imply the Moufang identities: $ax \cdot ya = a(xy)a$; $axa \cdot a^{-1}y = a \cdot xy$; $xa^{-1} \cdot aya = xy \cdot a$.

(4) If $a \in G$ the following are equivalent:

(i) a is the image of 1 under a monotopy;
(ii) (L_a, R_a, B_a) is an autotopy;
(iii) the Moufang identities hold for a.

A Moufang loop (or "Moup") is an inverse loop in which every a, x, y satisfies the Moufang identities. Then G is a Moufang loop if and only if the monotopies act transitively on G.

(Hint. (3) $(\beta, \iota\gamma\iota, \iota\alpha\iota) \circ (\gamma, \iota\beta\iota, \alpha)^{-1} = (\beta\gamma^{-1}, \iota\gamma\beta^{-1}\iota, \iota\alpha\iota\alpha^{-1}) = (L_a, R_a, \iota\alpha\iota\alpha^{-1})$ is an autotopy, so that $\iota\alpha\iota\alpha^{-1}(xy) = ax \cdot ya$ for every x, y. Then $B_a(x) = ax \cdot a = a \cdot xa$ and (L_a, R_a, B_a) works. The six autotopies derived from this one provide other examples.)

20. **Other norm forms.** Fix $e \neq 0$ in $\mathbb{R}^8$ and let $\mathrm{Comp}^e(8)$ be the set of all multiplications $m \in \mathrm{Bil}(8)$ which make $\mathbb{R}^8$ into a composition division algebra with identity element e. Here we do not assume that the standard inner product is the norm form. Then $\mathrm{Comp}^e(8) \subseteq \mathrm{Div}^{11}(8)$. Is $\mathrm{Comp}^e(8)$ a nice topological space? What is its dimension?

(Hint. If $\mathrm{PD}(n) = \{$positive definite quadratic forms on $\mathbb{R}^n\}$, then $\dim \mathrm{PD}(n) = n(n+1)/2$ since $\mathrm{PD}(n) \cong \mathrm{GL}(n)/\mathrm{O}(n)$. Then $\mathrm{PD}^1(8) = \{q \in \mathrm{PD}(8) : q(e) = 1\}$ has dimension 35. Is there a bijection: $\mathrm{Comp}^e(8) \leftrightarrow \mathrm{Comp}^{11}(8) \times \mathrm{PD}^1(8)$?)

21. For which $\alpha, \beta, \gamma \in \mathrm{GL}(8)$ does the action of (α, β, γ) on $\mathrm{Bil}(8)$ preserve the subset $\mathrm{Div}^{11}(8)$?

(*Idea.* Let $m_1(x, y) = xy$ be the octonion multiplication with identity e. If $\varphi \in \mathrm{GL}(8)$ with $\varphi(e) = e$ then $m_\varphi = (\varphi, \varphi, \varphi) \bullet m_1$ is in $\mathrm{Div}^{11}(8)$. Then $(r\varphi, s\varphi, rs\varphi)$ preserves $\mathrm{Div}^{11}(8)$ when $r, s \in \mathbb{R}^\bullet$. Conversely if (α, β, γ) preserves it then $\varphi^{-1}\gamma^{-1}(x) = \varphi^{-1}\alpha^{-1}(x) \cdot \varphi^{-1}\beta^{-1}(e)$ and $\varphi^{-1}\gamma^{-1}(y) = \varphi^{-1}\alpha^{-1}(e) \cdot \varphi^{-1}\beta^{-1}(y)$ for every $x, y \in D$ and every such φ. Must $\alpha^{-1}(e)$ and $\beta^{-1}(e)$ be scalar multiples of e?)

22. **Split octonion algebras.** In (8.17) through (8.21) we assumed that the octonion algebra D is a division algebra (so the norm form $[x]$ is anisotropic). Are the same results true when D is a "split" octonion algebra, that is, when the norm form $[x]$ on D is hyperbolic?

(Note. If F is infinite the non-invertible elements form the zero set of a polynomial function. Therefore almost all elements of D are invertible.)

23. **Robert's Thesis (1912).** Let $\mathcal{A}$ be the set of all $n \times n$ matrices A whose entries are $\mathbb{C}$-linear forms in $X = (x_1, \dots, x_s)$ and which satisfy $A^\top \cdot A = (x_1^2 + \cdots + x_s^2) \cdot I_n$.

(1) Each $A \in \mathcal{A}$ corresponds to a unique $m \in \mathrm{Comp}_{\mathbb{C}}(s, n)$.

(2) $\mathrm{O}(n) \times \mathrm{O}(n)$ acts on $\mathcal{A}$ by: $(P, Q) * A = P \cdot A \cdot Q^\top$. This corresponds to the action on Comp described above. Consequently $\mathcal{A}$ is an algebraic variety, and we know the number of components and their dimensions.

(Hint. (1) Recall the original treatment by Hurwitz as described in Chapter 0.)

Notes on Chapter 8

The ideas presented in the first part of the Chapter are based on results of Petersson (1971) and of Bier and Schwardmann (1982). The homology and stable homotopy groups of the topological spaces $\mathrm{Comp}^1(s, n)$ were computed by Bier and Schwardmann.

Zorn characterized finite dimensional alternative division algebras over any base field. One proof appears in Schafer (1966), p. 56. The result has a remarkable generalization, due to Kleinfeld, Bruck and Skornyakov:

Theorem. *Any simple alternative ring, which is not a nilring and which is not associative, must be an octonion algebra over its center.*

This theorem is proved in Kleinfeld (1953) and in Zhevlakov et al. (1982), §7.3. An easier proof, assuming characteristic $\neq 2$, is given in Kleinfeld (1963).

There are more constructions of real division algebras, usually done by "twisting" the standard algebras in various ways. For example see Althoen, Hansen and Kugler (1994). Further information on real division algebras is contained in Myung (1986). Certain "pseudo-octonion" algebras are 8-dimensional division algebras (without an identitiy element) which are especially symmetric. See also Elduque and Myung (1993).

The dimension argument after (8.15) showing that not all division algebra multiplications are isotopic to a composition algebra is due to Petersson.

Dimension counts show how hard it might be to get a useful classification of real division algebras. However, there is a positive result about general elements of $\mathrm{Div}^{11}(n)$.

Theorem. *If D is a real division algebra with identity and* $\dim D > 1$*, then D contains a subalgebra isomorphic to $\mathbb{C}$. That is, there exists $a \in D$ with $a^2 = -1$.*

Proofs appear in Yang (1981) and Petro (1987). Both proofs use topological properties to prove that the map $x \mapsto x^2$ is surjective on D.

Following (8.15), $\text{Div}(n) = \text{Nsing}(n, n, n)$. Bier (1979) showed that $\text{Nsing}(r, s, n)$ is a semi-algebraic set and hence has a finite number of connected components. He also proved that if $n \geq r + s - 1$ then $\text{Nsing}(r, s, n)$ is dense in $\text{Bil}(r, s, n)$ and if moreover $n > (r \# s) + r + s - 1$ then $\text{Nsing}(r, s, n)$ is connected. (This notation $r \# s$ is defined in Chapter 12.)

The viewpoint and terminology of autotopies and monotopies, as defined in (8.17), was explained to me in 1980 by J. H. Conway. Versions of Conway's approach are also seen in Exercises 16 and 20, as well as in the appendix to Chapter 1.

Our presentation of the Triality Principle 8.19 basically follows van der Blij and Springer (1960), who prove it without restrictions on the characteristic of the ground field. Some simplifications in the proof use Conway's approach. Other authors use the terms autotopism and isotopism. See Hughes and Piper (1973), Chapter VIII.

Over any field F (with characteristic $\neq 2$), every $m \in \text{Comp}(4, 4)$ is isotopic to a quaternion algebra H. Letting xy be the multiplication in H, then the multiplication $m(x, y)$ is expressible as one of four types:

$$(1)\ axcyb \qquad (2)\ axb\bar{y}c \qquad (3)\ c\bar{x}ayb \qquad (4)\ a\bar{x}c\bar{y}b$$

where $a, b, c \in H$ and $N(abc) = 1$. For what choices of a, b, c are two of these algebras isomorphic? This question is analyzed by Stampfli-Rollier (1983).

Kuz'min (1967) discusses the topological space of all isomorphism classes of n-dimensional real division algebras (with identity). He considers the subspaces of power-associative algebras, quadratic algebras, etc., and determines their dimensions.

Exercise 4. Bier and Schwardmann (1982) discuss this number of components.

Exercise 7. (2) A similar remark is made in Althoen and Weidner (1978).

(3) Stronger theorem: If every non-zero element of A has a strong right inverse, then A is alternative. This result is related to the geometry of projective planes. See Hughes and Piper (1973), pp. 140–149.

Exercise 8. Buchanan's proof uses homotopy theory.

Define $\mathcal{A}(n) = \{A \in \text{GL}_n(\mathbb{R}) : A \text{ has no real eigenvalues}\}$ and $\mathcal{W}(n) = \{W \in \text{O}(n) : W \text{is skew-symmetric}\}$. Buchanan proves $\mathcal{W}(n)$ is a strong deformation retract of $\mathcal{A}(n)$. The space $\mathcal{W}(n)$ has two connected components, separated by the Pfaffian (see (10.8)). Any $m \in \text{Div}^{11}(n)$ induces $\hat{m} : \mathbb{R}^n - \{0\} \to \mathcal{A}(n)$ and this maps to $\mathcal{W}(n)$. The standard composition algebras yield multiplications xy and yx with unequal Pfaffians. Hence $\text{Div}^{11}(n)$ has at least two components. A computation of $\pi_{n-2}(\mathcal{A}(n))$ leads to a proof that there are only two components.

A somewhat simpler proof in the case $n = 4$ is given by Gluck, Warner and Yang (1983), §8. The components are separated by their "handedness".

Exercise 11. The group $\mathrm{Aut}^{\%}(m)$ was studied by Riehm (1982), a work motivated by a question of A. Kaplan (1981). Those ideas were extended in Riehm (1984).

Exercise 15–16. This threefold symmetry for α, β, γ in $\mathrm{O}^{+}(8)$ is one aspect of triality. The sign ambiguities can be removed if we work with the covering group Spin(8) instead. From Exercise 16(3) it follows that $\mathrm{Autot}^{\mathrm{o}}(8) \cong \mathrm{Spin}(8)$. Many aspects of triality have appeared in the mathematical literature. For example see Knus et al. (1998), §35, and Chapter 10.

Exercise 19. This approach to Moufang loops is due to J. H. Conway. Connections between Moufang loops and geometry are described in Bruck (1963).

Exercise 23. E. Robert, in his 1912 thesis, analyzed these matrices A in the cases $r = n = 4$, 8. He showed essentially that $\mathrm{Comp}_{\mathbb{C}}(n, n)$ consists of two orbits of $\mathrm{O}(n) \times \mathrm{O}(n)$, distinguished by the “character”.

Chapter 9

The Pfister Factor Conjecture

We focus now on the form q rather than on (σ, τ). Suppose F is a field (in which $2 \neq 0$). Given n, which n- dimensional forms q over F admit the largest possible families in $\mathrm{Sim}(q)$? We stated the following conjecture in (2.17).

9.1 Pfister Factor Conjecture. Let q be a quadratic form over F with $\dim q = n = 2^m n_0$ where n_0 is odd. If there is an $(m+1, m+1)$-family in $\mathrm{Sim}(q)$ then $q \simeq \varphi \otimes \omega$ where φ is an m-fold Pfister form and $\dim \omega$ is odd.

One attraction of this conjecture is that it relates the forms involved in the Hurwitz–Radon type of "multiplication" of quadratic forms with the multiplicative quadratic forms studied by Pfister. We will reduce the question to the case $n = 2^m$ and to prove it whenever $m \leq 5$. The difficulties in extending our proof seem closely related to the difficulties in extending Pfister's result (3.21) for forms in I^3F. For certain special classes of fields we can prove the conjecture. For example, it is true for every global field. In the appendix we describe (without proofs) some results about function fields of quadratic forms and use that theory to provide another proof of the cases $m \leq 5$.

This conjecture can be restated in terms of the original sort of composition defined in Chapter 1. For as noted in the (7.12), if $\dim q = 2^m \cdot (\text{odd})$, then there exists $\sigma < \mathrm{Sim}(q)$ with $\dim \sigma = \rho(n)$ if and only if there exists an $(m+1, m+1)$-family in $\mathrm{Sim}(q)$.

If either σ or τ is isotropic then $(\sigma, \tau) < \mathrm{Sim}(q)$ implies that q is hyperbolic, by (1.9). In this case the conjecture is trivial so we may assume that σ and τ are anisotropic.

9.2 Conjecture PC(m). Suppose q is a quadratic form over F with $\dim q = 2^m$. If there exists an $(m+1, m+1)$-family in $\mathrm{Sim}(q)$, then q is similar to a Pfister form.

Proof that $\mathrm{PC}(m)$ *is equivalent to the Pfister Factor Conjecture* 9.1. Certainly (9.1) implies $\mathrm{PC}(m)$. Conversely assume $\mathrm{PC}(m)$ and suppose q is given with $\dim q = n = 2^m n_0$ and with an $(m+1, m+1)$-family $(\sigma, \tau) < \mathrm{Sim}(q)$. The Decomposition Theorem 4.1 implies that all the (σ, τ)-unsplittables have the same dimension 2^k. Since q is a sum of unsplittables, $2^k \mid n$ so that $k \leq m$. If φ is an unsplittable then $s + t = 2m + 2$ implies $\dim \varphi = 2^m$. Then the uniqueness in (7.2) implies that all (σ, τ)-unsplittables are similar to φ. Therefore $q \simeq \varphi \otimes \omega$ for some form ω of dimension n_0, which is odd. The form φ is similar to a Pfister form by PC(m). Absorbing the scale factor into ω, we may assume φ is a Pfister form. □

9.3 Lemma. PC(m) *is true for* $m \leq 3$.

Proof. The cases $m = 1, 2$ are vacuous. Suppose $m = 3$ and $\dim q = 8$ and q admits a $(4, 4)$-family. By (1.10) a $(3, 0)$-family $\langle 1, a, b\rangle < \mathrm{Sim}(q)$ already implies that $\langle\langle a, b\rangle\rangle \mid q$, forcing q to be similar to a Pfister form. □

Suppose $\dim q = 2^m$ and $(\sigma, \tau) < \mathrm{Sim}(q)$ is an $(m + 1, m + 1)$-family. As mentioned after (7.1) we have $d\sigma = d\tau$, $c(\sigma) = c(\tau)$, so that $\sigma \equiv \tau \pmod{J_3(F)}$. If applications of the Shift Lemma can transform the pair (σ, τ) into some pair (δ, δ), then (2.16) implies the Conjecture PC(m). To state this idea more formally we introduce the set $\mathcal{P}_m$ of all (s, t)- pairs of quadratic forms over F where $s + t = 2m + 2$. Define the relation $\approx$ on $\mathcal{P}_m$ to be the equivalence relation generated by three "elementary" relations motivated by the ideas in Chapter 2:

(1) $(\sigma, \tau) \approx (\tau, \sigma)$.

(2) $(\sigma, \tau) \approx (\langle a\rangle\sigma, \langle a\rangle\tau)$ whenever $a \in D_F(\sigma)D_F(\tau)$.

(3) $(\sigma \perp \varphi, \tau \perp \psi) \approx (\sigma \perp \langle d\rangle\psi, \tau \perp \langle d\rangle\varphi)$ whenever $\dim \varphi \equiv \dim \psi \pmod 4$ and $\langle d\rangle = (\det \varphi)(\det \psi)$.

The motivation for this definition arises from the following basic observation:

If $(\sigma, \tau) \approx (\sigma', \tau')$ then: $(\sigma, \tau) < \mathrm{Sim}(V, B)$ if and only if $(\sigma', \tau') < \mathrm{Sim}(V, B)$.

9.4 Definition. Let $\mathcal{P}_m^\circ$ be the set of all (s, t)-pairs (σ, τ) such that $s + t = 2m + 2$, $d\sigma = d\tau$, $c(\sigma) = c(\tau)$ and $s \equiv t \pmod 8$. Equivalently, $\mathcal{P}_m^\circ$ is the set of all $(\sigma, \tau) \in \mathcal{P}_m$ such that $\sigma \equiv \tau \pmod{J_3(F)}$ and $s \equiv t \pmod 8$.

We first observe that $\mathcal{P}_m^\circ$ is a subset of $\mathcal{P}_m$ preserved by the equivalence relation.

9.5 Lemma. *Suppose* $(\sigma, \tau) \in \mathcal{P}_m$.

(1) $(\sigma, \tau) \in \mathcal{P}_m^\circ$ *if and only if* $(\sigma, \tau) < \mathrm{Sim}(q)$ *for some* q *with* $\dim q = 2^m$.

(2) *If* $(\sigma, \tau) \approx (\sigma', \tau')$ *and* $(\sigma, \tau) \in \mathcal{P}_m^\circ$, *then* $(\sigma', \tau') \in \mathcal{P}_m^\circ$.

Proof. (1) Apply (7.3).

(2) This follows from (1) and ideas from Chapter 2. Here is a more direct proof. We may assume that the (s', t')-pair (σ', τ') is obtained from the (s, t)-pair (σ, τ) by applying one of the three elementary relations. Since $s \equiv t \pmod 8$ is easily follows that $s' \equiv t' \pmod 8$. Let $\beta = \sigma - \tau$ and $\beta' = \sigma' - \tau'$. The elementary relations

imply the following equations in the Witt ring:

$$\begin{array}{ll} \beta' = -\beta & \text{if type 1.} \\ \beta' = \langle a\rangle\beta & \text{if type 2.} \\ \beta' = \beta + \langle\langle d\rangle\rangle \otimes (\varphi \perp -\psi) & \text{if type 3.} \end{array}$$

Now $\beta \in I^2F$ so that $\beta \equiv \langle x\rangle\beta \pmod{I^3F}$ for every $x \in F^\bullet$. Also since $d(\varphi \perp -\psi) = (d\varphi)(d\psi) = \langle d\rangle$, Exercise 3.7 (4) implies $\langle\langle d\rangle\rangle \otimes (\varphi \perp -\psi) \in I^3F$. Then in each case $\beta' \equiv \beta \pmod{I^3F}$. Since $I^3F \subseteq J_3(F)$ we have $\beta' \in J_3(F)$ so that $(\sigma', \tau') \in \mathcal{P}_m^\circ$. □

In trying to prove $\mathrm{PC}(m)$ by induction we are led to a related question.

9.6 The Shift Conjecture SC(m). If $(\sigma, \tau) \in \mathcal{P}_m^\circ$ then $(\sigma, \tau) \approx (\sigma', \tau')$ where σ' and τ' represent a common value.

Of course σ' and τ' represent a common value if and only if the form $\beta' = \sigma' \perp -\tau'$ is isotropic. If $\mathrm{SC}(m')$ is true for every $m' \leq m$ then $\mathrm{PC}(m)$ follows. Here is a more formal statement of this idea.

9.7 Lemma. *If* $\mathrm{SC}(m)$ *and* $\mathrm{PC}(m-1)$ *are true over* F *then* $\mathrm{PC}(m)$ *is also true over* F.

Proof. Suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an $(m+1, m+1)$-family where $\dim q = 2^m$. Then (7.3) implies $(\sigma, \tau) \in \mathcal{P}_m^\circ$. By $\mathrm{SC}(m)$ we may alter σ, τ to assume $\sigma \simeq \sigma' \perp \langle a\rangle$ and $\tau \simeq \tau' \perp \langle a\rangle$. The Eigenspace Lemma 2.10 implies that $q \simeq q' \otimes \langle\langle a\rangle\rangle$ and $(\sigma', \tau') < \mathrm{Sim}(q')$. By $\mathrm{PC}(m-1)$ this q' is similar to a Pfister form and therefore so is q. □

If $\mathrm{SC}(m)$ is true over F for all m then the Pfister Factor Conjecture holds over F. In nearly every case where $\mathrm{PC}(m)$ has been proved for a field F, the condition $\mathrm{SC}(m)$ can be proved as well.

