BILINEAR FORMS

KEITH CONRAD

The geometry of $\mathbf{R}^n$ is controlled algebraically by the dot product. We will abstract the dot product on $\mathbf{R}^n$ to a bilinear form on a vector space and study algebraic and geometric notions related to bilinear forms (especially the concept of orthogonality in all its manifestations: orthogonal vectors, orthogonal subspaces, and orthogonal bases).

Section 1 defines a bilinear form on a vector space and offers examples of the two most common types of bilinear forms: symmetric and alternating bilinear forms. In Section 2 we will see how a bilinear form looks in coordinates. Section 3 describes the important condition of non-degeneracy for a bilinear form. Orthogonal bases for symmetric bilinear forms are the subject of Section 4. Symplectic bases for alternating bilinear forms are discussed in Section 5. Quadratic forms are in Section 6 (characteristic not 2) and Section 7 (characteristic 2). The tensor product viewpoint on bilinear forms is briefly discussed in Section 8.

Vector spaces in Section 1 are arbitrary, but starting in Section 2 we will assume they are finite-dimensional. It is assumed that the reader is comfortable with abstract vector spaces and how to uses bases of (finite-dimensional) vector spaces to turn vectors into column vectors and linear maps into matrices. It is also assumed that the reader is familiar with duality on finite-dimensional vector spaces: dual spaces, dual bases, the dual of a linear map, and the natural isomorphism of finite-dimensional vector spaces with their double duals (which identifies the double dual of a basis with itself and the double dual of a linear map with itself). For a vector space V we denote its dual space as $V^\vee$. The dual basis of a basis $\{e_1, \ldots, e_n\}$ of V is denoted $\{e_1^\vee, \ldots, e_n^\vee\}$, so the $e_i^\vee$'s are the coordinate functions on V relative to that basis: $e_i^\vee(e_j)$ is 1 for $i = j$ and 0 for $i \neq j$.

Although V is naturally isomorphic to $V^{\vee\vee}$, students are always cautioned against identifying V with $V^\vee$, since "there is no natural isomorphism." In a nutshell, the subject of bilinear forms is about what happens if you make an identification of V with $V^\vee$ and keep track of it. Different identifications have different geometric properties.

1. Definitions and examples

Definition 1.1. Let F be a field and V be a vector space over F. A *bilinear form* on V is a function $B\colon V \times V \to F$ which is linear in each variable when the other one is fixed.

We call B *symmetric* when

$$B(v, w) = B(w, v) \text{ for all } v, w \in V$$

and *skew-symmetric* when

$$B(v, w) = -B(w, v) \text{ for all } v, w \in V.$$

We call B *alternating* when

$$B(v, v) = 0 \text{ for all } v \in V.$$

A *bilinear space* is a vector space equipped with a specific choice of bilinear form, and the space is called symmetric, skew-symmetric, or alternating when the bilinear form has the corresponding property.

A common synonym for skew-symmetric is anti-symmetric.

Example 1.2. The dot product $v \cdot w$ on $\mathbf{R}^n$ is a symmetric bilinear form.

Example 1.3. For a fixed matrix $A \in \mathrm{M}_n(\mathbf{R})$, the function $f(v, w) = v \cdot Aw$ on $\mathbf{R}^n$ is a bilinear form, but not necessarily symmetric like the dot product. All later examples are essentially generalizations of this construction.

Example 1.4. For any field F, viewed as a 1-dimensional vector space over itself, multiplication $m \colon F \times F \to F$ is a symmetric bilinear form and not alternating. It is skew-symmetric when F has characteristic 2.

Example 1.5. A skew-symmetric and alternating bilinear form on $\mathbf{R}^2$ is

$$B((x, y), (x', y')) := xy' - x'y = \det \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}.$$

For example, $B((2, 1), (3, 4)) = 5$ and $B((2, 1), (2, 1)) = 0$. Viewing $\mathbf{R}^2$ as $\mathbf{C}$ by $(x, y) \leftrightarrow x + iy$, $B(z, w) = \mathrm{Im}(\overline{z}w)$ for complex numbers z and w.

Among the three types of bilinear forms we have defined (symmetric, skew-symmetric, alternating), the first and third types are more basic than the second. In fact, we now show that a skew-symmetric bilinear form is just another name for a symmetric or an alternating bilinear form, depending on whether or not the characteristic of the field is 2.

Theorem 1.6. *In all characteristics, an alternating bilinear form is skew-symmetric. In characteristic not* 2*, a bilinear form is skew-symmetric if and only if it is alternating. In characteristic* 2*, a bilinear form is skew-symmetric if and only if it is symmetric.*

Proof. When B is alternating and $v, w \in V$, expanding the right side of the equation $0 = B(v + w, v + w)$ shows

$$0 = B(v, v) + B(v, w) + B(w, v) + B(w, w) = B(v, w) + B(w, v),$$

so $B(v, w) = -B(w, v)$. Therefore alternating bilinear forms are skew-symmetric in all characteristics (even in characteristic 2). Outside of characteristic 2, a skew-symmetric bilinear form is alternating since

$$B(v, v) = -B(v, v) \Longrightarrow 2B(v, v) = 0 \Longrightarrow B(v, v) = 0.$$

That skew-symmetric and symmetric bilinear forms coincide in characteristic 2 is immediate since $1 = -1$ in characteristic 2. □

Despite Theorem 1.6, the label "skew-symmetric" is still needed. One reason is that it is used in preference to "alternating" by many geometers who work over $\mathbf{R}$, where the two notions coincide. Another reason is that the concept of bilinear form makes sense on modules, not just vector spaces, and there are skew-symmetric bilinear forms on modules which are neither symmetric nor alternating (Exercise 2.8). However, we will only deal with bilinear forms on vector spaces.

Theorem 1.7. *In characteristic not 2, every bilinear form B is uniquely expressible as a sum $B_1 + B_2$, where B_1 is symmetric and B_2 is alternating (equivalently, skew-symmetric). In characteristic 2, the alternating bilinear forms are a subset of the symmetric bilinear forms.*

Proof. The last part is immediate from Theorem 1.6. Now we work in characteristic not 2. For a bilinear form B, suppose we can write $B = B_1 + B_2$ with symmetric B_1 and alternating (so skew-symmetric) B_2. Then for vectors v and w,

$$B(v,w) = B_1(v,w) + B_2(v,w) \tag{1.1}$$

and

$$\begin{aligned} B(w,v) &= B_1(w,v) + B_2(w,v) \\ &= B_1(v,w) - B_2(v,w). \end{aligned} \tag{1.2}$$

Adding and subtracting (1.1) and (1.2), we get formulas for B_1 and B_2 in terms of B:

$$B_1(v,w) = \frac{B(v,w) + B(w,v)}{2}, \quad B_2(v,w) = \frac{B(v,w) - B(w,v)}{2}. \tag{1.3}$$

Turning this reasoning around, the bilinear forms B_1 and B_2 defined by (1.3) are symmetric and alternating respectively, so we have established the existence and uniqueness of B_1 and B_2. □

Theorem 1.8. *In characteristic not 2, a symmetric bilinear form $B(v,w)$ is completely determined by its values $B(v,v)$ on the diagonal.*

Proof. For any v and w,

$$\frac{1}{2}(B(v+w,v+w) - B(v,v) - B(w,w)) = \frac{1}{2}(B(v,w) + B(w,v)) = B(v,w).$$

Note we used symmetry of B in the last equation. □

The fact that, for symmetric B, we can recover the 2-variable function $B(v,w)$ from the 1-variable function $B(v,v)$ outside of characteristic 2 is called *polarization*. For instance, it shows us that a symmetric bilinear form B is identically 0 if and only if $B(v,v) = 0$ for all v (*not* just $B(e_i,e_i) = 0$ on a basis; see Example 1.10). Polarization will play an important role when we treat quadratic forms later.

Let's look at some more examples of bilinear forms.

Example 1.9. On $\mathbf{R}^2$, $B((x,y),(x',y')) = xx' - yy'$ is symmetric. How is this formula different from the one in Example 1.5?

Example 1.10. On $\mathbf{R}^2$, $B((x,y),(x',y')) = xy' + yx'$ is symmetric. Since $B((x,y),(x,y)) = 2xy$, $B(e_i,e_i) = 0$ where $\{e_1,e_2\}$ is the standard basis of $\mathbf{R}^2$.

Example 1.11. Fix a vector u in $\mathbf{R}^3$. For v and w in $\mathbf{R}^3$, let $B_u(v,w) = u \cdot (v \times w)$, where $\times$ is the cross product. This is alternating.

Example 1.12. Let V be a finite-dimensional vector space over F. On the vector space $\mathrm{Hom}_F(V,V)$, set $B(L,L') = \mathrm{Tr}(LL')$. This is called the *trace form* on $\mathrm{Hom}_F(V,V)$. It is bilinear since the trace is linear. It is symmetric since $\mathrm{Tr}(LL') = \mathrm{Tr}(L'L)$.

Example 1.13. Let V be a finite-dimensional vector space over F with dual space $V^\vee$. On the vector space $V \oplus V^\vee$, set

$$B((v,\varphi),(w,\psi)) = \psi(v) - \varphi(w).$$

This is alternating. (Symbolically, $B((v,\varphi),(w,\psi)) = \left|\begin{smallmatrix} \psi & \varphi \\ w & v \end{smallmatrix}\right|$.) Can you interpret Example 1.5 in this context?

Example 1.14. Let's look at an infinite-dimensional example. On $C[0,1]$, the space of real-valued continuous functions $[0,1] \to \mathbf{R}$, we have the symmetric bilinear form $B(f,g) = \int_0^1 f(x)g(x)\,\mathrm{d}x$. To get other examples of bilinear forms, choose any continuous function $k\colon [0,1]^2 \to \mathbf{R}$ and set

$$B_k(f,g) = \int_{[0,1]^2} f(x)g(y)k(x,y)\,\mathrm{d}x\,\mathrm{d}y.$$

Can you find a k that makes $B_k = B$?

Example 1.15. On $\mathbf{C}^n$, let $H((z_1,\dots,z_n),(w_1,\dots,w_n)) = \sum_{i=1}^n z_i\overline{w}_i$. Regarding $\mathbf{C}^n$ as a real vector space, H is bilinear. But viewing $\mathbf{C}^n$ as a complex vector space, H is linear in its first component but it is not linear in its second component: $H(v,cw)$ equals $\overline{c}H(v,w)$ instead of $cH(v,w)$. Therefore H is *not* bilinear. Moreover, $H(v,w) = \overline{H(w,v)}$. Pairings such as H on a complex vector space, which are linear in one component, conjugate-linear in the other component, and get conjugated when the arguments are exchanged, are called *Hermitian*. Our focus is on bilinear forms.

A bilinear form is a generalization of the dot product, so the condition $B(v,w) = 0$ should be considered as a generalization of perpendicularity. With this in mind, write $v \perp w$ when $B(v,w) = 0$ and call v and w *perpendicular* or *orthogonal*. (We could write $v \perp_B w$ to stress the dependence of this notion of orthogonality on the choice of B, but this will not be done.) Since B is bilinear, perpendicularity behaves linearly:

$$v \perp w_1, v \perp w_2 \Longrightarrow v \perp (c_1w_1 + c_2w_2);\; v_1 \perp w, v_2 \perp w \Longrightarrow (c_1v_1 + c_2v_2) \perp w.$$

For a subspace $W \subset V$ and a vector $v \in V$ we write $v \perp W$ when $v \perp w$ for all $w \in W$ and write $W \perp v$ similarly.

Example 1.16. On $V = \mathbf{R}^2$, let $B((x,y),(x',y')) = xx' + xy' - x'y - yy'$. We have $(1,0) \perp (1,-1)$ but $(1,-1) \not\perp (1,0)$, so the perpendicularity relation for B is not symmetric.

Since it can happen that $v \perp w$ while $w \not\perp v$, we should give the property that $v \perp w$ and $w \perp v$ a name: we will say v and w are orthogonal to each other in both directions.

The most important bilinear forms are those where $\perp$ is a symmetric relation: $v \perp w$ if and only if $w \perp v$. Knowing the bilinear forms where this happens is a key foundational result. Here it is.

Theorem 1.17. *The perpendicularity relation on a bilinear space (V,B) is symmetric if and only if B is either symmetric or alternating.*

The proof is a series of elementary but somewhat tedious calculations. Nothing will be lost by skipping the proof on a first reading and coming back to it after the significance of the two types of bilinear forms becomes clearer.

Proof. If B is symmetric or alternating then we have $B(v, w) = \pm B(w, v)$, so $B(v, w)$ vanishes if and only if $B(w, v)$ vanishes.

To prove the converse direction, assume $\perp$ is a symmetric relation. Pick any vectors $u, v, w \in V$. We first will find a linear combination $av + bw$ such that $(av + bw) \perp u$. This is the same as

$$aB(v, u) + bB(w, u) = 0 \tag{1.4}$$

since B is linear in its first component. We can achieve (1.4) using $a = B(w, u)$ and $b = -B(v, u)$. Therefore set

$$x = B(w, u)v - B(v, u)w.$$

Then $B(x, u) = 0$, so $B(u, x) = 0$ by symmetry of the relation $\perp$. Computing $B(u, x)$ by linearity of B in its second component and setting it equal to zero, we obtain

$$B(w, u)B(u, v) = B(v, u)B(u, w). \tag{1.5}$$

This holds for *all* $u, v, w \in V$. We will show a bilinear form satisfying (1.5) is symmetric or alternating.

Use $w = u$ in (1.5):

$$B(u, u)B(u, v) = B(v, u)B(u, u). \tag{1.6}$$

Notice $B(u, u)$ appears on both sides of (1.6). Thus, for all u and v in V,

$$B(u, v) \neq B(v, u) \Longrightarrow B(u, u) = 0 \quad \text{(and similarly } B(v, v) = 0\text{)}. \tag{1.7}$$

Now assume that the relation $\perp$ for is symmetric and B is not a symmetric bilinear form. We will prove B is alternating. By assumption, there are $u_0, v_0 \in V$ such that

$$B(u_0, v_0) \neq B(v_0, u_0). \tag{1.8}$$

From this we will show $B(w, w) = 0$ for all $w \in V$, relying ultimately on (1.7). Note by (1.7) and (1.8) that

$$B(u_0, u_0) = 0, \quad B(v_0, v_0) = 0. \tag{1.9}$$

Pick any $w \in V$. If $B(u_0, w) \neq B(w, u_0)$ or $B(v_0, w) \neq B(w, v_0)$ then (1.7) shows $B(w, w) = 0$. Therefore to prove $B(w, w) = 0$ we may assume

$$B(u_0, w) = B(w, u_0), \quad B(v_0, w) = B(w, v_0). \tag{1.10}$$

In (1.5), set $u = u_0$ and $v = v_0$. Then

$$B(w, u_0)B(u_0, v_0) = B(v_0, u_0)B(u_0, w).$$

By (1.10),

$$B(u_0, w)(B(u_0, v_0) - B(v_0, u_0)) = 0.$$

This implies, by (1.8) and (1.10), that

$$B(u_0, w) = B(w, u_0) = 0. \tag{1.11}$$

Similarly, setting $u = v_0$ and $v = u_0$ in (1.5) tells us by (1.8) and (1.10) that

$$B(v_0, w) = B(w, v_0) = 0. \tag{1.12}$$

By (1.11), $B(u_0, v_0 + w) = B(u_0, v_0)$ and $B(v_0 + w, u_0) = B(v_0, u_0)$. These are distinct by (1.8), so (1.7) with $u = v_0 + w$ and $v = u_0$ implies

$$B(v_0 + w, v_0 + w) = 0.$$

Then by (1.9) and (1.12), $B(w, w) = 0$. □

The proof of Theorem 1.17 did not assume finite-dimensionality and it used additivity rather than linearity.

When $\perp$ is a symmetric relation on V, for any subspace W of V we set

$$W^\perp = \{v \in V : v \perp w \text{ for all } w \in W\} = \{v \in V : w \perp v \text{ for all } w \in W\}.$$

and call this the *orthogonal space* $W^\perp$. (This is often called the orthogonal complement of W in the literature, although it may not really look like a complement: it can happen that $W \cap W^\perp \neq \{0\}$.) For nonzero $v \in V$, write $(Fv)^\perp$ as $v^\perp$. That is, $v^\perp = \{v' \in V : v' \perp v\}$. The notation $W^\perp$ for a subspace W of a bilinear space V makes sense *only* when V is symmetric or alternating. This is a reason why the important bilinear spaces are the symmetric and alternating ones. (A third class of vector spaces where a perpendicularity relation is symmetric is the Hermitian spaces, as in Example 1.15, but they are not bilinear so Theorem 1.17 is not violated by them.)

By comparison to the dot product on $\mathbf{R}^n$, perpendicularity for other bilinear forms can have new features. The main non-intuitive feature that can arise is $v \perp v$ with $v \neq 0$. This is impossible for the dot product on $\mathbf{R}^n$, but is very common for other bilinear forms: $v \perp v$ *need not* force $v = 0$. In the symmetric bilinear space of Example 1.9 we have $(1,1) \perp (1,1)$, and in fact the subspace $W = \mathbf{R}(1,1)$ has $W^\perp = W$, so $W + W^\perp \neq \mathbf{R}^2$. On $\mathbf{R}^n$ with the dot product we have $\mathbf{R}^n = U \oplus U^\perp$ for any subspace U, but this direct sum decomposition is not generally valid for subspaces of other bilinear spaces. (However, see Theorem 3.10 for a characterization of the subspaces where this decomposition does take place.)

Here are two constructions of new bilinear spaces from old ones.

- Subspace: If (V, B) is a bilinear space and W is a subspace of V, then B restricts to a bilinear form on W, so we get a bilinear subspace denoted $(W, B|_W)$ or simply (W, B). (Strictly speaking, we should write $B|_{W \times W}$ since B is a function of two variables, but the more concise $B|_W$ shouldn't cause confusion.) It is obvious that if B is either symmetric, alternating, or skew-symmetric on V then that property is inherited by any subspace.
- Direct Sum: If (V_1, B_1) and (V_2, B_2) are bilinear spaces over the same field then $V_1 \oplus V_2$ becomes a bilinear space using the bilinear form $(B_1 \oplus B_2)((v_1, v_2), (v_1', v_2')) := B_1(v_1, v_1') + B_2(v_2, v_2')$. This formula is *not* mysterious; the idea is to treat V_1 and V_2 separately, just as the direct sum treats V_1 and V_2 separately. In $B_1 \oplus B_2$ we pair up the first components, then the second components, and add.

  If B_1 and B_2 are both symmetric, both alternating, or both skew-symmetric then $B_1 \oplus B_2$ inherits this property.

Definition 1.18. The bilinear space $(V_1 \oplus V_2, B_1 \oplus B_2)$ constructed above is called the *orthogonal direct sum* of V_1 and V_2 and is denoted $V_1 \perp V_2$.

Example 1.19. Thinking about $\mathbf{R}$ as a bilinear space under multiplication (Example 1.4), $\mathbf{R} \perp \mathbf{R}$ is $\mathbf{R}^2$ with the dot product and the n-fold orthogonal direct sum $\mathbf{R}^{\perp n} = \mathbf{R} \perp \cdots \perp \mathbf{R}$ is $\mathbf{R}^n$ with the dot product.

We embed V_1 into the orthogonal direct sum $V_1 \perp V_2$ in a natural way: $v_1 \mapsto (v_1, 0)$. Similarly we embed V_2 into $V_1 \perp V_2$ by $v_2 \mapsto (0, v_2)$.

If V_1 and V_2 are subspaces of the bilinear space V then we say they are orthogonal, and write $V_1 \perp V_2$, if $v_1 \perp v_2$ for all $v_1 \in V_1$ and $v_2 \in V_2$. In this context $\perp$ denotes a relation on subspaces, not to be confused with its use in the construction of the orthogonal direct sum of two bilinear spaces.

Theorem 1.20. *Let (V_1, B_1) and (V_2, B_2) be bilinear spaces. Viewing V_1 and V_2 as subspaces of $V_1 \oplus V_2$ in the natural way, $B_1 \oplus B_2$ restricts to B_i on the subspace V_i and elements of V_1 and V_2 are orthogonal to each other in both directions with respect to $B_1 \oplus B_2$. These two conditions determine $B_1 \oplus B_2$ as a bilinear form on $V_1 \oplus V_2$.*

Proof. Since $(B_1 \oplus B_2)((v_1, 0), (v_1', 0)) = B_1(v_1, v_1')$, $(B_1 \oplus B_2)|_{V_1} = B_1$. Similarly, $(B_1 \oplus B_2)|_{V_2} = B_2$.

For $v_1 \in V_1$ and $v_2 \in V_2$,

$$(B_1 \oplus B_2)((v_1, 0), (0, v_2)) = B_1(v_1, 0) + B_2(0, v_2) = 0$$

and

$$(B_1 \oplus B_2)((0, v_2), (v_1, 0)) = B_1(0, v_1) + B_2(v_2, 0) = 0.$$

Therefore $v_1 \perp v_2$ and $v_2 \perp v_1$ in $(V_1 \oplus V_2, B_1 \oplus B_2)$.

Assuming B_0 is any bilinear form on $V_1 \oplus V_2$ which restricts to B_i on V_i and in which elements of V_1 and V_2 are orthogonal to each other (in both directions), we have

$$\begin{aligned} B_0((v_1, v_2), (v_1', v_2')) &= B_0((v_1, 0), (v_1', 0)) + B_0((v_1, 0), (0, v_2')) + \\ &\qquad B_0((0, v_2), (v_1', 0)) + B_0((0, v_2), (0, v_2')) \\ &= B_0((v_1, 0), (v_1', 0)) + B_0((0, v_2), (0, v_2')) \\ &= B_1(v_1, v_1') + B_2(v_2, v_2'), \end{aligned}$$

so $B_0 = B_1 \oplus B_2$. □

If a bilinear space V can be expressed as a direct sum of two subspaces W and W' which are mutually perpendicular (in both directions) then Theorem 1.20 shows V behaves just like the orthogonal direct sum of W and W'. Most decompositions of a bilinear space into a direct sum of subspaces are *not* orthogonal direct sums since the subspaces may not be mutually perpendicular. This is already familiar from $\mathbf{R}^n$, which admits many direct sum decompositions into liner subspaces that are not mutually perpendicular.

We end this section with a very important link between bilinear forms and the dual space. For a bilinear form B on V, we can think about $B(v, w)$ as a function of w with v fixed or as a function of v with w fixed. Taking the first point of view, we think about the function $B(v, -) : V \to F$ which sends each w to $B(v, w)$. Since B is linear in its second component when the first is fixed, $w \mapsto B(v, w)$ is a linear map from V to F, so $B(v, -) \in V^\vee$ for each v. Set $L_B \colon V \to V^\vee$ by $L_B \colon v \mapsto B(v, -)$, so $L_B(v) = B(v, -)$. The values of L_B are in $V^\vee$, so they are functions on V (with the unknown substituted into the empty slot of $B(v, -)$). Since B $B(v + v', w) = B(v, w) + B(v', w)$ for all w, $B(v + v', -) = B(v, -) + B(v', -)$ in $V^\vee$, which means $L_B(v + v') = L_B(v) + L_B(v')$. Similarly, since $B(cv, w) = cB(v, w)$, $L_B(cv) = cL_B(v)$. Thus L_B is linear, so any bilinear form B on V gives a linear map L_B from V *to its dual space* $V^\vee$. Because $L_B(v)(w) = (B(v, -))(w) = B(v, w)$, we can recover B from L_B by evaluating L_B at any element $v \in V$ and then evaluating $L_B(v) \in V^\vee$ at any $w \in V$ to get $B(v, w)$.

Conversely, if we have a linear map $L \colon V \to V^\vee$ then to each $v \in V$ we have $L(v) \in V^\vee$, so we get a bilinear form $B(v, w) := L(v)(w)$ such that $B(v, -) = L(v)$. These correspondences from bilinear forms on V to linear maps $V \to V^\vee$ and back are inverses of one another.

In a similar way, from a bilinear form B we get functions $B(-, w) \in V^\vee$ (sending v to $B(v, w)$). Let $R_B \colon V \to V^\vee$ by $R_B \colon w \mapsto B(-, w)$, so $R_B(w) = B(-, w)$. The map R_B is linear from V to $V^\vee$, and passing from B to R_B is a second one-to-one correspondence between bilinear forms on V and linear maps $V \to V^\vee$ (Exercise 1.5).

These two ways of viewing a bilinear form B as a linear map $V \to V^\vee$ (using L_B or R_B) are related through double duality:

Theorem 1.21. *When V is finite-dimensional and B is a bilinear form on V, the linear maps L_B and R_B are dual to each other. Specifically, if we dualize $L_B \colon V \to V^\vee$ to $L_B^\vee \colon V^{\vee\vee} \to V^\vee$ and identify $V^{\vee\vee}$ with V in the natural way then $L_B^\vee = R_B$. Similarly, $R_B^\vee = L_B$.*

Proof. For a linear map $L \colon V \to W$, the dual $L^\vee \colon W^\vee \to V^\vee$ is defined by

$$L^\vee(\varphi)(v) = \varphi(L(v))$$

for $\varphi \in V^\vee$ and $v \in V$. Taking $W = V^\vee$, $L = L_B$, and writing the elements of $W^\vee = V^{\vee\vee}$ as evaluation maps at elements in V,

$$L_B^\vee(\mathrm{ev}_{v'})(v) = \mathrm{ev}_{v'}(L_B(v)) = \mathrm{ev}_{v'}(B(v, -)) = B(v, v') = R_B(v')(v).$$

Thus $L_B^\vee = R_B$ when we identify $V^{\vee\vee}$ with V in the usual way. The proof that $R_B^\vee = L_B$ is similar, or dualize the equation $L_B^\vee = R_B$. □

There are two ways of identifying bilinear forms on V with linear maps $V \to V^\vee$ because a bilinear form is a function of two variables in V and we can take preference for one variable over the other to get a linear map out of V. In Section 8, tensor products will be used to interpret a bilinear form on V as a linear map without biasing L_B over R_B.

Exercises.

1. Let B be a bilinear form on V. Prove B is skew-symmetric if and only if the diagonal function $V \to F$ given by $v \mapsto B(v, v)$ is additive.
2. Show any alternating bilinear form on $\mathbf{R}^3$ is some B_u as in Example 1.11.
3. In Example 1.14, show B_k is symmetric if and only if $k(x, y) = k(y, x)$ for all x and y. What condition on k makes B_k alternating?
4. Define a bilinear form on a module over a commutative ring and check any alternating bilinear form is skew-symmetric. Show the converse is true if there is no 2-torsion in the ring ($2x = 0 \Rightarrow x = 0$ for x in the ring).
5. Let $\mathrm{Bil}(V)$ be the set of all bilinear forms on V. It is a vector space under addition and scaling. For a bilinear form B on V, show the correspondence $B \to R_B$ is a vector space isomorphism from $\mathrm{Bil}(V)$ to $\mathrm{Hom}_F(V, V^\vee)$ (V need not be finite-dimensional).
6. Let B be a bilinear form on V. Set $V^{\perp_L} = \{v \in V : v \perp V\}$ and $V^{\perp_R} = \{v \in V : V \perp v\}$. Since $B(v, w + w') = B(v, w)$ when $w' \in V^{\perp_R}$, L_B induces a linear map $V \to (V/V^{\perp_R})^\vee$. Show this linear map has kernel $V^{\perp_L}$, so we get a linear embedding $V/V^{\perp_L} \hookrightarrow (V/V^{\perp_R})^\vee$. Use this and the analogous argument with R_B in place of L_B to show $\dim V^{\perp_L} = \dim V^{\perp_R}$ when V is finite-dimensional.

