

14.9 Alternating Forms and Darboux Bases

Almost every classification theorem so far in this chapter has carried the same asterisk — the exceptions being the crude invariants of Section 2, rank and the square class of the determinant, which need nothing of the field. Diagonalize a symmetric form: characteristic $\neq 2$. Split a form into a symmetric and an alternating half: characteristic $\neq 2$. Recover a form from its quadratic form: characteristic $\neq 2$. This section has no asterisk. Alternating forms admit a complete classification over **every** field, with no hypothesis on the characteristic at all, and the classification is as clean as a classification gets: one congruence class for each even rank.

Throughout, F is an arbitrary field, V is a finite-dimensional vector space over F , and β is an **alternating** bilinear form on V (Definition 7.2.2), meaning $\beta(v, v) = 0$ for **every** $v \in V$. Two facts from Section 3 are used constantly. First, β is then skew-symmetric, $\beta(u, v) = -\beta(v, u)$, by Theorem 14.3.3 (a) — and that direction needs no hypothesis on F . Second, by Proposition 14.3.2 (b) the matrix of β in any basis is skew-symmetric with **zero diagonal**, and we call such a matrix **alternating**. Symmetry of the situation is worth noting once: since $\beta(u, v) = 0$ if and only if $\beta(v, u) = 0$, “orthogonal” needs no left or right, and the radical $\text{rad}(\beta)$ of Definition 14.1.3 is what one would want it to be from either side.

14.9.1 The two-dimensional model

A symmetric form has a one-dimensional model to build from: on a line $\text{span}(v)$ it is $q(cv) = c^2q(v)$, a scalar multiple of the squaring function, and Section 4 assembled a general symmetric form out of such lines. An alternating form offers nothing on a line at all. For any v and any scalars c, d ,

$$\beta(cv, dv) = cd\beta(v, v) = 0,$$

so β restricted to any line is zero. The one-dimensional pieces are all identical and all trivial. The smallest place where an alternating form has something to say is a plane, and there is essentially only one thing it can say there.

Example. Alternating Forms on a Plane

Describe all alternating bilinear forms on F^2 , and decide which are nondegenerate.

Solution. An alternating 2×2 matrix has zero diagonal and $a_{21} = -a_{12}$, so it is

$$\mathbf{A} = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$$

for a single scalar $a \in F$, and every such matrix is alternating. By Theorem 14.1.1 the corresponding form is $\beta(\mathbf{x}, \mathbf{y}) = a(x_1y_2 - x_2y_1)$. Its determinant is a^2 , so by Proposition 14.1.2 the form is nondegenerate exactly when $a \neq 0$.

When $a \neq 0$, replacing the basis vector $\mathbf{e}_2$ by $a^{-1}\mathbf{e}_2$ replaces a by 1. So up to a change of basis there are exactly **two** alternating forms on F^2 : the zero form and the one with matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, whatever the field.

That last matrix is the atom of the theory, and the pair of vectors producing it deserves a name. It is the alternating counterpart of the hyperbolic plane of Section 7: a two-dimensional space

carrying a nondegenerate form on which the associated quadratic function vanishes identically. Here the vanishing is automatic, because *every* alternating form vanishes on the diagonal, so the whole content is in the pairing.

A hyperbolic pair is two vectors that pair to 1 and to nothing else.

Definition 14.9.1. Hyperbolic Pair

Let β be an alternating form on V . A **hyperbolic pair** for β is an ordered pair (u, w) of vectors of V with

$$\beta(u, w) = 1.$$

Its **span** $H = \text{span}(u, w)$ is called a **hyperbolic plane** for β .

The definition looks as though it asks for one condition, but it quietly supplies three more. Alternation already gives $\beta(u, u) = \beta(w, w) = 0$, and skewness gives $\beta(w, u) = -1$. So the matrix of β restricted to H in the ordered basis (u, w) is exactly $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Also, u and w are automatically linearly independent: if $w = cu$ then $\beta(u, w) = c\beta(u, u) = 0 \neq 1$, and $u \neq 0$ for the same reason. So H really is a plane, $\dim H = 2$, and β restricted to H is nondegenerate.

Warning. An alternating form is never diagonalizable, except when it is zero. Section 4 found an orthogonal basis for every symmetric form in characteristic $\neq 2$; no such basis exists here. If $\mathcal{B}$ is any basis and $[\beta]_{\mathcal{B}}^{\mathcal{B}}$ is diagonal, then its off-diagonal entries vanish by assumption and its diagonal entries vanish because β is alternating, so $[\beta]_{\mathcal{B}}^{\mathcal{B}} = \mathbf{O}$ and $\beta = 0$. The standard form below is a block form, and it has to be: the 2×2 block is irreducible.

14.9.2 Splitting off a hyperbolic pair

The move that drives the whole section is the one Section 7 used for isotropic vectors: find a small nondegenerate piece, and cut the space along it. Here the small piece is a hyperbolic plane, and it can always be found as soon as β is not identically zero.

Lemma 14.9.1. Peeling Off a Hyperbolic Plane

Let β be an alternating form on a finite-dimensional V , and suppose $\beta \neq 0$.

- (a) There is a hyperbolic pair (u, w) for β .
- (b) For any such pair, with $H = \text{span}(u, w)$ and

$$H^{\perp\beta} = \{v \in V : \beta(u, v) = \beta(w, v) = 0\},$$

we have $V = H \oplus H^{\perp\beta}$ and $\dim H^{\perp\beta} = \dim V - 2$.

- (c) $\text{rad}(\beta) = \text{rad}(\beta|_{H^{\perp\beta}})$. In particular, if β is nondegenerate then so is its restriction to $H^{\perp\beta}$.

Idea. For (a), the hypothesis $\beta \neq 0$ hands us two vectors pairing to something nonzero; divide one of them by that scalar. For (b), the two conditions cutting out $H^{\perp\beta}$ are two linear conditions, so the count should be $\dim V - 2$, and Rank–Nullity will say so once we check that the two conditions are independent — which is exactly what $\beta(u, w) = 1$ provides.

