II.D. Quadratic forms and orthogonal groups

We continue to take V an n-dimensional vector space over a field $\mathbb{F}$ of characteristic different from 2, with basis $\{e_i\}$. A *form* of degree 1 is just an element of $V^\vee$. For higher degree, we need the notion of symmetric powers of a vector space W. Though this is a bit off-topic, it is important enough to explain properly and clarifies the definition of quadratic forms.

First, tensor powers: we have already defined $W \otimes W$, and one extends this by induction to $W^{\otimes k} := W \otimes W^{\otimes k-1}$ (also written $T^k W$). Now, this carries two obvious actions of $\mathfrak{S}_k$, by $\sigma.(a_1 \otimes \cdots \otimes a_k) := a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(k)}$ or $\mathrm{sgn}(\sigma) a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(k)}$. The invariant subspaces in $W^{\otimes k}$ of these actions are the *symmetric k-tensors* $\mathrm{Sym}^k(W)$ and the *alternating k-tensors* $\mathrm{Alt}^k(W)$, respectively.

A related construction is to take the entire *tensor algebra* $TW := \oplus_{k \geq 0} W^{\otimes k}$ and divide out by the ideal generated by elements $x \otimes y - y \otimes x$ or $x \otimes y + y \otimes x$, yielding the *symmetric algebra* $SW = \oplus_{k \geq 0} S^k W$ and the *exterior algebra* $\bigwedge W = \oplus_{k \geq 0} \bigwedge^k W$. We already saw an explicit description of the latter in [**Algebra I**, V.A.12]; similarly, SW is nothing but the space of polynomials in a basis of W, with $S^k W$ the polynomials which are homogeneous of degree k.

The spaces $S^k W$ and $\bigwedge^k W$ are called the k^{th} *symmetric* resp. *exterior power* of W. Unlike $\mathrm{Sym}^k W$ and $\mathrm{Alt}^k W$, they are *not* subspaces of $V^{\otimes k}$ and so the elements aren't written with "$\otimes$", but rather as (linear combinations of symbols) $w_1 \cdots w_k$ resp. $w_1 \wedge \cdots \wedge w_k$. There are, however, natural maps $\mathrm{Sym}^k(W) \to S^k W$ and $\mathrm{Alt}^k(W) \to \bigwedge^k W$ which are isomorphisms provided $k!$ does not divide $\mathrm{char}(\mathbb{F})$. Moreover, one has in general that $\mathrm{Sym}^k(W) \cong (S^k W^\vee)^\vee$ and $\mathrm{Alt}^k(W) \cong (\bigwedge^k W^\vee)^\vee$.

We saw in [loc. cit.] that $\bigwedge^k W$ has dimension $\binom{n}{k}$ if $\dim W = n$. In the HW, you'll show that $\dim(S^k W) = \binom{n+k-1}{k}$.

II.D.1. Definition. (a) A **form** of degree k on V is an element

$$F \in S^k(V^\vee) \cong (\mathrm{Sym}^k V)^\vee.$$

That is, F is a homogeneous polynomial $\sum_{|I|=k} c_I e_{i_1}^{\vee} \cdots e_{i_k}^{\vee}$ of degree k in the $e_i^{\vee}$'s, where the sum is over multi-indices $I = (i_1, \ldots, i_k)$ with $i_1 \leq \cdots \leq i_k$.

(b) Equivalently, we may regard F as a map from V to $\mathbb{F}$, by applying it to the element $v \otimes \cdots \otimes v \in \mathrm{Sym}^k V$. Explicitly, this gives

$$v = \sum_{i=1}^{n} a_i e_i \quad \longmapsto \quad F(v) := \sum_{|I|=k} c_I a_{i_1} \cdots a_{i_k}.$$

More specifically, a **quadratic form** is a form of degree 2, or equivalently a map $Q \colon V \to \mathbb{F}$ such that

$$\text{(II.D.2)} \qquad \begin{cases} \text{(i) } Q(ax) = a^2 Q(x) \ \ [Q \text{ homogeneous of degree 2}] \\ \text{(ii) } B(x,y) := Q(x+y) - Q(x) - Q(y) \text{ is bilinear.} \end{cases}$$