2. Bilinear forms and matrices

From now on, all vector spaces are understood to be finite-dimensional.

A linear transformation $L \colon V \to W$ between two finite-dimensional vector spaces over F can be written as a matrix once we pick (ordered) bases for V and W. When $V = W$ and we use the same basis for the inputs and outputs of L then changing the basis leads to a new matrix representation which is conjugate to the old matrix. In particular, the trace, determinant, and (more generally) characteristic polynomial of a linear operator $L \colon V \to V$

are well-defined, independent of the choice of basis. In this section we will see how bilinear forms and related constructions can be described using matrices.

We start with a concrete example. In addition to the dot product on $\mathbf{R}^n$, additional bilinear forms on $\mathbf{R}^n$ are obtained by throwing a matrix into one side of the dot product: for an $n \times n$ real matrix M, the formula $B(v, w) = v \cdot Mw$ is a bilinear form on $\mathbf{R}^n$. It turns out this kind of construction describes all bilinear forms on any finite-dimensional vector space, once we fix a basis.

Let V have dimension $n \geq 1$ with basis $\{e_1, \ldots, e_n\}$. Pick v and w in V and express them in this basis: $v = \sum_{i=1}^n x_i e_i$ and $w = \sum_{j=1}^n y_j e_j$. For any bilinear form B on V, its bilinearity gives

$$\begin{aligned} B(v, w) &= B\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) \\ &= \sum_{i=1}^n x_i B\left(e_i, \sum_{j=1}^n y_j e_j\right) \\ &= \sum_{i=1}^n \sum_{j=1}^n x_i y_j B(e_i, e_j) \end{aligned}$$

Set $M := (B(e_i, e_j))$, which is an $n \times n$ matrix. By a calculation the reader can carry out,

$$B(v, w) = [v] \cdot M[w] \tag{2.1}$$

for all v and w in V, where $\cdot$ on the right is the usual dot product on F^n and

$$[v] = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad [w] = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

are the coordinate vectors of v and w for our choice of basis $\{e_1, \ldots, e_n\}$. The "coordinate" isomorphism $[\cdot]\colon V \to F^n$ will be understood to refer to a fixed choice of basis throughout a given discussion.

We call the matrix $M = (B(e_i, e_j))$ appearing in (2.1) the *matrix associated to* B in the basis $\{e_1, \ldots, e_n\}$.

Example 2.1. The matrix associated to the dot product on F^n in the standard basis of F^n is the identity matrix.

Example 2.2. In Example 1.5,

$$xy' - x'y = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

It is *easy* to read off the matrix from the formula on the left: there are no xx' or yy' terms, so the diagonal entries of the matrix are 0. Since xy' has coefficient 1, the $(1, 2)$ entry of the matrix is 1. The term $x'y = yx'$ corresponds to the $(2, 1)$ entry (because it involves the second of x and y and the first of x' and y', in that order), which must be the coefficient -1.

Theorem 2.3. *Let V be a vector space over F of dimension $n \geq 1$. For a fixed choice of basis $\{e_1, \dots, e_n\}$ of V, which gives an isomorphism $v \mapsto [v]$ from V to F^n by coordinatization, each bilinear form on V has the expression* (2.1) *for a unique $n \times n$ matrix M over F.*

Proof. We have shown every bilinear form looks like (2.1) once we choose a basis. It remains to verify uniqueness. Suppose $B(v, w) = [v] \cdot N[w]$ for some matrix N. Then $B(e_i, e_j) = [e_i] \cdot N[e_j]$, which is the (i, j) entry of N, so $N = (B(e_i, e_j))$. $\square$

Note the zero vector space has 1 bilinear form but no matrix. We will not be pedantic about including the zero vector space in our discussion.

Example 2.4. Let $V = \mathbf{R}^n$. Pick non-negative integers p and q such that $p + q = n$. For $v = (x_1, \dots, x_n)$ and $v' = (x'_1, \dots, x'_n)$ in $\mathbf{R}^n$, set

$$\begin{aligned} \langle v, v' \rangle_{p,q} &:= x_1 x'_1 + \cdots + x_p x'_p - x_{p+1} x'_{p+1} - \cdots - x_n x'_n \\ &= v \cdot \left(\begin{smallmatrix} I_p & O \\ O & -I_q \end{smallmatrix} \right) v'. \end{aligned}$$

This symmetric bilinear form is like the dot product, except the coefficients involve p plus signs and $n - p = q$ minus signs. The dot product on $\mathbf{R}^n$ is the special case $(p, q) = (n, 0)$. Example 1.9 is the special case $(p, q) = (1, 1)$.

The space $\mathbf{R}^n$ with the bilinear form $\langle \cdot, \cdot \rangle_{p,q}$ is denoted $\mathbf{R}^{p,q}$. We call $\mathbf{R}^{p,q}$ a *pseudo-Euclidean space* when p and q are both positive. Example 1.9 is $\mathbf{R}^{1,1}$. The example $\mathbf{R}^{1,3}$ or $\mathbf{R}^{3,1}$ is called Minkowski space and arises in relativity theory. A pseudo-Euclidean space is the same vector space as $\mathbf{R}^n$, but its geometric structure (*e.g.*, the notion of perpendicularity) is different. The label *Euclidean space* is actually not just another name for $\mathbf{R}^n$ as a vector space, but it is the name for $\mathbf{R}^n$ equipped with a specific bilinear form: the dot product.

Bilinear forms are not linear maps, but we saw at the end of Section 1 that each bilinear form B on V can be interpreted as a linear map $V \to V^\vee$, in fact in two ways as L_B and R_B. The matrix of B turns out to be the same as the matrix of one of these linear maps! Which one?

Theorem 2.5. *If B is a bilinear form on V, the matrix for B in the basis $\{e_1, \dots, e_n\}$ of V equals the matrix of the linear map $R_B \colon V \to V^\vee$ with respect to the given basis of V and its dual basis in $V^\vee$.*

Proof. Let $[\cdot] \colon V \to F^n$ be the coordinate isomorphism coming from the basis in the theorem and let $[\cdot]' \colon V^\vee \to F^n$ be the coordinate isomorphism using the dual basis. The matrix for R_B has columns $[R_B(e_1)]', \dots, [R_B(e_n)]'$. To compute the entries of the jth column, we simply have to figure out how to write $R_B(e_j)$ as a linear combination of the dual basis $\{e_1^\vee, \dots, e_n^\vee\}$ of $V^\vee$ and use the coefficients that occur.

There is one expression for $R_B(e_j)$ in the dual basis:

$$R_B(e_j) = c_1 e_1^\vee + \cdots + c_n e_n^\vee$$

in $V^\vee$, with unknown c_i's. To find c_i we just evaluate both sides at e_i: the left side is $(R_B(e_j))(e_i) = (B(-, e_j))(e_i) = B(e_i, e_j)$ and the right side is $c_i \cdot 1 = c_i$. Therefore the ith entry of the column vector $[R_B(e_j)]'$ is $B(e_i, e_j)$, which means the matrix for R_B is the matrix $(B(e_i, e_j))$; they agree column-by-column. $\square$

In terms of a commutative diagram, Theorem 2.5 says

$$
\begin{tikzcd}
V \arrow[r, "R_B"] \arrow[d, "{[\cdot]}"'] & V^\vee \arrow[d, "{[\cdot]'}"] \\
F^n \arrow[r, "(B(e_i,e_j))"] & F^n
\end{tikzcd}
\tag{2.2}
$$

commutes: $[R_B(v)]' = (B(e_i, e_j))[v]$ for all v in V.

Remark 2.6. That the matrix associated to B is the matrix of R_B rather than L_B is related to our *convention* that we view bilinear forms concretely using $[v] \cdot A[w]$ instead of $A[v] \cdot [w]$. If we adopted the latter convention then the matrix associated to B would equal the matrix for L_B.

Theorem 2.7. *Let (V, B) be a bilinear space and let B have associated matrix M in some basis. Then*

1. *B is symmetric if and only if $M^\top = M$,*
2. *B is skew-symmetric if and only if $M^\top = -M$,*
3. *B is alternating if and only if $M^\top = -M$ and the diagonal entries of M are zero.*

Matrices satisfying the conditions in (1), (2), and (3) are called symmmetric, skew-symmetric, and alternating matrices respectively.

Proof. The matrix M represents the linear map $R_B\colon V \to V^\vee$ using the given basis of V and its dual basis. Since L_B and R_B are dual maps in the sense of Theorem 1.21, the matrix representing L_B in these same bases is $M^\top$. Since B is symmetric precisely when $R_B = L_B$, the matrix condition for B to be symmetric is $M = M^\top$. Similarly, skew-symmetry of B means $R_B = -L_B$, which becomes $M = -M^\top$ in matrix language. The matrix condition on an alternating form is left as an exercise. □

The correspondence in (2.1) between bilinear forms and square matrices (once a basis is chosen) behaves well for some natural operations with bilinear forms. For instance, given bilinear forms B and $\widetilde{B}$ on V, we can talk about their sum $B + \widetilde{B}$, a scalar multiple cB, and the function with reversed arguments B_r:

$$(B + \widetilde{B})(v, w) = B(v, w) + \widetilde{B}(v, w), \quad (cB)(v, w) = cB(v, w),$$

$$B_r(v, w) = B(w, v).$$

These are all bilinear forms on V. If we fix a basis of V, so V is identified with F^n and each bilinear form on V is identified with an $n \times n$ matrix by (2.1), the sum and scalar multiple of bilinear forms corresponds to the sum and scalar multiple of the corresponding matrices. Conceptually, this means R_B is linear in B. Since $L_{B_r} = R_B$ and $R_{B_r} = L_B$, the matrix associated to reversing the arguments is the transposed matrix.

Once we pick a basis of V, linear transformations $V \to V$ and bilinear forms on V both get described by square matrices. Addition and scaling of either linear transformations or bilinear forms pass to addition and scaling of the corresponding matrices, and composition of linear transformations passes to multiplication of the corresponding matrices. There is *no* natural operation for bilinear forms on V which corresponds to multiplication of the corresponding matrices. This makes sense from the viewpoint of Exercise 1.5: bilinear forms on V can be viewed as linear maps $V \to V^\vee$, and these can't naturally be composed.

When a linear transformation $L \colon V \to V$ has matrix M in some basis, and C is the change-of-basis matrix expressing a new basis in terms of the old basis, then the matrix for L in the new basis is $C^{-1}MC$. Let's recall two proofs of this and then adapt them to compute the way a change of basis changes the matrix for a bilinear form.

The change-of-basis matrix C, whose columns express the coordinates of the second basis in terms of the first basis, satisfies

$$[v]_1 = C[v]_2 \tag{2.3}$$

for all $v \in V$, where $[\cdot]_i$ is the coordinate isomorphism of V with F^n using the ith basis. Indeed, both sides are linear in v, so it suffices to check this identity when v runs through the second basis, which recovers the definition of C by its columns. Since $[Lv]_1 = M[v]_1$ for all $v \in V$,

$$\begin{aligned} [Lv]_2 &= C^{-1}[Lv]_1 \\ &= C^{-1}M[v]_1 \\ &= C^{-1}MC[v]_2, \end{aligned}$$

so we've proved the matrix for L in the second basis is $C^{-1}MC$.

For a second proof, the identity (2.3) can be expressed as the commutative diagram

$$\begin{tikzcd} V \arrow[r, "\mathrm{id}_V"] \arrow[d, "{[\cdot]_2}"'] & V \arrow[d, "{[\cdot]_1}"] \\ F^n \arrow[r, "C"] & F^n \end{tikzcd} \tag{2.4}$$

and the fact that M is the matrix for L in the first basis means

$$\begin{tikzcd} V \arrow[r, "L"] \arrow[d, "{[\cdot]_1}"'] & V \arrow[d, "{[\cdot]_1}"] \\ F^n \arrow[r, "M"] & F^n \end{tikzcd} \tag{2.5}$$

commutes. To find the matrix for L in the second basis amounts to finding the linear map for the bottom row that makes

$$\begin{tikzcd} V \arrow[r, "L"] \arrow[d, "{[\cdot]_2}"'] & V \arrow[d, "{[\cdot]_1}"] \\ F^n \arrow[r, "?"] & F^n \end{tikzcd}$$

commute. Only one map fits since the vertical maps in this diagram are isomorphisms, so $? = [\cdot]_1 \circ L \circ [\cdot]_2^{-1}$. But what is "?" concretely?

We can obtain such a commutative diagram as the boundary of the commutative diagram with (2.5) in the middle and (2.4) on the two ends

$$\begin{tikzcd} V \arrow[r, "\mathrm{id}_V"] \arrow[d, "{[\cdot]_2}"'] & V \arrow[r, "L"] \arrow[d, "{[\cdot]_1}"'] & V \arrow[r, "\mathrm{id}_V"] \arrow[d, "{[\cdot]_1}"'] & V \arrow[d, "{[\cdot]_2}"'] \\ F^n \arrow[r, "C"] & F^n \arrow[r, "M"] & F^n \arrow[r, "C^{-1}"] & F^n \end{tikzcd}$$

where the composite across the top is L, so $? = C^{-1}MC$ (since composition is written right to left).

Theorem 2.8. *Let C be a change-of-basis matrix on V. A bilinear form on V with matrix M in the first basis has matrix $C^\top MC$ in the second basis.*

Proof. Let B be the bilinear form in the theorem. For a short matrix-based proof of this theorem, start with (2.3). It tells us[1]

$$B(v,w) = [v]_1 \cdot M[w]_1 = C[v]_2 \cdot MC[w]_2 = [v]_2 \cdot C^\top MC[w]_2,$$

so the matrix for B in the second basis is $C^\top MC$.

Now we give a proof using commutative diagrams. By (2.2), the matrix M for B occurs in the commutative diagram

(2.6)
$$\begin{tikzcd} V \arrow[r, "R_B"] \arrow[d, "{[\cdot]_1}"'] & V^\vee \arrow[d, "{[\cdot]'_1}"] \\ F^n \arrow[r, "M"] & F^n \end{tikzcd}$$

where $[\cdot]'_1$ is the coordinate isomorphism using the dual basis to the first basis of V. Finding the matrix for B in the second basis amounts to finding the matrix for the bottom row of a commutative diagram

(2.7)
$$\begin{tikzcd} V \arrow[r, "R_B"] \arrow[d, "{[\cdot]_2}"'] & V^\vee \arrow[d, "{[\cdot]'_2}"] \\ F^n \arrow[r, "?"] & F^n \end{tikzcd}$$

where $[\cdot]'_2$ is the coordinate isomorphism for the dual basis of the second basis of V.

Dualizing the maps and spaces in (2.4) gives the commutative diagram[2]

(2.8)
$$\begin{tikzcd} F^n \arrow[r, "C^\top"] \arrow[d, "{[\cdot]_1^\vee}"'] & F^n \arrow[d, "{[\cdot]_2^\vee}"] \\ V^\vee \arrow[r, "\mathrm{id}_{V^\vee}"] & V^\vee \end{tikzcd}$$

and now we use Exercise 2.7: for any coordinate isomorphism $[\cdot]\colon V \to F^n$ for a basis of V, the coordinate isomorphism $[\cdot]'\colon V^\vee \to F^n$ for the dual basis of $V^\vee$ is the inverse of the dual map $[\cdot]^\vee\colon F^n \to V^\vee$ (where F^n is identified with its dual space using the dot product). Therefore reversing the direction of the vertical maps in (2.8) by using their inverses lets us rewrite (2.8) as

(2.9)
$$\begin{tikzcd} V^\vee \arrow[r, "\mathrm{id}_{V^\vee}"] \arrow[d, "{[\cdot]'_1}"'] & V^\vee \arrow[d, "{[\cdot]'_2}"] \\ F^n \arrow[r, "C^\top"] & F^n \end{tikzcd}$$

---

[1]In F^n, $A\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot A^\top \mathbf{y}$ for any $A \in \mathrm{M}_n(F)$. Apply this with $A = C$.

[2]When $C\colon F^n \to F^n$ is dualized and we think about $(F^n)^\vee$ as F^n using the dot product, the dual map to C is $C^\top$.

so our desired diagram (2.7) can be found by sticking (2.4) and (2.9) on either side of (2.6) and looking at the boundary:

$$\begin{tikzcd} V \arrow[r, "\mathrm{id}_V"] \arrow[d, "{[\cdot]_2}"'] & V \arrow[r, "R_B"] \arrow[d, "{[\cdot]_1}"'] & V^\vee \arrow[r, "\mathrm{id}_{V^\vee}"] \arrow[d, "{[\cdot]'_1}"'] & V^\vee \arrow[d, "{[\cdot]'_2}"'] \\ F^n \arrow[r, "C"] & F^n \arrow[r, "M"] & F^n \arrow[r, "C^\top"] & F^n \end{tikzcd}$$

The composite across the top is R_B and the composite along the bottom is $C^\top MC$, so $C^\top MC$ is our desired matrix. $\square$

Definition 2.9. Two bilinear forms B_1 and B_2 on the respective vector spaces V_1 and V_2 are called *equivalent* if there is a vector space isomorphism $A\colon V_1 \to V_2$ such that

$$B_2(Av, Aw) = B_1(v, w)$$

for all v and w in V_1.

Equivalence of bilinear forms is an equivalence relation. Concretely, if we write everything in coordinates so V_1 and V_2 are replaced by F^n (same n; otherwise there couldn't possibly be an equivalence of bilinear forms on the spaces), then Definition 2.9 says: two bilinear forms on F^n are equivalent when there is a linear change of variables turning one into the other. In particular, when B_1 and B_2 are symmetric bilinear forms on F^n, so they are determined by their diagonal values $B_1(v, v)$ and $B_2(v, v)$ (Theorem 1.8), B_1 and B_2 are equivalent when there is a linear change of variables turning $B_2(v, v)$ into $B_1(v, v)$.

Example 2.10. On $\mathbf{R}^2$, let

$$B(v, w) = v \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) w, \quad \widetilde{B}(v, w) = v \cdot \left(\begin{smallmatrix} 0 & 1/2 \\ 1/2 & 0 \end{smallmatrix}\right) w.$$

Both of these are symmetric. For $v = w = (x, y)$, we have $B(v, v) = x^2 - y^2$ and $\widetilde{B}(v, v) = xy$. Since $x^2 - y^2 = (x + y)(x - y)$, we can pass from B to $\widetilde{B}$ by the linear change of variables $x' = x + y$ and $y' = x - y$. Then $B((x, y), (x, y)) = \widetilde{B}((x', y'), (x', y'))$. Since $\binom{x'}{y'} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)\binom{x}{y}$, $B(v, v) = \widetilde{B}(\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)v, \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)v)$. Therefore $B(v, w) = \widetilde{B}(\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)v, \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)w)$, so B and $\widetilde{B}$ are equivalent by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.

In terms of commutative diagrams, B_1 and B_2 are equivalent when there is a vector space isomorphism $A\colon V_1 \to V_2$ such that the diagram

$$\begin{tikzcd} V_1 \arrow[r, "R_{B_1}"] \arrow[d, "A"'] & V_1^\vee \\ V_2 \arrow[r, "R_{B_2}"] & V_2^\vee \arrow[u, "A^\vee"'] \end{tikzcd} \tag{2.10}$$

commutes. (Verify!)

We saw in Theorem 2.8 that matrix representations M_1 and M_2 of a single bilinear form in two different bases are related by the rule $M_2 = C^\top M_1 C$ for an invertible matrix C. Let's show this rule more generally links matrix representations of equivalent bilinear forms on possibly different vector spaces.

Theorem 2.11. *Let bilinear forms B_1 and B_2 on V_1 and V_2 have respective matrix representations M_1 and M_2 in two bases. Then B_1 is equivalent to B_2 if and only if $M_1 = C^\top M_2 C$ for some invertible matrix C.*

Proof. The equivalence of B_1 and B_2 means, by (2.10), there is an isomorphism $A\colon V_1 \to V_2$ such that $A^\vee R_{B_2} A = R_{B_1}$. Using the bases on V_i ($i = 1, 2$) in which B_i is represented by M_i and the dual bases on $V_i^\vee$, this equation is equivalent to $C^\top M_2 C = M_1$, where C represents A. (Invertibility of C is equivalent to A being an isomorphism.) $\square$

Example 2.12. Returning to Example 2.10, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = C^\top \left(\begin{smallmatrix} 0 & 1/2 \\ 1/2 & 0 \end{smallmatrix}\right) C$ for $C = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.

Although all matrix representations of a linear transformation $V \to V$ have the same determinant ($\det(C^{-1}MC) = \det M$), the matrix representations of a bilinear form on V have the same determinant up to a nonzero square factor: $\det(C^\top MC) = (\det C)^2 \det M$. Since equivalent bilinear forms can be represented by the same matrix using suitable bases, the determinants of any matrix representations for two equivalent bilinear forms must differ by a nonzero square factor. This provides a sufficient (although far from necessary) condition to show two bilinear forms are inequivalent.

Example 2.13. Let d be a squarefree positive integer. On $\mathbf{Q}^2$, the bilinear form $B_d(v, w) = v \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) w$ has a matrix with determinant d, so different (squarefree) d's give inequivalent bilinear forms. Note B_1 is the usual dot product on $\mathbf{Q}^2$. As bilinear forms on $\mathbf{R}^2$ rather than $\mathbf{Q}^2$, all these B_d's are equivalent: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) = C^\top I_2 C$ for $C = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{smallmatrix}\right)$. Another way of putting this is that, relative to coordinates in the basis $\{(1, 0), (0, 1/\sqrt{d})\}$ of $\mathbf{R}^2$, B_d looks like the dot product B_1.

Example 2.14. When q is positive and even, $\langle \cdot, \cdot \rangle_{p,q}$ and the dot product on $\mathbf{R}^{p+q}$ both are represented by matrices with determinant 1, but they are not equivalent: the dot product takes only non-negative values at diagonal pairs (v, v) while $\langle \cdot, \cdot \rangle_{p,q}$ assumes some negative values on the diagonal when $q > 0$. We will see in Section 6 that all the bilinear forms $\langle \cdot, \cdot \rangle_{p,q}$ (with $p + q$ fixed) are inequivalent for different pairs (p, q).

Exercises.

1. Compute the matrix associated to the bilinear forms in Examples 1.9, 1.10, 1.11 and 1.16 relative to the standard basis of column vectors.
2. For $v \in \mathbf{R}^3$, let $L_v\colon \mathbf{R}^3 \to \mathbf{R}^3$ by $L_v(w) = v \times w$. Set $B(v, w) = \mathrm{Tr}(L_v L_w)$. Show B is a symmetric bilinear form on $\mathbf{R}^2$ and compute its matrix relative to the standard basis of $\mathbf{R}^2$.
3. For $x, y \in F$, $\binom{x}{y} \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \binom{x}{y} = x^2$ and $\binom{x}{y} \cdot \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right) \binom{x}{y} = x^2$. Why doesn't this contradict Theorem 2.3?
4. Complete the proof of Theorem 2.7.
5. Show a matrix representation for the trace form on $\mathrm{M}_2(F)$ (Example 1.12) has determinant -1.
6. When V has dimension n, the vector space $\mathrm{Bil}(V)$ of all bilinear forms on V also has dimension n (Exercise 1.5). What are the dimensions of the two subspaces of symmetric and alternating bilinear forms?
7. Let V be n-dimensional over F. Given a basis of V, let $[\cdot]\colon V \to F^n$ be the corresponding coordinate isomorphism and let $[\cdot]'\colon V^\vee \to F^n$ be the coordinate isomorphism coming from the dual basis on $V^\vee$. When we identify F^n with its dual space

using the dot product (that is, view elements of $(F^n)^\vee$ as the maps "dot with a fixed vector"), show the dual map $[\cdot]^\vee : F^n \to V^\vee$ is inverse to $[\cdot]'$.

8. Let $m \geq 4$ be even and $B(v,w) = v \cdot \left(\begin{smallmatrix} m/2 & 1 \\ -1 & m/2 \end{smallmatrix}\right) w$ for $v, w \in (\mathbf{Z}/(m))^2$. Viewing $(\mathbf{Z}/(m))^2$ as a $\mathbf{Z}/(m)$-module, show B is a bilinear form which is skew-symmetric but is neither symmetric nor alternating. Where does the argument break down if $m = 2$?

3. Non-degenerate bilinear forms

Although there is not a natural operation on bilinear forms which corresponds to multiplication of matrices, there is a condition on a bilinear form which corresponds to invertibility of its matrix representation.

Theorem 3.1. *Let (V, B) be a bilinear space. The following conditions are equivalent:*

(1) *for some basis $\{e_1, \ldots, e_n\}$ of V, the matrix $(B(e_i, e_j))$ is invertible,*
(2) *if $B(v, v') = 0$ in for all $v' \in V$ then $v = 0$,*
(3) *every element of $V^\vee$ has the form $B(v, -)$ for some $v \in V$,*
(4) *every element of $V^\vee$ has the form $B(v, -)$ for a unique $v \in V$.*

When this occurs, every matrix representation for B is invertible.

Proof. The matrix $(B(e_i, e_j))$ is a matrix representation of the linear map $R_B : V \to V^\vee$ by Theorem 2.5. So condition (1) says R_B is an isomorphism.

The functions $B(v, -)$ in $V^\vee$ are the values of $L_B : V \to V^\vee$, so condition (2) says $L_B : V \to V^\vee$ is injective. Condition (3) says L_B is surjective and (4) says L_B is an isomorphism. Since L_B is a linear map between vector spaces of the same dimension, injectivity, surjectivity, and isomorphy are equivalent properties. So (2), (3), and (4) are equivalent. Since L_B and R_B are dual to each other (Theorem 1.21), (1) and (4) are equivalent.

Different matrix representations M and M' of a bilinear form are related by $M' = C^\top MC$ for some invertible matrix C, so if one matrix representation is invertible then so are the others. $\square$

The key point of Theorem 3.1 is that V parametrizes its own dual space by the functions $B(v, -)$ exactly when a matrix for B is invertible. When this happens, each element of the dual space is also described as $B(-, v)$ for a some v, necessarily unique, by interchanging the roles of L_B and R_B in the proof of Theorem 3.1.

Definition 3.2. Let (V, B) be a nonzero bilinear space. We call V or B *non-degenerate* if the equivalent conditions in Theorem 3.1 hold. A bilinear space or bilinear form which is not non-degenerate is called *degenerate*.

A bilinear form on V is essentially the same as a linear map $V \to V^\vee$ (Exercise 1.5), so a choice of non-degenerate bilinear form on V is really the same thing as a choice of isomorphism $V \to V^\vee$. Since $V \cong V^\vee$ when $V = \{0\}$, for completeness the zero vector space with its only (zero) bilinear form is considered to be non-degenerate although there is no matrix.