Part (c) is the bookkeeping that lets the induction in the theorem keep its hypothesis.

Proof.

- (a) Since $\beta \neq 0$ there are $u_0, w_0 \in V$ with $c := \beta(u_0, w_0) \neq 0$. Put $u = u_0$ and $w = c^{-1}w_0$, which is legitimate because $c \neq 0$ and F is a field. Then $\beta(u, w) = c^{-1}\beta(u_0, w_0) = 1$ by linearity in the second argument.
- (b) Define $\varphi: V \rightarrow F^2$ by $\varphi(v) = (\beta(u, v), \beta(w, v))$. It is linear, because β is linear in its second argument, and $\ker \varphi = H^{\perp_\beta}$ by the definition of $H^{\perp_\beta}$. It is surjective:

$$\varphi(w) = (\beta(u, w), \beta(w, w)) = (1, 0), \quad \varphi(u) = (0, -1),$$

using $\beta(w, w) = \beta(u, u) = 0$ and $\beta(w, u) = -1$, and these two values span F^2 . Hence $\text{rank } \varphi = 2$ and $\dim H^{\perp_\beta} = \dim V - 2$ by Rank–Nullity (Theorem 2.3.1).

Next, $H \cap H^{\perp_\beta} = \{0\}$. Let $v = au + bw$ lie in $H^{\perp_\beta}$. Then $0 = \beta(u, v) = a\beta(u, u) + b\beta(u, w) = b$, and $0 = \beta(w, v) = a\beta(w, u) = -a$, so $a = b = 0$. Hence the sum $H + H^{\perp_\beta}$ is direct (Theorem 1.7.4), and by Theorem 1.7.3 its dimension is $2 + (\dim V - 2) = \dim V$, so it is all of V (Theorem 1.6.8).

- (c) ($\supseteq$) Let $v \in H^{\perp_\beta}$ satisfy $\beta(z, v) = 0$ for every $z \in H^{\perp_\beta}$. Any $y \in V$ decomposes as $y = h + z$ with $h \in H$ and $z \in H^{\perp_\beta}$ by (b), and $\beta(h, v) = -\beta(v, h) = 0$ because $v \in H^{\perp_\beta}$ and h is a combination of u and w . Hence $\beta(y, v) = 0$ for every $y \in V$, so $v \in \text{rad}(\beta)$.

($\subseteq$) Let $v \in \text{rad}(\beta)$. Then in particular $\beta(u, v) = \beta(w, v) = 0$, so $v \in H^{\perp_\beta}$, and $\beta(z, v) = 0$ for every z at all, so v lies in the radical of the restriction. This proves the lemma. ■

Notice what the proof did **not** use: it never divided by 2, never distinguished β from $-\beta$, and never needed a vector with $\beta(v, v) \neq 0$ — which is fortunate, since no such vector exists. Compare the corresponding step for symmetric forms, Lemma 14.4.1 in Section 4: there the whole difficulty was producing a vector on which the quadratic form did not vanish, and producing it cost the hypothesis $\text{char } F \neq 2$. Here the quadratic form vanishes everywhere and we do not care.

14.9.3 The standard form

With the lemma in hand the classification is an induction that peels two dimensions at a time.

Theorem 14.9.2. Standard Form of an Alternating Form

Let F be **any** field, let V be a vector space over F with $\dim V = n$, and let β be an alternating bilinear form on V . Then there are an integer $m \geq 0$ with $2m \leq n$ and a basis

$$\mathcal{B} = (u_1, \dots, u_m, w_1, \dots, w_m, z_1, \dots, z_{n-2m})$$

of V such that, for all i, j ,

$$\beta(u_i, w_j) = \delta_{ij}, \quad \beta(u_i, u_j) = \beta(w_i, w_j) = 0,$$

and $\beta(z_k, v) = 0$ for every k and every $v \in V$. Equivalently, in this basis

$$[\beta]_{\mathcal{B}}^{\mathcal{B}} = \Omega_{2m} \oplus \mathbf{O}_{n-2m}, \quad \Omega_{2m} := \begin{pmatrix} \mathbf{O} & \mathbf{I}_m \\ -\mathbf{I}_m & \mathbf{O} \end{pmatrix}. \quad (14.9.1)$$

In particular:

- (a) every alternating $\mathbf{A} \in M_n(F)$ is congruent to $\Omega_{2m} \oplus \mathbf{O}_{n-2m}$ for exactly one m ;
- (b) if β is nondegenerate then $n = 2m$ is **even** and $[\beta]_{\mathcal{B}}^{\mathcal{B}} = \Omega_n$.

Idea. Induction on n , two dimensions at a time. ① If $\beta = 0$, take $m = 0$ and any basis; this is the base case and also the case that stops the recursion. ② Otherwise [Lemma 14.9.1](#) produces a hyperbolic pair (u_1, w_1) and splits $V = H \oplus H^{\perp\beta}$ with $\dim H^{\perp\beta} = n - 2$; apply the induction hypothesis to β restricted to $H^{\perp\beta}$, and put the pieces together. ③ Finally reorder the basis so that all the u 's come before all the w 's, which turns a string of 2×2 blocks into the one block matrix displayed. The radical, by part (c) of the lemma, is exactly what the last stage of the recursion leaves behind.

Proof. Existence, by induction on $n = \dim V$. For $n = 0$ and $n = 1$ every alternating form is zero: in dimension 1, $\beta(cv, dv) = cd\beta(v, v) = 0$. Take $m = 0$.

Let $n \geq 2$ and assume the statement for all spaces of dimension less than n .

Case 1: $\beta = 0$. Take $m = 0$ and any basis of V ; every required equation reads $0 = 0$.