Before discussing small cases of this conjecture we note that: if F satisfies $\mathrm{SC}(m)$ for all m then $I^3F = J_3(F)$, which is a major part of Merkurjev's Theorem. Therefore it seems unlikely that an easy proof of the Shift Conjecture will arise.

9.8 Proposition. *Suppose* $\mathrm{SC}(m')$ *is true over* F *for all* $m' \leq m$. *If* $\beta \in J_3(F)$ *and* $\dim\beta = 2m+2$ *then* $\beta \in I^3F$.

Proof. Write $\beta = \sigma \perp -\tau$ for some forms σ, τ of dimension $m+1$. Then $(\sigma, \tau) \in \mathcal{P}_m^\circ$ and application of $\mathrm{SC}(m')$ for $m' = m, m-1, m-2, \dots$ implies that $(\sigma, \tau) \approx (\delta, \delta)$ for some form δ. By the proof of (9.5), $\beta = \sigma - \tau \equiv \delta - \delta \equiv 0 \pmod{I^3F}$. □

9.9 Proposition. $\mathrm{SC}(m)$ *is true for* $m \leq 4$.

Proof. Let $(\sigma, \tau) \in \mathcal{P}_m^\circ$. If $m \leq 2$ the equal invariants imply that $\sigma \simeq \tau$ (see Exercise 3.5). If $m = 3$ then $(\sigma, \tau) \approx (\varphi, 0)$ where $\varphi \simeq \sigma \perp (d\tau)\tau$. Then $\dim \varphi = 8$ and $\varphi \in J_3(F)$ so that φ is similar to a Pfister form by (3.21). If $\varphi \simeq \langle a\rangle\langle\langle x, y, z\rangle\rangle$ then $(\varphi, 0) \approx (\delta, \delta)$ where $\delta \simeq \langle a\rangle\langle 1, x, y, z\rangle$. Now suppose $m = 4$. Then $\beta = \sigma \perp -\tau \in J_3(F)$ and $\dim \beta = 10$. This β must be isotropic by Pfister's Theorem (3.21), and σ and τ represent a common value. □

It seems difficult to know whether a general pair (σ, τ) can be shifted to some better (σ', τ'). In some cases knowledge of certain types of subforms yields the result.

9.10 Lemma. *Suppose (σ, τ) is an (s, t)-pair. Then $(\sigma, \tau) \approx (\sigma', \tau')$ for some σ' and τ' which represent a common value, provided there exist subforms $\varphi \subset \sigma$ and $\psi \subset \tau$ such that $\varphi \neq 0, \sigma$; $\dim \varphi \equiv \dim \psi \pmod 4$ and $\det \varphi = \det \psi$.*

For example, this definition holds if $s > 2$ and σ and τ contain 2-dimensional subforms of equal determinant. The condition also holds if $s > 4$ and σ contains a 4-dimensional subform of determinant $\langle 1\rangle$.

Proof. Express $\sigma = \sigma_1 \perp \varphi$ and $\tau = \tau_1 \perp \psi$. Since $\varphi \neq 0, \sigma$, we may express $\sigma_1 = \langle x\rangle \perp \sigma_2$ and $\varphi = \langle a\rangle \perp \varphi_1$. Use (2.6) to shift $\langle x\rangle \perp \varphi_1$ and ψ. Since $\det(\langle x\rangle \perp \varphi_1))(\det \psi) = \langle ax\rangle$ we obtain $(\sigma', \tau') = (\sigma_2 \perp \langle a\rangle \perp \langle ax\rangle\psi, \tau_1 \perp \langle ax\rangle(\langle x\rangle \perp \varphi_1))$. Both σ' and τ' represent a. □

9.11 Proposition. SC(5) *is true.*

Proof. Suppose $(\sigma, \tau) \in \mathcal{P}_5^\circ$. We may shift (σ, τ) to a (10, 2)-pair (σ_0, τ_0). Then $\beta = \sigma_0 \perp -\tau_0$ is a 12-dimensional element of $J_3(F)$. If β is isotropic then σ_0 and τ_0 represent a common value and we are done. Assume β is anisotropic and write $\tau_0 \simeq \langle -a\rangle\langle 1, -b\rangle$, for some $a, b \in F^\bullet$. Then $\beta \simeq \langle a\rangle\langle\langle -b\rangle\rangle \perp \sigma_0$. Pfister's Theorem 3.21 implies that $\beta \simeq \varphi_1 \perp \varphi_2 \perp \varphi_3$, where $\langle a\rangle\langle\langle -b\rangle\rangle \subset \varphi_1$ and each φ_i is 4-dimensional of determinant $\langle 1\rangle$. Then $\varphi_2 \subset \sigma$ and (9.10) applies. □

We have been unable to prove SC(6) over an arbitrary field because we lack information about 14-dimensional forms in I^3F. Rost (1994) proved that any such form β is a transfer of the pure part of some 3-fold Pfister form over a quadratic extension of F. Hoffmann and Tignol (1998) deduced from this that β must contain an Albert subform. (Recall that an Albert form is a 6-dimensional form in I^2F.) This information leads to a possible approach to SC(6).

9.12 Lemma. *If the following hypothesis holds true over F, then* SC(6) *is true over F. Hypothesis: Whenever β is an anisotropic* 14*-dimensional form in I^3F and $\gamma \subset \beta$ is a given* 3*-dimensional subform, then there exists an Albert form α such that $\gamma \subset \alpha \subset \beta$.*

Proof. Suppose $(\sigma, \tau) \in \mathcal{P}_6^\circ$ is an (11, 3)-family. Then $\beta = \sigma \perp -\tau$ is a 14-dimensional form in $J_3(F)$. By Merkurjev's Theorem, $\beta \in I^3F$. If β is isotropic the conclusion of SC(6) is clear. If β is anisotropic the hypothesis provides an Albert form α with $-\tau \subset \alpha \subset \beta$. Expressing $\alpha = \alpha' \perp -\tau$ we have $\dim \alpha' = \dim \tau = 3$, $\alpha' \subset \sigma$ and $\det \alpha' = \det \tau$. Then (9.10) applies. □

It is not at all clear whether the strong condition in (9.12) is always true. Finding a counterexample to it would be interesting. But it might be much more interesting to construct a non-Pfister form of dimension 64 admitting a (7, 7)-family!

If the field F satisfies some nice properties, then the conjecture SC(m) is true for all m. Recall that the u-invariant $u(F)$ of a non-real field F is the maximal dimension of an anisotropic quadratic form over F.

9.13 Corollary. *If F satisfies one of the properties below then* SC(m) *is true over F for all m.*

(1) *F is nonreal and $u(F) < 14$.*

(2) *Every anisotropic form σ over F with $\dim \sigma \geq 11$ contains a 4-dimensional subform of determinant $\langle 1 \rangle$.*

Proof. We may assume $m \geq 6$ and $(\sigma, \tau) \in \mathcal{P}_m^\circ$.

(1) By hypothesis, every quadratic form over F of dimension ≥ 14 is isotropic. Since $\dim(\sigma \perp -\tau) = 2m + 2 \geq 14$, σ and τ must represent a common value.

(2) We can shift the given (σ, τ) to assume $\dim \sigma \geq 11$. The claim then follows from (9.10). □

Every algebraic number field satisfies condition (2) above. More generally, every "linked" field satisfies (2). Recall that two 2-fold Pfister forms φ and ψ are said to be linked if they can be written with a "common slot": $\varphi \simeq \langle\langle a, x \rangle\rangle$ and $\psi \simeq \langle\langle a, y \rangle\rangle$ for some $a, x, y \in F^\bullet$. The field F is said to be *linked* if every pair of 2-fold Pfister forms is linked.

9.14 Lemma. *The following conditions are equivalent for a field F.*

(1) *F is linked.*

(2) *The quaternion algebras form a subgroup of the Brauer group.*

(3) *For every form q over F, $c(q) =$ quaternion.*

(4) *Every 6-dimensional form α over F with $d\alpha = \langle 1 \rangle$ is isotropic.*

(5) *Every 5-dimensional form over F contains a 4-dimensional subform of determinant $\langle 1 \rangle$.*

We omit the details of the proof. Most of the work appears in Exercise 3.10.

The standard examples of linked fields are finite fields, local fields, global fields, fields of transcendence degree ≤ 2 over $\mathbb{C}$, fields of transcendence degree 1 over $\mathbb{R}$. Of course by (9.13) we know that $\mathrm{SC}(m)$, and hence the Pfister Factor Conjecture, is true over any linked field.

We digress for a moment to discuss the Pfister behavior of general unsplittable modules over linked fields. If (σ, τ) is an (s, t)-pair over a linked field, is every unsplittable (σ, τ)-module necessarily similar to a Pfister form? The exceptions are called "special" pairs.

9.15 Definition. A pair (σ, τ) is *special* if $s \equiv t \pmod 8$ and the form $\beta = \sigma \perp -\tau$ satisfies: $d\beta \neq \langle 1 \rangle$ and $c(\beta)$ is a quaternion algebra not split by $F(\sqrt{d\beta})$.

In the notation of Theorem 7.8 the special pairs are exactly the ones having unsplittables of dimension 2^{m+2}. We are assuming throughout that σ represents 1.

9.16 Proposition. *Suppose F is a linked field and (σ, τ) is a pair which is not special. Then every unsplittable (σ, τ)-module is similar to a Pfister form.*

Proof. Theorem 7.8 applies here since F is linked so that $c(\beta)$ must be quaternion. Let $m = \delta(s, t)$ and suppose α is an unsplittable (σ, τ)-module. If $\dim \alpha = 2^m$ then $s + t \geq 2m - 1$ and the Expansion Proposition 7.6 implies that there is an $(m + 1, m + 1)$-family in $\mathrm{Sim}(\alpha)$. Then $\mathrm{PC}(m)$ implies that α is similar to a Pfister form. Suppose $\dim \alpha = 2^{m+1}$. If $s + t \geq 2m + 1 = 2(m + 1) - 1$, we are done as before using $\mathrm{PC}(m + 1)$. The remaining cases have $s + t = 2m$ and $s \equiv t \pm 2$ or $t + 4 \pmod 8$. Dropping one dimension from σ or from τ we can find an (s', t')-pair $(\sigma', \tau') \subset (\sigma, \tau)$ where $s' + t' = 2m - 1$ and $s' \equiv t' \pm 3 \pmod 8$. Again since F is linked we may use Theorem 7.8 to get an unsplittable (σ', τ')-module ψ of dimension 2^m. Then $\mathrm{PC}(m - 1)$ implies ψ is similar to a Pfister form. Furthermore (σ', τ') is a minimal pair and (7.18) implies that ψ is the unique (σ', τ')-unsplittable. Therefore $\alpha \simeq \psi \otimes \langle a, b \rangle$ for some $a, b \in F^\bullet$ and α is also similar to a Pfister form. The last case when $\dim \alpha = 2^{m+2}$ occurs only when (σ, τ) is special. □

The special pairs really do behave differently. Using (5.11) we gave examples of special $(2, 2)$-pairs over the rational field $\mathbb{Q}$ which have 8-dimensional unsplittable modules which are not similar to Pfister forms.

The Pfister Factor Conjecture can be reformulated purely in terms of algebras with involution. (Compare (6.12).) This version is interesting but seems harder to work with than the original conjecture.

9.17 Conjecture. In the category of F-algebras with involution, suppose $(A, K) \cong (Q_1, J_1) \otimes \cdots \otimes (Q_m, J_m)$ where each (Q_k, J_k) is a quaternion algebra with involution. If the algebra A is split, then there is a decomposition

$$(A, K) \cong (Q'_1, J'_1) \otimes \cdots \otimes (Q'_1, J'_m)$$

where each (Q_1', J_k') is a split quaternion algebra with involution.

Claim. (9.17) *is equivalent to* PC(m).

Proof. Assume (9.17) and suppose $(\sigma, \tau) \in \mathcal{P}_m^\circ$ with associated Clifford algebra C. By hypothesis, $C \cong C_0 \times C_0$ and $C_0 \cong \mathrm{End}(V)$ for a space V of dimension 2^m. Since $s \equiv t \pmod 8$ the involution $J = J_S$ on C induces an involution J_0 of type 1 on C_0 as in (7.4). This provides the involution I_q on $\mathrm{End}(V)$ corresponding to a quadratic form q on V. The conjecture PC(m) says exactly that this q must be a Pfister form. The algebra C_0 can be decomposed as a tensor product of quaternion subalgebras, each preserved by the involution J_0 (compare Exercise 3.14). Therefore we may apply (9.17) to conclude that (C_0, J_0) is a product of split quaternion algebras with involution, (Q_1', J_k'). Expressing $Q_k' \cong \mathrm{End}(U_k)$ where $\dim U_k = 2$, the involution J_k' induces a λ_k-form B_k on U_k. It follows that $V \cong U_1 \otimes \cdots \otimes U_m$ and $q \simeq B_1 \otimes \cdots \otimes B_m$. If all the types λ_k are 1 then q is a product of binary quadratic forms, so it is similar to a Pfister form. Otherwise some skew forms occur in the product (necessarily an even number of them) and q is hyperbolic, so again it is Pfister.

Conversely, assume PC(m) and let (A, K) be a split algebra with a decomposition as in (9.17). Then $A \cong \mathrm{End}(V)$ where $\dim V = 2^m$ and the involution K induces a regular λ-form B on V.

Claim. It suffices to decompose $(V, B) \simeq \bigotimes(U_j, B_j)$ for some λ_j-spaces with $\dim U_j = 2$. For if such a factorization exists we can use (6.10) to see that $(A, K) \cong \bigotimes(\mathrm{End}(U_j), I_{B_j})$ as required.

Since A is a product of quaternions we may reverse the procedure in (3.14) to view A as some Clifford algebra: $A \cong C(W, q)$. Since K preserves each quaternion algebra it also preserves the generating space W. Then K is an (s, t)-involution on $C(W, q)$, for some (s, t) where $s + t = 2m + 1$. The isomorphism $(A, K) \cong (\mathrm{End}(V), I_B)$ then provides an (s, t)-family in $\mathrm{Sim}(V, B)$. If $\lambda = 1$, PC(m) implies that (V, B) is similar to a Pfister form, so it has a decomposition into binary forms, as in the claim. If $\lambda = -1$, then $(V, B) \simeq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes 2^{m-1}\langle 1 \rangle$ (compare Exercise 1.7) and again a (V, B) is a product of binary forms. □

A direct proof of the Conjecture 9.17 does not seem obvious even for the cases $m \leq 3$.

One tiny bit of evidence for the truth of PC(m) is the observation that if $\dim q = 2^m$ and there is an $(m + 1, m + 1)$-family in $\mathrm{Sim}(q)$, then $q \otimes q$ is a Pfister form. This follows from Exercise 7.14 (3). Of course this condition is far weaker that saying that q itself is a Pfister form.

Appendix to Chapter 9. Pfister forms and function fields

In this appendix we discuss, without proofs, the notion of the function field $F(q)$ of a quadratic form q over F. That theory yields another proof of PC(m) for $m \leq 5$. These "transcendental methods" in quadratic form theory were clarified in the Generic Splitting papers of Knebusch (1976, 1977a). Expositions of this theory appear in Lam's lectures (1977), in Scharlau's text (1985) and in the booklet by Knebusch and Scharlau (1980).

As usual, all quadratic forms considered here are regular and F is a field of characteristic not 2. If q is a form over F and K is an extension field of F we write q_K for $q \otimes K$. We use the notation $q \sim 0$ to mean that q is hyperbolic. (This " $\sim$" stands for Witt equivalence.)

A quadratic form φ of dimension n over F can be considered from two viewpoints. It can be viewed geometrically as an inner product space (V, φ) or it can be viewed algebraically as a polynomial $\varphi(X) = \varphi(x_1, \dots, x_n)$ homogeneous of degree 2 in n variables. Over the field $F(X)$ of rational functions it is clear that the form $\varphi \otimes F(X)$ represents the value $\varphi(X)$. For example the form $\langle a, b\rangle$ represents the value $ax_1^2 + bx_2^2$ over $F(x_1, x_2)$. Furthermore if $\varphi \subset q$ (i.e. φ is isometric to a subform of q) then $q \otimes F(X)$ represents the value $\varphi(X)$.

A.1 Subform Theorem. *Let φ, q be quadratic forms over F such that q is anisotropic. The following statements are equivalent.*

(1) $\varphi \subset q$.

(2) *For every field extension K of F, $D_K(\varphi_K) \subseteq D_K(q_K)$.*

(3) *$q \otimes F(X)$ represents $\varphi(X)$, where $X = (x_1, \dots, x_n)$ is a system of $n = \dim \varphi$ indeterminates.*

This theorem, due to Cassels and Pfister, has many corollaries. Among them is the following characterization of Pfister forms as the forms which are "generically multiplicative".

A.2 Corollary. *Let φ be an anisotropic form over F with $\dim \varphi = n$. Let X, Y be systems of n indeterminates. The following statements are equivalent.*

(1) *φ is a Pfister form.*

(2) *For every field extension K of F, $D_K(\varphi_K)$ is a group.*

(3) *$\varphi \otimes F(X, Y)$ represents the value $\varphi(X) \cdot \varphi(Y)$.*

(4) $\varphi(X) \in G_{F(X)}(\varphi_{F(X)})$.

Suppose φ is a quadratic form of dimension n over F and X is a system of n indeterminates. If $n \geq 2$ and $\varphi \not\simeq \mathbb{H}$ then $\varphi(X)$ is an irreducible polynomial and we define the *function field*

$$F(\varphi) = \text{the field of fractions of } F[X]/(\varphi(X)).$$

Certainly φ becomes isotropic over $F(\varphi)$, for if $\xi_i \in F(\varphi)$ is the image of x_i, then $\varphi(\xi_1, \dots, \xi_n) = 0$. In fact $F(\varphi)$ is a "generic zero field" for φ in the sense of Knebusch (1976). Changing the variables in φ or multiplying φ by a non-zero scalar alters the function field $F(\varphi)$ only by an isomorphism.

If $\varphi \simeq \langle 1 \rangle \perp \psi$ then $\varphi(X) = x_1^2 + \psi(X')$ where $X' = (x_2, \dots, x_n)$ and we calculate that

$$F(\varphi) \cong F(X')(\sqrt{\psi(X')}).$$

For example if $\varphi \simeq \langle 1, a \rangle$ then $F(\varphi) \cong F(x)(\sqrt{-a})$, a purely transcendental extension of $F(\sqrt{-a})$. If φ is isotropic then $F(\varphi)$ is a purely transcendental extension of F. (See Exercise 12.) To simplify later statements let us define $F(\mathbb{H}) = F(x)$, where x is an indeterminate.

Using results about quadratic forms over valuation rings Knebusch proved the following result about norms of similarities.

A.3 Norm Theorem. *Let φ, q be quadratic forms over F such that φ represents* 1 *and* $\dim \varphi = m \geq 2$. *Let X be a system of m indeterminates. The following are equivalent.*

(1) $q \otimes F(\varphi) \sim 0$.

(2) $\varphi(X) \in G_{F(X)}(q_{F(X)})$.

The condition (2) here is equivalent to the existence of a "rational composition formula"

$$\varphi(X) \cdot q(Y) = q(Z)$$

where $X = (x_1, \dots, x_m)$ and $Y = (y_1, \dots, y_n)$ are systems of independent indeterminates and each entry z_k of Z is a linear form in Y with coefficients in $F(X)$. If each z_k is actually bilinear in X, Y then we have $\varphi < \operatorname{Sim}(q)$, as in (1.9) (3).