Example 3.3. The dot product on $\mathbf{R}^n$ is non-degenerate: if $v \cdot w = 0$ for all $w \in \mathbf{R}^n$, then in particular $v \cdot v = 0$, so $v = 0$. (Alternatively, the matrix representation for the dot product in the standard basis is I_n, which is invertible.) Thus each element of $(\mathbf{R}^n)^\vee$ has the form $\varphi(w) = v \cdot w$ for a unique $v \in \mathbf{R}^n$; the elements of $(\mathbf{R}^n)^\vee$ are just dotting with a fixed vector.

Example 3.4. The symmetric bilinear form $\langle \cdot, \cdot \rangle_{p,q}$ which defines $\mathbf{R}^{p,q}$ (Example 2.4) is non-degenerate: for nonzero $v = (c_1, \dots, c_n)$ in $\mathbf{R}^{p,q}$, it may happen that $\langle v, v \rangle_{p,q} = 0$, but certainly *some* coordinate c_i is nonzero, so $\langle v, e_i \rangle_{p,q} = \pm c_i \neq 0$ for that i. (Alternatively, the matrix for $\langle \cdot, \cdot \rangle_{p,q}$ in the standard basis is $M = \left(\begin{smallmatrix} I_p & O \\ O & -I_q \end{smallmatrix}\right)$, which is invertible.) Thus each $\varphi \in (\mathbf{R}^{p,q})^\vee$ looks like $\varphi(w) = \langle v, w \rangle_{p,q}$ for a unique $v \in \mathbf{R}^{p,q}$.

At the same time, a dual space doesn't know about bilinear forms: letting $n = p + q$, $\mathbf{R}^{p,q}$ equals $\mathbf{R}^n$ as vector spaces, so their dual spaces are the same. How can we reconcile the descriptions of the dual space here and in Example 3.3? Well, $\langle v, w \rangle_{p,q} = v \cdot Mw$, where M is symmetric and $M = M^{-1}$. Therefore the descriptions of the dual space of $\mathbf{R}^n$ using the dot product and using $\langle \cdot, \cdot \rangle_{p,q}$ match up as follows:

$$\langle v, - \rangle_{p,q} = Mv \cdot (-), \quad v \cdot (-) = \langle Mv, - \rangle_{p,q}.$$

Example 3.5. Example 1.5 is non-degenerate: pairing a nonzero vector with at least one of $(1, 0)$ or $(0, 1)$ will give a nonzero result. Alternatively, this bilinear form is represented by an invertible matrix.

Example 3.6. The alternating bilinear form on $V \oplus V^\vee$ in Example 1.13 is non-degenerate. Indeed, assume (v, φ) lies in $(V \oplus V^\vee)^\perp$, so $\psi(v) = \varphi(w)$ for all $w \in V$ and $\psi \in V^\vee$. Taking for ψ the zero dual vector, $\varphi(w) = 0$ for all w, so $\varphi = 0$. Therefore $\psi(v) = 0$ for all $\psi \in V^\vee$, so $v = 0$.

Example 3.7. Let's see a degenerate bilinear form. On $\mathbf{R}^2$ set $B(v, w) = v \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) w$. In coordinates, $B((x, y), (x', y')) = xx'$. This is degenerate since the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is not invertible. We have $(0, 1) \perp w$ for all w. The matrix representing B is not invertible.

Remark 3.8. On a real vector space, a bilinear form B is called *positive-definite* if $B(v, v) > 0$ for every $v \neq 0$. The dot product on $\mathbf{R}^n$ is positive-definite. Any positive-definite bilinear form is non-degenerate (using $w = v$). Non-degeneracy is the right generalization of positive-definiteness to bilinear forms on vector spaces over general fields (where positivity no longer makes sense). Positive-definite symmetric bilinear forms play an important role in analysis (real Hilbert spaces) and geometry (Riemannian manifolds). For geometers, the impetus to explore the consequences of weakening positive-definitness to non-degeneracy came from physics, where the local model spaces in relativity theory are pseudo-Euclidean (Example 2.4); they carry a symmetric bilinear form which is not positive-definite but is non-degenerate. Real vector spaces equipped with a non-degenerate alternating bilinear form are the local models for phase spaces in Hamiltonian mechanics.

Example 3.9. Although $\mathbf{R}^{2,1}$ is non-degenerate, the plane spanned by $v_1 = (1, 0, 1)$ and $v_2 = (0, 1, 0)$ in $\mathbf{R}^{2,1}$ is degenerate (that is, the restriction of $\langle \cdot, \cdot \rangle_{2,1}$ to this plane is degenerate) since $v_1 \perp v_1$ and $v_1 \perp v_2$. There are vectors in $\mathbf{R}^{2,1}$ which are not perpendicular to v_1, such as $(1, 0, 0)$, but such vectors don't lie in the plane of v_1 and v_2.

Example 3.9 is good to remember: a non-degenerate bilinear form on a vector space might restrict to a degenerate bilinear form on a subspace. Such behavior is impossible if V is a real vector space and B is positive-definite (Remark 3.8): when $B(v, v) > 0$ for all nonzero $v \in V$, this property remains true on *any* nonzero subspace $W \subset V$, so the restriction $B|_W$ is also positive-definite and thus is also non-degenerate.

Theorem 3.10. *Let V be a bilinear space which is either symmetric or alternating and let W be a subspace of V.*

(1) *The following are equivalent:*
 - *W is non-degenerate,*
 - *$W \cap W^\perp = \{0\}$,*
 - *$V = W \oplus W^\perp$.*

(2) *For non-degenerate V, $\dim W + \dim W^\perp = \dim V$ and $(W^\perp)^\perp = W$.*

In particular, if V is non-degenerate then a subspace W is non-degenerate if and only if $W^\perp$ is non-degenerate.

Part (1) characterizes the subspaces of a symmetric or alternating bilinear space which are non-degenerate: they are exactly the subspaces which are complementary to their orthogonal space in the sense of linear algebra. The validity of this theorem for $W = \{0\}$ is a reason for declaring the zero space to be non-degenerate.

Proof. Let B be the given bilinear form on V.

(1) Suppose B is non-degenerate on W. This is equivalent to saying no nonzero element of W lies in $W^\perp$, or equivalently $W \cap W^\perp = \{0\}$.

Trivially if $V = W \oplus W^\perp$ then $W \cap W^\perp = \{0\}$. Now assume $W \cap W^\perp = \{0\}$. We will show $V = W + W^\perp$; the directness of the sum is immediate since the subspaces intersect in $\{0\}$.

Since $W \cap W^\perp$ is the kernel of the linear map $W \to W^\vee$ given by $w \mapsto B(w, -)|W$, this map is an isomorphism: every element of $W^\vee$ has the form $B(w, -)|_W$ for some $w \in W$. To show each $v \in V$ is a sum of elements of $w \in W$ and $w' \in W^\perp$, think about $B(v, -)|_W$. It has the form $B(w, -)|_W$ for a $w \in W$. Then $B(v, w') = B(w, w')$ for all $w' \in W$, so $B(v - w, w') = 0$ for all w'. Thus $v - w \in W^\perp$, so $v \in W + W^\perp$ and we're done.

(2) Consider how elements of v pair with elements in W. This amounts to looking at the map $v \mapsto B(v, -)|_W$, which is the composite of $L_B \colon V \to V^\vee$ with the restriction map $V^\vee \to W^\vee$. The first is an isomorphism (since V is non-degenerate) and the second is onto (why?), so the composite is onto. The kernel of the composite is $W^\perp$, so $V/W^\perp \cong W^\vee$. Taking the dimension of both sides, $\dim V - \dim W^\perp = \dim W^\vee = \dim W$.

Easily $W \subset (W^\perp)^\perp$; since their dimensions are equal, the spaces coincide. Since $(W^\perp)^\perp = W$ for non-degenerate V, the condition on W being non-degenerate is symmetric in the roles of W and $W^\perp$, so W is non-degenerate if and only if $W^\perp$ is. $\square$

Example 3.11. We continue with Example 3.9. Let W be the plane in $\mathbf{R}^{2,1}$ spanned by $(1, 0, 1)$ and $(0, 1, 0)$. Since $\langle \cdot, \cdot \rangle_{2,1}$ is non-degenerate on $\mathbf{R}^{2,1}$, $\dim W + \dim W^\perp = 3$, so $W^\perp$ is one-dimensional. A direct calculation shows $W^\perp = \mathbf{R}(1, 0, 1)$. Since $W^\perp \subset W$, $\mathbf{R}^{2,1}$ is not the (direct) sum of W and $W^\perp$, which is consistent with W being a degenerate subspace of $\mathbf{R}^{2,1}$.

Example 3.12. We look at the symmetric bilinear space $(\mathbf{R}^2, B)$ in Example 3.7, which is degenerate. Let $W = \mathbf{R}(1, 0)$. This subspace is non-degenerate, so $\mathbf{R}^2 = W \oplus W^\perp$. Indeed, $W^\perp = \mathbf{R}(0, 1)$. However, since the whole space is degenerate we need not have $(W^\perp)^\perp = W$, and in fact $(W^\perp)^\perp = \mathbf{R}^2$. Thus W is non-degenerate but $W^\perp$ is degenerate.

Remark 3.13. Do not confuse the two conditions $V = W \oplus W^\perp$ and $\dim W^\perp = \dim V - \dim W$. The first implies the second, but the converse is false: W and $W^\perp$ can overlap nontrivially and their dimensions can still be complementary. By Theorem 3.10, when V is symmetric or alternating we have $\dim W^{\perp} = \dim V - \dim W$ if V is non-degenerate and W is an arbitrary subspace or if V is arbitrary and W is a non-degenerate subspace.

Theorem 3.14. *Let (V, B) be non-degenerate.*

(1) *Every hyperplane*[3] *in V has the form $\{w : v \perp w\}$ for some $v \neq 0$ and $\{w : w \perp v'\}$ for some $v' \neq 0$.*
(2) *If $B(v, w) = B(v, w')$ for all $v \in V$ then $w = w'$.*
(3) *If A and A' are linear maps $V \to V$ and $B(v, Aw) = B(v, A'w)$ for all v and w in V then $A = A'$.*
(4) *Every bilinear form on V looks like $B(v, Aw)$ for some linear map $A\colon V \to V$.*

Proof. (1) Let $H \subset V$ be a hyperplane. The quotient space V/H has dimension 1, so it is (non-canonically) isomorphic to F. Pick an isomorphism $V/H \cong F$. The composite $V \to V/H \cong F$ is a nonzero linear map to F, with kernel H, so $H = \ker \varphi$ for some nonzero $\varphi \in V^{\vee}$. (This has nothing to do with bilinear forms: hyperplanes in V always are kernels of nonzero elements of the dual space of V; the converse is true as well.) Since (V, B) is non-degenerate, $\varphi = B(v, -)$ for some nonzero v and $\varphi = B(-, v')$ for some nonzero v', so $H = \{w : B(v, w) = 0\} = \{w : B(w, v') = 0\}$.

(2) The hypothesis of (2) says $R_B(w) = R_B(w')$, so $w = w'$ since R_B is an isomorphism.

(3) By (2), $Aw = A'w$ for all w, so $A = A'$.

(4) When $A\colon V \to V$ is linear, let $\varphi_A\colon V \times V \to F$ by $\varphi_A(v, w) = B(v, Aw)$. Then φ_A is a bilinear form on V. The correspondence $A \mapsto \varphi_A$ is a map from $\mathrm{Hom}_F(V, V)$ to the space $\mathrm{Bil}(V)$ of all bilinear forms on V (Exercise 1.5), and it is linear. (That is, $\varphi_{A+A'} = \varphi_A + \varphi_{A'}$ and $\varphi_{cA} = c\varphi_A$.) Part (2) says $A \mapsto \varphi_A$ is injective. Since $\mathrm{Hom}_F(V, V)$ and $\mathrm{Bil}(V)$ have the same dimension, this correspondence is an isomorphism. $\square$

Concerning the second property in Theorem 3.14, if $B(v, w) = B(v, w')$ for just one v we can't conclude $w = w'$, even in $\mathbf{R}^n$ with the dot product.

Although all bilinear forms have the form $B(v, Aw)$, we can certainly write down bilinear forms in other ways, such as $B(Av, w)$. Theorem 3.14 says this bilinear form can be written as $B(v, A^*w)$ for some linear map $A^*\colon V \to V$.

Definition 3.15. When (V, B) is non-degenerate and $A\colon V \to V$ is linear, the unique linear map $A^*\colon V \to V$ satisfying

$$B(Av, w) = B(v, A^*w) \tag{3.1}$$

for all v and w in V is called the *adjoint* of A relative to B

Example 3.16. On F^n, let $B(v, w) = v \cdot w$. For $A \in \mathrm{M}_n(F)$, $Av \cdot w = v \cdot A^{\top}w$ for all v and w in F^n, so the adjoint of A relative to the dot product is the transpose of A. This close relation between the dot product and transpose is one of the reasons that the transpose is important, especially when $F = \mathbf{R}$.

Example 3.17. On $\mathbf{R}^2$, let $B(v, w) = v \cdot \left(\begin{smallmatrix} 3 & 0 \\ 0 & -2 \end{smallmatrix}\right) w$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, viewed as a linear map $\mathbf{R}^2 \to \mathbf{R}^2$. We want to work out the map $A^*\colon \mathbf{R}^2 \to \mathbf{R}^2$. For $v = \binom{x}{y}$ and $w = \binom{x'}{y'}$ in $\mathbf{R}^2$,

$$\begin{aligned} B(Av, w) &= 3(ax + by)x' - 2(cx + dy)y' \\ &= 3axx' + 3bx'y - 2cxy' - 2dyy'. \end{aligned}$$

[3]A hyperplane is a subspace with dimension $n - 1$, where $n = \dim V$; they are the natural complements to linear subspaces.

Writing $A^* = \left(\begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix}\right)$,

$$\begin{aligned} B(v, A^*w) &= 3x(a^*x' + b^*y') - 2y(c^*x' + d^*y') \\ &= 3a^*xx' - 2c^*x'y + 3b^*xy' - 2d^*yy'. \end{aligned}$$

Coefficients must match in the two formulas for $B(Av, w)$ and $B(v, A^*w)$, since bilinear forms have the same matrix, so $a^* = a$, $b* = -(2/3)c$, $c^* = -(3/2)b$, and $d^* = d$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^* = \left(\begin{smallmatrix} a & -(2/3)c \\ -(3/2)b & d \end{smallmatrix}\right)$. Notice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^*$ has the same trace and determinant as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Let's see how to compute the matrix of the adjoint of a linear map for abstract vector spaces when bases are chosen. The formula will show that the adjoint on $\mathrm{Hom}_F(V, V)$ and transpose on $\mathrm{M}_n(F)$ are closely related.

Theorem 3.18. *Let $A\colon V \to V$ be linear. Fix a basis of V. In terms of this basis, let $[A], [A^*]$, and M be the matrices for A, A^*, and B. Then*

$$[A^*] = M^{-1}[A]^\top M.$$

Proof. We will give two proofs.

For a matrix-algebra proof, the choice of basis on V gives an isomorphism $[\cdot]\colon V \to F^n$. Let's write both sides of (3.1) in matrix form relative to the chosen basis. The left side is

$$[Av] \cdot M[w] = [A][v] \cdot M[w] = [v] \cdot [A]^\top M[w]$$

and the right side is

$$[v] \cdot M[A^*w] = [v] \cdot M[A^*][w].$$

Since this holds for all v and w,

$$[A]^\top M = M[A^*],$$

which is equivalent to the desired formula since M is invertible.

For a different proof, we use the fact that M is the matrix for R_B (Theorem 2.5). Since $R_B A^* = A^\vee R_B$ (Exercise 3.20), $A^* = R_B^{-1} A^\vee R_B$ as linear maps from V to V. Passing to matrix representations, $[A^*] = M^{-1}[A]^\top M$. $\square$

We will put the construction of the adjoint to work to answer an interesting question: when (V, B) is a non-degenerate bilinear space, we want to describe the linear maps $A\colon V \to V$ which preserve orthogonality for B:

$$v \perp w \Longrightarrow Av \perp Aw. \tag{3.2}$$

(We are not insisting that the converse holds, only that A carries orthogonal vectors to orthogonal vectors.) For instance, if $B(Av, Aw) = B(v, w)$ for all v and w (that is, if A "preserves" B) then (3.2) holds. But (3.2) can take place under more general circumstances: if there is a scalar $c \in F$ such that $B(Av, Aw) = cB(v, w)$ for all v and w then (3.2) still holds. It turns out that this sufficient condition for (3.2) is also necessary when B is non-degenerate.

Theorem 3.19. *Let (V, B) be non-degenerate. For a linear transformation $A\colon V \to V$, the following properties are equivalent:*

1. *$v \perp w \Longrightarrow Av \perp Aw$ for all v and w in V,*
2. *there is a constant $c \in F$ such that $B(Av, Aw) = cB(v, w)$ for all v and w in V.*
3. *there is a constant $c \in F$ such that $A^*A = c\,\mathrm{id}_V$.*

The heart of the proof of Theorem 3.19 is the following lemma from linear algebra which characterizes scaling transformations geometrically (and has nothing to do with bilinear forms).

Lemma 3.20. *If V is finite-dimensional over F and a linear transformation $L\colon V \to V$ carries every linear subspace into itself then L is a scaling transformation: $Lv = cv$ for some $c \in F$ and all $v \in V$. The same conclusion holds if L carries every hyperplane into itself.*

Another way of describing the first part of the lemma is that the only linear map which has all (nonzero) vectors as eigenvectors is a scaling transformation. The application to Theorem 3.19 will use the hyperplane case of the lemma.

Proof. For each nonzero $v \in V$, L carries the line Fv into itself, so $Lv = c_v v$ for some $c_v \in F$. We want to show all the constants c_v ($v \neq 0$) are the same. Then calling this common value c gives us $Lv = cv$ for all $v \neq 0$ and this is trivially also true at $v = 0$, so we'd be done with the linear subspace case of the theorem.

Pick any nonzero v and v' in V. If v and v' are linearly dependent then $v = av'$ for some $a \in F^\times$. Applying L to both sides,

$$c_v v = L(v) = L(av) = aL(v) = ac_{v'}v' = c_{v'}v,$$

so $c_v = c_{v'}$. If v and v' are linearly independent, then we consider the constants associated to v, v', and $v + v'$. Since $L(v + v') = Lv + Lv'$,

$$c_{v+v'}(v + v') = c_v v + c_{v'}v'.$$

By linear independence of v and v', $c_{v+v'} = c_v$ and $c_{v+v'} = c_{v'}$, so $c_v = c_{v'}$ again.

Now we turn to the hyperplane case: assume $L(H) \subset H$ for every hyperplane $H \subset V$. We are going to convert this condition about L on hyperplanes in V into a condition about the dual map $L^\vee\colon V^\vee \to V^\vee$ on linear subspaces of $V^\vee$, to which the first case can be applied.

Pick a linear subspace of $V^\vee$, say $F\varphi$ for some nonzero $\varphi \in V^\vee$. Then $H := \ker \varphi$ is a hyperplane in V, so by hypothesis $L(H) \subset H$. That is, if $\varphi(v) = 0$ then $\varphi(L(v)) = 0$. (Verify!) Since $\varphi \circ L = L^\vee(\varphi)$, we obtain that if $\varphi(v) = 0$ then $(L^\vee(\varphi))(v) = 0$, so $\ker \varphi \subset \ker L^\vee(\varphi)$. Since $H = \ker \varphi$ has dimension $n - 1$ (let $n = \dim V$), either $\ker L^\vee(\varphi) = H$ or $\ker L^\vee(\varphi) = V$. If $\ker L^\vee(\varphi) = H$ then $L^\vee(\varphi)$ and φ have the same kernel, so they both induce isomorphisms $V/H \to F$. An isomorphism between two one-dimensional vector spaces is multiplication by a nonzero constant, so there is some constant $c_\varphi \in F^\times$ such that $L^\vee(\varphi) = c_\varphi \varphi$ as functions on V/H and thus also as functions pulled back to V itself. That shows $L^\vee(\varphi) \in F\varphi$. On the other hand, if $\ker L^\vee(\varphi) = V$ then $L^\vee(\varphi)$ is the zero functional and then we certainly have $L^\vee(\varphi) \in F\varphi$. Either way, $L^\vee$ carries every nonzero element of $V^\vee$ to a scalar multiple of itself (perhaps the zero multiple), so $L^\vee$ carries all linear subspaces of $V^\vee$ back to themselves.

Apply the first part of the lemma to the vector space $V^\vee$ and the linear map $L^\vee$: there is some $c \in F$ such that $L^\vee(\varphi) = c\varphi$ for all $\varphi \in V^\vee$. Applying both sides to any $v \in V$, we get $\varphi(L(v)) = c\varphi(v) = \varphi(cv)$ for all $\varphi \in V^\vee$. Two vectors at which all elements of the dual space are equal must themselves be equal, so $L(v) = cv$. We have shown this for all $v \in V$, so $L = c\,\mathrm{id}_V$. $\square$

Now we prove Theorem 3.19.

Proof. Trivially (2) implies (1). To show (1) implies (2), (1) tells us that if $B(v,w)=0$ then $B(Av,Aw)=0$, so $B(v,A^*Aw)=0$. When $v\neq 0$, $\{w : v\perp w\}$ is a hyperplane in V and A^*A carries this hyperplane back to itself. Every hyperplane in V has the form $\{w : v\perp w\}$ for some nonzero v (Theorem 3.14(1)), so A^*A carries every hyperplane of V into itself. Therefore $A^*A = c\,\mathrm{id}_V$ for some $c\in F$ by Lemma 3.20.

To show (2) and (3) are equivalent, the condition $B(Av,Aw)=cB(v,w)$ for all v and w is the same as $B(v,A^*Aw)=B(v,cw)$, which is equivalent to $A^*A=c\,\mathrm{id}_V$ by Theorem 3.14(3). $\square$

Example 3.21. Let $B(v,w)=v\cdot\left(\begin{smallmatrix}3&0\\0&-2\end{smallmatrix}\right)w$ on $\mathbf{R}^2$. Theorem 3.19 says that a matrix $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ preserves B-orthogonality exactly when it affects B-values by a universal scaling factor. We will find such a matrix, which will amount to solving a system of equations.

We found in Example 3.17 that $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)^*=\left(\begin{smallmatrix}a&-(2/3)c\\-(3/2)b&d\end{smallmatrix}\right)$, so

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}^*\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a^2-(2/3)c^2 & ab-(2/3)cd\\ -(3/2)ab+cd & -(3/2)b^2+d^2\end{pmatrix}.$$

The product is a scalar diagonal matrix when $ab=(2/3)cd$ and $a^2-(2/3)c^2=d^2-(3/2)b^2$. Take $b=2$ and $c=3$ (to avoid denominators), so our conditions reduce to $a=d$. Therefore $A=\left(\begin{smallmatrix}a&2\\3&a\end{smallmatrix}\right)$, with $A^*A=(a^2-6)I_2$. Let $a=4$, just to fix ideas, so $A=\left(\begin{smallmatrix}4&2\\3&4\end{smallmatrix}\right)$ satisfies $B(Av,Aw)=10B(v,w)$.

Although the adjoint operation satisfies many algebraic properties of the transpose (Exercise 3.17), there is one important distinction. Sometimes $A^{**}\neq A$. Let's see why. Applying Theorem 3.18 twice,

$$[A^{**}]=M^{-1}M^\top[A](M^{-1})^\top M,$$

so $A^{**}=A$ for all A only when $M^{-1}M^\top$ is a nonzero scalar matrix. (Abstractly, this means $R_B^{-1}L_B$ is a nonzero scaling transformation.) Right away we see that in the most important cases of symmetric or alternating bilinear forms, where $M^\top=\pm M$, we *do* have $A^{**}=A$, but in other cases it need not happen. (A counterexample is in Exercise 3.16.)

The failure of $A^{**}=A$ may seem puzzling. Why shouldn't it be true? The reason is that our definition of the adjoint had a built-in bias: it was defined to satisfy $B(Av,w)=B(v,A^*w)$ for all v and w rather than $B(v,Aw)=B(A^*v,w)$ for all v and w. The second equation defines an alternate adjoint for A, just as L_B and R_B are alternate isomorphisms of V with $V^\vee$.

Table 1 collects several constructions we have met.

Coordinate-free	Matrix Version
Bilinear form B	$B(v,w)=[v]\cdot M[w]$
Change of basis	$M \rightsquigarrow C^\top MC$
B is symmetric	$M^\top = M$
B is skew-symmetric	$M^\top=-M$
B is alternating	$M^\top=-M$, diagonals $=0$
B is non-degenerate	M is invertible
A^*	$M^{-1}[A]^\top M$

TABLE 1. Abstract and Concrete Viewpoints

Exercises.