Case 2: $\beta \neq 0$. By [Lemma 14.9.1](#) (a) there is a hyperbolic pair (u_1, w_1) , and by (b) we have $V = H \oplus W$ with $H = \text{span}(u_1, w_1)$ and $W = H^{\perp\beta}$ of dimension $n - 2$. The restriction $\beta|_W$ is again alternating, being a restriction of an alternating form, so the induction hypothesis applies to it: there is a basis

$$(u_2, \dots, u_m, w_2, \dots, w_m, z_1, \dots, z_{n-2m})$$

of W in which $\beta|_W(u_i, w_j) = \delta_{ij}$, all other pairings among the u 's and w 's vanish, and each z_k lies in $\text{rad}(\beta|_W)$.

Putting u_1 and w_1 in front gives a basis of $V = H \oplus W$. The required equations hold: within H they are the definition of a hyperbolic pair together with alternation; within W they are the induction hypothesis; and across the two, every pairing of u_1 or w_1 with a vector of W vanishes because $W = H^{\perp\beta}$ and β is skew-symmetric. Finally each z_k lies in $\text{rad}(\beta|_W) = \text{rad}(\beta)$ by [Lemma 14.9.1](#) (c), which is the last assertion.

The matrix. Order the basis as $\mathcal{B} = (u_1, \dots, u_m, w_1, \dots, w_m, z_1, \dots, z_{n-2m})$. By Definition 14.1.2 the (i, j) entry of $[\beta]_{\mathcal{B}}^{\mathcal{B}}$ is the pairing of the i -th and j -th basis vectors, and the equations above say precisely that the top-left $m \times m$ block and the w - w block are $\mathbf{O}$, the u - w block is $\mathbf{I}_m$, the w - u block is $-\mathbf{I}_m$, and every row and column indexed by a z_k is zero. That is [Eq. 14.9.1](#).

(a). Given alternating $\mathbf{A} \in M_n(F)$, let $\beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^{\top} \mathbf{A} \mathbf{y}$ on F^n ; it is alternating by Proposition 14.3.2 (b). The basis just constructed gives $\mathbf{P}^{\top} \mathbf{A} \mathbf{P} = \Omega_{2m} \oplus \mathbf{O}_{n-2m}$ with $\mathbf{P}$ the matrix whose columns are the basis vectors, by Theorem 14.2.1, so $\mathbf{A} \simeq \Omega_{2m} \oplus \mathbf{O}_{n-2m}$. Uniqueness

of m : congruence preserves rank (Theorem 14.2.3), and $\text{rank}(\Omega_{2m} \oplus \mathbf{O}_{n-2m}) = 2m$ because Ω_{2m} is invertible, its square being $-\mathbf{I}_{2m}$. So $2m = \text{rank } \mathbf{A}$ is determined by $\mathbf{A}$.

(b). If β is nondegenerate then $\text{rad}(\beta) = \{0\}$ by Definition 14.1.4, so there are no z_k , that is $n = 2m$. This proves the theorem. ■

Definition 14.9.2. Symplectic Basis

A basis of V as in Theorem 14.9.2 is a **symplectic basis**, or a **Darboux basis**, for the alternating form β . A nondegenerate alternating form on a finite-dimensional space is called a **symplectic form**, and the pair (V, β) a **symplectic vector space**.

Now read the hypotheses of the theorem again, and notice what is missing. There is no “char $F \neq 2$ ”, and there is no place one could be inserted, because no step of the proof divided by 2. Compare the statements this chapter has accumulated:

- Theorem 14.3.3: skew implies alternating only when $\text{char } F \neq 2$.
- Theorem 14.3.4: the splitting into halves exists only when $\text{char } F \neq 2$.
- Theorem 14.3.5: a symmetric form is recovered from its quadratic form only when $\text{char } F \neq 2$.
- Theorem 14.4.2: a symmetric form has an orthogonal basis only when $\text{char } F \neq 2$.
- Theorem 14.9.2: no hypothesis.

Over $\mathbb{F}_2$, where every one of the first four statements is false, the last one is true and gives a complete classification. The reason is visible in the proof: the symmetric theory needs a vector with $q(v) \neq 0$, and that vector is manufactured by a polarization identity that divides by 2. The alternating theory needs a *pair* with $\beta(u, w) \neq 0$, and a pair is handed over by the assumption $\beta \neq 0$ itself, free of charge. Symmetric forms are hard in characteristic 2; alternating forms are not hard anywhere.

Quick check. Over $\mathbb{F}_2$ we have $-1 = 1$, so $\Omega_{2m} = \begin{pmatrix} \mathbf{O} & \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{O} \end{pmatrix}$, which is a **symmetric** matrix. Does that contradict the warning above, that an alternating form is never diagonalizable?

Solution. No. Over $\mathbb{F}_2$ every alternating matrix is symmetric, since skew-symmetric and symmetric are the same condition there (Theorem 14.3.3 and the warning after it). What distinguishes alternating from merely symmetric over $\mathbb{F}_2$ is the zero diagonal, and Ω_{2m} does have a zero diagonal. The warning says a **diagonal** alternating matrix must be $\mathbf{O}$, and Ω_{2m} is symmetric but not diagonal. Concretely, over $\mathbb{F}_2$ the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the Gram matrix of the alternating form $\beta(\mathbf{x}, \mathbf{y}) = x_1y_2 + x_2y_1$, and no change of basis makes it diagonal.

14.9.4 Running the algorithm

The proof is an algorithm, and it is short enough to carry out by hand. Each round of the induction does three things: find a pair with $\beta(u, w) \neq 0$, rescale to make the value 1, and then correct every remaining basis vector so that it becomes orthogonal to both. The correction is a

formula worth recording. If $\beta(u, w) = 1$, put

$$v' := v - \beta(v, w)u + \beta(v, u)w. \quad (14.9.2)$$

Expanding and using $\beta(u, u) = \beta(w, w) = 0$, $\beta(u, w) = 1$, and $\beta(w, u) = -1$,

$$\begin{aligned} \beta(v', u) &= \beta(v, u) - \beta(v, w) \cdot 0 + \beta(v, u) \cdot (-1) = 0, \\ \beta(v', w) &= \beta(v, w) - \beta(v, w) \cdot 1 + \beta(v, u) \cdot 0 = 0, \end{aligned}$$

so $v' \in H^{\perp\beta}$. It is the alternating analogue of subtracting a projection in Gram–Schmidt, with one difference: nothing is divided by a length, so it works over any field.