A.4 Corollary. *Let φ be an anisotropic form which represents* 1 *and* $\dim \varphi \geq 2$ *over F. Then φ is a Pfister form if and only if $\varphi \otimes F(\varphi) \sim 0$.*

Proof. If φ is a Pfister form then since $\varphi \otimes F(\varphi)$ is isotropic it must be hyperbolic by (5.2) (2). The converse follows from (A.3) and (A.2). □

A.5 Corollary. *Suppose q is an anisotropic form and $q \otimes F(\varphi) \sim 0$. Then φ is similar to a subform of q. In particular* $\dim \varphi \leq \dim q$.

Proof. Let $b \in D_F(\varphi)$ so that $\langle b \rangle \varphi$ represents 1. The Norm Theorem then implies that $b \cdot \varphi(X) \in G_{F(X)}(q_{F(X)})$. For any $a \in D_F(q)$ it follows that $q_{F(X)}$ represents $ab \cdot \varphi(X)$ and the Subform Theorem implies that $\langle ab \rangle \varphi \subset q$. □

A.6 Corollary. *Let φ be a Pfister form and q and anisotropic form over F. Then $q \otimes F(\varphi) \sim 0$ if and only if $\varphi \mid q$.*

Proof. If $\varphi \mid q$ apply (A.4). Conversely suppose $q \otimes F(\varphi) \sim 0$. Then (A.5) implies $q \simeq \langle a_1 \rangle \varphi \perp q_1$ for some $a_1 \in F^\bullet$ and some form q_1. But then $q_1 \otimes F(\varphi) \sim 0$, since φ is a Pfister form, and we may proceed by induction. □

This corollary is a direct generalization of Lemma 3.20(2) since if $\varphi = \langle\langle b \rangle\rangle$ then $F(\varphi)$ is a purely transcendental extension of $F(\sqrt{-b})$. Now let us apply these results to our questions about spaces of similarities.

A.7 Lemma. *If $\sigma < \mathrm{Sim}(q)$ where $\dim \sigma \geq 2$ then $q \otimes F(\sigma) \sim 0$.*

Proof. For any field extension K of F, $\sigma_K < \mathrm{Sim}(q_K)$. Since $\sigma \otimes F(\sigma)$ is isotropic the claim follows from (1.4). Here is another proof: We may assume σ represents 1. Let X be a system of $s = \dim \sigma$ indeterminates. Since $\sigma_{F(X)}$ represents $\sigma(X)$ and $\sigma_{F(X)} < \mathrm{Sim}(q_{F(X)})$ we conclude that $\sigma(X) \in G_{F(X)}(q_{F(X)})$. The Norm Theorem applies. □

The anisotropic cases of (1.10) follow as corollaries. For example, suppose $\langle 1, a, b \rangle < \mathrm{Sim}(q)$ where q is anisotropic. Let $\varphi = \langle\langle a, b \rangle\rangle$ and note that $\langle 1, a, b \rangle \otimes F(\varphi)$ is isotropic. Then the argument in (A.7) implies that $q \otimes F(\varphi) \sim 0$ and (A.6) implies that $\varphi \mid q$.

By the Expansion Proposition 7.6 the following statement of the conjecture is equivalent to "PC(m) over all fields":

Pfister Factor Conjecture. If $\sigma < \mathrm{Sim}(q)$ where $\dim q = 2^m$ and $\dim \sigma = \rho(2^m)$ then q is similar to a Pfister form.

A.8 Lemma. *The following statement is equivalent to the Pfister Factor Conjecture. Suppose $\sigma < \mathrm{Sim}(q)$ where $\dim q = 2^m$ and $\dim \sigma = \rho(2^m)$. If q is isotropic then q is hyperbolic.*

Proof. If q is similar to a Pfister form and is isotropic then it is hyperbolic by (5.2). Conversely suppose the statement here is true and $\sigma < \mathrm{Sim}(q)$ over F where $\dim q = 2^m$ and $\dim \sigma = \rho(2^m)$. Then $\sigma \otimes F(q) < \mathrm{Sim}(q \otimes F(q))$ and the assumed statement implies that $q \otimes F(q)$ is hyperbolic. By (A.4) it follows that q is similar to a Pfister form. □

In trying to prove this conjecture we suppose that $\sigma < \mathrm{Sim}(q)$ as above. Assuming that q is isotropic but not hyperbolic we try to derive a contradiction. Express $q = q_a \perp k\mathbb{H}$ where q_a is anisotropic and non-zero. Then $q_a \otimes F(\sigma) \sim 0$ by (A.7) and therefore $\dim q_a \geq \dim \sigma = \rho(2^m)$, by (A.5). If $m \leq 3$ this already provides a contradiction since $\rho(2^m) = 2^m = \dim q$ in those cases. The case $m = 4$ is settled by the next lemma which we could have proved after (1.4).

A.9 Lemma. *Suppose $S \subseteq \mathrm{Sim}(V, q)$ is a (regular) subspace where* $\dim S = s$. *Suppose q is isotropic but not hyperbolic and $v \in V$ is an isotropic vector. Then $S \cdot v$ is a totally isotropic subspace of V of dimension s.*

Proof. If $f \in S$ then $q(f \cdot v) = \mu(f)q(v) = 0$. Therefore $S \cdot v$ is totally isotropic. Suppose f is in the kernel of the evaluation map $\varepsilon : S \to S \cdot v$. Then $f(v) = 0$ so that f is not injective and it follows that $\mu(f) = 0$. However (1.4) implies that S is anisotropic and consequently $f = 0$. Therefore ε is a bijection. □

Now suppose $m = 4$, so that $\dim q = 16$ and $\dim \sigma = 9$. The lemma implies that q has a totally isotropic subspace of dimension 9 which is certainly impossible since $9\mathbb{H}$ cannot fit inside q. If $m = 5$ then $\dim q = 32$ and $\dim \sigma = 10$ and the lemma shows that $10\mathbb{H} \subset q$. Therefore $10 \le \dim q_a \le 12$, since the earlier argument implies that $\dim q_a \ge \dim \sigma = 10$. The next idea is to observe that these inequalities hold over any extension field K such that $q \otimes K$ is not hyperbolic.

A.10 Proposition. *Suppose q is a form of even dimension which is not hyperbolic over F. Then there exists an extension field K such that $q \otimes K \simeq \psi \perp k\mathbb{H}$ and ψ is similar to an anisotropic (non-zero) Pfister form.*

Proof. Suppose $q \simeq q_0 \perp i_0\mathbb{H}$ where q_0 is anisotropic. Let $F_1 = F(q_0)$ be the function field so that $q_0 \otimes F_1 \simeq q_1 \perp i_1\mathbb{H}$ for some anisotropic form q_1 and some $i_1 \ge 1$. If $q_1 \ne 0$ let $F_2 = F_1(q_1)$ and express $q_1 \otimes F_2 \simeq q_2 \perp i_2\mathbb{H}$ for some anisotropic form q_2 and some $i_2 \ge 1$. Repeat this process to get a tower of fields $F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_h$ where $q \otimes F_h \sim 0$ but $q \otimes F_{h-1} \not\sim 0$. Let $K = F_{h-1}$ and express $q \otimes K \simeq \psi \perp k\mathbb{H}$ where $\psi = q_{h-1}$ is anisotropic. By construction $\psi \ne 0$ and $\psi \otimes K(\psi) \sim 0$. Therefore ψ is similar to a Pfister form by (A.4). □

A.11 Proposition. *The Pfister Factor Conjecture is true if $m \le 5$.*

Proof. We already settled the cases $m \le 4$ and showed that if $m = 5$ then $10 \le \dim q_a \le 12$. Replacing F by the field K of (A.10) we get the extra information that $\dim q_a$ is a power of 2. This contradiction completes the proof. □

Exercises for Chapter 9

1. ***u*-invariants.** For a nonreal field F, $u(F)$ is defined to be the maximal dimension of an anisotropic quadratic form over F.

(1) Suppose $u = u(F(\sqrt{a}))$ is finite. Then every anisotropic form σ over F with $\dim \sigma \ge u + 3$ contains a 4-dimensional subform of determinant $\langle 1 \rangle$.

(2) If $u(F(\sqrt{a})) \le 8$ then for every m, SC(m) is true over F. For example this condition holds if F is an extension of $\mathbb{R}$ of transcendence degree ≤ 3.

(Hint. (1) Use Lemma 3.20.
(2) The theory of C_i-fields shows that if $K/\mathbb{C}$ has transcendence degree ≤ 3 then $u(K) \le 8$. See e.g. §2.15 of Scharlau (1985).)

2. If every form over F of dimension 12 contains a 4-dimensional subform of determinant $\langle 1\rangle$, then PC(m) is true for all m.

(Hint. If $m = 6$ suppose $(\sigma, \tau) < \mathrm{Sim}(q)$ is an (11, 3)-family where $\dim q = 64$. Find a related (12, 0)-family and apply (9.11) and (2.10) to find that $q \simeq \langle\langle a\rangle\rangle \otimes q'$ where $\dim q' = 32$ and q' admits a (7, 3)-family. From $\rho_3(32) = 7$ use (7.12) to find a (6, 6)-family in $\mathrm{Sim}(q')$.)

3. (1) Suppose (σ, τ) is a pair such that $\dim \sigma \ge 8$ and σ contains an Albert subform. Then $(\sigma, \tau) \approx (\sigma', \tau')$ where τ' is isotropic. Consequently, if $(\sigma, \tau) < \mathrm{Sim}(q)$ then q must be hyperbolic. Compare Exercise 6.4 (4).
(2) Extend the definition of the equivalence $\approx$ to include cases as mentioned in Exercise 2.4 (1). Will this change the validity of results in Chapter 9?

(Hint. (1) Scale to assume $\sigma \simeq \langle a, b, ab\rangle \perp \langle -x, -y, -xy\rangle \perp \langle u, v, \ldots\rangle$. Shift twice.)

4. Let $F((t))$ be the field of formal Laurent series over F. Then PC(m) over $F((t))$ implies PC(m) and PC$(m-1)$ over F.

(Hint. Use Springer's Theorem about quadratic forms over valued fields.) Compare Exercise 10.

5. Suppose q is a form of dimension 2^m over F and there is an $(m+1, m+1)$-family in $\mathrm{Sim}(q)$. Then $q \in I^3F$. What are the possible values of the signature $\mathrm{sgn}_P(q)$ when P is an ordering of F?

6. **PC(6).** Suppose $\sigma < \mathrm{Sim}(V, q)$ over F where $\dim \sigma = 11$ and $\dim q = 2^6 = 64$. As usual, let $C = C(-\sigma_1)$ and $A = \mathrm{End}_C(V)$, so that $C \otimes A \cong \mathrm{End}(V)$. Then A is a quaternion algebra with induced involution "bar". If there is a quadratic extension L/F such that $\sigma \otimes L$ is isotropic and $c(\sigma) = [A]$ is split by L, then q must be similar to a Pfister form?

7. **Pfister unsplittables.** Suppose (C, J) is the Clifford algebra with involution associated to an (s, t)-pair (σ, τ) where $s + t = 2m + 1$. Then $(C, J) \cong (Q_1, J_1) \otimes \cdots \otimes (Q_m, J_m)$ where each (Q_k, J_k) is a quaternion algebra with involution as in Exercise 6.4. Suppose $Q_k \cong (a_k, b_k)$ corresponding to generators e_k, f_k where $J(e_k) = \pm e_k$ and $J(f_k) = \pm f_k$.

(1) Suppose all a_k belong to a two element set $\{1, d\}$. Then every (σ, τ)-unsplittable is similar to a Pfister form.

(2) For what (s, t)-pairs does the condition in (1) apply? We can use Exercise 3.14 to get explicit quaternion algebras in C. For example (1) applies when $\sigma = \langle 1 \rangle \perp \langle\langle -c \rangle\rangle \otimes \alpha$ and $\tau = 0$. It also applies when $(\sigma, \tau) = (\langle 1 \rangle \perp \alpha, \langle 1 \rangle \perp \alpha)$.

(Hint. (1) Note that $(d, u) \otimes (d, v) \cong (1, u) \otimes (d, uv)$ and the involution preserves the factors. Then $(C, J) \cong (C', J') \otimes (Q, J'')$ where Q is quaternion and $C' \cong \mathrm{End}(U)$ is a tensor product of split quaternions. Suppose (V, q) is unsplittable for (C, J) and apply (6.11) to find that $(V, q) \simeq (U, \varphi) \otimes (W, \omega)$, where (W, ω) is an unsplittable (Q, J'')-module. Show that φ and ω are Pfister.)

8. **Definition.** $I^n F$ is *linked* if every pair φ, ψ of n-fold Pfister forms is linked. That is, $\varphi \simeq \langle\langle a \rangle\rangle \otimes \alpha$ and $\psi \simeq \langle\langle b \rangle\rangle \otimes \alpha$ for some $(n-1)$-fold Pfister form α. The linked fields mentioned above are the ones where $I^2 F$ is linked.

Proposition. *If $I^3 F$ is linked then for every m,* SC(m) *is true over F.*

(Hint. If $I^n F$ is linked then every anisotropic $q \in I^n F$ has a "simple decomposition": $q \simeq \varphi_1 \perp \cdots \perp \varphi_k$ where each φ_j is similar to an n-fold Pfister form. (See Elman, Lam and Wadsworth (1979), Corollary 3.6.) Given $(\sigma, \tau) \in \mathcal{P}_m^\circ$ let $\beta = \sigma \perp -\tau$. By Merkurjev's Theorem $\beta \in I^3 F$. We may assume β is anisotropic. A simple decomposition implies $t \equiv 0 \pmod 4$. Shift to assume $\tau = 0$, use the decomposition and (9.10).)

9. **Adjusting signatures.** If P is an ordering of F then $\mathrm{sgn}_P(\sigma)$ denotes the signature of the form σ relative to P.

(1) Suppose P is an ordering of F. If $(\sigma, \tau) \in \mathcal{P}_m^\circ$ then

$$\mathrm{sgn}_P(\sigma) \equiv \mathrm{sgn}_P(\tau) \pmod 8.$$

(2) **Signature Shift Conjecture.** If $(\sigma, \tau) \in \mathcal{P}_m^\circ$ then $(\sigma, \tau) \approx (\sigma', \tau')$ for some pair (σ', τ') where $\dim \sigma' = \dim \tau'$ and $\mathrm{sgn}_P(\sigma') = \mathrm{sgn}_P(\tau')$ for all orderings P.

Definition. F has the property ED if for every $b \in F^\bullet$ and every form q over F such that $q \perp \langle -b \rangle$ is totally indefinite, q represents bt for some totally positive $t \in F^\bullet$.

Lemma. *If the field F satisfies ED then the Signature Shift Conjecture holds. This applies, for example, if F is an algebraic extension of a uniquely ordered field.*

Remark. It might be possible to find a counterexample to SC(m) by finding a field for which the Signature Shift Conjecture fails.

(Hint. (1) If $\beta \in I^3\mathbb{R}$ then $\dim \beta \equiv 0 \pmod 8$.

(2) Mimic the idea in (9.10).)

10. **Laurent series fields.** Let F be a complete discrete valued field with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m} = \pi\mathcal{O}$, and non-dyadic residue field $k = \mathcal{O}/\mathfrak{m}$ (i.e. char $k \neq 2$).

A quadratic form q over F has "good reduction" if there exists an orthogonal basis $\{e_1, \dots, e_n\}$ such that $q(e_i) \in \mathcal{O}^\bullet$. In this case let $L = \mathcal{O}e_1 + \cdots + \mathcal{O}e_n$, a free $\mathcal{O}$-module. There is a corresponding "reduced" form $\bar{q}$ over k obtained from $L/\mathfrak{m}L$. By Springer's Theorem the isometry class of $\bar{q}$ is independent of the choice of basis and $\bar{q}$ is isotropic iff q is isotropic. Any quadratic form q over F can be expressed as $q = q_1 \perp \langle\pi\rangle q_2$ where q_1 and q_2 have good reduction. These reduced forms $\bar{q}_1$ and $\bar{q}_2$ are uniquely determined up to Witt equivalence. (For more details see the texts of Lam or Scharlau.)

(1) **Lemma.** *Suppose (V, q) is anisotropic with good reduction, and $L \subseteq V$ as above. If $f \in \mathrm{Sim}(V, q)$ with norm $\mu(f) \in \mathcal{O}$ then $f(L) \subseteq L$.*

(2) **Corollary.** *Suppose q, σ, τ are anisotropic forms with good reduction over F. If $(\sigma, \tau) < \mathrm{Sim}(q)$ over F then $(\bar{\sigma}, \bar{\tau}) < \mathrm{Sim}(\bar{q})$ over k.*

(3) Suppose $F = k((t))$ is a Laurent series field. If (V, q) is a quadratic space over F then $(V, q) = (V_1, q_1) \perp (V_2, \langle t\rangle q_2)$ where q_1, q_2 are forms with good reduction. If q is anisotropic then the subspaces V_i are uniquely determined. E.g. $V_1 = \{v \in V : q(v) \in k\}$.

(4) **Corollary.** *Suppose σ, τ, q_1, q_2 are anisotropic forms over k. If $(\sigma, \tau) < \mathrm{Sim}(q_1 \perp \langle t\rangle q_2)$ over $k((t))$ then $(\sigma, \tau) < \mathrm{Sim}(q_1)$ and $(\sigma, \tau) < \mathrm{Sim}(q_2)$ over k.*

(5) **Corollary.** *Suppose σ, τ, q are anisotropic forms over k. Then $(\sigma \perp \langle t\rangle, \tau \perp \langle t\rangle) < \mathrm{Sim}(q \otimes \langle\langle t\rangle\rangle)$ over $k((t))$ iff $(\sigma, \tau) < \mathrm{Sim}(q)$ over k.*

(Hint. (1) Suppose $v \in L$ and let r be the smallest non-negative integer with $\pi^r \cdot f(v) \in L$. If $r > 0$ then $q(\pi^r \cdot f(v)) \in \mathfrak{m}$ and the anisotropy implies $\pi^r \cdot f(v) \in \mathfrak{m}L = \pi L$, contrary to the minimality.)

11. **History.** (1) The following result of Cassels (1964) was a major motivation for Pfister's theory: $1 + x_1^2 + \cdots + x_n^2$ is not expressible as a sum of n squares in $\mathbb{R}(x_1, \dots, x_n)$.

(2) The level $s(F)$ was defined in Exercise 5.5. Given m there exists a field of level 2^m. In fact let $X = (x_1, \dots, x_n)$ be a system of indeterminates, let $d = x_1^2 + \cdots + x_n^2$ and define $K_n = \mathbb{R}(X)(\sqrt{-d})$. If $2^m \le n < 2^{m+1}$ Pfister proved: $s(K_n) = 2^m$.

(3) The function field methods in quadratic form theory began with the "Hauptsatz" of Arason and Pfister:

Theorem. *If q is a non-zero anisotropic form in $I^n F$ then* $\dim q \ge 2^n$.

(Hint. (1) Use $q = n\langle 1\rangle$ and $\varphi(x) = x_0^2 + \cdots + x_n^2$ over $\mathbb{R}(x_0, \dots, x_n)$ in the Subform Theorem (A.1).

(2) Apply Exercise 5.5. Alternatively, K_n is equivalent to the function field $\mathbb{R}((n+1)\langle 1\rangle)$. Certainly $s(K_n) \le n$ hence $s(K_n) \le 2^m$. If not equal then $2^m\langle 1\rangle$ is isotropic, hence hyperbolic, over K_n. Get a contradiction using (A.5).

(3) Given $q \sim \langle c_1\rangle\varphi_1 \perp \cdots \perp \langle c_k\rangle\varphi_k$ where each φ_j is an n-fold Pfister form. Suppose $k > 1$ and assume the result for any such sum of fewer than k terms (over any field). If $q \otimes F(\varphi_1) \sim 0$ apply (A.5). Otherwise apply the induction hypothesis to the anisotropic part of $q \otimes F(\varphi_1)$.)

12. (1) Suppose $K = F(x_1, \dots, x_n)$ is a purely transcendental extension of F and q is a form over F. If $q \otimes K$ is isotropic then q must be isotropic over F.