1. In $\mathbf{R}^{2,2}$, let W be the plane spanned by $(1,0,0,0)$ and $(0,0,1,0)$. Compute $W^\perp$. Is W a degenerate subspace?
2. Let (V,B) be a bilinear space with B not identically zero. If B is symmetric show V has a one-dimensional non-degenerate subspace. If B is alternating show V has a two-dimensional non-degenerate subspace.
3. Let (V,B) be symmetric or alternating. Show B induces a non-degenerate bilinear form on $V/V^\perp$. Writing $V = V^\perp \oplus W$ for any subspace W which is complementary to $V^\perp$, show W is non-degenerate.
4. A 2-dimensional symmetric or alternating bilinear space is called a *hyperbolic plane* if it has a basis $\{v,w\}$ such that $v \perp v$, $w \perp w$, and $B(v,w) = 1$ (so $B(w,v) = \pm 1$). A pair of vectors with these three properties is called a *hyperbolic pair*. If V is a non-degenerate symmetric or alternating bilinear space and $v_0 \perp v_0$ for some nonzero v_0 in V, show every non-degenerate plane in V containing v_0 is a hyperbolic plane with v_0 as one member of a hyperbolic pair except perhaps if F has characteristic 2 and B is symmetric but not alternating.
5. When F has characteristic 2 and $B(v,w) = v \cdot \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) w$ for $v,w \in F^2$, show $(0,1) \perp (0,1)$ but there is no hyperbolic pair in F^2. Therefore the exceptional case in the previous exercise does occur.
6. Check that the reasoning in Example 3.4 shows the dot product on any F^n is non-degenerate. Why doesn't the argument in Example 3.3 apply to the dot product on every F^n?
7. Does the first result in Theorem 3.14 characterize non-degeneracy? That is, if each hyperplane in V has the form $\{w : v \perp w\}$ for some $v \neq 0$, is V non-degenerate?
8. Show B in Exercise 2.8 is non-degenerate if and only if $4|m$. (What should non-degenerate mean?)
9. Fix a non-degenerate bilinear form B on V. For a linear map $A \colon V \to V$, show the bilinear form on V given by $(v,w) \mapsto B(v, Aw)$ is non-degenerate if and only if A is invertible.
10. If V_1 and V_2 are bilinear spaces, show their orthogonal direct sum $V_1 \perp V_2$ is non-degenerate if and only if V_1 and V_2 are non-degenerate.
11. Suppose V is symmetric or alternating and non-degenerate. For any subspaces W_1 and W_2, show
$$(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp, \quad (W_1 \cap W_2)^\perp = W_1^\perp + W_2^\perp.$$
Show a subspace W is non-degenerate if and only if $V = W + W^\perp$.
12. For a subspace $W \subset V$, where V is finite-dimensional, define $W^\perp = \{\varphi \in V^\vee : \varphi(w) = 0 \text{ for all } w \in W\}$. (There is no hidden bilinear form on V: now $W^\perp$ is a subspace of the dual space of V.) Show $\dim W + \dim W^\perp = \dim V$.
13. Let (V,B) be non-degenerate, but not necessarily symmetric or alternating. For any subspace W of V, set $W^{\perp_L} = \{v \in V : v \perp W\}$ and $W^{\perp_R} = \{v \in V : W \perp v\}$. Show $W^{\perp_L}$ and $W^{\perp_R}$ both have dimension $\dim V - \dim W$ and $W^{\perp_L \perp_R} = W^{\perp_R \perp_L} = W$.
14. Use Theorem 3.18 to recompute the adjoint in Example 3.17.
15. On $\mathbf{R}^{1,1}$, show $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^* = \left(\begin{smallmatrix} a & -c \\ -b & d \end{smallmatrix}\right)$ using Theorem 3.18. Relative to the bilinear form on $\mathbf{R}^2$ from Example 1.5, show $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^* = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.
16. Let $B(v,w) = v \cdot \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) w$ on $\mathbf{R}^2$. In $(\mathbf{R}^2, B)$, show $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{**} \neq \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

17. With $A \rightsquigarrow A^*$ defined as in (3.1), verify the following.
    (1) $(A_1 + A_2)^* = A_1^* + A_2^*$ and $(cA)^* = cA^*$,
    (2) $\mathrm{id}_V^* = \mathrm{id}_V$,
    (3) $(A_1A_2)^* = A_2^*A_1^*$,
    (4) $(A^*)^{-1} = (A^{-1})^*$ if $A \in \mathrm{GL}(V)$,
    (5) $\det A^* = \det A$, $\mathrm{Tr}(A^*) = \mathrm{Tr}(A)$, and A and A^* have the same characteristic polynomial.
18. Let $n = \dim V \geq 2$ and fix an integer d from 1 to $n-1$. If $L\colon V \to V$ is a linear map carrying every d-dimensional subspace to itself show L is a scaling transformation. (Hint: Show by induction on the subspace dimension that L sends every hyperplane of V to itself, so Theorem 3.20 applies.)
19. When (V, B) is non-degenerate and $A\colon V \to V$ is linear, define an adjoint $A^\dagger\colon V \to V$ by $B(v, A(-)) = B(A^\dagger v, -)$ in $V^\vee$: $B(v, Aw) = B(A^\dagger v, w)$ for all v and w in V. When B is represented by the matrix M in some basis, what is the matrix for $A^\dagger$ in this basis?
20. Let (V, B) be non-degenerate. The bilinear form B gives us two ways of identifying V with $V^\vee$: $L_B(v) = B(v, -)$ and $R_B(v) = B(-, v)$.

    For a linear map $A\colon V \to V$, the dual map $A^\vee\colon V^\vee \to V^\vee$ does not depend on B, while A^* does. Show A^* fits into the following commutative diagram, where the columns are isomorphisms (depending on B).

$$\begin{array}{ccc} V & \xrightarrow{A^*} & V \\ {\scriptstyle R_B}\downarrow & & \downarrow{\scriptstyle R_B} \\ V^\vee & \xrightarrow{A^\vee} & V^\vee \end{array}$$

    What is the corresponding commutative diagram connecting $A^\vee$ and $A^\dagger$ in the previous exercise?
21. Redo the material on adjoints in this section so it applies to linear maps between different non-degenerate bilinear spaces. If $A\colon V_1 \to V_2$ is linear then the adjoint should be a map $A^*\colon V_2 \to V_1$. In particular, rework the previous exercise (and its application to Theorem 3.18) in this setting.

4. Orthogonal bases

Part of the geometric structure of $\mathbf{R}^n$ is captured by the phrase "orthogonal basis." This is a basis of mutually perpendicular vectors, and the lines through these vectors provide an orthogonal set of axes for $\mathbf{R}^n$. Let's generalize this idea.

Fix for this section a symmetric bilinear space (V, B).

Definition 4.1. A basis $\{e_1, \ldots, e_n\}$ of V is *orthogonal* when $e_i \perp e_j = 0$ for $i \neq j$.

Our convention in the one-dimensional case, where there aren't basis pairs $\{e_i, e_j\}$ with $i \neq j$ to compare, is that any basis is orthogonal. The zero bilinear space has no orthogonal basis (its basis is empty).

Example 4.2. On $\mathbf{R}^2$, let $B(v, w) = v \cdot \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) w$. The basis $\{(1, 0), (0, 1)\}$ is orthogonal with respect to B.

Example 4.3. On $\mathbf{R}^2$, let $B(v, w) = v \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) w$. The basis $\{(1, 0), (0, 1)\}$ is not orthogonal: $B((1, 0), (0, 1)) = 1$. In fact, there is no orthogonal basis containing $(1, 0)$ since the only vectors orthogonal to $(1,0)$ are scalar multiples of $(1,0)$. (We will understand this phenomenon better in Remark 4.9.) An orthogonal basis for B is $\{(1,1),(1,-1)\}$.

Example 4.4. When B is identically zero, any basis of V is an orthogonal basis.

Geometrically, an orthogonal basis of V gives a decomposition of V into an orthogonal direct sum of lines: $V = W_1 \perp W_2 \perp \cdots \perp W_n$, where $W_i = Fe_i$.

While Euclidean space has the more refined notion of an orthonormal basis, we will find essentially no use for this idea. The reason is that it usually doesn't exist! An orthonormal basis should be an orthogonal basis $\{e_1, \ldots, e_n\}$ in which $B(e_i, e_i) = 1$ for all i. But there is no orthonormal basis in Example 4.2 using $\mathbf{Q}^2$ in place of $\mathbf{R}^2$ since the equation $2x^2+3y^2 = 1$ has no rational solutions (Exercise 4.7).

The matrix representing a bilinear form in an orthogonal basis is diagonal, and thus is a symmetric matrix. This is why we only defined orthogonal bases for symmetric bilinear spaces. Our basic task in this section is to prove any symmetric bilinear space (degenerate or non-degenerate) admits an orthogonal basis provided the scalar field F does not have characteristic 2. In characteristic 2 we will see there are problems.

Lemma 4.5. *If B is not identically zero and the characteristic of F is not 2 then $B(v,v) \neq 0$ for some $v \in V$.*

Proof. See Theorem 1.8 for one proof. For another proof, let's show the contrapositive. If $B(v,v) = 0$ for all v then B is alternating, or equivalently (since we are not in characteristic 2) skew-symmetric. The only bilinear form which is both symmetric and skew-symmetric outside of characteristic 2 is identically zero. □

Lemma 4.6. *Let $v \in V$ satisfy $B(v,v) \neq 0$. Then $V = Fv \perp v^\perp$. If V is non-degenerate then the subspace $v^\perp$ is non-degenerate.*

Notice this is valid in characteristic 2.

Proof. Since B is non-degenerate on the subspace Fv, this lemma is a consequence of Theorem 3.10, but we give a self-contained proof anyway.

Since $B(v,v) \neq 0$, every element of F is a scalar multiple of $B(v,v)$. For $v' \in V$, let $B(v',v) = cB(v,v)$ for $c \in F$. Then $B(v'-cv, v) = 0$, so $v' - cv \in v^\perp$. Therefore the equation

$$v' = cv + (v' - cv)$$

shows $V = Fv + v^\perp$. Since $v \notin v^\perp$ (because $B(v,v) \neq 0$), we have $Fv \cap v^\perp = \{0\}$. Therefore $V = Fv \oplus v^\perp$. This direct sum is an orthogonal direct sum since $v \perp w$ for every $w \in v^\perp$.

To show B is non-degenerate on $v^\perp$ when it is non-degenerate on V, suppose some $v' \in v^\perp$ satisfies $B(v', w) = 0$ for all $w \in v^\perp$. Since $B(v',v) = 0$, $B(v', cv + w) = 0$ for any $c \in F$ and $w \in v^\perp$. Since $Fv + v^\perp = V$, we have $v' = 0$ by non-degeneracy of B on V. Thus B is non-degenerate on $v^\perp$. □

Theorem 4.7. *There is an orthogonal basis for V when F does not have characteristic 2.*

Proof. We argue by induction on $n = \dim V$. The result is automatic when $n = 1$, so take $n \geq 2$ and assume the theorem for spaces of smaller dimension.

If B is identically 0, then any basis of V is an orthogonal basis. If B is not identically 0, then $B(v,v) \neq 0$ for some v (Lemma 4.5). Using any such v, Lemma 4.6 says $V = Fv \perp v^\perp$. Since $v^\perp$ is a symmetric bilinear space with dimension $n-1$, by induction there is an orthogonal basis of $v^\perp$, say $\{e_1, \ldots, e_{n-1}\}$. The set $\{e_1, \ldots, e_{n-1}, v\}$ is a basis of V. Since $e_i \perp v$ for all i, this basis is orthogonal. □

Taking into account how the matrix for a bilinear form changes when the basis changes, Theorem 4.7 is equivalent to the following matrix-theoretic result: given any symmetric matrix M over a field of characteristic not 2, there exists an invertible matrix C such that $C^\top MC$ (not $C^{-1}MC$) is a diagonal matrix.

Corollary 4.8. *Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis for V. Then V is non-degenerate if and only if $e_i \not\perp e_i$ for each i.*

Proof. The matrix for B associated to the orthogonal basis is diagonal, where the diagonal entries are the numbers $B(e_i, e_i)$. Non-degeneracy of B is equivalent to invertibility of this diagonal matrix, which is equivalent to $B(e_i, e_i) \neq 0$ for all i. □

Remark 4.9. In Euclidean space, every nonzero vector is part of an orthogonal basis. The proof of Theorem 4.7 generalizes this: in a symmetric bilinear space outside of characteristic 2, any vector v with $v \not\perp v$ is part of an orthogonal basis. (If $v \perp v$ then Corollary 4.8 says v won't be part of an orthogonal basis if V is non-degenerate, *e.g.*, $(1, 0, 1)$ is not part of an orthogonal basis of $\mathbf{R}^{2,1}$ and $(1, 0)$ is not part of an orthogonal basis in Example 4.3.) Whether in Euclidean space or the more general setting of a symmetric bilinear space, the inductive construction of an orthogonal basis is the same: pick a *suitable* starting vector v, pass to the orthogonal space $v^\perp$, which has dimension one less, and then induct on the dimension of the space. In the proof of Lemma 4.6, the projection from V to $v^\perp$ via $v' \rightsquigarrow v' - cv = v' - (B(v', v)/B(v, v))v$ is exactly the idea in the classical Gram-Schmidt orthogonalization process.

Example 4.10. We look at Example 4.3 over a general field F: on F^2 let $B(v, w) = v \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) w$. When F does not have characteristic 2, the basis $\{(1, 1), (1, -1)\}$ is orthogonal. When F has characteristic 2, $(1, 1) = (1, -1)$ so this construction of an orthogonal basis breaks down. In fact, in characteristic 2 there is no orthogonal basis of (F^2, B). We give two proofs.

First, suppose there is an orthogonal basis $\{v_0, w_0\}$. Since $2 = 0$ in F, $B((x, y), (x, y)) = 2xy = 0$, so $v_0 \perp v_0$. Since v_0 is orthogonal to both v_0 and w_0, $v_0 \perp F^2$. This contradicts non-degeneracy of B.

Our second proof is matrix-theoretic. In order for B to have an orthogonal basis, there must be an invertible matrix $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $C^\top \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) C$ is a diagonal matrix. Since $C^\top \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) C = \left(\begin{smallmatrix} 2ac & ad+bc \\ ad+bc & 2bd \end{smallmatrix}\right)$, the diagonal terms always vanish in characteristic 2. Therefore this matrix can't be a diagonal matrix in characteristic 2: it would then be the zero matrix, but its determinant is $-(\det C)^2 \neq 0$.

Despite the behavior of Example 4.10, there is something worthwhile to say about the existence of an orthogonal basis for (non-degenerate) symmetric bilinear forms in characteristic 2. But we need to know something more. The situation will be explained in Exercise 5.4.

Exercises.

1. On $\mathbf{Q}^3$, let B be the bilinear form represented by the symmetric matrix
$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$
in the standard basis. Find an orthogonal basis for B.

2. View $\mathrm{M}_2(F)$ as a bilinear space relative to the trace form $B(L, L') = \mathrm{Tr}(LL')$ as in Example 1.12. Show $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \perp \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and explain why $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ can't be part of an orthogonal basis. Find an orthogonal basis when F does not have characteristic 2. Is there an orthogonal basis when F has characteristic 2?
3. Repeat the previous exercise with $B(L, L') = \mathrm{Tr}(LL'^{\top})$ on $\mathrm{M}_2(F)$.
4. Here is a "proof" that when V is symmetric any $v \neq 0$ is part of an orthogonal basis. Let $n = \dim V$. The orthogonal space $v^{\perp}$ has dimension n or $n-1$. Let H be an $(n-1)$-dimensional subspace of $v^{\perp}$. By induction H has an orthogonal basis $\{e_1, \ldots, e_{n-1}\}$. Since $e_i \perp v$ for all i, v is linearly independent from this basis so $\{e_1, \ldots, e_{n-1}, v\}$ is an orthogonal basis of V. Where is the error?
5. As a supplement to Remark 4.9, show when B is symmetric that a nonzero vector v with $B(v, v) = 0$ is part of an orthogonal basis if and only if $v \in V^{\perp}$.
6. Let V be symmetric. Show any orthogonal basis for a non-degenerate subspace of V can be extended to an orthogonal basis of V. (Hint: Use Theorem 3.10.)
7. Show the equation $2x^2 + 3y^2 = 1$ has no rational solutions. (Hint: If it did, clear the denominator to write $2a^2 + 3b^2 = c^2$ for integers a, b, and c, where none of them are 0. Work mod 3 to show a, b, and c are all multiples of 3. Then divide a, b, and c by 3 and repeat.)
8. Let (V, B) be non-degenerate and symmetric, so $V \cong V^{\vee}$ by $v \mapsto B(v, -)$. Under this isomorphism, show that a basis of V is its own dual basis (a "self-dual" basis) if and only if it is an orthonormal basis of (V, B), *i.e.*, an orthogonal basis $\{e_1, \ldots, e_n\}$ where $B(e_i, e_i) = 1$ for all i. Does $\mathrm{M}_2(\mathbf{R})$ with the trace form have a "self-dual" basis?

5. Symplectic bases

We now turn from symmetric bilinear spaces to alternating bilinear spaces. Before we find a good analogue of orthogonal bases, we prove a dimension constraint on non-degenerate alternating spaces.

Theorem 5.1. *If (V, B) is a non-degenerate alternating bilinear space, then* $\dim V$ *is even.*

Proof. First we give a proof valid outside of characteristic 2. When the characteristic is not 2, the alternating property is equivalent to skew-symmetry. Letting M be a matrix representation for the bilinear form, skew-symmetry is equivalent to $M = -M^{\top}$ by Theorem 2.7. Taking determinants, $\det M = (-1)^{\dim V} \det M$. Since the bilinear form is non-degenerate, M is invertible, so we can cancel $\det M$: $1 = (-1)^{\dim V}$. Since the characteristic is not 2, $\dim V$ is even.

Now we give a proof that $\dim V$ is even which is valid in all characteristics. We induct on the dimension. If $\dim V = 1$ with basis $\{v\}$, then B is identically 0 since $B(cv, c'v) = cc'B(v, v) = 0$. This contradicts non-degeneracy, so $\dim V \geq 2$. If $\dim V = 2$ we are done, so assume $\dim V > 2$.

Pick $v \neq 0$ in V. The function $B(v, -)\colon V \to F$ is onto by non-degeneracy, so there is $w \in V$ such that $B(v, w) = 1$. Let $U = Fv + Fw$, so $\dim U = 2$. The matrix for $B|_U$ with respect to the basis $\{v, w\}$ is $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, which is invertible, so the restriction of B to U is non-degenerate. By Theorem 3.10, $V = U \oplus U^{\perp}$ and the restriction of B to $U^{\perp}$ is non-degenerate. By induction $\dim(U^{\perp})$ is even, so $\dim V$ is even. $\square$

Example 5.2. Let B_u be the alternating bilinear form on $\mathbf{R}^3$ in Example 1.11, with $u \neq 0$. Since the space has odd dimension B_u must be degenerate, and indeed $(\mathbf{R}^3)^\perp = \mathbf{R}u$ relative to B_u.

The proof of Theorem 5.1 provides us, given any nonzero $v \in V$, a second vector $w \in V$ such that

- $B(v, w) = 1$,
- $V = U \perp U^\perp$, where $U = Fv + Fw$,
- the restrictions of B to U and $U^\perp$ are non-degenerate.

Rather than getting a splitting of the space into a line and its orthogonal space, as in Lemma 4.6, we get a splitting of the space into a plane and its orthogonal space.

Definition 5.3. Let (V, B) be non-degenerate and alternating with dimension $2m \geq 2$. A *symplectic basis* of V is a basis $e_1, f_1, \ldots, e_m, f_m$ such that $B(e_i, f_i) = 1$ and the planes $U_i = Fe_i + Ff_i$ are mutually perpendicular.

There is a built-in asymmetry between the e_i's and f_i's since $B(f_i, e_i) = -1$ (well, this is an asymmetry outside of characteristic 2).

Using induction on the dimension, starting with the decomposition $V = U \perp U^\perp$ above, our work so far in this section proves the following.

Theorem 5.4. *Any non-degenerate alternating bilinear space has a symplectic basis.*

There are two standard ways to order a symplectic basis: the ordering $e_1, f_1, \ldots, e_m, f_m$ and the ordering $e_1, \ldots, e_m, f_1, \ldots, f_m$. We could call the first ordering numerical and the second ordering alphabetical, but that is non-standard terminology.

In the plane U_i, the matrix of $B|_{U_i}$ with respect to the (ordered) basis $\{e_i, f_i\}$ is $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, so the matrix of B on V with respect to the (ordered) basis $\{e_1, f_1, \ldots, e_m, f_m\}$ has m blocks $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ along the main diagonal and 0 elsewhere:

$$[B] = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 \end{pmatrix}. \tag{5.1}$$

The word symplectic is Greek for "complex." An alternating bilinear space with a symplectic basis is "almost complex," for instance it is even-dimensional and in a suitable basis the bilinear form is a matrix of blocks $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, which is the matrix for multiplication by i on the complex numbers in the basis $\{i, 1\}$.

If we order the symplectic basis alphabetically as $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$, then the matrix for B looks like $\left(\begin{smallmatrix} O & I_m \\ -I_m & O \end{smallmatrix}\right)$. The formula for B in these coordinates (writing a typical element of F^{2m} as a pair $(\mathbf{x}, \mathbf{y})$) is

$$\begin{aligned} B((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')) &= x_1 y_1' - y_1 x_1' + \cdots + x_m y_m' - y_m x_m' \\ &= \begin{vmatrix} x_1 & x_1' \\ y_1 & y_1' \end{vmatrix} + \cdots + \begin{vmatrix} x_m & x_m' \\ y_m & y_m' \end{vmatrix}. \end{aligned} \tag{5.2}$$

Notice (5.1) and (5.2) are determined by $m = (1/2) \dim V$ alone (except for the issue of the basis ordering). The following is a precise statement along these lines.

Corollary 5.5. *Any two non-degenerate alternating bilinear spaces with a given even dimension are equivalent.*

Proof. Let the dimension be $2m$. Using a suitable ordering of a symplectic basis, the matrix for a non-degenerate alternating bilinear form is $\left(\begin{smallmatrix} O & I_m \\ -I_m & O \end{smallmatrix}\right)$. Since all non-degenerate alternating bilinear forms in dimension $2m$ can be brought to a common matrix representation (in suitably chosen bases), these forms are equivalent by Theorem 2.11.

Alternatively, we can argue by induction. We already know any two non-degenerate alternating bilinear spaces in dimension 2 are equivalent (sending a symplectic basis $\{e, f\}$ to a symplectic basis $\{e', f'\}$ sets up the equivalence). Letting V and V' have dimension at least 4, split off a non-degenerate plane from both: $V = U \perp U^\perp$ and $V' = U' \perp U'^\perp$. From the 2-dimensional case, U and U' are equivalent. By induction $U^\perp$ and $U'^\perp$ are equivalent. Therefore V and V' are equivalent. $\square$

Thus, although there can be many inequivalent non-degenerate *symmetric* bilinear forms in a given dimension depending on the field (Example 2.13), over any field there is essentially just one non-degenerate *alternating* bilinear form in each even dimension and it looks like (5.1) in suitable coordinates. The bilinear form on F^{2m} represented by the matrix (5.1) relative to the standard basis is called the *standard* alternating bilinear form on F^{2m}, and the standard basis of F^{2m} is a symplectic basis for it.

Suppose now that (V, B) is an alternating bilinear space which is *degenerate*: $V^\perp \neq \{0\}$. What kind of basis can we use on V which is adapted to B? Pick any vector space complement to $V^\perp$ in V, and call it W: $V = W \oplus V^\perp$. (This decomposition is not canonical, since there are many choices of W, although $\dim W = \dim V - \dim V^\perp$ is independent of the choice of W.) Since $W \cap V^\perp = \{0\}$, B is non-degenerate on W. Therefore the restriction $B|_W$ has a symplectic basis. Augmenting a symplectic basis of W with any basis of $V^\perp$ gives a basis of V with respect to which B is represented by a block diagonal matrix

$$\begin{pmatrix} O & I_r & O \\ -I_r & O & O \\ O & O & O \end{pmatrix}, \tag{5.3}$$

where $2r = \dim W = \dim(V/V^\perp)$. This matrix is completely determined by $\dim V$ and $\dim V^\perp$, so all alternating bilinear forms on vector spaces with a fixed dimension and a fixed "level" of degeneracy (that is, a fixed value for $\dim V^\perp$) are equivalent. The non-degenerate case is $\dim V^\perp = 0$.

We end this section with an interesting application of Corollary 5.5 to the construction of an "algebraic" square root of the determinant of alternating matrices. (Recall a matrix M is called alternating when $M^\top = -M$ and the diagonal entries of M equal 0.)

Lemma 5.6. *The determinant of any invertible alternating matrix over a field F is a perfect square in F.*

Proof. Let M be an invertible alternating $n \times n$ matrix. On F^n, the bilinear form $B(v, w) = v \cdot Mw$ is non-degenerate and alternating. Therefore n is even, say $n = 2m$, and B has the matrix representation $\left(\begin{smallmatrix} O & I_m \\ -I_m & O \end{smallmatrix}\right)$ in a suitable basis. Letting C be the change of basis from the standard basis of F^n to this other basis, $C^\top MC = \left(\begin{smallmatrix} O & I_m \\ -I_m & O \end{smallmatrix}\right)$. Taking determinants, $(\det C)^2 \det M = 1$, so $\det M$ is a square in F. $\square$

Example 5.7. When $n = 2$,

$$\det \begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix} = x^2.$$

Example 5.8. When $n = 4$,

$$\det \begin{pmatrix} 0 & x & y & z \\ -x & 0 & a & b \\ -y & -a & 0 & c \\ -z & -b & -c & 0 \end{pmatrix} = (xc - yb + az)^2.$$

Let's look at the generic example of an alternating matrix in characteristic 0. For a positive even integer $n = 2m$, let x_{ij} for $1 \leq i < j \leq n$ be independent indeterminates over $\mathbf{Q}$. The matrix

$$(5.4) \qquad M(x_{ij}) = \begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} & \cdots & x_{1n} \\ -x_{12} & 0 & x_{23} & x_{24} & \cdots & x_{2n} \\ -x_{13} & -x_{23} & 0 & x_{34} & \cdots & x_{3n} \\ -x_{14} & -x_{24} & -x_{34} & 0 & \cdots & x_{4n} \\ \cdots & \cdots & \cdots & \cdots & \ddots & \cdots \\ -x_{1n} & -x_{2n} & -x_{3n} & -x_{4n} & \cdots & 0 \end{pmatrix}$$

is the "generic" alternating matrix over $\mathbf{Q}$. View it as a matrix over the field $F = \mathbf{Q}(x_{ij})$ obtained by adjoining all the x_{ij}'s to $\mathbf{Q}$. (The total number of variables here is $n(n-1)/2$.) The determinant lies in $\mathbf{Z}[x_{ij}]$. It is not the zero polynomial, since for instance when we set $x_{12} = x_{34} = \cdots = x_{n-1\ n} = 1$ and the other x_{ij}'s to 0 we get the block diagonal matrix with blocks $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, whose determinant is 1. Thus $M(x_{ij}) \in \mathrm{GL}_n(\mathbf{Q}(x_{ij}))$, so $\det M(x_{ij})$ is a perfect square in $\mathbf{Q}(x_{ij})$ by Lemma 5.6.

Since the determinant of $M(x_{ij})$ actually lies in $\mathbf{Z}[x_{ij}]$, which has unique factorization and fraction field $\mathbf{Q}(x_{ij})$, $\det M(x_{ij})$ is a square in $\mathbf{Z}[x_{ij}]$:

$$(5.5) \qquad \det(M(x_{ij})) = (\mathrm{Pf}(x_{ij}))^2$$

for some integral polynomial $\mathrm{Pf}(x_{ij})$ in the x_{ij}'s. This polynomial is called the *Pfaffian* of $M(x_{ij})$. It is so far only determined up to an overall sign. Except for the determination of this sign, which we will deal with in a moment, (5.5) shows by specializing the variables into any field, or any commutative ring for that matter, that there is a universal algebraic square root of invertible alternating matrices. Since $\det M(x_{ij})$ is a homogeneous polynomial of degree n, $\mathrm{Pf}(x_{ij})$ is a homogeneous polynomial of degree $n/2$. (We perhaps should write Pf_n to indicate the dependence on n, but this is not done for det and we follow that tradition for Pf too.)

To fix the sign in the Pfaffian, we can specify the value of the Pfaffian at one nonzero specialization of the variables. The matrix in (5.4) with each $x_{i\ i+1}$ equal to 1 for odd i and the other x_{ij}'s equal to 0 has determinant 1, whose square roots are ± 1. Choosing the square root as 1 pins down the sign on the Pfaffian. That is, define $\mathrm{Pf}(x_{ij})$ to be the polynomial over $\mathbf{Z}$ satisfying (5.5) and the condition that the coefficient of $x_{12}x_{34} \cdots x_{2m-1\ 2m}$ in $\mathrm{Pf}(x_{ij})$ is 1. In particular, this makes the Pfaffian for $n = 2$ and $n = 4$ the polynomials which are being squared on the right side in Examples 5.7 and 5.8, *e.g.*, $\mathrm{Pf}(x) = x$ (not $-x$).