Example. A Symplectic Basis for a 4×4 Form

Let $\beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top \mathbf{A} \mathbf{y}$ on $\mathbb{Q}^4$, where

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 0 & 1 & 1 \\ -2 & -1 & 0 & 0 \\ -3 & -1 & 0 & 0 \end{pmatrix}.$$

Find a symplectic basis, and the matrix $\mathbf{P}$ with $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \mathbf{\Omega}_4$.

Solution. The matrix is skew-symmetric with zero diagonal, so β is alternating (Proposition 14.3.2 (b)).

Round 1. The entry $a_{12} = \beta(\mathbf{e}_1, \mathbf{e}_2) = 1$ is already 1, so $(\mathbf{u}_1, \mathbf{w}_1) = (\mathbf{e}_1, \mathbf{e}_2)$ is a hyperbolic pair and no rescaling is needed. Correct $\mathbf{e}_3$ and $\mathbf{e}_4$ by Eq. 14.9.2, reading the needed values off the matrix: $\beta(\mathbf{e}_3, \mathbf{e}_2) = a_{32} = -1$, $\beta(\mathbf{e}_3, \mathbf{e}_1) = a_{31} = -2$, $\beta(\mathbf{e}_4, \mathbf{e}_2) = a_{42} = -1$, $\beta(\mathbf{e}_4, \mathbf{e}_1) = a_{41} = -3$. So

$$\begin{aligned} \mathbf{v}_3 &= \mathbf{e}_3 + \mathbf{e}_1 - 2\mathbf{e}_2 = (1, -2, 1, 0), \\ \mathbf{v}_4 &= \mathbf{e}_4 + \mathbf{e}_1 - 3\mathbf{e}_2 = (1, -3, 0, 1). \end{aligned}$$

Round 2. Both $\mathbf{v}_3$ and $\mathbf{v}_4$ pair to zero with $\mathbf{e}_1$ and $\mathbf{e}_2$, as the formula guarantees, so the recursion continues inside $\text{span}(\mathbf{v}_3, \mathbf{v}_4)$. Compute $\mathbf{A} \mathbf{v}_4$ row by row with $\mathbf{v}_4 = (1, -3, 0, 1)$: row 1 gives $0 - 3 + 0 + 3 = 0$, row 2 gives $-1 + 0 + 0 + 1 = 0$, row 3 gives $-2 + 3 + 0 + 0 = 1$, row 4 gives $-3 + 3 + 0 + 0 = 0$. So $\mathbf{A} \mathbf{v}_4 = (0, 0, 1, 0)^\top$, and

$$\beta(\mathbf{v}_3, \mathbf{v}_4) = \mathbf{v}_3^\top (\mathbf{A} \mathbf{v}_4) = 1 \cdot 0 + (-2) \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 1.$$

The pair $(\mathbf{u}_2, \mathbf{w}_2) = (\mathbf{v}_3, \mathbf{v}_4)$ is therefore hyperbolic, and the recursion stops: the two remaining dimensions are used up.

The answer. The symplectic basis is $\mathcal{B} = (\mathbf{e}_1, \mathbf{v}_3, \mathbf{e}_2, \mathbf{v}_4)$, listing the $\mathbf{u}$'s first and then the $\mathbf{w}$'s. The matrix whose columns are these four vectors is

$$\mathbf{P} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -2 & 1 & -3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{P}^\top \mathbf{A} \mathbf{P} = \mathbf{\Omega}_4.$$

A check of two entries confirms the pattern: the $(1, 3)$ entry of $\mathbf{P}^\top \mathbf{A} \mathbf{P}$ is $\beta(\mathbf{e}_1, \mathbf{e}_2) = 1$ and the $(2, 4)$ entry is $\beta(\mathbf{v}_3, \mathbf{v}_4) = 1$, while the $(1, 2)$ entry is $\beta(\mathbf{e}_1, \mathbf{v}_3) = a_{11} + a_{12}(-2) + a_{13} = 0 - 2 + 2 = 0$.

14.9.5 What the standard form classifies

The theorem is a classification, and it is worth reading off exactly what it classifies and how coarsely.

Corollary 14.9.3. Alternating Matrices Are Classified by Rank

Let F be any field and let $\mathbf{A}, \mathbf{B} \in M_n(F)$ be alternating.

- (a) rank $\mathbf{A}$ is **even**.
- (b) $\mathbf{A} \simeq \mathbf{B}$ if and only if rank $\mathbf{A} = \text{rank } \mathbf{B}$.
- (c) There are exactly $\lfloor n/2 \rfloor + 1$ congruence classes of alternating matrices in $M_n(F)$, one for each even rank $0, 2, 4, \dots$ up to n .
- (d) If n is odd, every alternating $\mathbf{A} \in M_n(F)$ is singular.

Proof.