Let's check the equivalency carefully here: given $Q = \sum_{i \leq j} c_{ij} e_i^{\vee} e_j^{\vee} \in S^2(V^{\vee})$, we clearly have (i); and (ii) follows by computing (with $x = \sum_i x_i e_i$ and $y = \sum_i y_i e_i$)

$$\sum_{i \leq j} c_{ij}(x_i + y_i)(x_j + y_j) - \sum_{i \leq j} c_{ij} x_i x_j - \sum_{i \leq j} y_i y_j = \sum_{i \leq j} c_{ij}(x_i y_j + x_j y_i).$$

For the converse, assuming (i) and (ii), observe that

$$\begin{aligned} Q(ax+by) &= Q(ax) + Q(by) + B(ax, by) \\ &= a^2 Q(x) + b^2 Q(y) + ab B(x,y); \end{aligned}$$

iterating this gives

$$Q(\textstyle\sum_i a_i e_i) = \sum_i a_i^2 Q(e_i) + \sum_{i<j} a_i a_j B(e_i, e_j) = \sum_{i \leq j} c_{ij} a_i a_j$$

where $c_{ii} = Q(e_i)$ and $c_{ij} = B(e_i, e_j)$ $(i < j)$. Clearly this agrees with II.D.1(b).

Symmetric bilinear forms.

Notice one other thing here: that the bilinear form in (II.D.2)(ii) is *symmetric*. So the entries of $[B]_e$ are $(B(e_i, e_j) =)\ c_{ij}$ for $i < j$, c_{ji} for $i > j$, and (for $i = j$) $B(e_i, e_i) = Q(2e_i) - 2Q(e_i) = 4Q(e_i) - 2Q(e_i) = 2c_{ii}$. Since we can recover Q from B (because $\mathrm{char}(\mathbb{F}) \neq 2$), the problems of classifying quadratic forms, studying their isometry groups, etc. can be thought of in terms of B.

So let B be a symmetric bilinear form on V. As usual, the *rank* of B is that of any $[B]_e$, which is independent of the choice of basis since cogredience preserves rank. We have the following analogue of II.C.1:

II.D.3. PROPOSITION. *Writing* $r := \mathrm{rank}(B)$, *there exists a basis* $\varepsilon = \{\varepsilon_1, \ldots, \varepsilon_r; \varepsilon_{r+1}, \ldots, \varepsilon_n\}$ *in which* $[B]_\varepsilon = \mathrm{diag}\{b_1, \ldots, b_r; 0, \ldots, 0\}$, *with* $b_i \in \mathbb{F}^*$.

PROOF. Begin with our arbitrary basis $e_1, \ldots, e_n$. The result is trivial if B is zero, so assume otherwise.

If every $B(e_i, e_i) = 0$, then some $2B(e_i, e_j) = B(e_i + e_j, e_i + e_j) - B(e_i, e_i) - B(e_j, e_j) = B(e_i + e_j, e_i + e_j)$ must be nonzero, and we can perform a slight change of basis to make this $e_i + e_j$ one of our basis elements. After reordering, we may assume that $b_1 := B(e_1, e_1) \neq 0$. Replace each $e_{j>1}$ by $f_j := e_j - B(e_j, e_1)b_1^{-1}e_1$, and note that

$$B(e_1, f_j) = B(e_1, e_j) - B(e_j, e_1)b_1^{-1}B(e_1, e_1) = 0 \quad \Longrightarrow \quad f_j \in \mathbb{F}\langle e_1 \rangle^\perp.$$

At this point we have written V as the direct sum of $U_1 := \mathbb{F}\langle e_1 \rangle$ (with basis $\varepsilon_1 := e_1$) and $U_1^\perp$ (with basis $f_2, \ldots, f_n$).

Inductively assume that we have a k-dimensional subspace $U_k := \mathbb{F}\langle \varepsilon_1, \ldots, \varepsilon_k \rangle$ with $B(\varepsilon_i, \varepsilon_j) = b_i \delta_{ij}$ ($b_i \neq 0$) and $V = U_k \oplus U_k^\perp$. Then either $B|_{U_k^\perp} = 0$ (and any basis of $U_k^\perp$ will do) or the last paragraph provides $\varepsilon_{k+1} \in U_k^\perp$ (with nonzero $b_{k+1} := B(\varepsilon_{k+1}, \varepsilon_{k+1})$) and a decomposition $U_k^\perp = \mathbb{F}\langle \varepsilon_{k+1} \rangle \oplus V_k$, where $V_{k+1} := U_k^\perp \cap \mathbb{F}\langle \varepsilon_{k+1} \rangle^\perp$. Setting $U_{k+1} := U_k \oplus \mathbb{F}\langle \varepsilon_{k+1} \rangle$, we see that $V = U_{k+1} \oplus V_{k+1}$ and $V_{k+1} = U_{k+1}^\perp$, which completes the inductive step. □