When $A = (a_{ij})$ is an $n \times n$ alternating matrix, for even n, we write $\mathrm{Pf}\, A$ for the specialization of $\mathrm{Pf}(x_{ij})$ using $x_{ij} = a_{ij}$. Since a Pfaffian is a square root of a determinant, it should be multiplicative "up to sign." However, some care is needed since the product of two alternating matrices is not again alternating (try the 2×2 case!).

Theorem 5.9. *Let n be even. For $n \times n$ matrices M and C, where M is alternating,* $\operatorname{Pf}(C^\top MC) = (\det C) \operatorname{Pf} M$.

Proof. This is obvious up to sign, by squaring both sides and using properties of the determinant. The point is to pin down the sign correctly.

It suffices to verify it as a universal polynomial identity over $\mathbf{Z}$ where $M = (x_{ij})$ is a generic $n \times n$ alternating matrix in $n(n-1)/2$ variables and $C = (y_{ij})$ is a generic $n \times n$ matrix in n^2 extra variables. Specialize C to be the $n \times n$ identity matrix. Then $\operatorname{Pf}(C^\top MC)$ becomes $\operatorname{Pf} M$ and $(\det C)\operatorname{Pf} M$ becomes $\operatorname{Pf} M$, so the two sides of the identity are equal as polynomials. $\square$

The identity in Theorem 5.9 ultimately goes back to the equivalence of all non-degenerate alternating bilinear forms in a given dimension (over a given field).

Exercises.

1. In Example 1.11, describe a basis of $\mathbf{R}^3$ which turns B_u into a matrix like (5.3) when $u \neq 0$.
2. On F^{2m} with alternating bilinear form $B = \left(\begin{smallmatrix} O & I_m \\ -I_m & O \end{smallmatrix}\right)$, show a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{M}_{2m}(F)$ acting on F^{2m} has adjoint matrix $\left(\begin{smallmatrix} D^\top & -B^\top \\ -C^\top & A^\top \end{smallmatrix}\right)$.
3. Let V be m-dimensional over F and let B be the alternating bilinear form on $V \oplus V^\vee$ from Example 1.13. It is non-degenerate by Example 3.6. When $\{e_1, \dots, e_m\}$ is a basis of V and $\{e_1^\vee, \dots, e_m^\vee\}$ is the dual basis of $V^\vee$, show $\{e_1, e_1^\vee, \dots, e_m, e_m^\vee\}$ is a symplectic basis of $V \oplus V^\vee$ and the matrix for B in these coordinates is (5.1).
4. Let (V, B) be non-degenerate and symmetric over a field of characteristic 2. Recall the alternating bilinear forms are a subset of the symmetric bilinear forms in characteristic 2. Prove (V, B) has an orthogonal basis if and only if B is *not* alternating. (Hint: Without loss of generality, $\dim V \geq 2$. The only if direction is trivial by Corollary 4.8. For the if direction, pick v_0 such that $a := B(v_0, v_0) \neq 0$. Then $v_0^\perp$ is non-degenerate by Lemma 4.6. If B is non-alternating on $v_0^\perp$ then we're done by induction. If B is alternating on $v_0^\perp$ then $v_0^\perp$ has a symplectic basis, say including a pair $\{e, f\}$ with $B(e, f) = 1$, $B(e, e) = 0$, and $B(f, f) = 0$. Show $B(v_0 + e + f, v_0 + e + f) \neq 0$ and B is non-alternating on $(v_0 + e + f)^\perp$.)
5. Check Example 5.8.
6. Let M be an $n \times n$ alternating matrix, where n is even.
   (1) Show $\operatorname{Pf}(M^\top) = (-1)^{n/2} \operatorname{Pf} M$.
   (2) If M is not invertible, show $\operatorname{Pf} M = 0$. If M is invertible and C is an invertible matrix such that $C^\top MC$ is the matrix in (5.1), show $\operatorname{Pf} M = 1/\det C$.

6. Quadratic forms

Concretely, a quadratic form is a homogeneous polynomial of degree 2, such as $x^2+y^2+z^2$ or $x^2 + 5xy - y^2$. We call the first one a diagonal quadratic form since it involves no mixed terms. The second quadratic form is not diagonal, but we can make it so by completing the square:

$$x^2 + 5xy - y^2 = \left(x + \frac{5}{2}y\right)^2 - \frac{29}{4}y^2 = x'^2 - 29y'^2,$$

where $x' = x + \frac{5}{2}y$ and $y' = \frac{1}{2}y$.

The simplest example of an n-variable quadratic form is $x_1^2 + \cdots + x_n^2$. This sum of squares, which plays an important role in the geometry of $\mathbf{R}^n$, is closely related to the dot product. First, we can write

$$x_1^2 + \cdots + x_n^2 = v \cdot v,$$

where $v = (x_1, \ldots, x_n)$. Conversely, the dot product of two vectors v and w in $\mathbf{R}^n$ can be expressed in terms of sums of squares:

$$v \cdot w = \frac{1}{2}(Q(v + w) - Q(v) - Q(w)), \tag{6.1}$$

where $Q(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2$ (check!).

The relation (6.1) between a sum of squares (a particular quadratic form) and the dot product (a particular bilinear form) motivates the following coordinate-free definition of a quadratic form.

Definition 6.1. A *quadratic form* on a vector space V over a field F with characteristic not 2 is a function $Q \colon V \to F$ such that

(1) $Q(cv) = c^2 Q(v)$ for $v \in V$ and $c \in F$,
(2) the function $B(v, w) := \frac{1}{2}(Q(v + w) - Q(v) - Q(w))$ is bilinear.

We call B the bilinear form associated to Q. Note B is *symmetric*. The factor $\frac{1}{2}$ is included in condition (2) because of (6.1). This is the reason we avoid fields where $2 = 0$, although admittedly the bilinearity of B has nothing to do with a choice of nonzero scaling factor out front. Quadratic forms in characteristic 2 are discussed in Section 7. We will very frequently use (2) as

$$Q(v + w) = Q(v) + Q(w) + 2B(v, w). \tag{6.2}$$

In particular, note $B(v, w) = 0$ is equivalent to $Q(v + w) = Q(v) + Q(w)$.

For the rest of this section, F does not have characteristic 2.

Definition 6.1 doesn't require that V be finite-dimensional, but the examples and theorems we discuss concern the finite-dimensional case. We call $\dim V$ the *dimension* of the quadratic form. Whenever we refer to a quadratic form "on F^n" we are thinking of F^n as an F-vector space.

To connect the concrete and coordinate-free descriptions of quadratic forms, we show that quadratic forms on a vector space are nothing other than homogeneous quadratic polynomials once a basis is chosen. Starting with $Q \colon V \to F$ as in Definition 6.1, induction on the number of terms in (6.2) gives

$$Q(v_1 + \cdots + v_r) = Q(v_1) + \cdots + Q(v_r) + 2\sum_{i<j} B(v_i, v_j) \tag{6.3}$$

for any $r \geq 2$ and vectors $v_i \in V$. Therefore, if $\{e_1, \ldots, e_n\}$ is a basis of V,

$$\begin{aligned} Q(x_1 e_1 + \cdots + x_n e_n) &= \sum_{i=1}^n Q(x_i e_i) + 2\sum_{i<j} B(x_i e_i, x_j e_j) \\ &= \sum_{i=1}^n a_i x_i^2 + \sum_{i<j} a_{ij} x_i x_j, \qquad (6.4) \end{aligned}$$

where $a_i = Q(e_i)$ and $a_{ij} = 2B(e_i, e_j)$. This exhibits Q as a homogeneous quadratic polynomial in coordinates.

Conversely, let's show any function $V \to F$ which is a homogeneous quadratic polynomial in the coordinates of some basis is a quadratic form on V. Let $Q(x_1e_1 + \cdots + x_ne_n)$ be a polynomial as in (6.4). Easily $Q(cv) = c^2Q(v)$ for $c \in F$. Letting $v = x_1e_1 + \cdots + x_ne_n$ and $v' = x_1'e_1 + \cdots + x_n'e_n$, define

$$
\begin{aligned}
B(v, v') &:= \frac{1}{2}(Q(v + v') - Q(v) - Q(v')) \\
&= \sum_{i=1}^{n} a_i x_i x_i' + \frac{1}{2} \sum_{1 \le i < j \le n} a_{ij}(x_i x_j' + x_i' x_j) \qquad (6.5) \\
&= [v] \cdot M[v'],
\end{aligned}
$$

where

$$
M = \begin{pmatrix} a_1 & a_{12}/2 & \cdots & a_{1n}/2 \\ a_{12}/2 & a_2 & \cdots & a_{2n}/2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}/2 & a_{2n}/2 & \cdots & a_n \end{pmatrix}. \qquad (6.6)
$$

Therefore B is a bilinear form on V, so Q is a quadratic form on V.

Example 6.2. On $\mathrm{Hom}_F(V, V)$ let $Q(L) = \mathrm{Tr}(L^2)$. For example, if $V = F^2$ then $Q((\begin{smallmatrix} x & y \\ z & t \end{smallmatrix})) = x^2 + 2yz + t^2$, which is a quadratic form in 4 variables. Check that $\frac{1}{2}(Q(L+L') - Q(L) - Q(L'))$ is bilinear in L and L'; in fact, it is the trace form on $\mathrm{Hom}_F(V, V)$ (Example 1.12).

We can express a quadratic form in terms of its associated bilinear form by setting $w = v$:

$$
B(v, v) = \frac{1}{2}(Q(2v) - 2Q(v)) = \frac{1}{2}(4Q(v) - 2Q(v)) = Q(v), \qquad (6.7)
$$

so

$$
Q(v) = B(v, v). \qquad (6.8)
$$

Conversely, every symmetric bilinear form B on V defines a quadratic form by the formula (6.8), and the bilinear form associated to this quadratic form is B (this is "polarization"; see Theorem 1.8). For example, Q is identically zero if and only if B is identically zero.

Outside of characteristic 2 there is a (linear) bijection between between quadratic forms on V and symmetric bilinear forms on V. Once we choose a basis for V we get a further (linear) bijection with $n \times n$ symmetric matrices, where $n = \dim V$.

In matrix notation, writing $B(v, w) = [v] \cdot M[w]$ for a symmetric matrix M relative to a choice of basis, (6.8) becomes $Q(v) = [v] \cdot M[v]$. We call M the *matrix associated to* Q in this basis. It is the same as the matrix associated to B in this basis. Concretely, when we write Q as a polynomial (6.4), its matrix is (6.6). Changing the basis changes the matrix M for Q to $C^\top MC$ for some $C \in \mathrm{GL}_n(F)$.

Example 6.3. When Q is the sum of n squares quadratic form on F^n, its matrix in the standard basis of F^n is I_n and $Q(v) = v \cdot v = v \cdot I_n v$.

Example 6.4. The polynomial $Q(x, y) = ax^2 + bxy + cy^2$, as a quadratic form on F^2, is represented by the matrix $(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix})$ in the standard basis: $Q(x, y) = \binom{x}{y} \cdot (\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix})\binom{x}{y}$. Even though $Q(x, y) = \binom{x}{y} \cdot (\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix})\binom{x}{y}$ too, the matrix $(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix})$ is not symmetric (for $b \neq 0$) and therefore is not considered a matrix for Q.

Definition 6.5. The *discriminant* of Q is $\det M$ modulo nonzero squares, where M is a matrix for Q.

Example 6.6. The discriminant of the quadratic form in Example 6.4 equals $ac - b^2/4$. In particular, $x^2 - y^2$ has discriminant -1.

Theorem 6.7. *Let Q be a quadratic form on an n-dimensional vector space over a field of characteristic not 2. In a suitable basis, Q is diagonalized:*[4]

$$Q\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} a_i x_i^2. \tag{6.9}$$

In this basis, the discriminant of Q is $a_1 a_2 \cdots a_n \bmod (F^\times)^2$.

Proof. Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis of the symmetric bilinear form associated to Q (Theorem 4.7). In this basis, the cross terms in (6.4) vanish and Q is diagonalized. The matrix (6.6) for Q in this basis is diagonal, so the discriminant of Q is the product of the a_i's. □

The construction of an orthogonal basis can be carried out systematically from the bilinear form. Start by picking any vector e_1 where $Q(e_1) \neq 0$. Then look in the subspace $e_1^\perp$ to find e_2 with $Q(e_2) \neq 0$. The vectors e_1 and e_2 are orthogonal and linearly independent. Then look in $e_1^\perp \cap e_2^\perp$ to find an e_3 with $Q(e_3) \neq 0$, and so on. The process eventually ends with a subspace where Q is identically 0. If this is the subspace $\{0\}$ then the vectors we have already picked are a basis in which Q is diagonal. If this process reaches a nonzero subspace on which Q is identically 0 then the vectors already picked plus any basis for the subspace we reached are a basis of the whole space in which Q is diagonal.

Example 6.8. Consider $Q(x, y, z) = xy + xz + yz$. We want to write

$$Q = ax'^2 + by'^2 + cz'^2$$

where x', y', z' are linear in x, y, z and a, b, and c are constants. Blind algebraic calculation is unlikely to diagonalize Q (try!), but thinking geometrically leads to a solution, as follows.

The bilinear form on F^3 for Q is

$$B(v, w) = \frac{1}{2}(Q(v + w) - Q(v) - Q(w)) = v \cdot \begin{pmatrix} 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \\ 1/2 & 1/2 & 0 \end{pmatrix} w.$$

Pick any vector at which Q doesn't vanish, say $e_1 := (1, 0, 1)$. Then, using the above bilinear form B, the space orthogonal to e_1 is

$$e_1^\perp = \{(x, y, z) : \frac{1}{2}x + y + \frac{1}{2}z = 0\}.$$

One vector in here at which Q doesn't vanish is $e_2 = (1, -1/2, 0)$. Since $B(e_2, (x, y, z)) = -x/4 + y/2 + z/4$, a vector $v = (x, y, z)$ satisfies $v \perp e_1$ and $v \perp e_2$ when $x/2 + y + z/2 = 0$ and $-x/4 + y/2 + z/4 = 0$, so (after some algebra) $(x, y, z) = (0, y, -2y)$. Taking $y = 1$

[4]Theorem 6.7 is special to degree 2. For example, $f(x, y) = x^2 y$ is homogeneous of degree 3 and an explicit calculation shows no $A \in \mathrm{GL}_2(F)$ satisfies $f(A\binom{x}{y}) = ax^3 + by^3$. Here F is any field, even of characteristic 2 or 3.

here, let $e_3 := (0, 1, -2)$. Then $\{e_1, e_2, e_3\}$ is an orthogonal basis of F^3 with respect to B and in this basis

$$Q(x'e_1 + y'e_2 + z'e_3) = Q(e_1)x'^2 + Q(e_2)y'^2 + Q(e_3)z'^2 = x^2 - \frac{1}{2}y^2 - 2z^2,$$

so we diagonalized Q.

Corollary 6.9. *Let Q be a quadratic form on V. An $a \in F^\times$ can occur as the coefficient of Q in some diagonalization if and only if $a \in Q(V)$.*

Proof. The coefficients in a diagonalization of Q are the Q-values of an orthogonal basis, so any nonzero coefficient which occurs in a diagonalization is a Q-value.

Conversely, assume $a \neq 0$ in F and $a = Q(v)$ for some v. Then $a = B(v, v)$, so by the proof of Theorem 4.7 there is an orthogonal basis of V having first vector v. The first coefficient in the diagonalization of Q relative to this orthogonal basis is a by (6.4). □

Example 6.10. The quadratic form $2x^2 + 3y^2$ on $\mathbf{Q}^2$ can't be written in the form $x'^2 + by'^2$ by a linear change of variables on $\mathbf{Q}^2$: otherwise the coefficient 1 is a value of $2x^2 + 3y^2$ on $\mathbf{Q}^2$, which is not true (Exercise 4.7).

Definition 6.11. For F-vector spaces V_1 and V_2, quadratic forms Q_i on V_i are called *equivalent* if there is a linear isomorphism $A\colon V_1 \to V_2$ such that $Q_2(Av) = Q_1(v)$ for all $v \in V_1$.

Example 6.12. The quadratic forms $x^2 - y^2$ and xy on F^2 are equivalent since $x^2 - y^2 = (x+y)(x-y)$ is a product (call it $x'y'$ if you wish), and the passage from (x, y) to $(x+y, x-y)$ is linear and invertible outside characteristic 2. This is just Example 2.10 in disguise.

Theorem 6.13. *Quadratic forms are equivalent if and only if their associated bilinear forms are equivalent in the sense of Definition* 2.9.

Proof. Let Q_1 and Q_2 have associated bilinear forms B_1 and B_2. If $Q_2(Av) = Q_1(v)$ for all $v \in V$ then $B_2(Av, Av) = B_1(v, v)$. Therefore $B_2(Av, Aw) = B_1(v, w)$ for all v and w in V (Theorem 1.8), so B_1 and B_2 are equivalent. The converse direction is trivial. □

Definition 6.14. A quadratic form is called *non-degenerate* if a (symmetric) matrix representation for it is invertible, *i.e.*, its discriminant is nonzero.

Example 6.15. The polynomial $ax^2+bxy+cy^2$, as a quadratic form on F^2, has discriminant $ac - b^2/4$, so this quadratic form is non-degenerate if and only if $b^2 - 4ac \neq 0$.

The following table collects different descriptions of the same idea for symmetric bilinear forms and for quadratic forms.

Condition	Symm. Bil. Form	Quadratic Form
Matrix Rep.	$B(v, w) = [v] \cdot M[w]$	$Q(v) = [v] \cdot M[v]$
$v \perp w$	$B(v, w) = 0$	$Q(v + w) = Q(v) + Q(w)$
Orthog. basis	$B(e_i, e_j) \neq 0$ $(i \neq j)$	$Q(\sum_i x_i e_i)$ is diagonal
Discriminant	$\det M$	$\det M$
Equivalent	$B_2(Av, Aw) = B_1(v, w)$	$Q_2(Av) = Q_1(v)$
Non-degenerate	$\det M \neq 0$	$\det M \neq 0$

TABLE 2. Comparisons

The next result puts some of this terminology to work.

Theorem 6.16. *Let Q be a quadratic form on a two-dimensional space. The following conditions on Q are equivalent:*

1. *Q looks like $x^2 - y^2$ in a suitable basis,*
2. *$\operatorname{disc} Q = -1$ modulo nonzero squares,*
3. *Q is non-degenerate and takes on the value 0 nontrivially.*

Taking on the value 0 nontrivially means $Q(v) = 0$ for some v which is nonzero.

Proof. The first property easily implies the second and third properties (since $x^2 - y^2$ vanishes at $(x, y) = (1, 1)$). We now show each of these properties (separately) forces there to be a basis in which Q is $x^2 - y^2$.

Assume $\operatorname{disc} Q = -1$. Choosing an orthogonal basis $\{e_1, e_2\}$ we have $Q(x_1e_1 + x_2e_2) = ax_1^2 + bx_2^2$. Since $ab = -1 \bmod (F^\times)^2$, in a suitable basis Q looks like

$$ax^2 - \frac{1}{a}y^2 = a\left(x^2 - \frac{y^2}{a^2}\right) = a\left(x + \frac{y}{a}\right)\left(x - \frac{y}{a}\right) = (ax + y)\left(x - \frac{1}{a}y\right).$$

Set $x' = ax + y$ and $y' = x - y/a$, so in these coordinates (that is, in the basis $e_1' := ae_1 + e_2$ and $e_2' := e_1 - (1/a)e_2$) Q looks like $x'y'$, which can be written as a difference of squares by a further linear change of variables (Example 2.10).

Assume now that Q is non-degenerate and takes the value 0 nontrivially. By Theorem 6.22 Q is universal, so it takes the value 1. By Corollary 6.9 there is an orthogonal basis with respect to which the quadratic form has a coefficient equal to 1, so Q looks like $x^2 + cy^2$, with $c \neq 0$ by non-degeneracy. In these coordinates suppose $Q(x_0, y_0) = 0$ with $(x_0, y_0) \neq (0, 0)$. (There is such a vector by hypothesis.) Then $x_0^2 = -cy_0^2$, so x_0 and y_0 are both nonzero. Thus c is the negative of a square, which lets us rewrite $x^2 + cy^2$ as $x^2 - y^2$ after a linear change of variables. □

We turn now to the classification of non-degenerate quadratic forms up to equivalence over certain fields: the real numbers, the complex numbers, and finite fields of odd characteristic.

Theorem 6.17. *Every non-degenerate quadratic form on an n-dimensional complex vector space is equivalent to $x_1^2 + \cdots + x_n^2$ on $\mathbf{C}^n$. Every non-degenerate quadratic form on an n-dimensional real vector space is equivalent to $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2$ on $\mathbf{R}^n$ for a unique p between 0 and n.*

Proof. In an orthogonal basis, an n-dimensional non-degenerate quadratic form is a sum of n nonzero monomials $a_ix_i^2$. Since $ac^2Q(v) = aQ(cv)$, a nonzero square factor c^2 in a diagonal coefficient of Q can be removed by replacing the corresponding basis vector v with cv in the basis. Over $\mathbf{C}$ every nonzero number is a square, so the coefficients can be scaled to 1. Thus any non-degenerate quadratic form over $\mathbf{C}$ looks like $\sum_{i=1}^n x_i^2$ in a suitable basis. Over $\mathbf{R}$ the positive coefficients can be scaled to 1 and the negative coefficients can be scaled to -1.

We now show the quadratic forms $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2$ and $y_1^2 + \cdots + y_{p'}^2 - y_{p'+1}^2 - \cdots - y_n^2$ on $\mathbf{R}^n$ are equivalent only when $p = p'$. Equivalence means there is a single quadratic form Q on $\mathbf{R}^n$ which looks like each polynomial in some basis. Let Q look like the first polynomial in the basis $\{e_1, \ldots, e_n\}$ and let it look like the second polynomial in the basis $\{f_1, \ldots, f_n\}$.

Let W be the span of $e_1, \ldots, e_p$ and let W' be the span of $f_{p'+1}, \ldots, f_n$. For $w \in W$, $Q(w) \geq 0$ with equality if and only if $w = 0$. For $w' \in W'$, $Q(w') \leq 0$ with equality if and only if $w' = 0$. Therefore $W \cap W' = \{0\}$. Thus $\dim(W + W') = \dim W + \dim W' = p + (n - p')$.

Since $W + W' \subset \mathbf{R}^n$, $\dim(W + W') \leq n$, so $p + n - p' \leq n$. Thus $p \leq p'$. By switching the roles of the two bases we get the reverse inequality, so $p = p'$. $\square$

Corollary 6.18. *When $p + q = p' + q'$, $\langle \cdot, \cdot \rangle_{p,q}$ and $\langle \cdot, \cdot \rangle_{p',q'}$ are equivalent if and only if $p = p'$ and $q = q'$.*

Proof. By Theorem 6.13, $\langle \cdot, \cdot \rangle_{p,q}$ and $\langle \cdot, \cdot \rangle_{p',q'}$ are equivalent if and only if the corresponding quadratic forms are equivalent, which means $p = p'$ (so also $q = q'$) by Theorem 6.17. $\square$

A non-degenerate quadratic form on $\mathbf{R}^n$ is determined up to equivalence by the pair (p, q) coming from a diagonalization, where p is the number of plus signs and $q = n - p$ is the number of minus signs. This ordered pair (p, q) is called the *signature* of the quadratic form. Once we know the dimension n, either of p or q determines the other since $p + q = n$ (we have in mind only the non-degenerate case).[5] It may seem natural to write real diagonal quadratic forms with the positive terms coming first, but some physicists prefer to put the negative terms first.

Definition 6.19. A quadratic form Q on a real vector space is called *positive-definite* if $Q(v) > 0$ for all $v \neq 0$ and *negative-definite* if $Q(v) < 0$ for all $v \neq 0$.[6]

All positive-definite real quadratic forms with a common dimension n are equivalent to a sum of n squares and thus are equivalent to each other. Similarly, all negative-definite quadratic forms with a common dimension are equivalent to each other. Unlike the property of being a sum of squares, positive-definiteness doesn't depend on the choice of coordinates.

Example 6.20. We will put to use the normalization of a positive-definite quadratic form as a sum of squares to compute the multivariable analogue of a Gaussian integral.

In one dimension, $\int_{\mathbf{R}} e^{-x^2/2} \, \mathrm{d}x = \sqrt{2\pi}$, or equivalently $\int_{\mathbf{R}} e^{\pi x^2} \, \mathrm{d}x = 1$. We now consider $\int_{\mathbf{R}^n} e^{-\pi Q(v)} \, \mathrm{d}v$ where $Q \colon \mathbf{R}^n \to \mathbf{R}$ is a positive-definite quadratic form. Write $Q(v) = v \cdot Mv$ in *standard* coordinates on $\mathbf{R}^n$. That Q can be brought to a sum of n squares means for some $A \in \mathrm{GL}_n(\mathbf{R})$, $Q(Av) = v \cdot v$, so $A^\top MA = I_n$. By doing a linear change of variables in the integral with A,

$$\int_{\mathbf{R}^n} e^{-\pi Q(v)} \, \mathrm{d}v = \int_{\mathbf{R}^n} e^{-\pi Q(Av)} \, \mathrm{d}(Av) = (\det A) \int_{\mathbf{R}^n} e^{-\pi v \cdot v} \, \mathrm{d}v.$$

The last integral breaks up into the product of 1-dimensional integrals $\int_{\mathbf{R}} e^{-\pi x_i^2} \, \mathrm{d}x_i$, which are each 1, so

$$\int_{\mathbf{R}^n} e^{-\pi Q(v)} \, \mathrm{d}v = \det A.$$

Since $A^\top MA = I_n$, taking determinants gives $(\det A)^2 \det M = 1$, so $\det A = 1/\sqrt{\det M}$. Therefore $\int_{\mathbf{R}^n} e^{-\pi Q(v)} \, \mathrm{d}v = 1/\sqrt{\det M}$, where $Q(v) = v \cdot Mv$.

Now we will classify non-degenerate quadratic forms over a finite field of odd characteristic. The essential property is that a quadratic form with high enough dimension always takes on the value 0 nontrivially:

Theorem 6.21. *Let $\mathbf{F}$ be a finite field with odd characteristic and Q be a non-degenerate quadratic form over $\mathbf{F}$. If Q has dimension at least 3 then there is a solution to $Q(v) = 0$ with $v \neq 0$.*

---

[5]Some refer to p alone as the signature.

[6]A non-degenerate real quadratic form which is neither positive-definite nor negative-definite it is called *indefinite*, such as $x^2 - y^2$.

Proof. First we handle the case of dimension 3. In an orthogonal basis, write

$$Q(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2,$$

where a, b, and c are all nonzero. We will find a solution to $Q(v) = 0$ with $z = 1$: the equation $ax^2 + by^2 + c = 0$ has a solution in $\mathbf{F}$.