- (a) By Theorem 14.9.2 (a), $\mathbf{A} \simeq \Omega_{2m} \oplus \mathbf{O}_{n-2m}$ for some m , and congruence preserves rank (Theorem 14.2.3), so rank $\mathbf{A} = 2m$.
- (b) $(\Rightarrow)$ is Theorem 14.2.3. $(\Leftarrow)$ If rank $\mathbf{A} = \text{rank } \mathbf{B} = 2m$ then by (a) and Theorem 14.9.2 both are congruent to $\Omega_{2m} \oplus \mathbf{O}_{n-2m}$, and congruence is an equivalence relation (Proposition 14.2.2), so $\mathbf{A} \simeq \mathbf{B}$.
- (c) By (a) and (b) the classes are in bijection with the even integers $2m$ satisfying $0 \leq 2m \leq n$, and there are $\lfloor n/2 \rfloor + 1$ of those.
- (d) By (a), rank $\mathbf{A}$ is even and at most n ; since n is odd, rank $\mathbf{A} \leq n - 1 < n$, so $\mathbf{A}$ is not invertible. ■

Part (d) deserves a second look, because there is a one-line proof of it that works only half the time. If $\mathbf{A}^\top = -\mathbf{A}$ with n odd, then $\det \mathbf{A} = \det(\mathbf{A}^\top) = \det(-\mathbf{A}) = (-1)^n \det \mathbf{A} = -\det \mathbf{A}$, so $(1 + 1)\det \mathbf{A} = 0$ and $\det \mathbf{A} = 0$ — provided $1 + 1 \neq 0$. In characteristic 2 that argument collapses, and it collapses for a real reason: over $\mathbb{F}_2$ the matrix $\text{diag}(1, 0, 0)$ is skew-symmetric (because skew means symmetric there) and has odd rank 1. Part (d) survives because it is a statement about *alternating* matrices, and the standard form proves it without ever touching the determinant.

Warning. “Skew-symmetric” is not enough. Every statement in Corollary 14.9.3 is about alternating matrices: skew-symmetric **with zero diagonal**. Over $\mathbb{F}_2$, $\mathbf{I}_2$ is skew-symmetric and has rank 2, which is harmless; but $\text{diag}(1, 0) \in M_2(\mathbb{F}_2)$ is skew-symmetric of rank 1, and $\mathbf{I}_3 \in M_3(\mathbb{F}_2)$ is skew-symmetric and invertible. Both would contradict the corollary if “skew-symmetric” could be substituted for “alternating”. In characteristic $\neq 2$ the two words agree (Theorem 14.3.3 (b)) and the distinction can be forgotten; nowhere else.

14.9.6 The determinant, and the Pfaffian

Part (a) of [Theorem 14.9.2](#) says that in even size an invertible alternating matrix is congruent to Ω_n . Congruence multiplies the determinant by a square ([Theorem 14.2.5](#)), so the determinant of an alternating matrix is heavily constrained.

Corollary 14.9.4. The Determinant of an Alternating Matrix Is a Square

Let F be any field and let $\mathbf{A} \in M_n(F)$ be alternating. Then $\det \mathbf{A}$ is a square in F : there is $c \in F$ with $\det \mathbf{A} = c^2$.

Proof. If $\mathbf{A}$ is singular then $\det \mathbf{A} = 0 = 0^2$. So assume $\mathbf{A}$ is invertible. Then $\text{rank } \mathbf{A} = n$ is even by [Corollary 14.9.3](#) (a), say $n = 2m$, and [Theorem 14.9.2](#) (a) supplies an invertible $\mathbf{P}$ with $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \Omega_{2m}$. Taking determinants and using [Theorem 14.2.5](#),

$$\det \Omega_{2m} = (\det \mathbf{P})^2 \det \mathbf{A}.$$

Now $\det \Omega_{2m} = 1$. Indeed, performing the m row swaps $R_i \leftrightarrow R_{m+i}$ for $i = 1, \dots, m$ turns Ω_{2m} into $(-\mathbf{I}_m) \oplus \mathbf{I}_m$, so by [Theorem 7.5.1](#) (a) and [Theorem 7.8.4](#),

$$(-1)^m \det \Omega_{2m} = \det((-\mathbf{I}_m) \oplus \mathbf{I}_m) = (-1)^m,$$

and $(-1)^m$ is invertible, so $\det \Omega_{2m} = 1$. Hence $\det \mathbf{A} = (\det \mathbf{P})^{-2} = ((\det \mathbf{P})^{-1})^2$, a square, since $\det \mathbf{P} \neq 0$. This proves the corollary. ■

The corollary says a square root of $\det \mathbf{A}$ exists; it does not produce one. In fact there is a canonical choice. For every even n there is a polynomial Pf in the entries a_{ij} with $i < j$, with integer coefficients, called the **Pfaffian**, satisfying $\det \mathbf{A} = \text{Pf}(\mathbf{A})^2$ for every alternating $\mathbf{A}$. Constructing it in general is a piece of multilinear algebra that we do not carry out, so we record only the name and the two smallest cases, both of which can be checked by expanding the determinant.

Example. The Pfaffian in Sizes 2 and 4

For $n = 2$,

$$\mathbf{A} = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}, \quad \det \mathbf{A} = a^2, \quad \text{Pf}(\mathbf{A}) = a.$$

For $n = 4$, write the six independent entries as $a = a_{12}$, $b = a_{13}$, $c = a_{14}$, $d = a_{23}$, $e = a_{24}$, $f = a_{34}$. Expanding the 4×4 determinant gives

$$\det \mathbf{A} = (af - be + cd)^2, \quad \text{Pf}(\mathbf{A}) = af - be + cd.$$

The three terms pair up $\{1, 2\}\{3, 4\}$, $\{1, 3\}\{2, 4\}$, and $\{1, 4\}\{2, 3\}$: the Pfaffian sums over the ways of splitting $\{1, 2, 3, 4\}$ into two pairs, with a sign. For the matrix $\mathbf{A}$ of [Example \(A Symplectic Basis for a \$4 \times 4\$ Form\)](#) this reads $\text{Pf}(\mathbf{A}) = 1 \cdot 0 - 2 \cdot 1 + 3 \cdot 1 = 1$, and indeed $\det \mathbf{A} = 1$.

Remark. The Pfaffian is not merely a square root: it is the one that behaves well under congruence, satisfying $\text{Pf}(\mathbf{P}^\top \mathbf{A} \mathbf{P}) = \det(\mathbf{P}) \text{Pf}(\mathbf{A})$. That identity is the reason the Pfaffian matters. Section 10 records one of its consequences for the symplectic group, without proof and without leaning on it. We do not prove the identity either.