In view of II.A.2(ii), we have the immediate

II.D.4. COROLLARY. *Any symmetric matrix in* $M_n(\mathbb{F})$ *is cogredient to a diagonal one.*

When $\mathbb{F}$ is algebraically closed, we can scale each ε_i by $1/\sqrt{b_i}$ to make the new $\{b_i\}$ all 1. This yields

II.D.5. COROLLARY. *If $\mathbb{F} = \bar{\mathbb{F}}$, then two symmetric $n \times n$ matrices are cogredient if and only if they have the same rank.*

This describes the situation over $\mathbb{C}$. When $\mathbb{F} = \mathbb{R}$, it is more interesting:

II.D.6. SYLVESTER'S THEOREM. (a) *Two diagonal matrices in $M_n(\mathbb{R})$ are cogredient* (*via some $S \in \mathrm{GL}_n(\mathbb{R})$*) $\iff$ *the numbers of positive, negative, and zero diagonal entries are the same.*

(b) *Given a symmetric bilinear form B on a real vector space V, let $[B]_\varepsilon$ be as in II.D.3. Define the* ***signature*** *of B* (*and the symmetric matrix $[B]_e$ for any e*) *to be the pair (p, q),*[10] *where p* [*resp. q*] *denotes the number of positive* [*resp. negative*] *$\{b_i\}$. This is well-defined.*

(c) *Two symmetric bilinear forms on V* [*resp. two symmetric matrices in $M_n(\mathbb{R})$*] *are equivalent* [*resp. cogredient*] *if and only if they have the same signature.*

PROOF. The well-definedness claimed in (b) follows from (a), and (c) is immediate from (a) and II.D.3. The "if" in (a) is also clear.

To see the "only if" in (a), recall from II.A.9 that a pair of cogredient (symmetric) matrices may be regarded as the matrices of a single (symmetric) bilinear form B with respect to two bases. So let ε be a basis of the type in II.D.3, with $b_i > 0$ for $1 \leq i \leq p$ and $b_i < 0$ for $p+1 \leq i \leq r = p+q$; and let ε' be another, with invariants p', q', r'. (We can make this assumption on the ordering of the positive and negative entries because permutation matrices satisfy $P^{-1} = {}^tP$ so we can conjugate by them for free.)

Obviously rank does not change under cogredience, so $r = r'$. To see that $p = p'$, observe that $U_1 := \mathbb{R}\langle \varepsilon_1, \ldots, \varepsilon_p \rangle$ and $U_2 := \mathbb{R}\langle \varepsilon'_{p'+1}, \ldots, \varepsilon'_n \rangle$ have dimensions p and $n - p'$. If $z \in U_1 \cap U_2$, then $z = \sum_{i=1}^p a_i \varepsilon_i \implies B(z,z) = \sum_{i=1}^p a_i^2 b_i \geq 0$ with equality iff $z = 0$; while $z = \sum_{j=p'+1}^n a'_j \varepsilon'_j \implies B(z,z) \leq 0$. This forces $z = 0$ hence $U_1 \cap U_2 = \{0\}$, which implies $n \geq p + (n - p')$ thus $p' \geq p$. A symmetric argument gives $p \geq p'$, hence equality. $\square$

[10] Some authors, including [**Jacobson**], consider the signature to be the number $p - q$. What we call signature records both this number and the rank $p + q = r$.

Henceforth we assume that B is nondegenerate, i.e. that $r = n$. We introduce two more properties which are invariant under equivalence:

II.D.7. DEFINITION. A nondegenerate symmetric bilinear form B is called

(i) **isotropic** if $\exists v \in V \backslash \{0\}$ with $B(v, v) = 0$.
(ii) **universal** if $B(v, v) = b$ has a solution for every $b \in \mathbb{F}^*$.