(2) Let φ be a form over F with $\dim \varphi \geq 2$. Then $F(\varphi)/F$ is purely transcendental if and only if φ is isotropic.

(Hint. (2) Suppose φ is isotropic with $\dim \varphi > 2$. Changing variables we may assume that $\varphi(X) = x_1 x_2 + \alpha$ where $\alpha = \alpha(X')$ is a non-zero quadratic form in $X' = (x_3, \dots, x_n)$.)

13. **More versions of PC(m).** The following statements are equivalent to PC(m) (over all fields):

(1) If $\dim \varphi = 2^m$, φ represents 1, and there is an $(m+1, m+1)$-family in $\text{Sim}(V, \varphi)$, then φ is round. That is: for every $c \in D_F(\varphi)$ there exists $f \in \text{Sim}^\bullet(\varphi)$ with $\mu(f) = c$.

(2) Suppose (A, K) is a tensor product of m quaternion algebras with involution, as in (9.17). Suppose A is split and there exists $0 \neq h \in A$ with $J(h) \cdot h = 0$. Then for every $c \in F$ there exists $f \in A$ such that $J(f) \cdot f = c$.

(Hint. (1) Use (A.2).

(2) Let $A \cong \text{End}(V)$ where $\dim V = 2^m$ with J corresponding to I_φ, for a quadratic form φ on V. Equivalently $\text{Sim}(V, \varphi)$ admits an $(m+1, m+1)$-family. The condition $I_\varphi(h) \cdot h = 0$ implies φ is isotropic. The conclusion says that φ is round.)

14. **Pfister neighbors.** (1) If φ is a hyperbolic form and $\alpha \subset \varphi$ with $\dim \alpha > \frac{1}{2} \dim \varphi$ then α must be isotropic.

(2) A form α is called a *Pfister neighbor* if there is a Pfister form ρ such that $\alpha \subset \langle a \rangle \rho$ for some $a \in F^\bullet$ and $\dim \alpha > \frac{1}{2} \dim \rho$. In this case: α is isotropic iff ρ is hyperbolic. Every form of dimension ≤ 3 is a Pfister neighbor.

(3) If α is a Pfister neighbor then the associated Pfister form is unique.

(4) Suppose α is Pfister neighbor associated to ρ. If $\alpha < \text{Sim}(q)$ and q is anisotropic then $\rho \mid q$. In fact, if $\alpha < \text{Sim}(q)$ and $q \simeq q_0 \perp m\mathbb{H}$ where q_0 is anisotropic, then $\rho \mid q_0$.

(Hint. (1) Viewed geometrically, the space (V, φ) of dimension $2m$ has a totally isotropic subspace S with $\dim S = m$. The subspace (A, α) has $\dim A > m$. Then $A \cap S \neq \{0\}$.

(3) If α is associated to ρ and to ψ then $\psi \otimes F(\rho)$ is isotropic, hence hyperbolic.)

15. **More on Pfister neighbors.** If φ is an m-fold Pfister form and $\langle 1, a, b \rangle \subset \varphi$ then $\varphi \cong \langle\langle a, b, c_3, \dots, c_m \rangle\rangle$ for some $c_j \in F^\bullet$. (Compare (5.2) (3) and Exercise 5.23.) More generally:

Proposition. *Suppose φ is a Pfister form and α is a Pfister neighbor with associated Pfister form ρ. If $\alpha \subset \varphi$ then $\varphi \cong \rho \otimes \delta$ for some Pfister form δ.*

(Hint. Assume φ is anisotropic. Exercise 14 (1) and (A.6) imply that $\rho \mid \varphi$. Then $\varphi \cong \rho \perp \gamma$ for some form γ. If $\dim \gamma > 0$ choose $c \in D_F(\gamma)$ and let $\rho_1 := \rho \otimes \langle\langle c \rangle\rangle$.

Since $\rho \perp \langle c\rangle$ is a subform of φ and is a Pfister neighbor associated to ρ_1 we have $\rho_1 \mid \varphi$. Iterate the argument.)

16. If there is a counterexample to the Pfister Factor Conjecture when $m = 6$, then there exists a field F and $\sigma < \mathrm{Sim}(q)$ where $\dim \sigma = 12$, $\dim q = 64$ and $q \simeq \psi \perp k\mathbb{H}$ where ψ is an anisotropic Pfister form of dimension 16 or 32.

Notes on Chapter 9

Several of the ideas used in the proof of SC(m) for $m \le 5$ are due to Wadsworth. In particular he had the idea of examining 4-dimensional subforms of determinant $\langle 1\rangle$. The approach to the Pfister Factor Conjecture given in the appendix follows Wadsworth and Shapiro (1977a).

The property SC(m) was proved in (9.13) for certain classes of fields. However there exist fields not satisfying any of these properties. For example there is a field F and a quadratic form β such that $\beta \in I^3F$, $\dim \beta = 14$ and β contains no 4-dimensional subform of determinant $\langle 1\rangle$. If fact, if k is a field and $F = k((t_1))((t_2))((t_3))$ is the iterated Laurent series field then there are examples of such β over F. This is proved in Hoffmann and Tignol (1998), where the stated property is called D(14).

The class of linked fields as defined in Lemma 9.14 was first examined by Elman and Lam (1973b). Some of their proofs were simplified by Elman (1977), Elman, Lam and Wadsworth (1979) and Gentile (1985).

(A.10) is due to Knebusch (1976). The Pfister form ψ there is called the "leading form" of q. For further information see Knebusch and Scharlau (1980) or Scharlau (1985), p. 163–165.

Exercise 7. See Yuzvinsky (1985).

Exercise 9. This property ED (for "effective diagonalization") was introduced by Ware and studied by Prestel and Ware (1979).

Exercise 10 follows a communication from A. Wadsworth (1976).

Exercise 14–15. For Pfister neighbors see Knebusch (1977a) or Knebusch and Scharlau (1980).

Chapter 10

Central Simple Algebras and an Expansion Theorem

Our previous expansion result (7.6) followed from an explicit analysis of the possible involutions on a quaternion algebra. The Expansion Theorem in this chapter depends on similar information about involutions on a central simple algebra of degree 4. Albert (1932) proved that any such algebra A is a tensor product of two quaternion algebras. However there can exist involutions J on A which do not arise from quaternion subalgebras. It is the analysis of these "indecomposable involutions" which provides the necessary information for the Expansion Theorem. The principal ingredient is Rowen's observation that a symplectic involution on a central simple algebra of degree 4 must be decomposable.

The chapter begins with a discussion of maximal (s, t)-families and a characterization of those dimensions for which expansions are always possible. The Expansion Theorem requires knowledge of involutions on algebras of degree 4. We derive the needed results from a general theory of Pfaffians. This theory is first described for matrix rings, then lifted to central simple algebras, and finally specialized to algebras of degree 4. The exposition would be considerably shortened if we restrict attention to the degree 4 case from the start. (Most of the results needed here appear in Knus et al. (1998), Ch. IV.) Our long digression about general Pfaffians is included here since it is a novel approach and it helps clarify some of the difficulties of generalizing the theory to larger algebras.

Suppose $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family. If $\dim V = 2^m$ and $s+t = 2m-1$ the Expansion Proposition (7.6) says that (S, T) can be enlarged to some family of maximal size. We will sharpen this result by showing families of certain smaller sizes can also be enlarged. For example let us consider the case $\dim q = 16$. If $S \subseteq \mathrm{Sim}(V, q)$ where $\dim S = 5$ then there exists T such that $(S, T) \subseteq \mathrm{Sim}(V, q)$ is a $(5, 5)$-family. On the other hand there exist quadratic forms q with $\dim q = 16$ such that $\mathrm{Sim}(q)$ has $(3, 3)$-families but admits no (s, t)-families of larger size. See Exercise 1.

The Expansion Lemma (2.5) provides examples of maximal families. For instance if $S_0 \subseteq \mathrm{Sim}(V, q)$ is a 3-dimensional subspace with orthogonal basis $\{1_V, f, g\}$ then it can be expanded by adjoining fg. The expanded space $S = \mathrm{span}\{1_V, f, g, fg\}$ is maximal family because no non-zero map can anticommute with f, g and fg.

If $\mu(f) = a$ and $\mu(g) = b$ the quadratic form on S is $\sigma = \langle 1, a, b, ab\rangle$ and the associated Clifford algebra is $C = C(-\sigma_1) = C(\langle -a, -b, -ab\rangle)$. If $\{e_1, e_2, e_3\}$ is the set of generators of C then $z = e_1e_2e_3$ is the element of highest degree, generating the center of C. If $\pi : C \to \mathrm{End}(V)$ is the representation corresponding to S we see that $\pi(z) = (f)(g)(fg) = -ab\cdot 1_V$, a scalar. Then π is not faithful (i.e. not injective). This sort of behavior always occurs when a family arises from the Expansion Lemma. More generally recall the properties of the character $\chi(S, T)$ defined in (7.17). The next lemma is a repetition of (7.18).

10.1 Lemma. *Suppose $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family with forms (σ, τ). If $\chi(S, T) \neq 0$ then $s \equiv t \pmod 4$, $d\sigma = d\tau$ and (S, T) is maximal.*

We call this sort of family “trivially maximal”. If $s + t$ is odd then no (s, t)-family can be maximal since we can always expand by one dimension to get a non-faithful (maximal) family. To avoid this sort of triviality we will investigate when (S, T) can be expanded by 2 (or more) dimensions.

We have already considered some expansion results. For example Proposition 7.6 states that if $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family such that $\dim q = 2^m$ and $s + t = 2m - 1$, then (S, T) can be expanded by 3 dimensions. As another example, recall that $\langle 1, a\rangle < \mathrm{Sim}(q)$ if and only if $(\langle 1, a\rangle, \langle 1, a\rangle) < \mathrm{Sim}(q)$, and similarly for $\langle 1, a, b\rangle < \mathrm{Sim}(q)$. These results are be generalized in the next proposition, which is a mild refinement of (7.12).

10.2 Proposition. *Let (σ, τ) be a minimal pair with unsplittable (σ, τ)-modules of dimension 2^m. Suppose $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family with forms (σ, τ). Then there is an associated (s', t')-family in $\mathrm{Sim}(V, q)$ with $s' + t' = 2m + 2$.*

Proof. If (S, T) is trivially maximal, this associated family cannot be an actual expansion of (S, T). Let $C = C(-\sigma_1 \perp \tau)$ with the usual involution J, and let (W, ψ) be an unsplittable (C, J)-module. If C does not act faithfully on W, we replace (S, T) by a smaller family obtained by deleting one dimension. This smaller family is still minimal. By (7.11) we know that every unsplittable module is (C, J)-similar to (W, ψ). The Decomposition Theorem 4.1 then yields a (C, J) isometry $(V, q) \simeq (W, \psi) \otimes_F \langle a_1, \dots, a_r\rangle$ for some $a_i \in F^\bullet$. Now the Expansion Proposition 7.6 can be applied to (W, ψ) to produce the larger family as desired. □

Suppose $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family with $s + t$ odd. Let (σ, τ) be the corresponding forms and $C = C(-\sigma_1 \perp \tau)$ the associated Clifford algebra. Then C is a central simple F-algebra of dimension 2^{s+t-1} and the given representation $\pi : C \to \mathrm{End}(V)$ induces an isomorphism

$$C \otimes A \cong \mathrm{End}(V)$$

where $A = \mathrm{End}_C(V)$ is the centralizer of C in $\mathrm{End}(V)$. Then A is also a central simple F-algebra and since the involution J on C and I_q on $\mathrm{End}(V)$ are compatible, there is an induced involution K on A.

10.3 Lemma. *(S, T) can be expanded by 2 dimensions if and only if there is a quaternion subalgebra $Q \subseteq A$ which is preserved by the involution K.*

Proof. Such Q exists if and only if there exist $a, b \in A$ such that a^2 and b^2 are in $F^\bullet$, a, b anticommute, $K(a) = \pm a$ and $K(b) = \pm b$. Let z be an element of highest degree in C so that z anticommutes with $S_1 + T$, $z^2 \in F^\bullet$ and $J(z) = \pm z$. Let $f = za$ and $g = zb$. Then Q exists if and only if there exist $f, g \in \mathrm{End}(V)$ which anticommute with $S_1 + T$, f^2 and g^2 are in $F^\bullet$, $I_q(f) = \pm f$ and $I_q(g) = \pm g$. This occurs if and only if (S, T) can be expanded by 2 dimensions. □

Of course this lemma is just a slight generalization of the Expansion Proposition 7.6. In order to go further we need information about quaternion subalgebras of larger algebras with involution. Recall that if A is a central simple F-algebra then $\dim_F A = n^2$ is a perfect square (since over some splitting field E, $A \otimes E \cong \mathbb{M}_n(E)$ for some n). Define the *degree* of the algebra A to be this integer n. Then a quaternion algebra has degree 2.

The basic examples of central simple F-algebras with involution are tensor products of split algebras and quaternion algebras. For instance if $A \cong Q_1 \otimes Q_2$ where Q_1 and Q_2 are quaternion algebras, then A is a central simple algebra of degree 4. Certainly this A has an involution, since we can use $J = J_1 \otimes J_2$ where J_i is an involution on Q_i. We consider the converse.

10.4 Definition. Let A be a central simple F-algebra. Then A is *decomposable* if

$$A \cong A_1 \otimes A_2$$

for some central simple F-algebras A_i with $\deg A_i > 1$.

If J is an involution on A then (A, J) is *decomposable* if $(A, J) \cong (A_1, J_1) \otimes (A_2, J_2)$ for some central simple F-algebras A_i with involutions J_i and with $\deg A_i > 1$. When the algebra A is understood we say that the involution J is decomposable.

Note that J is decomposable if and only if there exists a proper J-invariant central simple subalgebra A_1 of A. For A_2 can be recovered as the centralizer of A_1.

Every algebra of prime degree is certainly indecomposable. In particular, quaternion algebras are indecomposable. If $A \cong \mathrm{End}(V)$ is split and J is any involution of symplectic type on A then J is decomposable if and only if $\deg A > 2$. Similarly if $J = I_q$ is the adjoint involution of a quadratic form q on V and if $q \simeq \alpha \otimes \beta$ for some quadratic forms α, β of dimension > 1, then J is decomposable. (See (6.10).)

Let us now concentrate on algebras of degree 4. Albert (1932) proved that if A has degree 4 and possesses an involution then A is decomposable as a tensor product of quaternion subalgebras. Rowen (1978) used Pfaffians to prove that symplectic involutions on a division algebra of degree 4 are always decomposable. The next theorem is a refinement of these results.

10.5 Theorem. *Let A be a central simple F-algebra of degree* 4 *with involution. Then $A \simeq Q_1 \otimes Q_2$ for some quaternion algebras Q_i.*

(1) *If J is an involution on A of symplectic type then J is decomposable. Furthermore if $y \in A - F$ such that $y^2 \in F^\bullet$ and $J(y) = \pm y$, then there exists a J-invariant quaternion subalgebra Q with $y \in Q$.*

(2) *Suppose J is an involution on A of orthogonal type. Then J is decomposable if and only if there exists $y \in A$ such that $y^2 \in F^\bullet$ and $J(y) = -y$. Furthermore if such y is given, then there exists a J-invariant quaternion subalgebra Q with $y \in Q$.*

Certainly there exist indecomposable involutions on split algebras of degree 4, provided F is not quadratically closed. (Just use I_q on $\text{End}(V)$ where $(V, q) \simeq \langle 1, 1, 1, c\rangle$ for some non-square $c \in F$.) Indecomposable involutions on division algebras of degree 4 were first exhibited by Amitsur, Rowen, Tignol (1979). These examples were clarified by work of Knus, Parimala, Sridharan on the "discriminant" of an involution. We present an exposition of the theory of Pfaffians, the characterization of indecomposable involutions on algebras of degree 4, and a proof of Theorem 10.5.

Before beginning those tasks, we mention an easy lemma and then apply that theorem to deduce another expansion result for (s, t)-families.

10.6 Lemma. *Suppose A is a central simple F-algebra of degree* 4 *with involution J. Then (A, J) is decomposable if and only if $(A, J) \cong (C(U, \alpha), J')$ for some* 4*-dimensional quadratic space (U, α) and some involution J' which preserves U.*

Proof. Suppose A is a product of two invariant quaternion algebras. Choose generators which are J-invariant (i.e. $J(x) = \pm x$). Alter the two quaternion algebras to a Clifford algebra as in (3.14), and note that the Clifford generators are still J-invariant. □

Suppose $(S, T) \subseteq \text{Sim}(V, q)$ is an (s, t)-family where $\dim q = 2^m$ and $s + t = 2m - 3$. Then $\dim C = 2^{2m-4}$ and the centralizer A will be central simple of degree 4. If the induced involution K on A has symplectic type then (10.3) and (10.5) imply that (S, T) can be expanded to a family of maximal size. This is the situation mentioned at the start, when $S \subseteq \text{Sim}(q)$ where $\dim q = 16$ and $\dim S = 5$.

For exactly which dimensions s, t and 2^m are we guaranteed that a family will expand to one of maximal size? One necessary condition is easily verified: if $s = \rho_t(2^{m-2})$ then there exists some (s, t)-family on 2^m-space (over some field) which cannot be expanded by 2 dimensions.

In fact we can construct one over the real field $\mathbb{R}$. For such s, t, m there is a family $(s\langle 1\rangle, t\langle 1\rangle) < \mathrm{Sim}(2^{m-2}\langle 1\rangle)$. Therefore $(s\langle 1\rangle, t\langle 1\rangle) < \mathrm{Sim}(q)$ where $q = 2^{m-2}\langle 1, 1, 1, -1\rangle$. Then $\dim q = 2^m$ but q is not a Pfister form. Then $\mathrm{Sim}(q)$ admits no family of maximal size because $\mathrm{PC}(m)$ holds over $\mathbb{R}$. We prove that this necessary condition is also sufficient.

10.7 Expansion Theorem. *Suppose $(S, T) \subseteq \mathrm{Sim}(V, q)$ is an (s, t)-family and $\dim q = 2^m$. If $s > \rho_t(2^{m-2})$ then there is an associated (s', t')-family $(S', T') \subseteq \mathrm{Sim}(V, q)$ where $s' + t' = 2m + 2$.*

Here the family (S', T') might not be an expansion of (S, T), since (S, T) could be trivially maximal. For such cases $s + t$ is even and the representation is not faithful. Then we first pass to a subfamily of (S, T) of codimension 1 and expand that to the family (S', T').

Note. That inequality is equivalent to:

$$s + t \geq \begin{cases} 2m - 3 & \text{if } m \equiv t \\ 2m - 1 & \text{if } m \equiv t + 1 \\ 2m - 2 & \text{if } m \equiv t + 2 \\ 2m - 3 & \text{if } m \equiv t + 3 \end{cases} \pmod 4.$$

Of course this condition is related to the condition for minimal pairs given in (7.9). In this situation an unsplittable (σ, τ)-module must have dimension 2^{m-1} or 2^m. In the former case we find that (σ, τ) is a minimal pair and the unsplittable module $(S, T) \subseteq \mathrm{Sim}(W, \varphi)$ is unique by (7.11). Since (V, q) is a sum of unsplittable components, it follows that $(S, T) \subseteq \mathrm{Sim}(V, q)$ expands uniquely to a family of maximal size. Therefore the new content of the theorem occurs when unsplittables have dimension 2^m.

Proof. If $s + t = 2m - 1$ then (7.6) implies that the family always expands by 3 dimensions. Suppose $s + t = 2m - 3$ and $m \equiv t$ or $t + 3 \pmod 4$. Then $C \otimes A \cong \mathrm{End}(V)$ with involutions $J \otimes K \cong I_q$, where (A, K) is an algebra of degree 4 with involution. Since $s = 2m - 3 - t \equiv t \pm 3 \pmod 8$ we see from (7.4) that the involution J on C has type -1. Then (6.9) implies that K has type -1 on A. Now (10.5) and (10.6) imply that

$$(A, K) \cong (C(U, \alpha), J')$$

where $\dim U = 4$ and J' preserves U. Then there exists an orthogonal basis $h_1, \ldots, h_4$ of U such that $J'(h_i) = \pm h_i$. Then the elements zh_i, along with $zh_1h_2h_3h_4$, can be adjoined to (S, T) to provide a family of maximal size $(s' + t' = 2m + 2)$.