14.9.7 Symmetric against alternating

Put the two halves of the chapter side by side. Both are theories of a bilinear form under congruence; the answers could hardly be more different.

	Symmetric forms	Alternating forms
Field hypothesis	$\text{char } F \neq 2$ for every theorem	none
Canonical form	diagonal, entries not canonical	$\Omega_{2m} \oplus \mathbf{O}_{n-2m}$
Complete invariants	rank and more: over $\mathbb{R}$ the signature, over $\mathbb{Q}$ the discriminant and local data	rank alone
Classes in $M_n(\mathbb{R})$	$\frac{1}{2}(n+1)(n+2)$	$\lfloor n/2 \rfloor + 1$
Classes in $M_n(\mathbb{C})$	$n+1$	$\lfloor n/2 \rfloor + 1$
Classes in $M_n(\mathbb{Q})$	infinitely many already for $n=1$	$\lfloor n/2 \rfloor + 1$
Possible ranks	every r with $0 \leq r \leq n$	even r only
Effect of the field	decisive	none

Two entries carry the point. Over $\mathbb{Q}$, the 1×1 symmetric matrices $[1], [2], [3], [5], \dots$ are pairwise noncongruent, because congruence in size 1 multiplies by a nonzero square (Theorem 14.2.5) and distinct squarefree positive integers lie in distinct classes of $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$. So the symmetric classification over $\mathbb{Q}$ is an infinite problem in number theory — Section 4 said as much. The alternating classification over $\mathbb{Q}$ has four classes in size 6, and the same four over $\mathbb{F}_2$, over $\mathbb{R}$, and over any field whatsoever.

The reason, one last time, is the two-dimensional model. A symmetric form on a line is $c \mapsto ac^2$, and rescaling changes a by a square, so the diagonal entry carries the field's arithmetic with it. An alternating form on a plane is $\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$, and rescaling *one* of the two basis vectors changes a to ca for any $c \neq 0$ — an arbitrary nonzero scalar, not a square. There is nothing left for the field to remember.

14.9.8 Exercises

14.9.8.1 A. Check your understanding

Exercise. A1

- Define a hyperbolic pair for an alternating form, and say why its two vectors are automatically linearly independent.
- State [Theorem 14.9.2](#), and say which hypothesis on F it needs.
- Determine whether the following is correct: every skew-symmetric matrix over every

field has even rank. Justify your answer.

- (d) Why can an alternating form never have a diagonal Gram matrix, unless the form is zero?
- (e) How many congruence classes of alternating matrices are there in $M_5(\mathbb{R})$? In $M_5(\mathbb{F}_7)$?

Solution.

- (a) A pair (u, w) with $\beta(u, w) = 1$ (Definition 14.9.1). If $w = cu$, then $\beta(u, w) = c\beta(u, u) = 0 \neq 1$, so $w \notin \text{span}(u)$; and $u \neq 0$ since $\beta(0, w) = 0$. Two vectors, neither in the span of the other, are independent.
- (b) Every alternating form on an n -dimensional V has a basis in which its matrix is $\Omega_{2m} \oplus \mathbf{O}_{n-2m}$, with $2m = \text{rank } \beta$; equivalently every alternating matrix is congruent to exactly one such matrix. **No** hypothesis on F is needed — in particular none on $\text{char } F$.
- (c) Incorrect. Over $\mathbb{F}_2$, $\text{diag}(1, 0)$ is skew-symmetric, because $-1 = 1$ makes skew-symmetric and symmetric the same condition, and it has rank 1. The correct statement is about **alternating** matrices, Corollary 14.9.3 (a). In characteristic $\neq 2$ the two notions coincide (Theorem 14.3.3 (b)) and the statement is true.
- (d) The off-diagonal entries of a diagonal matrix are 0 by definition, and the diagonal entries of the Gram matrix of an alternating form are $\beta(v_i, v_i) = 0$. So the whole matrix is $\mathbf{O}$, and then $\beta = 0$ by Theorem 14.1.1 (b).
- (e) $\lfloor 5/2 \rfloor + 1 = 3$ in both cases, by Corollary 14.9.3 (c): the ranks 0, 2, 4. The field makes no difference.

14.9.8.2 B. Practice

Exercise. B1: A symplectic basis

Let $\beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top \mathbf{B} \mathbf{y}$ on $\mathbb{Q}^4$, with

$$\mathbf{B} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ -1 & -2 & 0 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix}.$$

Find a symplectic basis for β and an invertible $\mathbf{P} \in M_4(\mathbb{Q})$ with $\mathbf{P}^\top \mathbf{B} \mathbf{P} = \Omega_4$.

Solution. $\mathbf{B}$ is skew-symmetric with zero diagonal, hence alternating (Proposition 14.3.2 (b)).

Round 1. Here $\beta(\mathbf{e}_1, \mathbf{e}_2) = 0$, so the first two standard basis vectors are **not** a hyperbolic pair; this is the step the worked example did not need. Look for any nonzero entry: $\beta(\mathbf{e}_1, \mathbf{e}_3) = 1$. Take $\mathbf{u}_1 = \mathbf{e}_1$, $\mathbf{w}_1 = \mathbf{e}_3$.