Let $q = \#\mathbf{F}$. The number of squares in $\mathbf{F}$ is $(q + 1)/2$. (There are $(q - 1)/2$ *nonzero* squares since the squaring map $\mathbf{F}^\times \to \mathbf{F}^\times$ is 2-to-1; thus its image has size $(q - 1)/2$; add 1 to this count to include 0^2.) The two sets $\{ax^2 : x \in \mathbf{F}\}$ and $\{-by^2 - c : y \in \mathbf{F}\}$ are in bijection with the set of squares, so each has size $(q + 1)/2$. Since $\mathbf{F}$ has q terms, the two sets must overlap. At an overlap we have $ax^2 = -by^2 - c$, so $ax^2 + by^2 + c = 0$.

If Q has dimension greater than 3, write it in an orthogonal basis as

$$Q(x_1e_1 + x_2e_2 + \cdots + x_ne_n) = a_1x_1^2 + a_2x_2^2 + \cdot + a_nx_n^2,$$

where the a_i's are all nonzero. Set $x_i = 0$ for $i > 3$ and $x_3 = 1$. Then we are looking at $a_1x_1^2 + a_2x_2^2 + a_3$, which assumes the value 0 by the previous argument. □

The bound $\dim V \geq 3$ in Theorem 6.21 is sharp: the 2-dimensional quadratic form $x^2 - cy^2$, where c is a non-square in $\mathbf{F}^\times$, doesn't take the value 0 except when $x = y = 0$.

The reason that taking on the value 0 nontrivially (that is, at a nonzero vector) matters is the following result over any field not of characteristic 2.

Theorem 6.22. *If $Q \colon V \to F$ is a non-degenerate quadratic form which takes on the value 0 nontrivially then it takes on all values: $Q(V) = F$.*

Proof. Let B be the bilinear form for Q and let $Q(v) = 0$ with $v \neq 0$. Since $Q(cv) = c^2Q(v) = 0$ and Q is not identically zero (otherwise it couldn't be non-degenerate), $\dim V \geq 2$. By non-degeneracy of Q (equivalently, of B), there is a $w \in V$ such that $B(v, w) \neq 0$. Then for any $c \in F$,

$$Q(cv + w) = Q(cv) + Q(w) + 2B(cv, w) = Q(w) + 2B(v, w)c.$$

Since $2B(v, w) \neq 0$, this is a linear function of c and therefore takes on all values in F as c varies. □

Theorem 6.22 is false for some degenerate Q. Consider $Q(x, y) = x^2$ on $\mathbf{R}^2$, where $Q(0, 1) = 0$.

Definition 6.23. A quadratic form $Q \colon V \to F$ is *universal* if $Q(V) = F$.

Example 6.24. On $\mathbf{R}^3$, $x^2 + y^2 + z^2$ is not universal but $x^2 + y^2 - z^2$ is.

Corollary 6.25. *Every non-degenerate quadratic form of dimension ≥ 2 over a finite field $\mathbf{F}$ of characteristic not 2 is universal.*

Proof. When the dimension is at least 3, Theorems 6.21 and 6.22 tell us the quadratic form is universal. In two dimensions, after diagonalizing we want to know a polynomial of the form $ax^2 + by^2$, for a and b in $\mathbf{F}^\times$, takes on all values in $\mathbf{F}$. This was explained in the proof of Theorem 6.21. □

Theorem 6.26. *Fix a non-square $d \in \mathbf{F}^\times$. For $n \geq 1$, any non-degenerate quadratic form on an n-dimensional vector space over $\mathbf{F}$ is equivalent to exactly one of*

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + x_n^2 \text{ or } x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + dx_n^2$$

on $\mathbf{F}^n$. In particular, the dimension and discriminant determine a non-degenerate quadratic form over $\mathbf{F}$ up to equivalence.

Proof. The two forms provided are inequivalent, since the first has discriminant 1 and the second has discriminant d, which are unequal in $\mathbf{F}^\times/(\mathbf{F}^\times)^2$.

To see any n-dimensional non-degenerate quadratic form over $\mathbf{F}$ is equivalent to one of these, we argue by induction on n. Any non-degenerate one-dimensional quadratic form in coordinates is $Q(x) = ax^2$, where (insofar as the equivalence class of Q is concerned) a only matters up to a nonzero square factor. This gives us the two choices x^2 and dx^2.

When $n \geq 2$, Corollary 6.25 tells us that Q takes on the value 1. By Corollary 6.9, there is an orthogonal basis $\{e_1, \dots, e_n\}$ such that $Q(e_1) = 1$:

$$Q(x_1e_1 + x_2e_2 + \cdots + x_ne_n) = x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2,$$

where $a_i \in \mathbf{F}^\times$. The quadratic form $Q(x_2e_2 + \cdots + x_ne_n) = Q|_{e_1^\perp}$ is non-degenerate of dimension $n-1$, so by induction we can write it after a linear change of variables (not involving x_1) as $y_2^2 + \cdots + y_{n-1}^2 + ay_n^2$, where $a = 1$ or $a = d$. Add x_1^2 to this and we're done. □

To give a sense of other techniques, we will redo the classification of non-degenerate quadratic forms over $\mathbf{F}$ by a second method, which gives a more "geometric" description of the quadratic forms. First we introduce some terminology.

Definition 6.27. A *quadratic space* is a vector space along with a choice of quadratic form on it. We call it non-degenerate when the underlying quadratic form is non-degenerate.

This is the analogue for quadratic forms of the notion of a bilinear space for bilinear forms. Outside of characteristic 2 (which is the case throughout this section), quadratic spaces are essentially the same thing as symmetric bilinear spaces. In Section 7 we will see that this is no longer true in characteristic 2!

Definition 6.28. Two quadratic spaces (V_1, Q_1) and (V_2, Q_2) are called *isomorphic* if there is a linear isomorphism $A\colon V_1 \to V_2$ such that $Q_2(Av) = Q_1(v)$ for all $v \in V_1$.

Definition 6.29. Let (V_1, Q_1) and (V_2, Q_2) be quadratic spaces over a common field F. Their *orthogonal direct sum* $V_1 \perp V_2$ is the vector space $V_1 \oplus V_2$ with the quadratic form $Q(v_1, v_2) = Q_1(v_1) + Q_2(v_2)$. We write $V^{\perp n}$ for the n-fold orthogonal direct sum of a quadratic space V with itself.

Example 6.30. If we view F as a 1-dimensional quadratic space with quadratic form $Q(x) = x^2$, the quadratic space $F^{\perp n}$ is the vector space F^n equipped with the standard sum of n squares quadratic form.

Definition 6.31. Let $Q\colon V \to F$ be a quadratic form. A *null vector* for Q (or for V) is any nonzero $v \in V$ such that $Q(v) = 0$.

In terms of the associated bilinear form B, a null vector is a nonzero solution to $B(v, v) = 0$. Null vectors are self-orthogonal nonzero vectors. (Other names for null vectors are isotropic vectors and singular vectors, the former being very widely used.) The spaces $\mathbf{R}^{p,q}$ for positive p and q have plenty of null vectors. Theorem 6.21 says all non-degenerate quadratic forms in dimension at least 3 over a finite field (with characteristic not 2) have a null vector, while Theorem 6.22 says any non-degenerate quadratic form outside of characteristic 2 with a null vector is universal.

Here is the key concept for our second approach to the classification over finite fields.

Definition 6.32. A *hyperbolic plane* is a two-dimensional quadratic space where the quadratic form looks like $x^2 - y^2$ in some basis.

We could just as well have used xy as the model quadratic form since $x^2 - y^2$ and xy are equivalent (we are not in characteristic 2). A hyperbolic plane is denoted $\mathbf{H}$, or $\mathbf{H}(F)$ if the field F is to be specified.

Example 6.33. The quadratic space $\mathbf{R}^{2,1}$, where the quadratic form is $x^2 + y^2 - z^2 = x^2 - z^2 + y^2$, is isomorphic to $\mathbf{H} \perp \mathbf{R}$ since $x^2 - z^2$ gives us a hyperbolic plane and y^2 is the standard quadratic form on $\mathbf{R} = \mathbf{R}^{1,0}$. More generally, $\mathbf{R}^{p,q}$ contains as many independent hyperbolic planes as $\min(p, q)$. What is left after collecting an equal number of x_i^2 and $-x_j^2$ together is a sum of squares (or a negative sum of squares (if $q > p$). So $\mathbf{R}^{p,q} = \mathbf{H}^{\perp m} \perp W$ where $m = \min(p, q)$ and W is a quadratic space of dimension $|p - q|$ which is positive-definite if $p > q$, negative-definite if $q > p$, or $\{0\}$ if $p = q$.

Theorem 6.16 tells us that a hyperbolic plane is the same thing as a 2-dimensional non-degenerate quadratic space with a null vector. The importance of the hyperbolic plane is in the next result, which says that hyperbolic planes always explain null vectors in non-degenerate quadratic spaces:

Theorem 6.34. *Let (V, Q) be a non-degenerate quadratic space. If Q has a null vector then $V \cong \mathbf{H} \perp W$ and W is non-degenerate.*

Proof. Let $Q(v) = 0$ with $v \neq 0$. We will find a second null vector for Q which is not orthogonal to v.

Since (V, Q) is non-degenerate and v is nonzero, $v^\perp \neq V$. Pick any u at all outside of $v^\perp$, so $B(u, v) \neq 0$. We will find a null vector of the form $u + cv$ for some $c \in F$. Then, since $B(u + cv, v) = B(u, v) + cB(v, v) = B(u, v)$, $u + cv$ is not orthogonal to v.

For all $c \in F$,

$$Q(u + cv) = Q(u) + Q(cv) + 2B(u, cv) = Q(u) + 2cB(u, v).$$

Let $c = -Q(u)/2B(u, v)$, so $Q(u + cv) = 0$. Now rename $u + cv$ as u, so u is a null vector for Q and $B(u, v) \neq 0$. Since $v \perp v$ and $u \not\perp v$, u and v are linearly independent.

In $Fu + Fv$, $Q(xu + yv) = 2xyB(u, v)$, which equals xy after scaling u so that $B(u, v) = 1/2$. (Since $B(u, v) \neq 0$, $B(au, v) = aB(u, v)$ becomes $1/2$ for some $a \in F$.) Now $Fu + Fv$ as a quadratic space is a hyperbolic plane, since xy and $x^2 - y^2$ are equivalent. Since a hyperbolic plane is non-degenerate, $V = (Fu + Fv) \perp W$ where $W = (Fu + Fv)^\perp$ (Theorem 3.10). □

Theorem 6.34 says that after a linear change of variables, a non-degenerate quadratic form with a null vector has the expression

$$Q(x_1, x_2, \ldots, x_n) = x_1^2 - x_2^2 + Q'(x_3, \ldots, x_n).$$

The merit of Theorem 6.34 is that it conveys this in a more geometric way.

Let's take another look at quadratic forms over a finite field $\mathbf{F}$ (with odd characteristic). If (V, Q) is a non-degenerate quadratic space over $\mathbf{F}$ with $n := \dim V \geq 3$, there is a null vector in V (Theorem 6.21), so $V \cong \mathbf{H} \perp W$ and $\dim W = n - 2$. If $\dim W \geq 3$, there is a null vector in W and we can split off another hyperbolic plane: $V \cong \mathbf{H}^{\perp 2} \perp W'$. This can be repeated until we reach a subspace of dimension ≤ 2, so $V \cong \mathbf{H}^{\perp m} \perp U$ for $m = [(n-1)/2]$ and U is non-degenerate with $\dim U = 1$ or 2. The analysis of U will duplicate our previous work in these low-dimensional cases. If $\dim U = 1$ then the underlying quadratic form on it is x^2 or cx^2 where c is a (fixed) square in $\mathbf{F}^\times$. If $\dim U = 2$ then $Q|_U$ is universal (Corollary 6.25) so we can write it as $x^2 - ay^2$ for some $a \neq 0$. Here a only matters modulo squares, so we can replace it with either 1 (if a is a square) or c (if a is not a square). The first case gives us a hyperbolic plane and the second doesn't (no null vector). There are 2 choices for U in both dimensions 1 and 2, which can distinguished by their discriminants.

Since $\operatorname{disc}(V) = \operatorname{disc}(\mathbf{H})^m \operatorname{disc}(U) = (-1)^{[(n-1)/2]} \operatorname{disc}(U)$, we have once again shown that there are 2 non-degenerate quadratic forms of each dimension over $\mathbf{F}$, and they can be distinguished from each other by their discriminant (modulo nonzero squares, as always). Moreover, this second approach gives another way to express the two choices of quadratic forms in each dimension. Choosing coordinates in a hyperbolic plane so the quadratic form is xy rather than $x^2 - y^2$, a non-degenerate n-dimensional quadratic form over $\mathbf{F}$ is equivalent to

$$x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + \begin{cases} x_{n-1}x_n, \text{ or} \\ x_{n-1}^2 - cx_n^2, \end{cases} \tag{6.10}$$

if n is even and

$$x_1x_2 + x_3x_4 + \cdots + x_{n-4}x_{n-3} + x_{n-2}x_{n-1} + \begin{cases} x_n^2, \text{ or} \\ cx_n^2, \end{cases} \tag{6.11}$$

if n is odd.

While this second classification of quadratic forms over $\mathbf{F}$ appears more complicated than Theorem 6.26, it more closely resembles the classification of non-degenerate quadratic forms over finite fields with characteristic 2 (Theorem 7.20 below).

We conclude this section with some odds and ends: a number of conditions equivalent to non-degeneracy for a quadratic form and a theorem of Jordan and von Neumann on the axioms for quadratic forms.

Theorem 6.35. *Let Q be a quadratic form on V. The following conditions are equivalent:*

(1) *Q is non-degenerate, i.e.,* $\operatorname{disc} Q \neq 0$,
(2) *there is no basis of V in which Q can be written as a polynomial in fewer than n variables, where $n = \dim V$,*
(3) *using any basis of V to express Q as a polynomial function, the only common solution in V to $(\partial Q/\partial x_i)(v) = 0$ for all i is $v = 0$.*

Proof. To show (1) and (2) are equivalent, assume (2): Q can't be written as a polynomial in fewer than n variables. Then relative to an orthogonal basis $\{e_1, \ldots, e_n\}$ the diagonal coefficients $Q(e_i)$ are all nonzero, so (1) holds.

Now assume Q can be written in fewer than n variables. That is, we can decompose V as a direct sum $V_1 \oplus V_2$ of nonzero subspaces such that $Q(v) = Q(v_1)$ for all $v \in V$, where v_1 is the projection of v onto its V_1-component. We will show $V^\perp \neq \{0\}$, so Q is degenerate. Note $Q(V_2) = \{0\}$. Pick a nonzero $w \in V_2$. For any $v \in V_1$, $Q(v + w) = Q(v)$. Therefore $Q(w) + 2B(v, w) = 0$. Since $Q(w) = 0$, we have $w \perp v$ (because $2 \neq 0$). Therefore $w \perp V_1$. For a second vector $w' \in V_2$, $Q(w + w') = 0$ and $Q(w) = Q(w') = 0$, so $2B(w, w') = 0$. This tells us $w \perp V_2$. Thus $w \perp V$, so $V^\perp \neq \{0\}$. (In particular, we found a nonzero element of $V^\perp$ at which Q vanishes.)

We now show (1) and (3) are equivalent. Choose a basis and write Q as the polynomial in (6.4). Then

$$\frac{\partial Q}{\partial x_k} = \sum_{i<k} a_{ik}x_i + 2a_kx_k + \sum_{k<j} a_{kj}x_j,$$

so all the partial derivatives vanish at a point $(c_1, \dots, c_n)$ if and only if

$$\begin{pmatrix} 2a_1 & a_{12} & \cdots & a_{1n} \\ a_{12} & 2a_2 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & 2a_n \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{6.12}$$

The matrix here is twice the matrix for Q in (6.6). The partial derivatives of Q all vanish simultaneously only at $\mathbf{0}$ in F^n precisely when the matrix in (6.12) is invertible, which is equivalent to the matrix in (6.6) being invertible (since $2 \neq 0$ in F), which is the definition of Q being non-degenerate. $\square$

Remark 6.36. If we replace the quadratic form Q with a homogeneous polynomial of degree greater than 2, the second and third properties of Theorem 6.35 are no longer the same [12, pp. 364, 376, 377].

Since Q is a homogeneous polynomial (once a basis is chosen), its zero set is naturally a projective hypersurface. In terms of this hypersurface, the algebraic condition of non-degeneracy for quadratic forms outside of characteristic 2 acquires a geometric interpretation in dimension at least 3:

Corollary 6.37. *Let V be an n-dimensional vector space over a field F not of characteristic 2 and let Q be a nonzero quadratic form on V. Pick a basis to view Q as a homogeneous polynomial function of n variables. If $n \geq 3$ then Q is non-degenerate on V if and only if the projective hypersurface $Q = 0$ in $\mathbf{P}^{n-1}(\overline{F})$ is irreducible and smooth. If $n = 2$ then the solution set to $Q = 0$ in $\mathbf{P}^1(\overline{F})$ contains 2 points if Q is non-degenerate and 1 point if Q is degenerate.*

Proof. Suppose $n \geq 3$. If Q as a polynomial is reducible over $\overline{F}$ then $Q = L_1 L_2$ where the L_i's are linear forms (homogeneous of degree 1) over $\overline{F}$. We will show from this factorization that Q is degenerate on V, so any non-degenerate quadratic form on V is irreducible as a polynomial over $\overline{F}$ when $n \geq 3$.

The zero sets of L_1 and L_2 in $\overline{F}^n$ have a common nonzero point: this is obvious if L_1 and L_2 are scalar multiples of each other, and if they are not scalar multiples then their zero sets are hyperplanes in $\overline{F}^n$ whose intersection has codimension $n - 2 > 0$. In either case, let P be a common zero of L_1 and L_2 in $\overline{F}^n - \{\mathbf{0}\}$. Then

$$\left.\frac{\partial Q}{\partial x_i}\right|_P = L_1(P) \left.\frac{\partial L_2}{\partial x_i}\right|_P + L_2(P) \left.\frac{\partial L_1}{\partial x_i}\right|_P = 0$$

for all i. Applying Theorem 6.35 to the polynomial Q as a quadratic form on $\overline{F}^n$, we see that $\operatorname{disc} Q = 0$. Therefore Q is degenerate on V too. (Concretely, if there is a nonzero vector in $\overline{F}^n$ at which all the partials of Q vanish then there is such a point in F^n because a matrix with entries in F which is not invertible over a larger field is also not invertible over F itself.)

If Q is non-degenerate on V it is an irreducible polynomial over $\overline{F}$, so the hypersurface $Q = 0$ in $\mathbf{P}^{n-1}(\overline{F})$ is defined by a single irreducible polynomial over $\overline{F}$. This hypersurface is smooth since the partials $\partial Q/\partial x_k$ do not all vanish at a common nonzero point in $\overline{F}^n$. Conversely, if this hypersurface is irreducible and smooth then the partials $\partial Q/\partial x_k$ do not all vanish at a common nonzero point in $\overline{F}^n$, so Q is non-degenerate over $\overline{F}$ and and thus over F (*i.e.*, on V).

When $n = 2$, write Q as $ax^2 + by^2$ in an orthogonal basis. This vanishes at two points on $\mathbf{P}^1(\overline{F})$ when $a \neq 0$ and $b \neq 0$, which is equivalent to Q being non-degenerate on V. $\square$

We have not yet mentioned an identity for quadratic forms called the parallelogram law:

$$Q(v + w) + Q(v - w) = 2(Q(v) + Q(w)). \tag{6.13}$$

To obtain this, replace w with $-w$ in the equation $Q(v + w) = Q(v) + Q(w) + 2B(v, w)$ to get $Q(v - w) = Q(v) + Q(w) - 2B(v, w)$, and then add. The B-terms cancel. (When Q is $x^2 + y^2$ in the plane, (6.13) says the sum of the squares of the diagonals of a parallelogram is twice the sum of the squares of adjacent sides.) If instead we subtract, then we get

$$Q(v + w) - Q(v - w) = 4B(v, w). \tag{6.14}$$

Since (6.14) describes B in terms of Q-values (in a different way than in (6.2)), could we use (6.13) and (6.14) as an alternate set of conditions for defining a quadratic form? This was examined by von Neumann and Jordan.[7] They did not show Q is a quadratic form and B is its bilinear form, but they came close:

Theorem 6.38. *Let a function $Q\colon V \to F$ satisfy* (6.13). *Define B by* (6.14). *Then B is symmetric, biadditive, and $B(v, v) = Q(v)$.*

Proof. We start by extracting a few properties from special cases of (6.13) and (6.14). Setting $w = v = 0$ in (6.13) implies $2Q(0) = 4Q(0)$, so $Q(0) = 0$. Setting $w = v$ in (6.13) implies $Q(2v) = 4Q(v)$. Setting $w = -v$ in (6.13) implies $Q(2v) = 2(Q(v) + Q(-v))$, so $4Q(v) = 2Q(v)+2Q(-v)$. Therefore $Q(-v) = Q(v)$. Now set $w = 0$ in (6.14): $0 = 4B(v, 0)$, so $B(v, 0) = 0$. Set $w = v$ in (6.14): $Q(2v) = 4B(v, v)$, so $B(v, v) = Q(v)$. Therefore

$$\begin{aligned}
B(v, w) &= \frac{1}{4}(Q(v + w) - Q(v - w)) \\
&= \frac{1}{4}(Q(v + w) + Q(v + w) - 2(Q(v) + Q(w))) \quad \text{by (6.13)} \\
&= \frac{1}{2}(Q(v + w) - Q(v) - Q(w)),
\end{aligned}$$

which is symmetric in v and w (and is the kind of formula we expected to hold anyway).

It remains to show B is biadditive. Since B is symmetric, we will just show additivity in the second component. From (6.14),

$$\begin{aligned}
4(B(v, w_1) + B(v, w_2)) &= Q(v + w_1) - Q(v - w_1) + Q(v + w_2) \\
&\qquad -Q(v - w_2) \\
&= Q(v + w_1) + Q(v + w_2) - Q(v - w_1) \\
&\qquad -Q(v - w_2) \\
&= \frac{1}{2}(Q(2v + w_1 + w_2) + Q(w_1 - w_2)) - \\
&\qquad \frac{1}{2}(Q(2v - w_1 - w_2) + Q(w_2 - w_1)) \quad \text{by (6.13)} \\
&= \frac{1}{2}(Q(2v + w_1 + w_2) - Q(2v - w_1 - w_2)) \\
&= 2B(2v, w_1 + w_2) \text{ by (6.14).}
\end{aligned}$$

[7]This is the physicist P. Jordan who introduced Jordan algebras, rather than the mathematician C. Jordan, as in Jordan canonical form.

Dividing by 4,

$$B(v, w_1) + B(v, w_2) = \frac{1}{2}B(2v, w_1 + w_2), \tag{6.15}$$

which is nearly what we want. Setting $w_2 = 0$ in (6.15) and multiplying by 2, $2B(v, w_1) = B(2v, w_1)$. Since w_1 is arbitrary, we get $2B(v, w_1 + w_2) = B(2v, w_1 + w_2)$. Therefore the right side of (6.15) is $B(v, w_1 + w_2)$, so B is additive in its second component. $\square$

Bi-additivity implies $\mathbf{Z}$-bilinearity. Therefore B in Theorem 6.38 is $\mathbf{Q}$-bilinear if F has characteristic 0 and $\mathbf{F}_p$-bilinear if F has characteristic p, which means Q is a quadratic form when $F = \mathbf{Q}$ or $\mathbf{F}_p$. If $F = \mathbf{R}$ then Q in Theorem 6.38 is a quadratic form over $\mathbf{R}$ if V is finite-dimensional and we add the extra assumption that Q is continuous (so B is continuous and therefore is $\mathbf{R}$-bilinear).

Exercises.

1. Diagonalize $x^2+y^2-z^2+3xy-xz+6yz$ over $\mathbf{Q}$. What is its signature as a quadratic form over $\mathbf{R}$?
2. When F has characteristic not 2, diagonalize $Q(L) = \operatorname{Tr}(L^2)$ on $\mathrm{M}_2(F)$ using the orthogonal basis in Exercise 4.2.
3. When F has characteristic not 2, show $\det\colon \mathrm{M}_2(F) \to F$ is a quadratic form. Find its associated bilinear form and a diagonalization.
4. Show the quadratic forms x^2+y^2 and $3x^2+3y^2$ over $\mathbf{Q}$ are inequivalent even though they have the same discriminant (modulo squares).
5. Let $K = \mathbf{Q}(\theta)$, where θ is the root of an irreducible cubic $f(X) = X^3 + aX + b$ in $\mathbf{Q}[X]$. Let $Q\colon K \to \mathbf{Q}$ by $Q(\alpha) = \operatorname{Tr}_{K/\mathbf{Q}}(\alpha^2)$. Viewing K as a $\mathbf{Q}$-vector space, show Q is a quadratic form over $\mathbf{Q}$ which is determined up to equivalence by the number $4a^3 + 27b^2$. (Hint: Diagonalize Q.)
6. Let B be any bilinear form on V, not necessarily symmetric. Show the function $Q(v) = B(v, v)$ is a quadratic form on V. What is its associated symmetric bilinear form, in terms of B? How does this look in the language of matrices?
7. Let Q be a quadratic form on a real vector space V. If there are v and w in V such that $Q(v) > 0$ and $Q(w) < 0$, show v and w are linearly independent and there is a null vector for Q in the plane spanned by v and w. Must this plane have a basis of null vectors?
8. In $\mathbf{R}^{p,q}$, let $\{e_1, \ldots, e_n\}$ be an orthogonal basis. Scale each e_i so $\langle e_i, e_i\rangle_{p,q} = \pm 1$. Show the number of e_i's with $\langle e_i, e_i\rangle_{p,q} = 1$ is p and the number with $\langle e_i, e_i\rangle_{p,q} = -1$ is q.
9. Let V be a non-degenerate real quadratic space with signature (p, q). Show p is geometrically characterized as the maximal dimension of a positive-definite subspace of V.
10. Show that a non-degenerate quadratic form over an ordered field has a well-defined signature relative to that ordering: after diagonalization, the number p of positive coefficients and q of negative coefficients in the ordering is independent of the diagonalization. Therefore we can talk about the signature (p, q) of a non-degenerate quadratic form on an ordered field. (Hint: First show that in the 2-dimensional case the diagonal coefficients have opposite sign precisely when the quadratic form takes both positive and negative values in the ordering.)

11. Let K/F be a quadratic field extension not in characteristic 2. Viewing K as an F-vector space, show the norm map $\mathrm{N}_{K/F}\colon K \to F$ is a non-degenerate quadratic form over F without null vectors.
12. In the text we classified non-degenerate quadratic spaces over $\mathbf{C}$, $\mathbf{R}$, and finite fields with odd characteristic. What about the degenerate case? Show a quadratic form on V induces a quadratic form on $V/V^{\perp}$ which is non-degenerate. In particular, show a quadratic space (V, Q) is determined up to isomorphism by the dimension of $V^{\perp}$ and the isomorphism class of the non-degenerate quadratic space $V/V^{\perp}$.

7. Quadratic forms in characteristic 2

Fields of characteristic 2 *have remained the pariahs of the theory.*

W. Scharlau [11, p. 231]

The concrete definition of a quadratic form in characteristic 2 is just like that in other characteristics: a function on a vector space which looks like a quadratic homogeneous polynomial in some (equivalently, any) basis. To give a coordinate-free definition, we copy Definition 6.1 but leave out the $\frac{1}{2}$.