Finally suppose that $s + t = 2m - 2$ and $m \equiv t + 2 \pmod 4$. Then $s \equiv t + 2 \pmod 8$, the involution K has type 1 and $J(z) = -z$. Then the representation $\pi : C \to \mathrm{End}(V)$ cannot send z to a scalar, and therefore π must be faithful. We may identify C with its image $\pi(C) \subseteq \mathrm{End}(V)$. Since C_0 is central simple of dimension 2^{2m-4} its centralizer

A is central simple of degree 4 and

$$C_0 \otimes A \cong \mathrm{End}(V).$$

Since the involutions J and I_q are compatible, I_q restricts to an involution K on A. Since z commutes with C_0 we find that $z \in A$ and $K(z) = J(z) = -z$. By Theorem 10.5(2) the involution K is decomposable, so that $(A, K) \cong (C(U, \alpha), J')$ as above. Furthermore in this isomorphism the element z corresponds to an element of U. We choose an orthogonal basis $\{z, h_1, h_2, h_3\}$ of U with $I_q(h_i) = \pm h_i$ and expand the family (S, T) by adjoining $\{h_1, h_2, h_3, zh_1h_2h_3\}$. □

There is a fine point to be made here about "maximal" families. Suppose $s+t$ is odd and an (s, t)-family $(S, T) \subseteq \mathrm{Sim}(V, q)$ is given. Let the corresponding forms be σ, τ and suppose that there exists $(\sigma, \tau) \subset (\sigma', \tau') < \mathrm{Sim}(q)$ where $s' + t' = s + t + 2$. It does not necessarily follow that the original family (S, T) can be expanded by 2 dimensions. The explanation is that a given (s, t)-pair (σ, τ) can have different realizations as an (s, t)-family in $\mathrm{Sim}(q)$. (See Exercise 2(2).)

We now begin our analysis of Pfaffians and central simple algebras, ultimately leading to a proof of Theorem 10.5. Few of the results here are new, but the properties of the set $\mathcal{D}(A)$ provide an interesting approach. As usual in this book we assume that F is a field of *characteristic not* 2. This restriction simplifies the exposition. The results have analogs in characteristic 2 and there exist treatments of the subject which unify both cases.

If A is an F-algebra (always assumed finite dimensional, associative and with 1) then $A^\bullet$ denotes the group of invertible elements in A. If $\mathcal{S} \subseteq A$ is a subset we write $\mathcal{S}^\bullet$ for the set $\mathcal{S} \cap A^\bullet$.

10.8 Classical Definition. Let S be a skew-symmetric $n \times n$ matrix over F such that n is even. Then the *Pfaffian* $\mathrm{Pf}(S) \in F$ is defined with the following properties:

(1) $\mathrm{Pf}(S)$ is a form (homogeneous polynomial) of degree $n/2$ in the entries of S. In particular $\mathrm{Pf}(cS) = c^{n/2}\,\mathrm{Pf}(S)$ for any $c \in F$.

(2) $\mathrm{Pf}(S)^2 = \det S$.

(3) $\mathrm{Pf}(P^\top \cdot S \cdot P) = \mathrm{Pf}(S) \cdot \det P$.

(4) $\mathrm{Pf}(S_n) = 1$ where $S_n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, with $n/2$ summands.

There are several proofs that $\mathrm{Pf}(S)$ is well defined. One way is to use the theory of alternating spaces to show that if S is skew-symmetric then $S = P^\top \cdot S_n \cdot P$ for some P. Then $\det S = (\det P)^2$. We could define $\mathrm{Pf}(S) = \det P$ and then prove that this value is independent of the choice of P (using the lemma: $Q \in \mathrm{Sp}_n$ implies $\det Q = 1$).

Alternatively we could use a "generic" skew-symmetric S over $\mathbb{Z}[s_{ij}]$, argue as above that $\det S$ is a square in $\mathbb{Q}(s_{ij})$. Then it is also a square in $\mathbb{Z}[s_{ij}]$. Choose a square root, $\mathrm{Pf}(S)$, for this generic case, with the sign chosen so that the specialization to S_n yields the value 1.

Another method avoids alternating spaces, using induction to prove directly that the generic S has a square determinant (see Jacobson (1968)). One can also define Pfaffians using exterior algebras and multilinear algebra. For example see Chevalley (1954) or (1955), Bourbaki (1959), §5, n$^{\mathrm{o}}$ 2.

Remark. There exists a “Pfaffian adjoint” $\mathrm{Pfadj}(S)$ which is a $n \times n$ skew- symmetric matrix satisfying

$$S \cdot \mathrm{Pfadj}(S) = \mathrm{Pfadj}(S) \cdot S = \mathrm{Pf}(S) \cdot I_n$$

The entries of $\mathrm{Pfadj}(S)$ are forms of degree $n/2 - 1$ in the entries of S. Consequently there exists a “Pfaffian expansion by minors” as well. The existence of Pfadj can be proved using the generic Pfaffian. Each cofactor S_{ij} in the matrix S must be a multiple of the (irreducible) polynomial $\mathrm{Pf}(S)$. Cancel $\mathrm{Pf}(S)$ from the equation $S \cdot \mathrm{adj}(S) = (\det S) \cdot I_n$ to obtain $\mathrm{Pfadj}(S)$. This approach appears in Jacobson (1968).

10.9 Corollary. (1) *If A, B are skew symmetric then*

$$\mathrm{Pf}\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = (\mathrm{Pf}\, A) \cdot (\mathrm{Pf}\, B).$$

(2) *If S is invertible and skew-symmetric $n \times n$ then* $\mathrm{Pf}(S^{-1}) = (-1)^{n/2}(\mathrm{Pf}\, S)^{-1}$.
(3) *For any $m \times m$ matrix C and an $m \times m$ skew-symmetric matrix S,*

$$\mathrm{Pf}\begin{pmatrix} S & C \\ -C^{\top} & 0 \end{pmatrix} = (-1)^{\frac{m(m-1)}{2}} \cdot \det C.$$

These properties are easy to derive from the definition. In particular, $\mathrm{Pf}\begin{pmatrix} 0 & 1_m \\ -1_m & 0 \end{pmatrix} = (-1)^{\frac{m(m-1)}{2}}$. In the 4×4 case let

$$S = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ & 0 & a_{23} & a_{24} \\ & & 0 & a_{34} \\ & & & 0 \end{pmatrix}$$

where we omit writing the lower half. Then

$$\mathrm{Pfadj}(S) = \begin{pmatrix} 0 & -a_{34} & a_{24} & -a_{23} \\ & 0 & -a_{14} & a_{13} \\ & & 0 & -a_{12} \\ & & & 0 \end{pmatrix},$$

and $\mathrm{Pf}(S) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$.

It is convenient to introduce a new notation for the eigenspaces of an involution J. If J has type λ on $\mathrm{End}(V)$ define

$$\begin{aligned}\mathrm{Sym}(J) &= \{f \in \mathrm{End}(V) : J(f) = \lambda f\},\\ \mathrm{Alt}(J) &= \{f \in \mathrm{End}(V) : J(f) = -\lambda f\}.\end{aligned}$$

Then for any J, if $\dim V = n$ then $\dim \mathrm{Alt}(J) = \frac{n(n-1)}{2}$. The classical Pfaffian map on matrices is defined on $\mathrm{Alt}(^\top)$. Note also that $\mathrm{Alt}(J) = \mathrm{image}(1 - \lambda J) = \{g - \lambda J(g) : g \in \mathrm{End}(V)\}$.

When J has symplectic type, there is a natural notion of "Pfaffian" for elements of $\mathrm{Alt}(J)$, defined independently of the matrix Pfaffian mentioned above. If $f \in \mathrm{Alt}(J)$ then $J(f) = f$ so the matrix B of f satisfies: $M^{-1} \cdot B^\top \cdot M = B$. Then the matrix $T = MB$ is skew-symmetric. Such a matrix B can also be characterized by: $B = ST$ for some skew-symmetric matrices S, T such that S is nonsingular. It quickly follows that the characteristic polynomial $\chi_f(x)$ is the square of another polynomial. (For $\chi_f(x) = \det(x1 - B) = \det M^{-1} \cdot \det(xM - T)$. Since M^{-1} and $xM - T$ are skew-symmetric over the field $F(x)$, $\chi_f(x)$ is a square in $F(x)$ and hence is a square in $F[x]$.) With a little more work we get a stronger result.

10.10 Lemma. *For f as above, every elementary divisor of f has even multiplicity.*

Proof of Theorem A.7. Here the elementary divisors are the polynomials which appear as the characteristic polynomials of blocks in the Rational Canonical Form for f. (Each of them is a power of an irreducible polynomial.) First assume that F contains all the eigenvalues of f. If λ is an eigenvalue the elementary divisors $(x - \lambda)^m$ are determined by the numbers $d_j = \dim\ker(\lambda 1 - f)^j$ for $j = 1, 2, \ldots$ Since MB is skew symmetric and hence has even rank we know that rank $f = \mathrm{rank}(MB) =$ even. Similarly since $(\lambda 1 - f)^j \in \mathrm{Alt}(J)$ we conclude that $d_j = n - \mathrm{rank}(\lambda 1 - f)^j =$ even. It follows that $(x - \lambda)^m$ occurs with even multiplicity.

In general if K/F is a field extension, the elementary divisors of $f \otimes K$ over K determine the elementary divisors of f over F. Passing to a field K containing all the eigenvalues of f the result follows. □

Proof #2, following Kaplansky (1983). We are given $B = M^{-1}T$ where M, T are skew-symmetric and M is invertible. Then $xI - B = M^{-1}(xM - T)$. The matrix $xM - T$ is skew-symmetric over the principal ideal domain $F[x]$. Applying the theory of alternating spaces over $F[x]$, (e.g. see Kaplansky (1949), p. 475 or Bourbaki (1959), §5, n$^\text{o}$ 1) there exists some invertible matrix R over $F[x]$ such that

$$R \cdot (aM - T) \cdot R^\top = \begin{pmatrix} 0 & p_1 \\ -p_1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & p_2 \\ -p_2 & 0 \end{pmatrix} \oplus \cdots$$

where $p_i \in F[x]$ and each p_i divides p_{i+1}. Absorbing the factor M^{-1} and applying some elementary column operations, we find that there exist invertible matrices P, Q over $F[x]$ such that $P \cdot (xI - B) \cdot Q = \mathrm{diag}(p_1, p_1, p_2, p_2, \ldots)$. Therefore the invariant factors of B are $p_1, p_1, p_2, p_2, \dots$ This shows that the invariant factors, and hence the elementary divisors, of B have even multiplicities. □

Proof #3. There is a more geometric proof due to Tignol (1991). Suppose (V, b) is a (regular) alternating space over F and $f \in \mathrm{End}(V)$ is self-adjoint (i.e. $I_b(f) = f$). Then there exists a decomposition $V = U \oplus U'$ such that U and U' are totally isotropic and f-invariant. The action of f on U' is dual to the action of f on U so that there exists a basis for which the matrix of f is $\begin{pmatrix} C & 0 \\ 0 & C^\top \end{pmatrix}$. The proof uses the "primary decomposition" of V relative to f but does not employ more complicated linear algebra. □

For a ring A and $a, b \in A$ define the relation $a \sim b$ to mean that $b = pap^{-1}$ for some $p \in A^\bullet$. If $A \cong \mathbb{M}_n(F)$ then $a \sim b$ if and only if a and b are "similar" matrices, or equivalently, they have exactly the same elementary divisors.

10.11 Proposition. *For $f \in \mathrm{End}(V)$ with $n \times n$ matrix B over F, the following are equivalent:*

(1) *$J(f) = f$ for some symplectic involution J on $\mathrm{End}(V)$.*

(2) *$B = ST$ for some skew-symmetric S, T such that S is nonsingular.*

(2′) *$B = S'T'$ for some skew-symmetric S', T' such that T' is nonsingular.*

(3) *All elementary divisors of f have even multiplicity.*

(4) *n is even and $B \sim \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$ for some $n/2 \times n/2$ matrix C.*

Proof. (1) $\Longleftrightarrow$ (2) is clear using $S = M^{-1}$. For (2) $\Longleftrightarrow$ (2′) note that $ST = (STS) \cdot S^{-1}$. The implication (1) $\Longrightarrow$ (3) is done in Lemma 10.10. (3) $\Longrightarrow$ (4) is standard linear algebra. (4) $\Longrightarrow$ (2): Since $C \sim C^\top$ we find that $B \sim \begin{pmatrix} C & 0 \\ 0 & C^\top \end{pmatrix} = ST$ where $S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -C^\top \\ C & 0 \end{pmatrix}$. Then there is an invertible matrix P such that $B = P \cdot ST \cdot P^{-1} = (PSP^\top) \cdot (P^{-\top}TP^{-1})$, verifying statement (2). □

We define $\mathcal{D} = \mathcal{D}(\mathrm{End}(V))$ to be the set of all $f \in \mathrm{End}(V)$ satisfying these equivalent conditions. When we consider $\mathbb{M}_n(F)$ rather than $\mathrm{End}(V)$, we write $\mathcal{D}_n$. Here are some basic properties of this set $\mathcal{D}$:

$\mathcal{D}$ is closed under polynomials. ($p \in F[x]$ and $f \in \mathcal{D}$ imply $p(f) \in \mathcal{D}$.)
$\mathcal{D}$ is closed under inverses. ($f \in \mathcal{D}^\bullet$ implies $f^{-1} \in \mathcal{D}$.)
$\mathcal{D}$ is closed under conjugation. ($f \in \mathcal{D}$ and $g \in \mathrm{GL}(V)$ imply $gfg^{-1} \in \mathcal{D}$.)
Let J be any involution on $\mathrm{End}(V)$.

If $f, g \in \mathrm{Alt}(J)$ and f or g is invertible, then $fg \in \mathcal{D}$.

If J has symplectic type then $\mathrm{Alt}(J) \subseteq \mathcal{D}$, a linear subspace of dimension $n(n-1)/2$.

We can now define Pfaffians on $\mathcal{D}$ by using that matrix C.

10.12 Definitions. Suppose $f \in \mathcal{D}(\mathrm{End}(V))$ where $n = \dim V$. Choose a basis of V such that the matrix of f is $\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$, as in Proposition 10.11.

Define $\mathrm{pf}(f) = \det C$, the Pfaffian of f. Define

$$\mathrm{pf}\,\chi_f(x) = \chi_C(x) = \det(xI_{n/2} - C),$$

the Pfaffian characteristic polynomial.

Define $\pi(f) \in \mathcal{D}(\mathrm{End}(V))$ to be the map with matrix $\begin{pmatrix} \mathrm{adj}\, C & 0 \\ 0 & \mathrm{adj}\, C \end{pmatrix}$.

Here we have used a lower case "p" to distinguish this Pfaffian from the previous "matrix Pfaffian" $\mathrm{Pf}(S)$. Of course we must verify that these definitions do not depend on the choice of the basis. Suppose f has matrix $\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$ with respect to one basis of V and has matrix $\begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$ with respect to another basis. Then C and D have the same elementary divisors, so that $C \sim D$. Consequently $\mathrm{pf}(f)$ and $\mathrm{pf}\,\chi_f(x)$ are well defined. One way to prove that this adjoint map is well defined is to recall the following fact about the classical adjoint:

Let $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ be the characteristic polynomial of C (and of D). If $p^*(x) = (-1)^{m-1} \cdot \frac{p(x)-p(0)}{x} = (-1)^{m-1}(x^{m-1} + a_{m-1}x^{m-2} + \cdots + a_1)$, then $\mathrm{adj}\, C = p^*(C)$. (See Exercise 7.) Since $\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix} = Q \cdot \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} \cdot Q^{-1}$ for some matrix Q, we find that $Q \cdot \begin{pmatrix} \mathrm{adj}\, D & 0 \\ 0 & \mathrm{adj}\, D \end{pmatrix} \cdot Q^{-1} = Q \cdot p^* \left\{ \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} \right\} \cdot Q^{-1} = p^* \left\{ \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix} \right\} = \begin{pmatrix} \mathrm{adj}\, C & 0 \\ 0 & \mathrm{adj}\, C \end{pmatrix}$. Therefore $\pi(f)$ is well defined (and $\pi(f) = p^*(f)$).

10.13 Lemma. *Suppose $n = \dim V$ is even and let $\mathcal{D} = \mathcal{D}(\mathrm{End}(V))$.*

(1) $\mathrm{pf} : \mathcal{D} \to F$ *is a polynomial map of degree* $n/2$. *If* $f \in \mathcal{D} = \mathcal{D}(\mathrm{End}(V))$ *then:*
$\mathrm{pf}(f)^2 = \det f$.
$\mathrm{pf}(g^{-1}fg) = \mathrm{pf}(f)$ *for any* $g \in \mathrm{GL}(V)$.
$\mathrm{pf}(f^k) = \mathrm{pf}(f)^k$. *In particular,* $\mathrm{pf}(1_V) = 1$ *and if* $f \in \mathcal{D}^\bullet$ *then* $\mathrm{pf}(f^{-1}) = \mathrm{pf}(f)^{-1}$.
If $f \in \mathcal{D}(\mathrm{End}(V))$ *and* $g \in \mathcal{D}(\mathrm{End}(W))$ *then* $\mathrm{pf}(f \oplus g) = \mathrm{pf}(f) \cdot \mathrm{pf}(g)$.

(2) $\mathrm{pf}\,\chi_f(x)$ *is a monic polynomial of degree* $n/2$ *and* $\mathrm{pf}\,\chi_f(f) = 0$.

(3) $\pi : \mathcal{D} \to \mathcal{D}$ *is a polynomial map of degree* $n/2$, *satisfying*

$$f \cdot \pi(f) = \pi(f) \cdot f = \mathrm{pf}(f) \cdot 1_V$$
$$\pi(g \cdot f \cdot g^{-1}) = g \cdot \pi(f) \cdot g^{-1}$$
$$\pi(\pi(f)) = \mathrm{pf}(f)^{\frac{n}{2}-2} \cdot f \text{ and } \mathrm{pf}(\pi(f)) = \mathrm{pf}(f)^{\frac{n}{2}-2}.$$

Proof. (1) Clear from the definitions.

(2) Apply the Cayley–Hamilton Theorem.

(3) Use standard properties of the classical adjoint $\mathrm{adj}\,C$. The second statement follows from the fact that $\mathrm{adj}\,f$ is well defined, independent of the basis chosen. For the final equations recall that $\mathrm{adj}(\mathrm{adj}\,C)) = (\det C)^{m-2} \cdot C$ for any $m \times m$ matrix C. (See Exercise 7.) Note that the situation needs some special interpretation when $n = 2$ and $f = 0_V$. □

This version of the Pfaffian on $\mathcal{D}$ is related to the classical version for skew-symmetric matrices.

10.14 Lemma. (1) *Suppose* M, T *are skew-symmetric* $n \times n$ *matrices and* M *is invertible. Then* $M^{-1} \cdot T \in \mathcal{D}_n$ *and* $\mathrm{pf}(M^{-1} \cdot T) = (\mathrm{Pf}\,M)^{-1} \cdot (\mathrm{Pf}\,T)$.

(2) *Suppose* $J(f) = f$ *for a symplectic involution* J. *Then for any* $g \in \mathrm{GL}(V)$, $\mathrm{pf}(J(g)fg) = \mathrm{pf}(f) \cdot \det g$.