Correct the other two by Eq. 14.9.2, using $\beta(\mathbf{e}_2, \mathbf{e}_3) = 2$, $\beta(\mathbf{e}_2, \mathbf{e}_1) = 0$, $\beta(\mathbf{e}_4, \mathbf{e}_3) = 0$, $\beta(\mathbf{e}_4, \mathbf{e}_1) = -1$:

$$\mathbf{v}_2 = \mathbf{e}_2 - 2\mathbf{e}_1 + 0 \cdot \mathbf{e}_3 = (-2, 1, 0, 0),$$

$$\mathbf{v}_4 = \mathbf{e}_4 - 0 \cdot \mathbf{e}_1 - \mathbf{e}_3 = (0, 0, -1, 1).$$

Round 2. Compute $\mathbf{B}\mathbf{v}_4$ with $\mathbf{v}_4 = (0, 0, -1, 1)$: row 1 gives $-1 + 1 = 0$, row 2 gives $-2 + 1 = -1$, rows 3 and 4 give 0. So $\mathbf{B}\mathbf{v}_4 = (0, -1, 0, 0)^\top$ and

$$\beta(\mathbf{v}_2, \mathbf{v}_4) = \mathbf{v}_2^\top (\mathbf{B}\mathbf{v}_4) = (-2) \cdot 0 + 1 \cdot (-1) = -1.$$

This is nonzero but not 1, so rescale: replace $\mathbf{v}_4$ by $\mathbf{w}_2 := -\mathbf{v}_4 = (0, 0, 1, -1)$, giving $\beta(\mathbf{v}_2, \mathbf{w}_2) = 1$. Set $\mathbf{u}_2 = \mathbf{v}_2$.

The answer. The symplectic basis is $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{w}_1, \mathbf{w}_2) = (\mathbf{e}_1, (-2, 1, 0, 0), \mathbf{e}_3, (0, 0, 1, -1))$, so

$$\mathbf{P} = \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathbf{P}^\top \mathbf{B} \mathbf{P} = \mathbf{\Omega}_4.$$

$\mathbf{P}$ is invertible, being block upper triangular with invertible diagonal blocks, and $\det \mathbf{P} = -1 \neq 0$.

Exercise. B2: Pfaffians and determinants

For each matrix below, compute the Pfaffian using the formula of [Example \(The Pfaffian in Sizes 2 and 4\)](#), and verify that its square is the determinant.

$$\mathbf{A}_1 = \begin{pmatrix} 0 & 2 & 0 & 1 \\ -2 & 0 & 1 & 0 \\ 0 & -1 & 0 & 3 \\ -1 & 0 & -3 & 0 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 0 \end{pmatrix}.$$

Hence write down, for each, an invertible matrix congruence class in the sense of [Corollary 14.9.3](#).

Solution. For $\mathbf{A}_1$: $a = 2, b = 0, c = 1, d = 1, e = 0, f = 3$, so $\text{Pf}(\mathbf{A}_1) = af - be + cd = 6 - 0 + 1 = 7$ and $\det \mathbf{A}_1 = 49$. Expanding the determinant along the first row confirms 49.

For $\mathbf{A}_2$: $a = b = c = d = e = f = 1$, so $\text{Pf}(\mathbf{A}_2) = 1 - 1 + 1 = 1$ and $\det \mathbf{A}_2 = 1$.

Both determinants are nonzero, so both matrices have rank 4, and by [Corollary 14.9.3](#) (b) both lie in the single congruence class of invertible alternating matrices in $M_4(\mathbb{Q})$: each is congruent to $\mathbf{\Omega}_4$, and therefore $\mathbf{A}_1 \simeq \mathbf{A}_2$. Note that the two have different determinants, 49 and 1; congruence changes the determinant by a square (Theorem 14.2.5), and $49 = 7^2$.

Exercise. B3: Determine which of the following

Determine which of the following matrices are alternating, and for those that are, give the rank and the standard form $\mathbf{\Omega}_{2m} \oplus \mathbf{O}_{n-2m}$ it is congruent to. Justify your answer.

- (a) $\begin{pmatrix} 0 & 5 \\ -5 & 0 \end{pmatrix}$ over $\mathbb{Q}$.
- (b) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ over $\mathbb{Q}$.
- (c) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ over $\mathbb{F}_2$.

- (d) The 5×5 matrix with $a_{ij} = j - i$ over $\mathbb{Q}$.

Solution.

- (a) Alternating: zero diagonal and $a_{21} = -a_{12}$. Its determinant is $25 \neq 0$, so the rank is 2 and it is congruent to Ω_2 . (Explicitly, scaling the second basis vector by $1/5$ does it.)
- (b) Not alternating. It is symmetric with $a_{12} = 1 \neq -1 = -a_{21}$, so it is not even skew-symmetric over $\mathbb{Q}$.
- (c) Alternating. Over $\mathbb{F}_2$ we have $1 = -1$, so the matrix is skew-symmetric, and its diagonal is zero. Its determinant is $-1 = 1 \neq 0$, so the rank is 2 and it is congruent to $\Omega_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ — it **is** Ω_2 , since $-1 = 1$. Comparing (b) and (c): the same array of symbols is alternating over one field and not over another.
- (d) Alternating: $a_{ii} = 0$ and $a_{ji} = i - j = -a_{ij}$. Its rank is even by Corollary 14.9.3 (a), and it is not zero, so the rank is 2 or 4. Every row is a combination of $(1, 2, 3, 4, 5)$ and $(1, 1, 1, 1, 1)$: indeed row i is $(j - i)_j = (1, 2, 3, 4, 5) - i(1, 1, 1, 1, 1)$. So the row space has dimension at most 2, and rows 1 and 2 are independent, giving rank exactly 2. Hence the matrix is congruent to $\Omega_2 \oplus \mathbf{O}_3$. In particular it is singular, as Corollary 14.9.3 (d) requires for odd size.

14.9.8.3 C. Going deeper

Exercise. C1: Lagrangian subspaces

Let β be a symplectic form on V with $\dim V = 2m$ (Definition 14.9.2), and call a subspace $U \subseteq V$ **totally isotropic** if $\beta(u, u') = 0$ for all $u, u' \in U$.

- (a) Prove that $\text{span}(u_1, \dots, u_m)$ is totally isotropic, for any symplectic basis.
- (b) Prove that every totally isotropic subspace satisfies $\dim U \leq m$.
- (c) Deduce that a symplectic form on a space of dimension $2m$ has a totally isotropic subspace of dimension exactly m , and no larger one. (These are the **Lagrangian** subspaces.)

Hint for (b): compare U with $U^{\perp_\beta}$ of Exercise (C2: Orthogonal complements for a form).