(These definitions also work for Q;[11] one speaks of Q or B "representing 0" when (i) holds, or "representing b" when (ii) holds.) If (i) fails, B [resp. Q] is **anisotropic**.

When might (i) and (ii) be interesting, and help organize equivalence classes of nondegenerate B's? If $\mathbb{F} = \bar{\mathbb{F}}$ they always hold, and if $\mathbb{F} = \mathbb{R}$ they hold precisely when the signature is *indefinite* (p and q both nonzero). So they are no help there. On the other hand, consider the form (or rather matrix) $\mathrm{diag}(1, -b) \in M_2(\mathbb{Q})$ of signature $(1, -1)$ (which makes sense since $\mathbb{Q}$ has one embedding in $\mathbb{R}$). Does this represent 0, i.e. is it isotropic? We are asking for a nontrivial solution to $x^2 - by^2 = 0$! Obviously this exists exactly if b is a square in $\mathbb{Q}$. The question of whether the form represents *nonzero* numbers gives instances of Pell's equation.

My point is that, with $\mathbb{F} = \mathbb{Q}$, there are (many) more equivalence classes, cogredience itself is a bit weird (as you'll see in HW), and the additional "invariants" supplied by this definition help make sense of things. The *Hasse-Minkowski theorem*, which also has generalizations to number fields, says (among other things) that a quadratic form represents 0 over $\mathbb{Q}$ precisely when it represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ (the p-adic rationals) for each p. It has a generalization to number fields and other "global fields" and was historically the first main instance of something called the "local-global principle" ($\mathbb{Q}$ being the "global"; $\mathbb{R}$ and $\mathbb{Q}_p$ the "local").

[11] though for the two versions to be the same, one should use $2Q$, since $B(v, v) = 2Q(v)$.

But this is a very deep result, and instead we'll content ourselves with something simple, namely a classification result in the finite field case.

II.D.8. LEMMA. *B isotropic $\implies$ B universal.*

PROOF. We have $v \in V\backslash\{0\}$ with $B(v,v) = 0$. Let $b \in \mathbb{F}^*$ be given. Since B is nondegenerate, there is a $u \in V$ with $B(u,v) = \frac{1}{2}$. Taking $w := av + u$, we have $B(w,w) = a + B(u,u)$; and then choosing $a := b - B(u,u)$ gives $B(w,w) = b$. □

II.D.9. LEMMA. *If $|\mathbb{F}| < \infty$ and $n \geq 2$, then any (nondegenerate) B is universal.*

PROOF. By passing to a subspace, it suffices to prove this for $n = 2$; and we may assume B anisotropic (otherwise we're done by II.D.8). Using II.D.3, we have $[B]_\varepsilon = \mathrm{diag}(a,b)$ with $ab \neq 0$ and $ax^2 + by^2 = 0$ insoluble in $\mathbb{F} \times \mathbb{F}\backslash\{(0,0)\}$; the claim is that, for any $c \in \mathbb{F}^*$, we can solve $ax^2 + by^2 = c$.

Clearly we can assume $a = 1$ (otherwise divide both equations by a). So the insolubility of $x^2 + by^2 = 0$ says that $\mathbb{E} := \mathbb{F}(\sqrt{-b})/\mathbb{F}$ is a nontrivial field extension. The other equation is then Pell's equation for finite fields: $N_{\mathbb{E}/\mathbb{F}}(x + \sqrt{-b}y) = c$. Writing $q := |\mathbb{F}|$, we have $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \{1, \varphi\}$ where $\varphi(u) := u^q$. So $N_{\mathbb{E}/\mathbb{F}}(u) = u \cdot u^q = u^{q+1}$. Since $\mathbb{E}^*$ is a cyclic group of order $q^2 - 1$, we should think of $N_{\mathbb{E}/\mathbb{F}}$ as multiplication by $q+1$ in $\mathbb{Z}_{q^2-1}$, whence $|\ker(N_{\mathbb{E}/\mathbb{F}})| = q+1$ and $|\mathrm{im}(N_{\mathbb{E}/\mathbb{F}})| = q - 1 = |\mathbb{F}^*|$. So the norm surjects onto $\mathbb{F}^*$ and we are done. □

II.D.10. THEOREM. *Assume $|\mathbb{F}| < \infty$. Then two nondegenerate symmetric bilinear forms on V [resp. two symmetric matrices in $M_n(\mathbb{F})$] are equivalent [resp. cogredient] if and only if their discriminants [resp. determinants] are equal in $\mathbb{F}^*/(\mathbb{F}^*)^2$.*

PROOF. It will suffice to show (a) that any such B has a matrix of the form $\mathrm{diag}(1, \ldots, 1, \Delta)$, and (b) that two such matrices are cogredient iff the ratio of Δ's is a square.