(3) *Suppose* J *is a symplectic involution on* $\mathrm{End}(V)$. *If* $f, g \in \mathrm{Alt}(J)$ *and either* f *or* g *is invertible then* $fg \in \mathcal{D}$. *In this case*

$$\mathrm{pf}(fg) = \mathrm{pf}(f) \cdot \mathrm{pf}(g) \quad \textit{and} \quad \pi(fg) = \pi(g) \cdot \pi(f).$$

In particular if $f \in \mathcal{D}$ *then* $\pi(f^k) = \pi(f)^k$.

Proof. (1) Choose independent generic skew-symmetric $n \times n$ matrices S_0, T_0 and use determinants to see that $\mathrm{pf}(S_0T_0) = \varepsilon \cdot \mathrm{Pf}(S_0) \cdot \mathrm{Pf}(T_0)$ for some $\varepsilon = \pm 1$. This formula specializes to all $n \times n$ skew-symmetric S, T over F, with the same sign ε. Evaluate ε by computing one special case.

(2) Pick a basis and let B be the matrix of f and P the matrix of g. Represent J as $J(X) = M^{-1} \cdot X^\top \cdot M$ where M is nonsingular skew-symmetric. Then MB is skew-symmetric and $J(P)BP = M^{-1} \cdot (P^\top \cdot MB \cdot P)$ so that $\mathrm{pf}(J(P)BP) = (\mathrm{Pf}\,M)^{-1} \cdot \mathrm{Pf}(P^\top \cdot MB \cdot P) = (\mathrm{Pf}\,M)^{-1} \cdot \mathrm{Pf}(MB) \cdot \det P = \mathrm{pf}(B) \cdot \det P$.

(3) Let B, C be the matrices of f, g and M is given as in (2). Since $J(f) = f$ we know that MB and BM^{-1} are skew-symmetric. Similarly MC and CM^{-1} are skew-symmetric. Suppose f is invertible. Then $\mathrm{pf}(f) \cdot \mathrm{pf}(g) = \mathrm{pf}(B) \cdot \mathrm{pf}(C) = \mathrm{pf}(BM^{-1} \cdot M) \cdot \mathrm{pf}(M^{-1} \cdot MC) = \mathrm{Pf}(MB^{-1})^{-1} \cdot \mathrm{Pf}(M) \cdot \mathrm{Pf}(M)^{-1} \cdot \mathrm{Pf}(MC) = \mathrm{pf}((MB^{-1})^{-1} \cdot MC) = \mathrm{pf}(BC) = \mathrm{pf}(fg)$, using several applications of part (1).

From (10.13) (3) we get $\pi(fg) \cdot fg = \mathrm{pf}(fg) = \mathrm{pf}(f) \cdot \mathrm{pf}(g) = \mathrm{pf}(f) \cdot \pi(g)g = \pi(g)(\mathrm{pf}(f)1_V)g = \pi(g)\pi(f) \cdot fg$. Then if $f, g \in \mathrm{Alt}(J)^\bullet$ we have $\pi(fg) = \pi(g) \cdot$

$\pi(f)$. Now for fixed $f \in \mathrm{Alt}(J)^\bullet$ we need to verify that formula for all $g \in \mathrm{Alt}(J)$. (The case when g is invertible is similar). If $|F|$ is infinite this follows since $\mathrm{Alt}(J)^\bullet$ is Zariski dense in $\mathrm{Alt}(J)$. For the general case we use a generic argument. Let $S = (s_{ij})$ be a generic skew-symmetric matrix and set $\hat{C} = M^{-1}S$. Then the given matrix B and this $\hat{C}$ are in $\mathrm{Alt}(J)^\bullet$ over the field $F(s_{ij})$ so that $\pi(B\hat{C}) = \pi(\hat{C})\pi(B)$. This equation holds over the ring $F[s_{ij}]$ (since $\pi(\hat{C}) = \sum_{j=0}^{n} a_j \hat{C}^j$ for some $a_j \in F[s_{ij}]$, as in Exercise 10). Therefore it can be specialized to any $C \in \mathrm{Alt}(J)$. □

Suppose $n = \dim V = 4$. We will analyze $\mathcal{D} = \mathcal{D}_4 = \mathcal{D}(\mathrm{End}(V))$ in further detail. The results above show that $\mathrm{pf} : \mathcal{D} \to F$ is a quadratic form and $\pi : \mathcal{D} \to \mathcal{D}$ is a linear form. These maps have natural extensions to the whole space $\mathrm{End}(V)$. To describe these extensions we use the trace map $\mathrm{tr}(f) = \mathrm{trace}(f)$. Note that $\mathrm{tr}(1_V) = n$.

10.15 Example. Suppose $n = 4$. Define $Q : \mathrm{End}(V) \to F$ by $Q(f) = \frac{1}{8} \cdot \mathrm{tr}(f)^2 - \frac{1}{4} \cdot \mathrm{tr}(f^2)$. Define $\pi' : \mathrm{End}(V) \to \mathrm{End}(V)$ by $\pi'(f) = \frac{1}{2} \cdot \mathrm{tr}(f) \cdot 1_V - f$.

(1) Then Q is a regular quadratic form extending $\mathrm{pf} : \mathcal{D} \to F$ and π' is a linear form extending $\pi : \mathcal{D} \to \mathcal{D}$. Also $Q(f) = \frac{1}{2} \cdot \mathrm{tr}(\pi'(f) \cdot f)$ and $Q(fg) = Q(gf)$ so that $Q(s^{-1}fs) = Q(f)$. Furthermore

$$\pi'(\pi'(f)) = f \quad \text{and} \quad Q(\pi'(f)) = Q(f).$$

Any $f \in \mathrm{End}(V)$ is expressed as $f = \alpha 1_V + f_0$ where $\alpha = \frac{1}{4} \cdot \mathrm{tr}(f)$ is a scalar and $\mathrm{tr}(f_0) = 0$. Then $\pi'(f) = \alpha 1_V - f_0$.

(2) If $f \in \mathcal{D}$ then f has minimal polynomial $m_f(x)$ of degree ≤ 2. The following are equivalent for any $f \in \mathrm{End}(V)$ which is not a scalar:

$m_f(x) = x^2 - \frac{1}{2} \cdot \mathrm{tr}(f) \cdot x + \beta$ for some $\beta \in F$

$f = \alpha 1_V + f_0$ such that $\mathrm{tr}(f_0) = 0$ and $f_0^2 \in F$.

$f \cdot \pi'(f) \in F$.

These conditions imply $f \in \mathcal{D}$, except in the case $f_0^2 = 0$ and $\mathrm{rank}\, f_0 = 1$. In particular if $m_f(x)$ is irreducible of degree 2 then $f \in \mathcal{D}$.

Proof. (1) If $f \in \mathcal{D}$ then the matrix of f is $\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$ for some 2×2 matrix C. The characteristic polynomial of C is $p(x) = x^2 - (\mathrm{tr}\, C)x + (\det C)$ so that $p^*(x) = (\mathrm{tr}\, C) - x$. Then $\pi(f) = p^*(f) = \frac{1}{2}\mathrm{tr}(f) - f$. Also since $\mathrm{pf}(f)$ is a scalar we find that $\mathrm{pf}(f) = \frac{1}{4} \cdot \mathrm{tr}(\mathrm{pf}(f)1_V) = \frac{1}{4} \cdot \mathrm{tr}(\pi(f) \cdot f) = \frac{1}{4} \cdot \mathrm{tr}((\frac{1}{2} \cdot \mathrm{tr}(f) \cdot 1_V - f) \cdot f) = \frac{1}{8} \cdot \mathrm{tr}(f)^2 - \frac{1}{4} \cdot \mathrm{tr}(f^2)$. Therefore π' extends π and Q extends pf. The remaining properties are easily checked. (Compare Exercise 10.)

(2) If $m_f(x) = x^2 - \frac{1}{2} \cdot \mathrm{tr}(f) \cdot x + \beta$ then $f_0^2 = (f - \frac{1}{4}\mathrm{tr}(f))^2 \in F$. If $f_0^2 \in F$ then $f \cdot \pi'(f) = (\alpha 1_V + f_0) \cdot (\alpha 1_V - f_0) = \alpha^2 1_V - f_0^2$ is a scalar. If $f \cdot \pi'(f) \in F$ then $(f - \frac{1}{4} \cdot \mathrm{tr}(f))^2 = f_0^2$ is a scalar, so that $f^2 - \frac{1}{2} \cdot \mathrm{tr}(f) \cdot f + \beta = 0_V$ for some $\beta \in F$. Then $m_f(x) = x^2 - \frac{1}{2} \cdot \mathrm{tr}(f) \cdot x + \beta$. Suppose these condition$s$ hold but

$f \notin \mathcal{D}$. Then $m_f(x)$ must be reducible (why?) so the minimal polynomial of f_0 must be $(x - \alpha)(x + \alpha)$ for some $\alpha \in F$. If $\alpha \neq 0$ each elementary divisor must equal $x \pm \alpha$, and f_0 is similar to a diagonal matrix. But then tr $f_0 = 0$ implies $f \in \mathcal{D}$. Therefore $\alpha = 0$ and $f_0^2 = 0_V$. Since $f_0 \notin \mathcal{D}$ the elementary divisors of f_0 must be $\{x, x, x^2\}$ so that f_0 has rank 1. □

Now let us turn to the main topic of this chapter: central simple algebras. We assume the standard facts about central simple F-algebras with involution, as presented in Scharlau's book, for example. We continue to assume all involutions here are of the "first kind", unless explicitly stated otherwise.

If J is a λ-involution on the central simple F-algebra A, we define

$$\mathrm{Alt}(A, J) = \mathrm{Alt}(J) = \{a \in A : J(a) = -\lambda a\}.$$

If A is an algebra of degree n then $\dim \mathrm{Alt}(A, J) = \frac{n(n-1)}{2}$.

10.16 Proposition. *Let A be a central simple F-algebra with involution. Suppose $n = \deg A$ is even. Define*

$$\mathcal{D}(A) = \{a \in A : J(a) = a \text{ for some } (-1)\text{-involution } J \text{ on } A\}.$$

For any involution J_0 on A,

$$\mathcal{D}(A) = \{bc : b \in \mathrm{Alt}(J_0)^\bullet \text{ and } c \in \mathrm{Alt}(J_0)\} = \{a \in A : \mathrm{Alt}(J_0)^\bullet \cdot a \cap \mathrm{Alt}(J_0) \neq \emptyset\}.$$

This set $\mathcal{D}(A)$ is closed under polynomials, under inverses and under conjugation.

(1) *There is a "reduced Pfaffian" map $\mathrm{pf}_A : \mathcal{D}(A) \to F$ which is a polynomial map of degree $n/2$ satisfying*

$\mathrm{pf}_A(a)^2 = \mathrm{nrd}(a)$
$\mathrm{pf}_A(p^{-1}ap) = \mathrm{pf}_A(a)$
$\mathrm{pf}_A(a^k) = \mathrm{pf}_A(a)^k$ *(In particular,* $\mathrm{pf}_A(1) = 1$ *and* $\mathrm{pf}_A(a^{-1}) = \mathrm{pf}_A(a)^{-1}$ *if* $a \in \mathcal{D}(A)^\bullet$*.)*

If $J(a) = a$ for a (-1)-involution J and if $b \in A^\bullet$ then $\mathrm{pf}_A(J(b)ab) = \mathrm{pf}_A(a) \cdot \mathrm{nrd}(b)$.

(2) *If $a \in \mathcal{D}(A)$ define the polynomial $p_a(x) = \mathrm{pf}_{A(x)}(x1 - a) \in F[x]$. Then $p_a(x)$ is monic of degree $n/2$ and $p_a(a) = 0$.*

(3) *There is a polynomial map $\pi_A : \mathcal{D}(A) \to \mathcal{D}(A)$ of degree $n/2 - 1$ satisfying*

$a \cdot \pi_A(a) = \pi_A(a) \cdot a = \mathrm{pf}_A(a) \cdot 1$
$\pi_A(bab^{-1}) = b \cdot \pi_A(a) \cdot b^{-1}$ *for any* $b \in A^\bullet$
$\pi_A(\pi_A(a)) = \mathrm{pf}_A(a)^{\frac{n}{2}-2} \cdot a$ *and* $\mathrm{pf}_A(\pi_A(a)) = \mathrm{pf}_A(a)^{\frac{n}{2}-1}$.

If J is a (-1)-involution $a, b \in \mathrm{Alt}(J)$ and either a or b is invertible then $ab \in \mathcal{D}(A)$ and

$$\mathrm{pf}_A(ab) = \mathrm{pf}_A(a) \cdot \mathrm{pf}_A(b) \quad \text{and} \quad \pi_A(ab) = \pi_A(b) \cdot \pi_A(a).$$

Proof. The equivalence of the two descriptions of $\mathcal{D}(A)$ and the various closure properties follow as before. To define pf_A we use "descent", following the standard definition of the reduced norm, nrd. Let K be a splitting field for A and choose an algebra isomorphism $\varphi : A \otimes_F K \xrightarrow{\cong} \mathbb{M}_n(K)$. Given the (-1)-involution J on A define the involution I on $\mathbb{M}_n(K)$ by requiring it to be K-linear and $I(\varphi(a \otimes 1)) = \varphi(J(a) \otimes 1)$ for every $a \in A$. That is, the diagram

$$\begin{tikzcd}
A \otimes K \arrow[r, "\varphi"] \arrow[d, "J \otimes 1"'] & \mathbb{M}_n(K) \arrow[d, "I"] \\
A \otimes K \arrow[r, "\varphi"] & \mathbb{M}_n(K)
\end{tikzcd}$$

commutes. Then I has symplectic type on $\mathbb{M}_n(K)$ and it follows that if $a \in \mathcal{D}(A)$ then $\varphi(a \otimes 1) \in \mathcal{D}_n$. Define $\operatorname{pf}_A(a) = \operatorname{pf}(\varphi(a \otimes 1)) \in K$.

First note that this value does not depend on the choice of K (for we may pass to an algebraic closure of F and note that the matrix is unchanged). Furthermore it is independent of the choice of the isomorphism φ. (Another isomorphism ψ differs from φ by an inner automorphism: there exists $p \in \mathrm{GL}_n(K)$ such that $\psi(x) = p^{-1}\varphi(x)p$ for all $x \in A \otimes K$. Recall that $\operatorname{pf}(p^{-1}xp) = \operatorname{pf}(x)$ for matrices.) Finally suppose that K/F is a Galois extension (using the theorem that there exists a separable splitting field). The standard "descent" argument (as in Scharlau (1985), pp. 296–297) used to prove that the reduced norm has values in F also applies here to show that $\operatorname{pf}_A(a) \in F$.

The stated properties of pf_A follow from the corresponding properties for the matrix Pfaffian. The polynomial $p_a(x)$ is the analog of the Pfaffian characteristic polynomial defined in (10.12) above.

The map π_A arises from the Pfaffian adjoint map discussed in (10.12) and (10.13). Defining $\pi_A(a) = \varphi^{-1}(\pi(\varphi(a \otimes 1))) \in \mathcal{D}(A \otimes K)$, the usual descent argument shows that this value lies in $\mathcal{D}(A)$. The stated formulas follow from Lemmas 10.13 and 10.14. □

A question about a central simple algebra can often be reduced to the split case after an extension to a splitting field. In order to exploit this idea we need a technical lemma.

10.17 Lemma. *Let K/F be an extension of infinite fields.*

(1) *Suppose U is a K-vector space and $p : U \to K$ is a polynomial function. If $U = V \otimes_F K$ for some F-vector space V and if p vanishes on $V \otimes 1$, then $p = 0$.*

(2) *If A is a finite dimensional F-algebra and $W \subseteq A$ is an F-linear subspace such that $(W \otimes K) \cap (A \otimes K)^{\bullet} \neq \emptyset$ then $W \cap A^{\bullet} \neq \emptyset$.*

Proof. (1) Choosing an F-basis of V this statement becomes: if $X = (x_1, \ldots, x_n)$ is a system of indeterminates and $p(X) \in K[X]$ vanishes on F^n then $p(X) = 0$. This follows by induction on n and the fact that a non-zero polynomial in one variable has finitely many roots.

(2) Let $\mathcal{L} : A \to \mathrm{End}_F(A)$ be the representation defined by: $\mathcal{L}(a)(x) = ax$. Define $N : A \to F$ by $N(c) = \det(\mathcal{L}(c))$. Then $p = N \otimes 1$ is a polynomial function on $A \otimes K$ and c is a unit in $A \otimes K$ if and only if $p(c) \neq 0$. Apply part (1). □

Note that these assertions are false over finite fields (see Exercise 11). The next result is related to (6.15) but is proved independently here.

10.18 Corollary. *Let A be a central simple F-algebra with involution J. There exists $a \in A^{\bullet}$ such that $J(a) = -a$, except when A is (split) of odd degree and J has orthogonal type. Consequently A admits a* 1*-involution, and it admits a* (-1)*-involution provided* deg *A is even.*

Proof. That exception is necessary since a skew-symmetric matrix must have even rank. Also recall that a division algebra with involution must have 2-power degree. (This was mentioned earlier in (6.17).) Then an algebra of odd degree with involution must be split.

Suppose $A \cong \mathbb{M}_n(F)$ is split and express $J(X) = M^{-1} \cdot X^{\top} \cdot M$ for some λ-symmetric matrix M. If J has symplectic type then $J(M) = -M$. If J has orthogonal type choose a nonsingular skew-symmetric matrix S, which exists since we assume that n is even. Then $J(M^{-1}S) = -(M^{-1}S)$.

Now suppose A is not split. As mentioned above this implies that $n = \deg A$ is even. In addition, Wedderburn's Theorem on finite division rings implies that F is infinite. Let $W = \{a \in A : J(a) = -a\}$. Let K be a splitting field, $\varphi : A \otimes K \xrightarrow{\cong} \mathbb{M}_n(K)$ and I the involution on $\mathbb{M}_n(K)$ corresponding to J. Since $W \otimes K$ contains units, by the split case analyzed above, (10.17) implies that W contains a unit of A. □

10.19 Corollary. *Let A be a central simple F-algebra with involution and let K be a splitting field with $\varphi : A \otimes K \xrightarrow{\cong} \mathbb{M}_n(K)$. Let $a, b \in A$ and $f = \varphi(a \otimes 1)$, $g = \varphi(b \otimes 1)$.*

(1) *$a \in \mathcal{D}(A)$ if and only if $f \in \mathcal{D}_n$.*

(2) *$a \sim b$ in A if and only if $f \sim g$ in $\mathbb{M}_n(K)$.*

(3) *For any involution J on A, $a \sim J(a)$.*

Proof. If $A \cong \mathbb{M}_n(F)$ is split, we may alter φ by an inner automorphism to assume that φ induces the inclusion $\mathbb{M}_n(F) \subseteq \mathbb{M}_n(K)$. Since the elementary divisors of $a \in \mathbb{M}_n(F)$ are determined by its elementary divisors over K, the assertions (1) and (2) follow. For (3) express J as $J(a) = M^{-1} \cdot a^{\top} \cdot M$. Then $a \sim a^{\top} \sim J(a)$ holds for every $a \in A$.

Suppose A is not split so that F is infinite by Wedderburn.

(1) Let J be a 1-involution on A and let $W = \{c \in A : J(c) = -c$ and $J(ca) = -ca\}$. If $c \in W \cap A^\bullet$ then $a = c^{-1} \cdot ca \in \mathcal{D}(A)$. The statement follows by applying Lemma 10.17 to this space W.

(2) Use $W = \{c \in A : ac = cb\}$.

(3) Use $W = \{c \in A : ac = cJ(a)\}$. □

We begin our discussion of algebras of degree 4 with a preliminary lemma.