Solution.

- (a) By Theorem 14.9.2, $\beta(u_i, u_j) = 0$ for all i, j . A general pair of elements of the span is $\sum_i c_i u_i$ and $\sum_j d_j u_j$, and bilinearity gives $\sum_{i,j} c_i d_j \beta(u_i, u_j) = 0$.
- (b) Let U be totally isotropic. By definition $\beta(u, v) = 0$ for all $u \in U$ and all $v \in U$, so $U \subseteq U^{\perp_\beta}$. Since β is nondegenerate, $\dim U^{\perp_\beta} = 2m - \dim U$ by Exercise (C2: Orthogonal complements for a form) (b). Therefore

$$\dim U \leq 2m - \dim U,$$

that is $2\dim U \leq 2m$. Both sides are integers, so $\dim U \leq m$. (No division by 2 inside the field occurs here: the inequality is between integers, not field elements, so the argument is valid in every characteristic.)

- (c) The subspace of (a) has dimension m , since the u_i are part of a basis, and it is totally

isotropic; by (b) no totally isotropic subspace has dimension greater than m .

Exercise. C2: The inverse of an alternating matrix

Let F be any field.

- (a) Prove that every alternating matrix of **odd** size over F is singular, without using determinants.
- (b) Let $\mathbf{A} \in M_n(F)$ be alternating and invertible. Prove that $\mathbf{A}^{-1}$ is alternating.

Hint for (b): the adjugate. The (i, i) entry of $\text{adj } \mathbf{A}$ is a minor of $\mathbf{A}$ of size $n - 1$.

Solution.

- (a) This is [Corollary 14.9.3](#) (d): by [Theorem 14.9.2](#) the rank is even, and an even number that is at most an odd n is at most $n - 1$, so the matrix is not invertible. The proof of the standard form uses no determinants.
- (b) Since $\mathbf{A}$ is invertible, Theorem 7.6.2 gives $\mathbf{A}^{-1} = (\det \mathbf{A})^{-1} \text{adj } \mathbf{A}$. First, skewness: $(\mathbf{A}^{-1})^\top = (\mathbf{A}^\top)^{-1} = (-\mathbf{A})^{-1} = -\mathbf{A}^{-1}$, using Theorem 0.9.5 and the fact that inversion turns $-\mathbf{A} = (-1)\mathbf{A}$ into $(-1)^{-1}\mathbf{A}^{-1} = -\mathbf{A}^{-1}$.

Now the diagonal. By Definition 7.6.2 the (i, i) entry of $\text{adj } \mathbf{A}$ is the cofactor $C_{ii} = (-1)^{2i} M_{ii} = M_{ii}$, the determinant of the matrix obtained from $\mathbf{A}$ by deleting row i and column i . Deleting a row and the matching column of an alternating matrix leaves an alternating matrix, since the surviving entries keep their positions relative to the diagonal. Its size is $n - 1$, and n is even by [Corollary 14.9.3](#) (a) applied to the invertible $\mathbf{A}$; so $n - 1$ is odd and $M_{ii} = 0$ by (a). Hence every diagonal entry of $\mathbf{A}^{-1}$ is 0, and with skewness this makes $\mathbf{A}^{-1}$ alternating.

Exercise. C3: Counting over a finite field

Let q be a power of an **odd** prime.

- (a) How many alternating bilinear forms are there on $\mathbb{F}_q^{2m}$? How many symmetric ones?
- (b) How many of the alternating forms on $\mathbb{F}_q^2$ are nondegenerate, and how many congruence classes do they fall into?
- (c) How many of the symmetric forms on $\mathbb{F}_q^1$ are nondegenerate, and how many congruence classes do they fall into? *Hint: the squaring map $\mathbb{F}_q^\times \rightarrow \mathbb{F}_q^\times$ has kernel $\{1, -1\}$.*
- (d) Explain in one or two sentences why the answers to (b) and (c) differ, in terms of what a change of basis can do to the single free parameter in each case.

Solution.

- (a) By Theorem 14.1.1 (c), forms correspond bijectively to matrices, so we count matrices. An alternating matrix of size $n = 2m$ is determined freely by its entries above the diagonal, of which there are $\binom{n}{2} = m(2m - 1)$; so there are $q^{m(2m-1)}$ alternating forms. A symmetric matrix is determined freely by its entries on and above the diagonal,

$\binom{n}{2} + n = m(2m + 1)$ of them, giving $q^{m(2m+1)}$.

- (b) The alternating forms on $\mathbb{F}_q^2$ have matrices $\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$, so there are q of them, and the nondegenerate ones are those with $a \neq 0$, of which there are $q - 1$. By [Corollary 14.9.3](#) (b) all of these have rank 2 and so lie in a **single** congruence class.
- (c) A symmetric form on $\mathbb{F}_q^1$ has matrix $[d]$ and is nondegenerate exactly when $d \neq 0$, so there are $q - 1$ of them. Congruence in size 1 replaces d by p^2d with $p \neq 0$ (Definition 14.2.1), so the classes are the cosets of the subgroup of squares in $\mathbb{F}_q^\times$. The squaring homomorphism $\mathbb{F}_q^\times \rightarrow \mathbb{F}_q^\times$ has kernel $\{x : x^2 = 1\} = \{1, -1\}$, which has **two** elements because q is odd; so its image has index 2, and there are exactly **two** congruence classes. For $q = 5$, for instance, the squares are $\{1, 4\}$ and the nonsquares $\{2, 3\}$, and $[1] \not\equiv [2]$.
- (d) In the alternating case a change of basis may replace a by ca for **any** $c \neq 0$, because the two slots of $\beta(u, w)$ hold different basis vectors and only one of them need be rescaled. In the symmetric case the parameter sits in $\beta(v, v)$, where both slots hold the same vector, so rescaling changes d to c^2d — by a **square** only. The square class then survives as an invariant, and over $\mathbb{F}_q$ it has two values.