Definition 7.1. A *quadratic form* on a vector space V over a field F with characteristic 2 is a function $Q\colon V \to F$ such that

(1) $Q(cv) = c^2Q(v)$ for $v \in V$ and $c \in F$,
(2) the function $B(v, w) := Q(v + w) - Q(v) - Q(w)$ is bilinear.

We will often use condition (2) as

$$Q(v + w) = Q(v) + Q(w) + B(v, w). \tag{7.1}$$

The function B is called the bilinear form associated to Q. Formally, this B is double the B from characteristic not 2. As in the case of characteristic not 2, we call $\dim V$ the *dimension* of the quadratic form and whenever we refer to a quadratic form "on F^n" we view F^n as an F-vector space.

From now on, V *is finite-dimensional.*

To see that Definition 7.1 turns a quadratic form into a quadratic homogeneous polynomial in a basis, we argue in a similar manner to the case of characteristic not 2, except certain factors of 2 will be missing.

Let $Q\colon V \to F$ satisfy Definition 7.1. Inducting on the number of terms in (7.1),

$$Q(v_1 + \cdots + v_r) = Q(v_1) + \cdots + Q(v_r) + \sum_{i<j} B(v_i, v_j) \tag{7.2}$$

for any $r \geq 2$ and vectors $v_i \in V$. Letting $\{e_1, \ldots, e_n\}$ be a basis of V, we obtain from (7.2)

$$Q(x_1e_1 + \cdots + x_ne_n) = \sum_{i=1}^{n} a_ix_i^2 + \sum_{i<j} a_{ij}x_ix_j, \tag{7.3}$$

where $a_i = Q(e_i)$ and $a_{ij} = B(e_i, e_j)$. Conversely, let $Q\colon V \to F$ be a function defined by (7.3) in a basis. For $v = x_1e_1 + \cdots + x_ne_n$ we can write $Q(v) = [v] \cdot N[v]$, where N is the upper-triangular (not symmetric!) matrix

$$N = \begin{pmatrix} a_1 & a_{12} & \cdots & a_{1n} \\ 0 & a_2 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}. \tag{7.4}$$

Clearly $Q(cv) = c^2Q(v)$. Letting $v' = x_1'e_1 + \cdots + x_n'e_n$, define

$$\begin{aligned} B(v,v') &:= Q(v+v') - Q(v) - Q(v') \\ &= [v+v'] \cdot N[v+v'] \\ &= [v] \cdot (N + N^\top)[v']. \end{aligned} \tag{7.5}$$

This is a bilinear form on V, so Q is a quadratic form on V. The matrix for B is

$$N + N^\top = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ a_{12} & 0 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & 0 \end{pmatrix}. \tag{7.6}$$

Formally, this is the matrix obtained by multiplying (6.6) by 2.

We could have used Definition 7.1 to define quadratic forms in all characteristics. This is the approach taken in [2], [3], [7], and [8]. For instance, outside of characteristic 2 the connection between quadratic forms and symmetric bilinear forms becomes $B(v,v) = 2Q(v)$ instead of $B(v,v) = Q(v)$. While some redundancy from the separate treatment of characteristic 2 is avoided if we use Definition 7.1 to describe quadratic forms in in all characteristics, this approach leads to the feature that the bilinear form associated to $\sum_{i=1}^n x_i^2$ is not the usual dot product but rather twice the dot product.

We return to characteristic 2. The matrix in (7.6) is symmetric, but it has no dependence on the diagonal coefficients a_i from (7.3). Notice B is identically 0 if and only if all cross terms a_{ij} vanish (equivalently, Q has a diagonalization in some basis). When the characteristic is not 2 we can eliminate the cross terms of any quadratic form (degenerate or non-degenerate) by using a suitable basis, but we *need* cross terms in characteristic 2 if the associated bilinear form is not going to be identically zero.

Example 7.2. Let F have characteristic 2 and let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form on F^2. For $v = (x,y)$ and $v' = (x',y')$ in F^2,

$$Q(v) = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

and

$$\begin{aligned} B(v,v') &= Q(v+v') - Q(v) - Q(v') \\ &= b(xy' + x'y) \\ &= \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}. \end{aligned}$$

So B is non-degenerate if and only if $b \neq 0$.

By definition, any quadratic form in characteristic 2 has an associated symmetric bilinear form, but the correspondence from quadratic forms to symmetric bilinear forms in characteristic 2 is neither injective nor surjective: different quadratic forms like x^2+xy and xy can have the same symmetric bilinear form, and some symmetric bilinear forms like $xx' + yy'$ do not arise as the bilinear form of any quadratic form. In matrix language, every quadratic form outside of characteristic 2 can be written as $Q(v) = [v] \cdot M[v]$ for some symmetric matrix M, but this is not true in characteristic 2. A quadratic form in characteristic 2 with cross terms in a basis is not represented by a symmetric matrix in any basis. The associated bilinear form, however, is *always* represented by a symmetric matrix. (See (7.5) and (7.6).) We have to be careful not to confuse a matrix like (7.4) for a quadratic form in characteristic 2 with a matrix like (7.6) for its bilinear form.

A key observation is that the symmetric bilinear form associated to a quadratic form in characteristic 2 is alternating:

$$B(v, v) = Q(2v) - 2Q(v) = Q(0) - 0 = 0.$$

(The matrix in (7.6) is indeed alternating.) In characteristic not 2, we were able to recover Q from B since $B(v, v) = Q(v)$. But in characteristic 2 the calculation of $B(v, v)$ instead tells us something more about B itself. Recall that any alternating bilinear form is symmetric in characteristic 2. We should think about the correspondence from Q to B in characteristic 2 as a map from quadratic forms to alternating (not just symmetric) bilinear forms. Then it is surjective, but still never injective (Exercises 7.4 and 7.5). That is, there is no concept like polarization in characteristic 2, so *knowledge of B alone does not let us recover Q*. Some concepts that can be discussed equally well in the language of quadratic forms or symmetric bilinear forms outside of characteristic 2 may no longer have formulations in both of these languages in characteristic 2.

One concept which is expressible in both settings is orthogonality of vectors. When the characteristic is not 2, $Q(v + w) = Q(v) + Q(w)$ if and only if $B(v, w) = 0$. This is also true in characteristic 2 (check!), so the condition $v \perp w$, which means $B(v, w) = 0$, can be described directly in terms of Q.

What is the characteristic 2 analogue of a diagonalization? Assume the bilinear form B associated to an n-dimensional quadratic form Q in characteristic 2 is non-degenerate. Then B is alternating and non-degenerate, so $n = 2m$ is even and there is a symplectic basis for B, say $\{e_1, f_1, \dots, e_m, f_m\}$. When $v_1, \dots, v_r$ are any vectors in V which are mutually perpendicular (*i.e.*, $B(v_i, v_j) = 0$ for $i \neq j$), (7.2) becomes

$$Q(v_1 + \cdots + v_r) = Q(v_1) + \cdots + Q(v_r).$$

Therefore the expression of Q in the symplectic basis for B is

$$\begin{aligned} Q(x_1e_1 + y_1f_1 + \cdots + x_me_m + y_mf_m) &= \sum_{i=1}^{m} Q(x_ie_i + y_if_i) \\ &= \sum_{i=1}^{m}(a_ix_i^2 + x_iy_i + b_iy_i^2), \end{aligned} \tag{7.7}$$

where $a_i = Q(e_i)$ and $b_i = Q(f_i)$. Conversely, if a quadratic form Q looks like (7.7) in some basis then its bilinear form B has the matrix representation (5.1) in a suitable ordering of that basis (the coefficients a_i, b_i don't show up in B), so B is non-degenerate.

The expression (7.7) is a characteristic 2 analogue of the diagonalization (6.9) except all quadratic forms outside characteristic 2 can be diagonalized while only those in characteristic 2 whose bilinear form is non-degenerate admit a representation in the form (7.7). Instead of writing Q as a sum of monomials ax^2, we have written it as a sum of two-variable quadratic forms $ax^2 + xy + by^2$. A matrix for Q in this symplectic basis is block diagonal with blocks $\left(\begin{smallmatrix} a_i & 1 \\ 0 & b_i \end{smallmatrix}\right)$. To extend (7.7) to the degenerate case, assume $V^\perp \neq \{0\}$. Write $V = W \oplus V^\perp$ for some subspace complement W. Then $B|_W$ is non-degenerate, so choosing a symplectic basis of W and tacking on any basis of $V^\perp$ to create a basis of V gives Q the expression

$$\sum_{i=1}^{m}(a_i x_i^2 + x_i y_i + b_i y_i^2) + \sum_{k=1}^{r} c_k z_k^2, \tag{7.8}$$

where $\dim W = 2m$ and $\dim V^\perp = r$. The coefficients c_k are the coefficients from any choice of basis for $V^\perp$. For instance, if Q vanishes at a nonzero vector in $V^\perp$ then we can arrange for some c_k to be 0, so Q is a polynomial in fewer than n variables, where $n = \dim V$.

We have referred already to the non-degeneracy of the bilinear form associated to a quadratic form, but we have not yet defined what it means for a quadratic form to be non-degenerate. The following theorem will be needed for that.

Theorem 7.3. *Let $Q\colon V \to F$ be a quadratic form in characteristic 2, with associated bilinear form B. The following conditions are equivalent:*

1. *the only $v \in V$ which satisfies $Q(v) = 0$ and $B(v, w) = 0$ for all $w \in V$ is $v = 0$,*
2. *the function $Q\colon V^\perp \to F$ is injective,*
3. *there is no basis of V in which Q can be written as a polynomial in fewer than n variables, where $n = \dim V$,*
4. *in any basis of V, the only common solution in V to $Q(v) = 0$ and $(\partial Q/\partial x_i)(v) = 0$ for all i is $v = 0$.*

This is an analogue of Theorem 6.35. Since $\sum_{k=1}^{n} x_k(\partial Q/\partial x_k) = 2Q$, outside of characteristic 2 the partials can all vanish only at a point where Q vanishes. But in characteristic 2 we have to explicitly include the condition $Q(v) = 0$ in (4).

Proof. Condition (1) is the same as saying the only element of $V^\perp$ at which Q vanishes is 0. For v and v' in $V^\perp$, $Q(v + v') = Q(v) + Q(v')$, so the kernel of $Q\colon V^\perp \to F$ is 0 if and only if $Q|_{V^\perp}$ is injective. Thus (1) and (2) are equivalent.

To show these conditions are equivalent to (3), a re-reading of the proof of Theorem 6.35 shows that even in characteristic 2 if Q is a polynomial in fewer than n variables in some basis of V then $V^\perp$ contains a nonzero vector at which Q vanishes. (One has to ignore a few factors of 2 in that proof.) Conversely, if there is a nonzero vector in $V^\perp$ at which Q vanishes then the discussion surrounding (7.8) shows Q is a polynomial in fewer than n variables relative to some basis of V.

We now show (4) is equivalent to (2). Write Q as in (7.3). Then

$$\frac{\partial Q}{\partial x_k} = \sum_{i<k} a_{ik} x_i + \sum_{k<j} a_{kj} x_j,$$

so the vanishing of all the partials of Q at a point $(c_1, \ldots, c_n) \in F^n$ is equivalent to

$$\begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ a_{12} & 0 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{7.9}$$

The matrix here, call it M, is a matrix for B: $B(v, w) = [v] \cdot M[w]$ (see (7.6)). If the partials all vanish at a nonzero point in F^n, say v, then $M[v] = 0$. Since $M^\top = M$, $M[v] = 0$ is equivalent to $B(v,w) = 0$ for all $w \in V$, which is equivalent to $v \in V^\perp$. That is,

$$V^\perp = \left\{ v \in V : \frac{\partial Q}{\partial x_i}(v) = 0 \text{ for all } i \right\}.$$

Therefore a common solution in V to $Q(v) = 0$ and $(\partial Q/\partial x_i)(v) = 0$ for all i is the same as an element of $\ker(Q|_{V^\perp})$, so (4) is equivalent to (2). $\square$

Definition 7.4. A quadratic form in characteristic 2 is called *non-degenerate* when the equivalent conditions in Theorem 7.3 hold. Otherwise it is called *degenerate*.

Example 7.5. A nonzero 1-dimensional quadratic form is non-degenerate. In two dimensions, the quadratic form $ax^2 + bxy + cy^2$ on F^2 is non-degenerate if $b \neq 0$ (*i.e.*, $V^\perp = \{0\}$) or if $b = 0$ (so $V^\perp = V$) and ac is not a square in F. Otherwise it is degenerate. For instance, xy on F^2 is non-degenerate while $x^2 + cy^2$ is non-degenerate if and only if c is a non-square in $F^\times$.

Example 7.6. Let $Q(x,y,z) = x^2 + xy + y^2 + z^2$ be a quadratic form on F^3. Its associated bilinear form is $B((x,y,z),(x',y',z')) = xy' + x'y$, so B is a degenerate bilinear form. However, we will see Q is a non-degenerate quadratic form according to Definition 7.4.

In matrix notation,

$$Q(x,y,z) = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

and the associated bilinear form has matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

whose kernel is $V^\perp = F(0,0,1)$. Since $Q(0,0,\gamma) = \gamma^2$, $\ker(Q|_{V^\perp}) = \{0\}$.

Remark 7.7. If B is non-degenerate (that is, $V^\perp = \{0\}$) then Q is non-degenerate. Some authors define Q to be non-degenerate in characteristic 2 only when B is non-degenerate. This rules out odd-dimensional examples. However, there are odd-dimensional non-degenerate quadratic forms according to Definition 7.4, as we just saw.

In characteristic not 2, non-degeneracy of a quadratic form (defined as invertibility of a representative symmetric matrix, with equivalent conditions given in Theorem 6.35) is unaffected by viewing it as a quadratic form over a larger base field. This is *not* usually true in characteristic 2.

Example 7.8. Let F have characteristic 2 and define Q on $V = F^2$ by $Q(x,y) = x^2 + cy^2$ where c is a non-square in F. Then $V^\perp = V$ and Q is injective on $V^\perp$, so Q is non-degenerate on F^2. But Q becomes degenerate on $\overline{F}^2$ since c is a square in $\overline{F}$.

Example 7.9. Letting c again be a non-square in F, the quadratic form $xy + z^2 + cw^2$ on F^4 is non-degenerate, but it is degenerate on $\overline{F}^4$ since the term $z^2 + cw^2$ becomes a complete square so the quadratic form can be written as a polynomial in fewer than 4 variables.

Definition 7.10. Let F have characteristic 2 and $Q\colon V \to F$ be a quadratic form. A *null vector* for Q is a nonzero $v \in V$ such that $Q(v) = 0$. We call Q *universal* if $Q(V) = F$. Quadratic forms $Q_1\colon V_1 \to F$ and $Q_2\colon V_2 \to F$ are called *equivalent* if there is a linear isomorphism $A\colon V_1 \to V_2$ such that $Q_2(Av) = Q_1(v)$ for all $v \in V_1$.

Remark 7.11. These terms have the same meaning as they did outside of characteristic 2, with one caveat: quadratic form equivalence and null vectors for a quadratic form outside of characteristic 2 can always be defined in terms of the associated bilinear form, but this is *false* in characteristic 2. For instance, in characteristic 2 $B(v,v)=0$ for all v (B is alternating) while the condition $Q(v)=0$ is restrictive.

To get used to the characteristic 2 terminology in Definitions 7.4 and 7.10, note that $Q\colon V\to F$ is non-degenerate precisely when $V^\perp$ contains no null vectors for Q. (This is also true outside of characteristic 2!) Equivalent quadratic forms either both have a null vector or neither has a null vector. Any degenerate quadratic form has a null vector (just like in characteristic not 2).

As further practice with the terminology we prove the following two theorems. The first one is a characteristic 2 analogue of Theorem 6.22.

Theorem 7.12. *If Q is non-degenerate and has a null vector then it is universal.*

Proof. The proof will be very close to that of Theorem 6.22, but note the few slight changes.

Let v be a null vector. Since $Q(cv)=c^2Q(v)=0$ and Q is not identically zero (otherwise it couldn't be non-degenerate), $\dim V\geq 2$. By non-degeneracy of Q there are no null vectors in $V^\perp$, so $v\notin V^\perp$. Therefore there is a $w\in V$ such that $B(v,w)\neq 0$. Then for any $c\in F$,

$$Q(cv+w)=Q(cv)+Q(w)+B(cv,w)=Q(w)+B(v,w)c.$$

Since $B(v,w)\neq 0$, this is a linear function of c and therefore takes on all values in F as c varies. $\square$

Theorem 7.13. *Let $Q\colon V\to F$ be a non-degenerate quadratic form. If Q has a null vector e, then it has a second null vector f such that $B(e,f)=1$ and B is non-degenerate on the plane $Fe+Ff$.*

Proof. Since Q is non-degenerate and e is a null vector, $e\notin V^\perp$. Therefore $B(e,w)\neq 0$ for some $w\in W$, so e and w are linearly independent. We can scale w so $B(e,w)=1$. Let $c=Q(w)$. Then e and $f:=ce+w$ are linearly independent null vectors and $B(e,f)=1$, so B is non-degenerate on the plane $Fe\perp Ff$. $\square$

Theorem 7.13 resembles the initial part of the construction of a symplectic basis for B, but it is a *stronger* condition to say v is a null vector of Q (that is, $Q(v)=0$) than to say $B(v,v)=0$. Besides, Theorem 7.13 makes sense in odd dimensions, where B is automatically degenerate and V has no symplectic basis.

We now turn to the classification of non-degenerate quadratic forms over a finite field $\mathbf{F}$ with characteristic 2. We will use repeatedly that every element in $\mathbf{F}$ is a square.

We begin with a series of lemmas.

Lemma 7.14. *Any quadratic form over $\mathbf{F}$ with dimension at least 3 has a null vector.*

Proof. This is the characteristic 2 analogue of Theorem 6.21. The odd characteristic proof used an orthogonal basis, which is not available in characteristic 2.

Let Q be the quadratic form and B be its associated bilinear form. Pick $v\neq 0$ in V. We may suppose $Q(v)\neq 0$. Since $\dim v^\perp\geq n-1\geq 2$, we can pick $w\in v^\perp$ with $w\notin\mathbf{F}v$. Then $Q(w)=aQ(v)$ for some $a\in\mathbf{F}$. Write $a=b^2$, so $Q(w)=Q(bv)$ and $w\neq bv$. Since $w\perp v$, $Q(w+bv)=Q(w)+Q(bv)=0$ and $w+bv\neq 0$. $\square$

The bound $\dim V\geq 3$ is sharp: there is a two-dimensional non-degenerate quadratic form over $\mathbf{F}$ without null vectors (Exercise 7.3).

Remark 7.15. There is a uniform proof of Theorem 6.21 and Lemma 7.14 for all finite fields using the Chevalley–Warning theorem [6, pp. 143–145].

Lemma 7.16. *Any quadratic form over* $\mathbf{F}$ *which is not identically zero is universal.*

Proof. Let $Q\colon V \to \mathbf{F}$ be a quadratic form and $Q(v_0) \neq 0$. For $c \in \mathbf{F}$, $Q(cv_0) = c^2Q(v_0)$. Squaring on $\mathbf{F}$ is a bijection, so $\{c^2Q(v_0) : c \in \mathbf{F}\} = \mathbf{F}$. Therefore Q is universal. $\square$

The analogous result for finite fields in odd characteristic (Corollary 6.25) required non-degeneracy and dimension at least 2.

Lemma 7.17. *If* $Q\colon V \to \mathbf{F}$ *is non-degenerate then* $\dim V^\perp \leq 1$. *More precisely,* $V^\perp = \{0\}$ *if* $\dim V$ *is even and* $\dim V^\perp = 1$ *if* $\dim V$ *is odd.*

Proof. Let B be the bilinear form attached to Q, so B is alternating. The induced alternating bilinear form on $V/V^\perp$ is non-degenerate, so $\dim(V/V^\perp)$ is even. Therefore the second part of the theorem (knowing $\dim V^\perp$ from the parity of $\dim V$) will follow once we know $\dim V^\perp \leq 1$.

Suppose $V^\perp \neq \{0\}$ and v_0 is a nonzero vector in $V^\perp$, so $Q(v_0) \neq 0$. We want to show $V^\perp = \mathbf{F}v_0$. For any $v' \in V^\perp$, $Q(v') = aQ(v_0)$ for some $a \in \mathbf{F}$. Write $a = b^2$ for some $b \in \mathbf{F}$. Then $Q(v') = Q(bv_0)$, so $Q(v' - bv_0) = 0$ (Q is additive on $V^\perp$). By non-degeneracy of Q, $v' - bv_0 = 0$, so $v' = bv_0$. Therefore $V^\perp = \mathbf{F}v_0$. $\square$

Remark 7.18. For quadratic forms $Q\colon V \to \mathbf{F}$ over a finite field with characteristic 2, Remark 7.7 and Lemma 7.17 tell us that non-degeneracy of Q is the same as non-degeneracy of its bilinear form when $\dim V$ is *even*.

In the classification of quadratic forms over finite fields with odd characteristic, the discriminant plays a key role. In characteristic 2 the discriminant is useless because every element of $\mathbf{F}$ is a square. Instead of working with squares and non-squares in the multiplicative group of the finite field, we will work with values and non-values of the function $\wp\colon \mathbf{F} \to \mathbf{F}$ given by $\wp(a) = a^2 + a$. The function $\wp$ is additive and has kernel $\{0, 1\}$, so $\wp$ takes on half the values in $\mathbf{F}$. Moreover, $\mathbf{F}/\wp(\mathbf{F})$ has size 2, so the sum of two non-$\wp$ values in $\mathbf{F}$ is a $\wp$-value. (Note the analogy to squaring nonzero numbers in odd characteristic, where the kernel is $\{\pm 1\}$, half the nonzero elements are squares, and the product of two non-squares is a square.)

Theorem 7.19. *Fix* $c \in \mathbf{F} - \wp(\mathbf{F})$. *Let* Q *be a non-degenerate quadratic form on* V *where* $\dim V$ *is* 1, 2, *or* 3. *Then* Q *is equivalent to one of the following:*

(1) x^2 *in dimension* 1,
(2) xy *or* $x^2 + xy + cy^2$ *in dimension* 2, *and these are inequivalent,*
(3) $xy + z^2$ *in dimension* 3.

Proof. Any non-degenerate one-dimensional quadratic form looks like ax^2 in a basis, and a is a square in $\mathbf{F}$, so the quadratic form is equivalent to x^2.

We now turn to the two-dimensional case. The quadratic forms xy and $x^2 + xy + cy^2$ on $\mathbf{F}^2$ are inequivalent, since the first one has a null vector (such as $(1, 0)$) and the second one does not: if it had a null vector (x_0, y_0) then $y_0 \neq 0$ and then $c = (x_0/y_0)^2 + x_0/y_0 \in \wp(\mathbf{F})$.

It remains, in the two-dimensional case, to show Q has one of the two indicated forms in some basis. Since Q is universal by Lemma 7.16, pick v such that $Q(v) = 1$. By Lemma

7.17 $V^\perp = \{0\}$, so B is non-degenerate. Therefore there is a w such that $B(v,w) = 1$. Then $\{v,w\}$ is a basis of V and

$$Q(xv + yw) = Q(xv) + Q(yw) + B(xv, yw) = x^2 + xy + Q(w)y^2.$$

If $Q(w) = a^2 + a$ for some a, then

$$x^2 + xy + Q(w)y^2 = x^2 + xy + (a^2 + a)y^2 = (x + ay)(x + (a+1)y) = x'y'$$

where $x' = x + ay$ and $y' = x + (a+1)y$. Therefore Q is equivalent to xy. If $Q(w) \neq a^2 + a$ for any a then $Q(w) = c$ in $\mathbf{F}/\wp(\mathbf{F})$, so $Q(w) + c = a^2 + a$ for some $a \in \mathbf{F}$. Thus

$$x^2 + xy + Q(w)y^2 = x^2 + xy + (a^2 + a + c)y^2 = (x + ay)^2 + (x + ay)y + cy^2,$$

which is the same as $x^2 + xy + cy^2$ after a linear change of variables.

Now we treat the three-dimensional case. By Lemma 7.14 there is a null vector, say e. By Theorem 7.13 there is a null vector f such that $B(e,f) = 1$ and B is non-degenerate on the plane $\mathbf{F}e + \mathbf{F}f$. In particular, this plane meets $V^\perp$ in $\{0\}$. Lemma 7.17 says $V^\perp$ is one-dimensional, so any nonzero element of $V^\perp$ along with e and f gives a basis of V. Let g be a nonzero vector in $V^\perp$, so $Q(g) \neq 0$ by non-degeneracy, Since $Q(ag) = a^2Q(g)$, by rescaling g we can suppose $Q(g) = 1$. Since $g \perp (\mathbf{F}e + \mathbf{F}f)$,

$$Q(xe + yf + zg) = Q(xe + yf) + Q(zg) = xyB(e,f) + z^2Q(g) = xy + z^2,$$

which is what we want since $\{e, f, g\}$ is a basis. □

Theorem 7.20. *Fix $c \in \mathbf{F} - \wp(\mathbf{F})$. For $n \geq 2$, any n-dimensional non-degenerate quadratic form over $\mathbf{F}$ is equivalent to exactly one of*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + \begin{cases} x_{n-1}x_n, & \text{or} \\ x_{n-1}^2 + x_{n-1}x_n + cx_n^2 \end{cases}$$

if n is even and

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2$$

if n is odd.

This is comparable to (6.10) and (6.11), except there is just one choice when n is odd. The theorem is not asserting that the two choices in the even case are inequivalent, although that does turn out to be true. We will return to this issue after proving the theorem.

Proof. We induct on n. By Theorem 7.19, we can suppose $n \geq 4$.

Let Q be a non-degenerate quadratic form on V, where $n = \dim V$. By Lemma 7.14 there is a null vector for Q, say v. By Theorem 7.13, there is an independent null vector w such that $B(v,w) = 1$ and B is non-degenerate on the plane $U = \mathbf{F}v + \mathbf{F}w$. Since Q has a null vector in U, $Q|_U$ looks like xy in a suitable basis by Theorem 7.19.

Assume n is even. Then $V^\perp = \{0\}$: B is non-degenerate on V. Thus $V = U \oplus U^\perp$ and $B|_{U^\perp}$ is non-degenerate (Theorem 3.10). Therefore $Q|_{U^\perp}$ is non-degenerate (Remark 7.18). We are now done by induction.