10.20 Lemma. *Let A be a central simple F-algebra of degree 4 with a (-1)-involution J. Then the restriction of* pf *to the* 6*-dimensional space* $\operatorname{Alt}(J)$ *is a regular quadratic form.*

Proof. We may extend scalars to assume $A \cong \operatorname{End}(V)$ is split. Then $J = I_b$ is the adjoint involution for some regular alternating form b on V. Choosing a symplectic basis for (V, b) we get the matrix of the form is $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in 2×2 blocks. Then B is the matrix of some $f \in \operatorname{Alt}(J)$ if and only if MB is skew-symmetric if and only if

$$B = \begin{pmatrix} x & y & 0 & r \\ z & w & -r & 0 \\ 0 & -s & x & z \\ s & 0 & y & w \end{pmatrix} \quad \text{for some } x, y, z, w, r, s \in F.$$

Then the formulas in Lemma 10.14(1) and after Corollary 10.9 show that $\operatorname{pf}(B) = -rs + xw - yz$. This is a regular quadratic form in 6 variables. □

10.21 Proposition (Albert, Rowen). *Suppose A is a central simple F-algebra of degree 4 with involution. Then any (-1)-involution on A is decomposable. In particular A is decomposable as an algebra.*

Proof. By (10.16) there is a linear map $\pi : \operatorname{Alt}(J) \to \operatorname{Alt}(J)$ such that $a \cdot \pi(a) = \pi(a) \cdot a = \operatorname{pf}(a)$ for every $a \in \operatorname{Alt}(J)$. Furthermore $\pi(\pi(a)) = a$. In fact, as in Example 10.15, π is the restriction of the linear map $\pi' : A \to A$ defined by $\pi'(x) = \frac{1}{2} \cdot \operatorname{trd}(x) - x$. Therefore $\operatorname{Alt}(J) = F \oplus W$ where W is the (-1)-eigenspace of π and $\dim W = 5$.

The quadratic form pf_J on $\operatorname{Alt}(J)$ has associated bilinear form B_J given by $2B_J(x, y) = \operatorname{pf}_J(x+y) - \operatorname{pf}_J(x) - \operatorname{pf}_J(y) = (x+y)\cdot\pi(x+y) - x\cdot\pi(x) - y\cdot\pi(y) = x\cdot\pi(y) + y\cdot\pi(x)$. If $y \in W$ then $2B_J(1, y) = (-y) + y = 0$. Hence $\operatorname{Alt}(J) \simeq F \perp W$ relative to the quadratic form pf_J and consequently the induced form on W is regular (using Lemma 10.20). Choose x, y as part of an orthogonal basis of W relative to pf_J. Then $x^2 = -x \cdot \pi(x) = -\operatorname{pf}(x) \in F^\bullet$ and similarly $y^2 \in F^\bullet$. Also $xy + yx = -2B_J(x, y) = 0$ and we conclude that $\{x, y\}$ generates a quaternion subalgebra Q of A. Since $W \subseteq \operatorname{Alt}(J)$ this Q is J-invariant. □

Although we are interested mainly in the case A has degree 4, we will define the Pfaffian associated to an orthogonal involution in the general case of a central simple algebra of degree n. Suppose that J is an involution of *orthogonal* type on A. We define a Pfaffian on $\mathrm{Alt}(J)$ in analogy to the classical Pfaffian on skew symmetric matrices. Since $\mathrm{Alt}(J)^\bullet \cdot \mathrm{Alt}(J) \subseteq \mathcal{D}(A)$, as mentioned in (10.16), we obtain a "Pfaffian" map and a "Pfaffian adjoint" associated to a fixed $s \in \mathrm{Alt}(J)^\bullet$:

$$\mathrm{Pf}_s : \mathrm{Alt}(J) \to F \text{ is defined by } \mathrm{Pf}_s(a) = \mathrm{pf}(sa).$$
$$\pi_s : \mathrm{Alt}(J) \to \mathrm{Alt}(J) \text{ is defined by } \pi_s(a) = \pi(sa)s.$$

Some aspects of these maps are independent of the choice of s.

10.22 Lemma. *Let J be a* 1*-involution on a central simple algebra A of even degree n. Let $s \in \mathrm{Alt}(J)^\bullet$.*

(1) *If $a, b \in \mathrm{Alt}(J)^\bullet$ then $\mathrm{pf}(a^{-1}b) = \mathrm{Pf}_s(a)^{-1} \cdot \mathrm{Pf}_s(b)$.*
If $s, t \in \mathrm{Alt}(J)^\bullet$ let $\lambda = \mathrm{pf}(ts^{-1})$. Then for every $a \in \mathrm{Alt}(J)$

$$\mathrm{Pf}_t(a) = \lambda \cdot \mathrm{Pf}_s(a) \quad \textit{and} \quad \pi_t(a) = \lambda \cdot \pi_s(a).$$

(2) $\mathrm{Pf}_s(a)^2 = \mathrm{nrd}(s) \cdot \mathrm{nrd}(a)$ *for every $a \in \mathrm{Alt}(J)$.*
$\mathrm{Pf}_s(J(b) \cdot a \cdot b) = \mathrm{Pf}_s(a) \cdot \mathrm{nrd}(b)$ *for every $a \in \mathrm{Alt}(J)$ and $b \in A^\bullet$.*

(3) *If $a \in \mathrm{Alt}(J)$ then $\pi_s(a) \cdot a = a \cdot \pi_s(a) = \mathrm{Pf}_s(a)$.*

(4) *If $a \in \mathrm{Alt}(J)$ then $\pi_s(\pi_s(a)) = (\mathrm{nrd}\, s) \cdot (-1)^{\frac{n}{2}} \cdot \mathrm{Pf}_s(a)^{\frac{n}{2}-2} \cdot a$.*

Proof. (1) This generalizes Lemma 10.14(1). Define another involution J_0, by setting $J_0(x) = s \cdot J(x) \cdot s^{-1}$. Then J_0 is a (-1)-involution (since $J(s) = -s$), $J_0(s) = -s$ and $\mathrm{Alt}(J_0) = s \cdot \mathrm{Alt}(J) = \mathrm{Alt}(J) \cdot s^{-1}$. Since sa and $sb \in \mathrm{Alt}(J_0)$ the last statement in (10.16) implies $\mathrm{pf}(a^{-1}b) = \mathrm{pf}((sa)^{-1} \cdot sb) = \mathrm{pf}(sa)^{-1}\,\mathrm{pf}(sb)$, as claimed. For the second statement, note that $ts^{-1} \in \mathrm{Alt}(J) \cdot s^{-1} = \mathrm{Alt}(J_0)$ and $sa \in s \cdot \mathrm{Alt}(J) = \mathrm{Alt}(J_0)$. Then (10.16)(3) implies: $\mathrm{Pf}_t(a) = \mathrm{pf}(ta) = \mathrm{pf}(ts^{-1} \cdot sa) = \mathrm{pf}(ts^{-1}) \cdot \mathrm{pf}(sa) = \lambda \cdot \mathrm{Pf}_s(a)$. The second equality is proved later.

(2) The first statement is clear. The second follows from (10.16)(1) since $\mathrm{pf}(sJ(b)ab) = \mathrm{pf}(J_0(b) \cdot sa \cdot b) = \mathrm{pf}(sa) \cdot \mathrm{nrd}(b)$.

(3) Certainly $\pi_s(a) \cdot a = \pi(sa) \cdot sa = \mathrm{pf}(sa) = \mathrm{Pf}_s(a)$. For the second equality recall that $sa \cdot \pi(sa) = \mathrm{Pf}_s(a)$ is a scalar so that $\mathrm{Pf}_s(a) = s^{-1} \cdot sa\pi(sa) \cdot s = a \cdot \pi_s(a)$. Now to finish the proof of (1): using (3) the equation $\pi_t(a) = \lambda \cdot \pi_s(a)$ holds whenever $a \in A^\bullet$. The standard "generic" argument now applies.

(4) This follows from the definition in terms of π and the properties of π stated in (10.16) (after noting that $s^2, sa \in \mathrm{Alt}(J_0)$ and $\mathrm{pf}(s^2) = (-1)^{\frac{n}{2}} \cdot (\mathrm{nrd}\, s)$.) Alternatively we note that if $a \in \mathrm{Alt}(J)^\bullet$ then $\pi_s(a) = \mathrm{Pf}_s(a) \cdot a^{-1}$. Then $\pi_s(\pi_s(a)) = \mathrm{Pf}_s(a)^{\frac{n}{2}-1} \cdot \mathrm{Pf}_s(a^{-1}) \cdot a$. Since $\mathrm{Pf}_s(a^{-1}) = (-1)^{\frac{n}{2}} \cdot \mathrm{Pf}_s(a)^{-1} \cdot \mathrm{nrd}(s)$ the claim holds. Since this claim is a polynomial equation valid for every $a \in A^\bullet$ the standard generic argument applies again. □

Let us now specialize again to the case of main interest: A has degree $n = 4$. Then $(\mathrm{Alt}(J), \mathrm{Pf}_s)$ is a quadratic space of dimension 6 whose similarity class is independent of the choice of s, depending only on the algebra A.

10.23 Corollary. *Let A be a central simple F-algebra with involution and degree 4. If J is an involution on A define the form $\varphi_J : \mathrm{Alt}(J) \to F$ as follows:*

If J has type -1 let $\varphi_J(a) = \mathrm{pf}(a)$.

If J has type 1 choose $s \in \mathrm{Alt}(J)^\bullet$ and define $\varphi_J(a) = \mathrm{Pf}_s(a)$.

Then $(\mathrm{Alt}(J), \varphi_J)$ is a regular 6-dimensional quadratic space, and all these spaces are similar.

Proof. First we prove the similarity. Let J be any 1-involution on A and choose $s \in \mathrm{Alt}(J)^\bullet$. Let J_1 be any (-1)-involution on A. Then there exists $t \in \mathrm{Alt}(J)^\bullet$ such that $J_1(x) = t \cdot J(x) \cdot t^{-1}$ so that $\mathrm{Alt}(J_1) = t \cdot \mathrm{Alt}(J)$. The left-multiplication map $\mathcal{L}_t : \mathrm{Alt}(J) \to \mathrm{Alt}(J_1)$ provides the desired similarity, since for any $a \in \mathrm{Alt}(J)$ we have $\varphi_{J_1}(\mathcal{L}_t(a)) = \mathrm{pf}(ta) = \mathrm{Pf}_t(a) = \lambda \cdot \mathrm{Pf}_s(a) = \lambda \cdot \varphi_J(a)$, where $\lambda = \mathrm{pf}(ts^{-1})$ as in (10.22). The regularity of φ_J now follows from (10.20). □

Define the *Albert form* α_A to be this 6-dimensional quadratic form associated to A. To calculate α_A note that A is decomposable (by (10.21)) so that $A \cong C(V, q)$ for some 4-dimensional quadratic space (V, q). Use the involution J_0 which is the identity on V, so that J_0 has type (-1) and $\mathrm{Alt}(J_0) = F \oplus V \oplus Fz$. Here $z = z(V, q)$ so that $z^2 = \delta$ where $dq = \langle\delta\rangle$. From Example 10.15 we know that $\pi(\alpha + v + \beta z) = \alpha - v - \beta z$. Therefore $\mathrm{pf}(\alpha + v + \beta z) = \alpha^2 - q(v) - \beta^2\delta$ and α_A is similar to $(\mathrm{Alt}(J_0), \mathrm{pf}_{J_0}) \simeq \langle 1, -dq\rangle \perp -q$.

It is this form for which Albert proved: A is a division algebra if and only if the form α_A is anisotropic. (See Exercises 3.10 (5) and 3.17.) This Albert form can also be expressed nicely in terms of a decomposition $A \cong Q_1 \otimes Q_2$ for quaternion algebras Q_i. Let φ_i be the norm form of Q_i with pure parts φ_i' (so that $\varphi_i \simeq \langle 1\rangle \perp \varphi_i'$). Then α_A is similar to the form $\varphi_1' \perp -\varphi_2'$. It is easy to recover the algebra A from the Albert form α_A since $c(\alpha_A) = c(\varphi_1 \perp -\varphi_2) = c(\varphi_1)c(\varphi_2) = [Q_1] \cdot [Q_2] = [A]$. If these formulas for the Albert form α_A are taken as the definition, the uniqueness properties do not seem clear. (See Exercise 3.17.)

10.24 Lemma. *Suppose A is a central simple F-algebra with involution J of orthogonal type. If A has even degree then $\mathrm{Alt}(J)^\bullet \neq \emptyset$ and all values of $\mathrm{nrd}(b)$ for $b \in \mathrm{Alt}(J)^\bullet$ lie in the same square class in $F^\bullet/F^{\bullet 2}$.*

Proof. We proved the first statement in Corollary 10.18. Now suppose $b, c \in \mathrm{Alt}(J)^\bullet$. Then $bc \in \mathcal{D}(A)$ and therefore $\mathrm{nrd}(b) \cdot \mathrm{nrd}(c) = \mathrm{nrd}(bc) = \mathrm{pf}(bc)^2 \in F^{\bullet 2}$. □

Define the *determinant* $\det(J) \in F^\bullet/F^{\bullet 2}$ to be that common square class. That is, if J is a 1-involution on the central simple algebra A and $\deg A$ is even, then $\det(J) = \langle \mathrm{nrd}(b)\rangle \in F^\bullet/F^{\bullet 2}$ for any $b \in \mathrm{Alt}(J)^\bullet$.

10.25 Lemma. (1) *Let (V, q) be a quadratic space of even dimension. Then* $\det(I_q) = \det q$ *in* $F^\bullet/F^{\bullet 2}$.

(2) *Suppose (A_i, J_i) are central simple F-algebras with involutions of orthogonal type and with even degrees. Then* $\det(J_1 \otimes J_2) = \langle 1 \rangle$.

Proof. (1) Pick a basis and let M be the symmetric matrix of the form q. Let B be the matrix of $b \in \mathrm{End}(V)$. Then $I_q(B) = M^{-1} \cdot B^\top \cdot M$. If $b \in \mathrm{Alt}(I_q)$ we find that MB is skew- symmetric so that $\det(MB)$ is a square. Therefore $\det(I_q) = \langle \det(B) \rangle = \langle \det(M) \rangle = \det q$ in $F^\bullet/F^{\bullet 2}$.

(2) If $\deg(A_i) = n_i$ and $a_i \in A_i$ recall that $\mathrm{nrd}(a_1 \otimes a_2) = (\mathrm{nrd}\, a_1)^{n_2}(\mathrm{nrd}\, a_2)^{n_1}$ where the reduced norms are computed in the appropriate algebras. Now simply choose $b \in \mathrm{Alt}(J_1)^\bullet$, which exists in A_1 by Corollary 10.18, note that $b \otimes 1 \in \mathrm{Alt}(J_1 \otimes J_2)^\bullet$ and compute $\mathrm{nrd}(b \otimes 1) = \mathrm{nrd}(b)^{n_2}$ is a square. □

Thus one necessary condition that a 1-involution J be decomposable (relative to subalgebras of even degree) is that $\det(J) = \langle 1 \rangle$. In the case A has degree 4 this was proved by Knus, Parimala and Sridharan to be a sufficient condition as well. The key idea is the linear map π_s discussed in (10.22).

10.26 Proposition. *Let A be a central simple F-algebra of degree* 4 *with involution J. Then J is indecomposable if and only if J has orthogonal type and* $\det(J) \neq \langle 1 \rangle$.

Proof. The “if” part is in (10.25). We proved in (10.21) that symplectic involutions are decomposable. Therefore we assume that J is an involution of orthogonal type with $\det(J) = \langle 1 \rangle$ and search for a J-invariant quaternion subalgebra. By definition there exists $b \in \mathrm{Alt}(J)^\bullet$ such that $\mathrm{nrd}(b) = \lambda^2$ for some $\lambda \in F^\bullet$. Then by (10.22) $\pi_s \circ \pi_s = \lambda^2 \cdot 1_{\mathrm{Alt}(J)}$ so the 6-dimensional space $\mathrm{Alt}(J)$ breaks into $\pm\lambda$-eigenspaces: $\mathrm{Alt}(J) = U^+ \oplus U^-$. Let B_s be the bilinear form associated to the quadratic form Pf_s. Then $2B_s(x, y) = \mathrm{Pf}_s(x + y) - \mathrm{Pf}_s(x) - \mathrm{Pf}_s(y) = x \cdot \pi_s(y) + y \cdot \pi_s(x)$. Similarly we argue that this quantity equals $\pi_s(x) \cdot y + \pi_s(y) \cdot x$.

If $x \in U^+$ and $y \in U^-$ then $2B_s(x, y) = x \cdot (-\lambda y) + (\lambda x) \cdot y = -\lambda \cdot (xy - yx)$ and it also equals $(\lambda x) \cdot y + (-\lambda y) \cdot x = \lambda \cdot (xy - yx)$. Therefore $xy - yx = 0$ and we conclude that U^+ centralizes U^- and that $\mathrm{Alt}(J) = U^+ \perp U^-$ relative to the quadratic form Pf_s. Consequently the restrictions of Pf_s to the subspaces U^+ and U^- are regular.

We may assume $\dim U^+ \geq 3$ (otherwise interchange λ and $-\lambda$). If $x, y \in U^+$ then $2B_s(x, y) = \lambda \cdot (xy + yx)$ and in particular $x^2, y^2 \in F$. Choose $x, y \in U^+$ to be part of an orthogonal basis relative to B_s. Then x, y are units and $xy + yx = 0$, so they generate a quaternion subalgebra $Q \subseteq A$. Since $x, y \in \mathrm{Alt}(J)$ this Q is certainly J-invariant. (In fact, the induced involution on Q is the standard “bar”.) □

Now we are in a position to prove Theorem 10.5.

Proof of Theorem 10.5. There are three cases to be considered. If y is given with $y^2 = d \in F^{\bullet 2}$, it suffices to find some $a \in \mathcal{D}(A)^\bullet$ which anti-commutes with y and with $J(a) = \pm a$. For with such a we know that $a^2 = \alpha a + \beta$ for some $\alpha, \beta \in F$, since $\deg(a) \leq 2$, by (10.16) (2). Conjugating by y and subtracting, we find that $\alpha = 0$ so that $a^2 = \beta \in F^\bullet$. Then y and a generate a J-invariant quaternion subalgebra Q.

Let K be a splitting field of A with $\sqrt{d} \in K$, let $\varphi : A \otimes K \xrightarrow{\cong} \mathrm{End}_K(V)$ and $f = \varphi(y \otimes 1)$. Then $f^2 = d \cdot 1_V$ so that f provides an eigenspace decomposition $V = V^+ \oplus V^-$ with dimensions $4 = n^+ + n^-$. The matrix of f relative to a compatible basis is

$$\begin{pmatrix} \sqrt{d} \cdot I_{n^+} & 0 \\ 0 & -\sqrt{d} \cdot I_{n^-} \end{pmatrix}.$$

(1) We know J is decomposable from (10.21). Suppose first that $J(y) = y$. Then $y \in \mathcal{D}(A)$. Since $f \in \mathcal{D}$ the dimensions n^+ and n^- are even. Then $n^+ = n^- = 2$, since $y \notin F$. Following the notations in the proof of (10.21) we see that $\mathrm{trd}(y) = 0$ so that $y \in W$. Extending $\{y\}$ to an orthogonal basis $\{y, a, \dots\}$ of W, we see that $a \in \mathrm{Alt}(J)^\bullet \subseteq \mathcal{D}(A)^\bullet$ and a, y anti-commute.

Suppose y is given with $J(y) = -y$. Then $J(f) = -f$ in $\mathrm{End}(V)$ so that $f \sim -f$. Therefore $n^+ = n^- = 2$ and hence $f \in \mathcal{D}(\mathrm{End}(V))$. Then $y \in \mathcal{D}(A)$ by (10.19) so there exists some (-1)-involution J_1 on A with $J_1(y) = y$. Express $J_1 = J^a$ so that $J(a) = a$ and $y = J^a(y) = a^{-1} \cdot J(y) \cdot a = -a^{-1}ya$. Then $a \in \mathcal{D}(A)$ and a, y anti-commute.

(2) If J is decomposable we can certainly find such an element y inside a J-invariant quaternion subalgebra. Conversely suppose J is a 1-involution with $J(y) = -y$. As before we find that $f \sim -f$ so that $n^+ = n^- = 2$. Then $\mathrm{nrd}(y) = \det(f) = (\sqrt{d})^2(-\sqrt{d})^2 = d^2$. Then $\det(J) = \langle 1 \rangle$ and (10.26) implies that J is decomposable. As above $y \in \mathcal{D}(A)$ so there exists some (-1)-involution J_1 with $J_1(y) = y$. Express $J_1 = J^a$ and note that $J(a) = -a$ and a, y anti-commute. Since $ay \in \mathcal{D}(A)$ and y, ay anticommute, the claim follows. □

The existence of an indecomposable involution on a degree 4 division algebra was first proved by Amitsur, Rowen and Tignol (1979). The Knus, Parimala and Sridharan Theorem (10.26) shows that the determinant $\det(J)$ determines whether J is indecomposable. This criterion is made clearer by the following result of Knus, Lam, Shapiro, Tignol (1992).

Proposition. *Let A be a central simple F-algebra of degree 4, with involution. The following subsets of $F^\bullet$ are equal.*

$\{d : \langle d \rangle = \det(J)$ *for some* 1-*involution* J *on* $A\}$.

$G_F(\alpha_A)$, *the group of similarity factors of an Albert form of* A.

$\mathrm{nrd}(A^\bullet) \cdot F^{\bullet 2}$, *the group of square classes of reduced norms.*

Consequently the algebra A admits an indecomposable involution if and only if the Albert form α_A has a similarity factor which is not a square.

Analogous decomposition results fail for algebras of larger degree. Any tensor product of three quaternion algebras is a central simple algebra of degree 8. However Amitsur, Rowen and Tignol (1979) found an example of a division algebra D of degree 8 over its center and such that D has an involution but is indecomposable (i.e. D has no quaternion subalgebras).

Several standard properties of quadratic forms have analogs for orthogonal involutions of central simple algebras. We end this chapter with some remarks about this correspondence. An orthogonal involution on $\operatorname{End}(V)$ must equal the adjoint involution I_q for some quadratic form q on V, unique up to scalar multiple. Any invariant of q which remains unchanged if q is altered by a similarity should be definable entirely in terms of the involution I_q. For example:

$\det q \in F^\bullet/F^{\bullet 2}$, in the case $n = \dim q$ is even.

$|\operatorname{sgn}_P(q)|$, the absolute value of the signature of q at an ordering P of F.

$C_0(q)$, the even Clifford algebra.

The Witt index of q.

$G_F(q)$, the group of similarity factors (or norms) of the form q.

Are there analogous invariants for orthogonal involutions on arbitrary central simple algebras, coinciding with the given invariants in the split case? Of course we hope that the newly defined invariant will be useful in the theory of involutions.

We have already seen one example of this program: the determinant $\det(J)$ is the analog of $\det q$. Lewis and Tignol (1993) have investigated the signature of an involution. The analog of the even Clifford algebra was done long ago by Jacobson (1964) and discussed further by Tits (1968). The determinant $\det(J)$ also arises naturally out of Jacobson's theory. This even Clifford algebra of an algebra with involution (A, J) is investigated extensively in Knus et al. (1998).

The Pfister Factor Conjecture provides another example of this theme. A quadratic space (V, q) is similar to a Pfister form when q is a tensor product of some binary forms. Equivalently, the algebra $(\operatorname{End}(V), I_q)$ is a tensor product of split quaternion algebras with involution. Motivated by this, let (A, J) be a central simple algebra with 1-involution and define it to be a "Pfister algebra" if it is a tensor product of some quaternion algebras with involution. The Pfister Factor Conjecture says: When A is split then these two notions coincide. A precise statement appears in (9.17).

Exercises for Chapter 10

1. **Maximal examples.** (1) If $\dim q = 16$ and $(\sigma, \tau) < \operatorname{Sim}(q)$ is an (s, t)- familiy where $s + t \geq 7$, then q is similar to a Pfister form. Find an example of q over $\mathbb{R}$ such that $\dim q = 16$ and $\operatorname{Sim}(q)$ has a (3, 3)-family but admits no families of larger size.

(2) There exists $(\langle 1, a\rangle, \langle x\rangle) < \mathrm{Sim}(V, q)$ where $\dim q = 12$ but such that $(\langle 1, a\rangle, \langle x\rangle)$ does not admit any expansion by 2 dimensions. (See Exercise 7.10.) Find similar examples $(\sigma, \tau) < \mathrm{Sim}(q)$ of an (s, t)-family where $s + t = 2m - 1$ and $\dim q = 2^m \cdot 3$, but σ admits no expansion by 2 dimensions.

(3) **Open question.** Are there similar examples in other dimensions? For instance, is there some $\sigma < \mathrm{Sim}(q)$ where $\dim \sigma = 5$, $\dim q = 48$, but the 5-plane does not expand by 2 dimensions? That involves a degree 4 Clifford algebra D (which must be a division algebra) and a (-1)-involution on $\mathbb{M}_3(D)$ having no invariant quaternion subalgebras. Does such an involution exist?

(4) When can $\langle 1, a\rangle < \mathrm{Sim}(q)$ be maximal as a subspace? Certainly if $\langle\langle a\rangle\rangle \mid q$ but q has no 2-fold Pfister factor then this occurs. The converse is unknown.

Open question. If $\langle\langle a\rangle\rangle \mid q$ and $\langle\langle x, y\rangle\rangle \mid q$ then must there exist $b \in F^\bullet$ with $\langle\langle a, b\rangle\rangle \mid q$?

(Hint. (1) If $s + t \geq 7$ then (10.7) shows that there is a (5, 5)-family and q is Pfister by PC(4). Find a proof that does not invoke Theorem 10.7.)

2. **Non-uniqueness.** (1) Suppose (σ, τ) is an (s, t)-pair where $s + t$ is odd, and let (C, J) be the corresponding Clifford algebra with involution. Then $(\sigma, \tau) < \mathrm{Sim}(V, q)$ if and only if there is a central simple F-algebra with involution (A, K) such that $(C \otimes A, J \otimes K) \cong (\mathrm{End}(V), I_q)$. However this (A, K) need not be unique.

(2) The two representations π_α and π_β of $C \to \mathrm{End}(V)$ arising from the two choices above yield two (2, 1)-families on the 8-dimensional space (V, q). One of them expands to a (4, 4)-family and the other does not admit any expansion of 2 or more dimensions.

(Hint. (1) Let $(\sigma, \tau) = (\langle 1, 1\rangle, \langle 1\rangle)$ so that $(C, J) \cong (\mathbb{M}_2(\mathbb{Q}), I_{\langle\langle 1\rangle\rangle})$. Let $q \simeq \langle\langle 1, 1, 1\rangle\rangle$, $\alpha = \langle 1, 1, 1, 1\rangle$ and $\beta = \langle 1, 1, 1, 2\rangle$. Then $\langle\langle 1\rangle\rangle \otimes \alpha \simeq \langle\langle 1\rangle\rangle \otimes \beta$ but α, β are not similar.)

3. **Matrix Pfaffians.** (1) If S, T are skew-symmetric $n \times n$ matrices which anticommute then ST is also skew-symmetric and $\mathrm{Pf}(ST) = \pm \mathrm{Pf}(S) \cdot \mathrm{Pf}(T)$. Is this sign independent of S, T?

(2) Suppose R commutes with some nonsingular skew-symmetric S. Then $R^\top \cdot R \in \mathcal{D}$ and $\mathrm{pf}(R^\top \cdot R) = \det R$.

(3) If $S, T \in \mathrm{GL}_n$ are skew-symmetric then $ST \in \mathcal{D}_n$ and $\mathrm{pf}(ST) = (-1)^{\frac{n}{2}}\, \mathrm{Pf}(S) \cdot \mathrm{Pf}(T)$. Consequently if $S_1S_2S_3S_4 = I_n$ where each S_i is skew-symmetric then $\mathrm{Pf}(S_1) \cdot \mathrm{Pf}(S_2) \cdot \mathrm{Pf}(S_3) \cdot \mathrm{Pf}(S_4) = 1$. Are there analogous results when I_n equals a product of some k skew-symmetric matrices?

(4) If S is skew-symmetric $n \times n$ then $\mathrm{Pfadj}(\mathrm{Pfadj}(S)) = (-1)^{\frac{n}{2}} \cdot (\mathrm{Pf}\, S)^{\frac{n}{2}-2} \cdot S$.

4. **Properties of $\boldsymbol{\pi}$.** (1) Let M, T be given as in 10.14. Then $\pi(M^{-1} \cdot T) = \mathrm{Pfadj}(M)^{-1} \cdot \mathrm{Pfadj}(T)$.

(2) If $f \in \mathrm{Alt}(J)$ and $g \in \mathrm{GL}(V)$ then $\pi(J(g)fg) = (\det g) \cdot g^{-1} \cdot \pi(f) \cdot J(g)^{-1}$.

5. Let A be a central simple F-algebra with involution. Suppose $\deg A = n$ is even and $n > 2$.

(1) **Lemma.** *$\mathcal{D}(A)$ contains an F-basis of A.*

(2) If J is an involution on A then $\mathrm{Alt}(J)$ generates A as an F-algebra. Does $\mathrm{Sym}(J)$ generate A as well?

Corollary. (i) *If J, J' are involutions on A then $J = J'$ if and only if* $\mathrm{Alt}(J) = \mathrm{Alt}(J')$.

(ii) $(A, J) \cong (A, J')$ *if and only if* $\mathrm{Alt}(J') = x \cdot \mathrm{Alt}(J) \cdot x^{-1}$ *for some* $x \in A^{\bullet}$.

(Note. This assertion is also true when A is quaternion.)

(3) Given the subspace $S = \mathrm{Alt}(J) \subseteq A$, express the subspace $\mathrm{Sym}(J)$ somehow directly in terms of S.

(Hint. (1) It suffices to settle the split case. An *ad hoc* proof can be given, but the claim follows immediately from a theorem of Kasch (1953). Further references appear in Leep, Shapiro, Wadsworth (1985), §4.

(3) $\mathrm{Sym}(J) = (\mathrm{Alt}(J))^{\perp}$ relative to the trace form $\tau : A \times A \to F$ defined by $\tau(x, y) = \mathrm{trd}(xy)$.)

6. (1) Let J be a λ-involution on $\mathrm{End}(V)$ and fix $s_0 \in \mathrm{Alt}(J)^{\bullet}$. Then $f \in \mathrm{Alt}(J)$ iff $f = J(g) \cdot s_0 \cdot g$ for some $g \in \mathrm{End}(V)$.

(2) Does (1) remain valid for involutions on a central simple algebra A?

(Hint. Let B be the λ-form on V corresponding to J, and B_0 the alternating form for J^{s_0}. Then (V, B_0) has a symplectic basis and the regular part of B^f has a symplectic basis. Choose a (not necessarily injective) isometry $g : (V, B^f) \to (V, B_0)$.)

7. Let C be an $m \times m$ matrix over F.

(1) If$p(x) = \det(xI_m - C)$ is the characteristic polynomial, define $p^*(x) = (-1)^{m+1} \cdot \frac{p(x)-p(0)}{x}$. Then $\mathrm{adj}\, C = p^*(C)$.

(2) $\mathrm{adj}(\mathrm{adj}\, C)) = (\det C)^{m-2} \cdot C$.

(3) If $\dim V = 2$, then $\mathcal{D}(\mathrm{End}(V)) = F \cdot 1_V$. If $f = \alpha \cdot 1_V$ for $\alpha \in F$, then $\mathrm{pf}(f) = \alpha$, $\mathrm{pf}\,\chi_f(x) = x - \alpha$ and $\pi(f) = 1_V$. Explain the difficulty in the definition when $f = 0_V$.

(Hint. (1) Verify first that $C \cdot p^*(C) = (\det C) \cdot I_m$. The claim follows for nonsingular C. Apply this case to a generic matrix C, or to the matrix $C + x \cdot I_m$ in $F(x)$, and then specialize to deduce it for arbitrary C.

(2) Apply the equation $X \cdot \mathrm{adj}\, X = (\det X) I_m$ to $X = C$ and $X = \mathrm{adj}\, C$ and deduce the claim when C is nonsingular. Complete the argument as before.)

8. **Subspaces of $\mathcal{D}$.** Let A be a degree 4 algebra with involution. If $S \subseteq \mathcal{D}(A)$ is a linear subspace with $\dim S = 6$ and $1_V \in S$, then $S = \mathrm{Alt}(J)$ for some (-1)-involution J.

(Hint. Let S_0 be the subspace of trace 0 elements. Then $(S, \mathrm{pf}) \simeq \langle 1\rangle \perp -\psi$ as a quadratic space, where $\psi(c) = c^2$ for $c \in S_0$. There is an induced algebra homomorphism $\pi : C(\psi) \to A$. If ψ is regular then π is surjective and the involution J_0 on $C(\psi)$ induces the desired J on A. Otherwise, pass to the split case and find $T \subseteq S_0$ with $\dim T = 3$ and $t^2 = 0$ for every $t \in T$. Get a contradiction using Jordan forms and the fact that every such t has even rank.)

9. **Albert forms.** Let A be a central simple algebra of degree 4, with involution. Then the Albert form α_A is uniquely defined up to a scale factor. If J is a (-1)-involution on A let $\mathrm{Alt}_0(J)$ be the subspace of trace 0 elements of $\mathrm{Alt}(J)$. Then α_A has a special presentation: $(\mathrm{Alt}(J), \mathrm{pf}) \simeq \langle 1\rangle \perp -\psi$ where $\psi(c) = c^2$ for $c \in \mathrm{Alt}_0(J)$. Conversely, if there is a realization of α_A which represents 1, then there is a corresponding (-1)-involution J. Consequently, if α is one choice for the Albert form, then there is a bijective correspondence:

$$\{\text{isomorphism classes of } (-1)\text{-involutions on } A\} \leftrightarrow D_F(\alpha)/G_F(\alpha).$$

10. If $f \in \mathcal{D}(\mathrm{End}(V))$ then $\pi(f)$ is a polynomial in f. For example, when $n = \dim V$:

$$\text{if } n = 4 \text{ then } \pi(f) = \tfrac{1}{2} \cdot (\mathrm{tr}\, f)1_V - f;$$

$$\text{if } n = 6 \text{ then } \pi(f) = f^2 - \tfrac{1}{2} \cdot (\mathrm{tr}\, f) \cdot f + \Big(\tfrac{1}{8} \cdot (\mathrm{tr}\, f)^2 - \tfrac{1}{4} \cdot (\mathrm{tr}\, f^2)\Big)1_V.$$

(Hint. If $n = 6$ then $\chi_f(x) = x^6 - c_1x^5 + c_2x^4 - \cdots = p(x)^2$ where $p(x) = x^3 + ax^2 + bx + c$. Then $\pi(f) = p^*(f)$ where $p^*(x) = x^2 + ax + b$. Then $a = -\frac{1}{2}c_1$ and $b = \frac{1}{2}c_2 - \frac{1}{8}c_1^2$. For the eigenvalues λ_i, $c_1 = \sum \lambda_i = \mathrm{tr}(f)$ and $c_2 = \sum \lambda_i\lambda_j = \frac{1}{2}((\mathrm{tr}\, f)^2 - \mathrm{tr}(f^2))$.)

11. **Finite field examples.** (1) Suppose $\mathcal{S} \subseteq \mathbb{M}_n(F)$ is a linear subspace of singular matrices, but that for some extension field K/F the space $\mathcal{S} \otimes K \subseteq \mathbb{M}_n(K)$ contains a nonsingular matrix. Then F must be finite and $n > |F|$.

(2) The set of all $\begin{pmatrix} x & * & * \\ 0 & y & * \\ 0 & 0 & x+y \end{pmatrix}$ provides a 5-dimensional example in $\mathbb{M}_3(\mathbb{F}_2)$. Find a similar example of $\mathcal{S} \subseteq \mathbb{M}_4(\mathbb{F}_3)$ with $\dim \mathcal{S} = 9$.

12. Suppose A is a central simple F-algebra.

(1) If J is an involution on A and $a \in A$ then $a \sim J(a)$, by Corollary 10.19. In fact $J(a) = bab^{-1}$ for some b such that $J(b) = \lambda b$, where $\lambda = \mathrm{type}(J)$.

(2) If $a \in A$ is nilpotent then $a \sim -a$.

13. **Linear algebra.** (1) **Lemma.** *If $C \in \mathbb{M}_n(F)$ then there exists some symmetric $S \in \mathrm{GL}_n(F)$ such that $S \cdot C \cdot S^{-1} = C^\top$.*

(2) **Corollary.** *Let A be a central simple F-algebra with involution and $a \in A$. Then there exists a 1-involution J on A such that $J(a) = a$.*

(3) **Proposition.** *Let A be as before and suppose $\varepsilon = \pm 1$ is given. If $a \in A^\bullet$ with $a \sim -a$ then there exists an ε-involution J such that $J(a) = -a$.*

(Hint. (1) Use the rational canonical form to reduce to the case C is a companion matrix. Now S can be exhibited explicitly. It can also be derived as the Gram matrix of a trace form on the algebra $F[x]/(p(x))$ where $p(x)$ is the characteristic polynomial of A.

(2) Suppose $A = \mathrm{End}(V)$ is split, choose a basis, apply (1) and define $J(X) = S^{-1} \cdot X^\top \cdot S$. If A is not split then F is infinite. Fix a 1-involution J_0, consider the linear subspace $W = \{c \in A : J_0(c) = c \text{ and } J_0(ca) = ca\}$, and apply (10.17).

(3) The same steps work, but the split case is harder. References appear in the Notes below.)

14. **Generalizing $\mathcal{D}$.** Define

$$\mathcal{D}_n^0 = \{B \in \mathbb{M}_n(F) : B = ST \text{ for some skew-symmetric } S, T\}.$$

(1) $\mathcal{D}_n \subseteq \mathcal{D}_n^0$ with strict containment if $n \geq 3$.

(2) If $B \in \mathcal{D}_n^0$ then every elementary divisor of B not of the form x^k occurs with even multiplicity.

(3) Find some $B \in \mathcal{D}_3^0$ with $\mathrm{rank}(B) = 1$. What conditions on the elementary divisors characterize elements of $\mathcal{D}_n^0$? (See the Notes for references.)

(Hint. (1) Find 4×4 skew-symmetric S, T such that ST has rank 1.

(2) Note that $QBQ^{-1} = (QSQ^\top)(Q^{-\top}TQ^{-1})$ and choose Q so that $QSQ^\top = \begin{pmatrix} H & 0 \\ 0 & 0 \end{pmatrix}$ for some nonsingular skew-symmetric H. Then $B \sim \begin{pmatrix} B_0 & B_1 \\ 0 & 0 \end{pmatrix}$ where $B_0 \in \mathcal{D}$. The multiplicity of a non-zero eigenvalue of B equals that of B_0 and (10.10) applies.)

15. (1) Let $f \in \mathrm{End}(V)$. Then f lies in $\mathcal{D} \iff f \sim \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$. Here is a "basis-free" version: $f \in \mathcal{D} \iff f$ centralizes some split quaternion subalgebra of $\mathrm{End}(V)$.

(2) **Proposition.** *Let A be a central simple F-algebra with involution and suppose $Q \subseteq A$ is a quaternion subalgebra. Then $C_A(Q) \subseteq \mathcal{D}(A)$. The converse is true if A is split of even degree or if A has degree 4.*

(Hint: (1) If $f \in \mathcal{D}$ then $V = U \oplus W$ with bases $\{u_1, \dots\}$ and $\{w_1, \dots\}$ such that $f(u_j) = \sum_i c_{ij} u_i$ and $f(w_j) = \sum_i c_{ij} w_i$. Define $g, h \in \mathrm{End}(V)$ by $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then f centralizes the algebra generated by g and h.