Assume n is odd, so $n \geq 5$. Then $\dim V^\perp = 1$ by Lemma 7.17. Since Q is not identically zero on $V^\perp$ by non-degeneracy, $Q|_{V^\perp}$ is x^2 in a suitable basis. Let W be a subspace of V complementary to $V^\perp$: $V = W \oplus V^\perp$, $\dim W$ is even and $B|_W$ is non-degenerate. Therefore

(Remark 7.18) $Q|_W$ is non-degenerate. By the even-dimensional case (for dimension $n-1$) $Q|_W$ is equivalent to one of

$$x_1x_2 + x_3x_4 + \cdots + x_{n-4}x_{n-3} + \begin{cases} x_{n-2}x_{n-1}, \text{ or} \\ x_{n-2}^2 + x_{n-2}x_{n-1} + cx_{n-1}^2. \end{cases}$$

Since $Q = Q|_W + Q|_{V^\perp}$ and $Q|_{V^\perp}$ looks like x_n^2 in a suitable basis, the expression of Q in the combined basis for W and $V^\perp$ looks like one of

$$x_1x_2 + x_3x_4 + \cdots + x_{n-4}x_{n-3} + \begin{cases} x_{n-2}x_{n-1} + x_n^2, \text{ or} \\ x_{n-2}^2 + x_{n-2}x_{n-1} + cx_{n-1}^2 + x_n^2. \end{cases} \tag{7.10}$$

The two "end choices" here are $xy + z^2$ and $x^2 + xy + cy^2 + z^2$. By generalizing Example 7.6, $x^2 + xy + cy^2 + z^2$ is a non-degenerate quadratic form on F^3. It is equivalent to $xy + z^2$ by Theorem 7.19, so the two possible expressions for Q in (7.10) are equivalent. □

We now explain why the two representative quadratic forms when n is even are inequivalent.

The smallest case, $n = 2$, involves xy and $x^2 + xy + cy^2$ where $c \notin \wp(\mathbf{F})$. These can be distinguished by counting null vectors in $\mathbf{F}^2$: xy has some and $x^2 + xy + cy^2$ has none. The same idea works for even $n > 2$: the two n-dimensional quadratic forms in Theorem 7.20 don't have the same number of null vectors, so they are inequivalent. We will prove this by counting.

Definition 7.21. Let $Q\colon V \to \mathbf{F}$ be a quadratic form over $\mathbf{F}$. Set $z(Q) = \#\{v \in V : Q(v) = 0\}$.

The number $z(Q)$ is 1 more than the number of null vectors of Q.

Example 7.22. If $V = \mathbf{F}^2$ and $Q\colon V \to \mathbf{F}$ is non-degenerate then Q is equivalent to either xy or $x^2 + xy + cy^2$, where $c \notin \wp(\mathbf{F})$. A calculation shows $z(xy) = 2q - 1$ and $z(x^2 + xy + cy^2) = 1$, where $q = \#\mathbf{F}$.

Any nonzero quadratic form Q over $\mathbf{F}$ is universal (Lemma 7.16), so the sets $Q^{-1}(a)$ are all non-empty as a varies in $\mathbf{F}$. Moreover, Q takes on each nonzero value in $\mathbf{F}$ equally often: if $a \in \mathbf{F}^\times$ and we write $a = b^2$, then the sets $Q^{-1}(a)$ and $Q^{-1}(1)$ are in bijection using $v \leftrightarrow (1/b)v$. However these sets need not be in bijection with $Q^{-1}(0)$, as we can see already in the case of $Q(x, y) = xy$: $\#Q^{-1}(a) = q - 1$ for $a \neq 0$ and $\#Q^{-1}(0) = 2q - 1$, where $q = \#\mathbf{F}$. The number $z(Q) = \#Q^{-1}(0)$ is therefore distinctive.

Lemma 7.23. *Let $Q\colon V \to \mathbf{F}$ be a quadratic form over $\mathbf{F}$ and set $q = \#\mathbf{F}$. Writing h for the quadratic form xy on $\mathbf{F}^2$,*

$$z(Q \perp h) = qz(Q) + (q-1)\#V,$$

where $Q \perp h$ is the quadratic form on $V \oplus \mathbf{F}^2$ given by $(Q \perp h)(v, u) = Q(v) + h(u)$.

Proof. The vanishing of $(Q \perp h)(v,u)$ is equivalent to $Q(v) = h(u)$. We count this event separately according to $h(u) = 0$ and $h(u) \neq 0$:

$$\begin{aligned} z(Q \perp h) &= \#\{(v,u) : Q(v) = h(u)\} \\ &= \sum_u \#Q^{-1}(h(u)) \\ &= \sum_{h(u)=0} \#Q^{-1}(0) + \sum_{h(u)\neq 0} \#Q^{-1}(h(u)) \\ &= z(h)z(Q) + \sum_{h(u)\neq 0} \#Q^{-1}(1) \\ &= (2q-1)z(Q) + (q^2 - z(h))\#Q^{-1}(1) \\ &= (2q-1)z(Q) + (q-1)^2\#Q^{-1}(1). \end{aligned}$$

We have $\#Q^{-1}(1) = (\#V - z(Q))/(q-1)$ since $Q\colon V \to \mathbf{F}$ takes nonzero values equally often. Substitute this into the formula for $z(Q \perp h)$ and simplify. $\square$

Theorem 7.24. *For $n = 2m$ with $m \geq 1$,*

$$z(x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + x_{n-1}x_n) = q^{2m-1} + q^m - q^{m-1}$$

and

$$z(x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + x_{n-1}^2 + x_{n-1}x_n + cx_n^2) = q^{2m-1} - q^m + q^{m-1}.$$

So the two quadratic forms for even n in Theorem 7.20 are inequivalent.

Proof. Induct on m, using Example 7.22 and Lemma 7.23. $\square$

Table 3 compares quadratic forms in different characteristics. In the table QF means quadratic form, SBF and ABF refer to symmetric/alternating bilinear forms, and $\mathbf{F}$ is a finite field.

Characteristic not 2	Characteristic 2
Bijection QF to SBF	Surjection QF to ABF
$Q(v) = [v] \cdot M[v]$, M symm.	$Q(v) = [v] \cdot N[v]$, N upper-tri.
$B(v,w) = [v] \cdot M[w]$	$B(v,w) = [v] \cdot (N + N^\top)[w]$
$B(v,v) = Q(v)$	$B(v,v) = 0$
$B(v,w) = 0 \Leftrightarrow Q(v+w) = Q(v) + Q(w)$	Same
Q nondeg. 2-d w/ null vec. $\Rightarrow Q \sim xy$	Same
Two nondeg. in each dim. over $\mathbf{F}$	Same in even dim., one in each odd dim.

Table 3. Quadratic Form Comparisons

An alternate approach to the inequivalence of the two quadratic forms over $\mathbf{F}$ in each even dimension can be based on a characteristic 2 substitute for the discriminant: the Arf invariant. This can be defined fairly (but not completely!) generally, not just over finite fields. Let F have characteristic 2 and let Q be a quadratic form over F whose *bilinear form B is non-degenerate.* (This is only a special case of non-degenerate Q, but when F is finite it is exactly the case of non-degenerate even-dimensional quadratic forms, which is the application we have in mind anyway.) When Q is expressed as in (7.7), the *Arf* *invariant* of Q is defined to be the class of the sum $\sum_{i=1}^{m} a_i b_i$ in the additive group $F/\wp(F)$. Equivalently, if $n = 2m$ and $\{e_1, f_1, \ldots, e_m, f_m\}$ is a symplectic basis of V then the Arf invariant of Q is

$$\sum_{i=1}^{m} Q(e_i)Q(f_i) \bmod \wp(F). \tag{7.11}$$

The quadratic form $x^2 + xy + cy^2$ has Arf invariant c.

The Arf invariant is an invariant: changing the symplectic basis changes (7.11) by an element of $\wp(F)$. See [4] or [10, pp. 340–341] for a proof. In particular, equivalent quadratic forms having non-degenerate bilinear forms have the same Arf invariant.

The classification of non-degenerate quadratic forms over finite fields with characteristic 2 extends to perfect fields. Lemmas 7.14, 7.16, and 7.17 work for perfect fields. Over any perfect field F of characteristic 2, there is one equivalence class of non-degenerate quadratic forms in each odd dimension and $\#(F/\wp(F))$ equivalence classes in each even dimension (distinguished by the Arf invariant).

We end our discussion of quadratic forms in characteristic 2 with the terminology of quadratic spaces.

Definition 7.25. A *quadratic space* in characteristic 2 is a vector space over a field of characteristic 2 equipped with a choice of quadratic form on it.

If (V, Q) is a quadratic space in characteristic 2 then it provides us with an alternating bilinear space (V, B), where $B(v, w) = Q(v + w) - Q(v) - Q(w)$. This correspondence from quadratic spaces to alternating bilinear spaces in characteristic 2 is surjective but not injective. That is, a quadratic space has more structure than an alternating bilinear space in characteristic 2.

Definition 7.26. A *hyperbolic plane* in characteristic 2 is a two-dimensional quadratic space in characteristic 2 where the quadratic form looks like xy in some basis.

Example 7.27. Let $V = F^2$, $Q_1(x, y) = x^2 + xy$, and $Q_2(x, y) = x^2 + xy + cy^2$ where $c \in F - \wp(F)$. Both Q_1 and Q_2 have the same (non-degenerate) bilinear form $B(v, w) = v \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) w$, but (V, Q_1) is a hyperbolic plane while (V, Q_2) is *not*. Thus a hyperbolic plane in the sense of quadratic spaces in characteristic 2 is stronger than in the sense of alternating bilinear spaces in characteristic 2 (Exercise 3.4).

Theorem 7.28. *Let (V, Q) be a two-dimensional quadratic space. The following conditions are equivalent:*

1. *(V, Q) is a hyperbolic plane,*
2. *Q is non-degenerate and has a null vector.*

Proof. This proof will be different from that of the analogous Theorem 6.16.

Clearly the first condition implies the second. Now we show the converse. Let v be a null vector for Q and let B be the bilinear form associated to Q. By Theorem 7.13 there is a null vector w such that $B(v, w) = 1$. Using the basis $\{v, w\}$,

$$Q(xv + yw) = Q(xv) + Q(yw) + B(xv, yw) = xyB(v, w) = xy.$$

□

Definition 7.29. Let F have characteristic 2 and (V_1, Q_1) and (V_2, Q_2) be quadratic spaces over F. Their *orthogonal direct sum* $V_1 \perp V_2$ is the vector space $V_1 \oplus V_2$ with the quadratic form $Q(v_1, v_2) = Q_1(v_1) + Q_2(v_2)$. The quadratic spaces (V_i, Q_i) are called *isomorphic* if there is a linear isomorphism $A\colon V_1 \to V_2$ such that $Q_2(Av) = Q_1(v)$ for all $v \in V_1$.

We used orthogonal direct sums already in Lemma 7.23. All hyperbolic planes over F are isomorphic. We denote a hyperbolic plane over F as $\mathbf{H}$ or $\mathbf{H}(F)$.

Theorem 7.20 says every non-degenerate quadratic space over a finite field of characteristic 2 is isomorphic to $\mathbf{H}^{\perp m} \perp W$ where $\dim W \leq 2$. This matches the situation in odd characteristic, except when $\dim W = 1$ there are two choices for W in odd characteristic but only one choice in characteristic 2.

For further discussion of quadratic forms in characteristic 2, see the last chapters of [5]. Other references are [7], [8], [9], and [10].

Exercises.

1. When F has characteristic 2, decide if the following quadratic forms are non-degenerate:
   (1) $Q(x, y, z) = ax^2 + xy + by^2 + cz^2$ on F^3 with $c \neq 0$,
   (2) $Q(x, y, z, t) = xy + yz + zt$ on F^4,
   (3) $\det\colon \mathrm{M}_2(F) \to F$,
   (4) $Q(L) = \mathrm{Tr}(L^2)$ on $\mathrm{Hom}_F(V, V)$ for finite-dimensional V.
2. If $c \in \wp(F)$, show by an explicit linear change of variables that $x^2 + xy + cy^2$ is equivalent to xy.
3. Redo Exercise 6.11 when F has characteristic 2, but show the quadratic form $\mathrm{N}_{K/F}$ is non-degenerate if and only if K/F is separable. When $F = \mathbf{F}$ is finite show $\mathrm{N}_{K/\mathbf{F}}$ looks like $x^2 + cxy + y^2$ in some basis, where $T^2 + cT + 1$ is irreducible over $\mathbf{F}$. Is this true for finite fields of odd characteristic?
4. Let V be n-dimensional over a field F of characteristic 2. Let B be an alternating bilinear form on V and $\{e_1, \ldots, e_n\}$ be a basis of V. For any $a_1, \ldots, a_n$ in F, show there is a unique quadratic form Q on V such that $Q(e_i) = a_i$ for all i and the bilinear form associated to Q is B.
5. When F has characteristic 2 and Q is a quadratic form on F^n, let N be a matrix representing Q in the standard basis: $Q(v) = v \cdot Nv$ for $v \in F^n$. Show a matrix represents Q in the standard basis if and only if it has the form $N + A$ where A is an alternating matrix.
6. Let F have characteristic 2. Show explicitly that if $ax^2 + xy + by^2$ and $a'x^2 + xy + b'y^2$ are equivalent then $ab \equiv a'b' \bmod \wp(F)$. Do not assume F is perfect. Is the converse true for all F?
7. Let n be a positive even integer and $\mathbf{F}$ be a finite field with characteristic 2. For a non-degenerate n-dimensional quadratic form Q over $\mathbf{F}$, its Arf invariant (7.11) is one of the two classes in $\mathbf{F}/\wp(\mathbf{F})$. Set $n_+(Q) = \#\{v \in V : Q(v) \in \wp(\mathbf{F})\}$ and $n_-(Q) = \#\{v \in V : Q(v) \notin \wp(\mathbf{F})\}$. Use Theorem 7.24 to show these numbers equal $q^n(q^n \pm 1)/2$, with $n_+(Q) > n_-(Q)$ when Q has Arf invariant $\wp(\mathbf{F})$ and $n_-(Q) > n_+(Q)$ when Q has Arf invariant $\neq \wp(\mathbf{F})$. Therefore the Arf invariant of Q is the class of $\mathbf{F}/\wp(\mathbf{F})$ where Q takes the majority of its values. (Topologists call this "Browder's democracy" [1, Prop. III.1.18].)
8. Here is a "proof" that $\dim_F(V^\perp) \leq 1$ for a non-degenerate Q over any field F of characteristic 2. By the definition of non-degeneracy, $Q\colon V^\perp \to F$ is injective, so

$\dim_F(V^\perp)$ equals the F-dimension of its image. An injective map in linear algebra does not increase dimensions, so $\dim_F(V^\perp) \leq \dim_F F = 1$. Where is the error?

8. Bilinear forms and tensor products

At the end of Section 1 we saw that a bilinear form B on a vector space V can be thought of in two ways as a linear map $V \to V^\vee$, namely L_B and R_B. For finite-dimensional V we saw in Section 2 that the matrix of B in a basis of V is also the matrix of R_B (using the same basis of V and its dual basis in $V^\vee$), while the matrix for L_B is the transpose of that for R_B since L_B and R_B are dual to each other (Theorem 1.21). Having the matrix for B match that of R_B rather than L_B is entirely an accident of the *convention* that we write general bilinear forms on F^n in terms of the dot product on F^n as $v \cdot Aw$ rather than as $Av \cdot w$ for varying matrices $A \in \mathrm{M}_n(F)$. A purist might ask if there is a way to think about a bilinear form as a linear map without taking preference for R_B over L_B or *vice versa*. Absolutely, using tensor products.

The tensor product construction turns bilinear maps into linear maps. If we have a bilinear form $B : V \times V \to F$, we obtain for free a linear map $T_B \colon V \otimes_F V \to F$ characterized by its value on simple tensors: $v \otimes w \mapsto B(v, w)$. The converse holds as well: any linear map $T \colon V \otimes_F V \to F$ can be considered as a bilinear form on V by composing it with the standard bilinear map $V \times V \to V \otimes_F V$ that is part of the ingredients defining the tensor product of vector spaces. Whereas L_B and R_B both map V to $V^\vee$, T_B maps $V \otimes_F V$ to F. Linear maps to F means dual space, so the space $\mathrm{Bil}(V)$ of all bilinear forms on V is naturally identifiable with $(V \otimes_F V)^\vee$, which is naturally isomorphic to $V^\vee \otimes_F V^\vee = (V^\vee)^{\otimes 2}$ using $(\varphi \otimes \psi)(v \otimes w) = \varphi(v)\psi(w)$. Thus the bilinear forms on V "are" the elements of $(V^\vee)^{\otimes 2}$.

One new thing we can do with bilinear forms in the tensor product language is multiply them in a natural way. This is worked out in Exercise 8.1. Recall that if we think about bilinear forms on V as linear maps $V \to V^\vee$ it makes no sense to compose such maps, so multiplication of bilinear forms was a meaningless concept before.

Another advantage to tensor products is its use in extending a bilinear form to a larger scalar field. First we describe this construction without tensor products. When we write a bilinear form as a matrix, so it becomes a bilinear form on F^n, we can view it as a bilinear form over a larger field $K \supset F$ by having the same matrix act as a bilinear form on K^n. (Why do this? Well, one might want to study a real bilinear form over the complex numbers.) If we use a different basis the bilinear form becomes a different matrix, and thus a different bilinear form on K^n. This second bilinear form on K^n is equivalent to the bilinear form on K^n from the first matrix, so this operation passing from bilinear forms over F to bilinear forms over K is well-defined if the result is considered as a bilinear form on K^n up to equivalence. Clearly it would be nicer if we had a coordinate-free way to pass from a bilinear form over F to a bilinear form over K and not something defined only up to equivalence. Using tensor products as a device to extend scalars, we can achieve this. If $B \colon V \times V \to F$ is bilinear and K/F is a field extension, then we obtain a bilinear form B^K on $K \otimes_F V$ by

$$B^K(\alpha \otimes v, \beta \otimes w) = \alpha\beta B(v, w).$$

That this formula yields a well-defined bilinear form B^K on $K \otimes_F V$ comes from the way one constructs maps out of tensor products, and is left to the reader.[8] Using an F-basis

[8] There is not a canonical construction of the tensor product, and different constructions will produce only equivalent bilinear forms over K, so strictly speaking we haven't really removed the "up to equivalence"

for V as a K-basis for $K \otimes_F V$, the matrix associated to B^K is the same as the matrix associated to B, so we recover the previous matrix-based construction.

In a similar way, a quadratic form $Q\colon V \to F$ can be extended to a quadratic form $Q^K\colon K \otimes_F V \to K$, where

$$Q^K(\alpha \otimes v) = \alpha^2 Q(v).$$

The bilinear form associated to Q^K is the extension to K of the bilinear form associated to Q. In concrete language, all we are doing here is writing a homogeneous quadratic polynomial with coefficients in F as a polynomial with its coefficients viewed in K. But the tensor language makes the construction coordinate-free.

Returning to the issue of L_B versus R_B, we can consider the choice that is always available between them by thinking about a general bilinear map $V \times W \to U$ where V, W, and U are any F-vector spaces. Such a bilinear map corresponds to a linear map $V \otimes_F W \to U$, and there are natural isomorphisms

$$\mathrm{Hom}_F(V \otimes_F W, U) \cong \mathrm{Hom}_F(V, \mathrm{Hom}_F(W, U)),$$

$$\mathrm{Hom}_F(V \otimes_F W, U) \cong \mathrm{Hom}_F(W, \mathrm{Hom}_F(V, U)).$$

The first isomorphism turns $f \in \mathrm{Hom}_F(V \otimes_F W, U)$ into $v \mapsto [w \mapsto f(v \otimes w)]$ and the second isomorphism turns f into $w \mapsto [v \mapsto f(v \otimes w)]$. In the special case $V = W$ and $U = F$ these becomes the two different isomorphisms of $(V \otimes_F V)^\vee$ with $\mathrm{Hom}_F(V, V^\vee)$ by $B \mapsto L_B$ and $B \mapsto R_B$. In the most general setting, though, we see L_B and R_B are analogues of linear maps between different spaces.

The two special classes of bilinear forms, symmetric and alternating, can be described in the language of symmetric and exterior squares. Viewing a bilinear form as a linear map $V \otimes_F V \to F$, it is symmetric when it kills all tensors of the form $v \otimes w - w \otimes v$ and it is alternating when it kills all tensors of the form $v \otimes v$. Therefore a symmetric bilinear form B is the same thing as a linear map $\mathrm{Sym}^2(V) \to F$ sending $v \cdot w$ to $B(v, w)$, where $\cdot$ is the symmetric product in $\mathrm{Sym}^2(V)$ (not the dot product, which only makes sense on vectors in F^n anyway). An alternating bilinear form B is the same thing as a linear map $\Lambda^2(V) \to F$ sending $v \wedge w$ to $B(v, w)$. Again, linear maps to F form the dual space, so symmetric bilinear forms on V are the elements of $\mathrm{Sym}^2(V)^\vee$ and alternating bilinear forms on V are the elements of $\Lambda^2(V)^\vee$. We can identify $\mathrm{Sym}^2(V)^\vee$ with $\mathrm{Sym}^2(V^\vee)$ and $\Lambda^2(V)^\vee$ with $\Lambda^2(V^\vee)$.

While $\mathrm{Sym}^2(V)$ and $\Lambda^2(V)$ are properly defined as quotient spaces of $V^{\otimes 2}$, outside of characteristic 2 we can identify these with subspaces of $V^{\otimes 2}$, using $v \otimes w + w \otimes v$ in place of $v \cdot w \in \mathrm{Sym}^2(V)$ and $v \otimes w - w \otimes v$ in place of $v \wedge w \in \Lambda^2(V)$. Using these identifications, the formula $v \otimes w = \frac{1}{2}(v \otimes w + w \otimes v) + \frac{1}{2}(v \otimes w - w \otimes v)$ on simple tensors shows $V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \Lambda^2(V)$. Replacing V with $V^\vee$, we get

$$(V^\vee)^{\otimes 2} = \mathrm{Sym}^2(V^\vee) \oplus \Lambda^2(V^\vee), \tag{8.1}$$

outside of characteristic 2, which is the coordinate-free expression of a general bilinear form as a unique sum of a symmetric and skew-symmetric bilinear form (Theorem 1.7).

Remark 8.1. There is a "flip" automorphism on $(V^\vee)^{\otimes 2} = V^\vee \otimes_F V^\vee$ determined by $\varphi \otimes \psi \mapsto \psi \otimes \varphi$, which has order 2. When F does not have characteristic 2, $V^\vee \otimes_F$

aspect of the construction by comparison to the matrix viewpoint. But at least the tensor construction is more elegant, and is coordinate-free.

$V^\vee$ decomposes into the ± 1-eigenspaces for the flip automorphism, and this eigenspace decomposition is (8.1).

Exercises.

1. If (V_1, B_1) and (V_2, B_2) are bilinear spaces, show $V_1 \otimes_F V_2$ is a bilinear space using $(B_1 \otimes B_2)(v_1 \otimes v_2, v_1' \otimes v_2') := B_1(v_1, v_1')B_2(v_2, v_2')$. (The proof that $B_1 \otimes B_2$ is well-defined can be simplified using Exercise 1.5.) This can be considered a multiplication for bilinear forms. If B_1 and B_2 are both symmetric, both alternating, or both skew-symmetric, does $B_1 \otimes B_2$ inherit the property?
2. Viewing bilinear forms on V as elements of $(V^\vee)^{\otimes 2}$, we can use B_1 and B_2 in the first exercise to form the simple tensor $B_1 \otimes B_2$ in $(V_1^\vee)^{\otimes 2} \otimes_F (V_2^\vee)^{\otimes 2}$, a vector space which is naturally isomorphic to $(V_1^\vee \otimes_F V_2^\vee)^{\otimes 2}$. If we further identify $V_1^\vee \otimes_F V_2^\vee$ with $(V_1 \otimes_F V_2)^\vee$, show that the simple tensor $B_1 \otimes B_2$ in $(V_1^\vee)^{\otimes 2} \otimes_F (V_2^\vee)^{\otimes 2}$ gets identified with the function $B_1 \otimes B_2$ on $(V_1 \otimes_F V_2)^{\otimes 2}$ in the previous exercise.
3. For bilinear spaces V_1 and V_2, describe the discriminant of $V_1 \otimes_F V_2$ in terms of the discriminants of V_1 and V_2. Conclude that $V_1 \otimes_F V_2$ is non-degenerate if and only if V_1 and V_2 are non-degenerate.
4. For quadratic spaces (V_1, Q_1) and (V_2, Q_2), show $V_1 \otimes_F V_2$ becomes a quadratic space using $(Q_1 \otimes Q_2)(v_1 \otimes v_2) = Q_1(v_1)Q_2(v_2)$. If B_1 and B_2 are the bilinear forms associated to Q_1 and Q_2 respectively, show the bilinear form associated to $Q_1 \otimes Q_2$ is $B_1 \otimes B_2$ from the first exercise. Allow fields of characteristic 2.
5. Let (V_1, Q_1) and (V_2, Q_2) be non-degenerate quadratic spaces over a common field not of characteristic 2. Express the quadratic forms relative to orthogonal bases as $Q_1 = \sum a_i x_i^2$ and $Q_2 = \sum b_j y_j^2$. Show the quadratic form $Q_1 \otimes Q_2$ has a diagonalization $\sum_{i,j} a_i b_j z_{ij}^2$.
6. (Continuation of Exercise 6.10) Let $<$ be an ordering on a field F. When Q is a non-degenerate quadratic form over F with signature (p, q) relative to $<$, define $\mathrm{sign}_<(Q) = p - q \in \mathbf{Z}$. For non-degenerate quadratic forms Q and Q' over F, show $\mathrm{sign}_<(Q \perp Q') = \mathrm{sign}_<(Q) + \mathrm{sign}_<(Q')$ and $\mathrm{sign}_<(Q \otimes Q') = \mathrm{sign}_<(Q)\,\mathrm{sign}_<(Q')$. (The behavior of $\mathrm{sign}_<$ under $\otimes$ explains why taking the difference in the order $p-q$ is more natural than in the order $q-p$; it would not be multiplicative in the other order.)

References

[1] W. Browder, "Surgery on Simply-Connected Manifolds," Springer-Verlag, Berlin, 1972.

[2] C. Chevalley, "The Algebraic Theory of Spinors," Columbia Univ. Press, New York, 1954.

[3] J. Dieudonne, "La Géometrie des Groupes Classiques," Springer-Verlag, Berlin, 1963.

[4] R. H. Dye, *On the Arf Invariant*, J. Algebra **53** (1978), 36–39.

[5] L. C. Grove, "Classical Groups and Geometric Algebra," Amer. Math. Society, Providence, 2002.

[6] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1990.

[7] I. Kaplansky, "Linear Algebra and Geometry: A Second Course," Allyn & Bacon, Boston, 1969

[8] M-A. Knus, A. Merkurjev, M. Rost, J-P. Tignol, "The Book of Involutions," Amer. Math. Soc., Providence, 1998.

[9] A. Pfister, "Quadratic Forms with Applications to Algebraic Geometry and Topology," Cambridge Univ. Press, Cambridge, 1995.

[10] W. Scharlau, "Quadratic and Hermitian Forms," Springer-Verlag, Berlin, 1985.

[11] W. Scharlau, *On the History of the Algebraic Theory of Quadratic Forms*, pp. 229–259 in: "Quadratic Forms and Their Applications," E. Bayer-Fluckiger, D. Lewis, A. Ranicki eds., Amer. Math. Soc., Providence, 2000.

[12] D. Shapiro, "Compositions of Quadratic Forms," de Gruyter, Berlin, 2000.