(a) In the proof of II.D.3, $B|_{U_k^\perp}$ is universal for $0 \leq k < n-1$ by II.D.9. So we can choose $\varepsilon_{k+1} \in U_k^\perp$ so that $b_{k+1} = B(\varepsilon_{k+1}, \varepsilon_{k+1}) = 1$, until we reach ε_n (since $\dim(U_{n-1}^\perp) = 1$, II.D.9 doesn't apply).

(b) If $B \sim B'$, then $\Delta/\Delta' \in (\mathbb{F}^*)^2$ by II.A.2(iii). Conversely, if $\Delta' = \alpha^2\Delta$, the matrices are cogredient by $S = \text{diag}(1, \ldots, 1, \alpha)$. □

Orthogonal groups.

In parallel with the alternating case, we make the following

II.D.11. DEFINITION. (i) Let V be an $\mathbb{F}$-vector space of dimension n, and B a *nondegenerate* symmetric bilinear form. Then (V, B) is called an **orthogonal vector space**, and B an **orthogonal form**.

(ii) The group of (self-)isometries of (V, B),

$$\text{O}(V, B) := \{T \in \text{Aut}_{\mathbb{F}}(V) \mid B(Tx, Ty) = B(x, y) \ (\forall x, y \in V)\},$$

is called an **orthogonal group**.

(iii) A basis ε in which $[B]_\varepsilon$ is diagonal is called an **orthogonal basis** for (V, B).

In (ii), I didn't write "$\text{O}_n(\mathbb{F})$" in analogy with $\text{Sp}_n(\mathbb{F})$, because the isomorphism class of the group depends on the equivalence class of the orthogonal form, and there may be lots of these depending on $\mathbb{F}$.

You will recall from §II.C that, regardless of the field, there is only one equivalence class of symplectic form in each (even) dimension. For orthogonal forms, we know that this is at least true for algebraically closed fields; so it makes sense to write $\text{O}_n(\mathbb{C})$. For $\mathbb{F} = \mathbb{R}$, we know that the classes are parametrized by the signature $(p, q) = (p, n-p)$ of B; and so while "$\text{O}_n(\mathbb{R})$" would be ambiguous, $\text{O}(p, q)$ ($\cong \text{O}(q, p)$) is well-defined. These orthogonal groups are called **indefinite** if $p, q > 0$, and **definite** in the remaining case $\text{O}(n, 0) \cong \text{O}(0, n) =: \text{O}(n)$.

The role of transvections in this setting is played by the **orthogonal reflections**

$$\rho_u(x) := x - 2\frac{B(x, u)}{B(u, u)}u$$

in the hyperplane $\mathbb{F}\langle u\rangle^{\perp}$. Indeed, applying this twice gives

$$\rho_u\left(x-2\tfrac{B(x,u)}{B(u,u)}u\right)=x-2\tfrac{B(x,u)}{B(u,u)}u-2\frac{B(x,u)-\frac{2B(x,u)}{B(u,u)}B(u,u)}{B(u,u)}u=x,$$

and they fix vectors orthogonal to u. You should check that they are orthogonal. The following result is proved in [**Jacobson**]:

II.D.12. THEOREM. $\mathrm{O}(V,B)$ *is generated by orthogonal reflections.*

Since reflections have determinant -1, it is *not* true that all orthogonal transformations have determinant 1. Rather, there is a normal subgroup of index 2, the **special orthogonal group** $\mathrm{SO}(V,B)$, obtained by intersecting $\mathrm{O}(V,B)$ with $\mathrm{SL}_n(\mathbb{F})$.

However, II.D.12 still does yield that the center of $\mathrm{O}(V,B)$ is $\{\pm\mathbf{1}\}$, and that the quotient of $D(\mathrm{O}(V,B))$ by its center ($\{\mathbf{1}\}$ or $\{\pm\mathbf{1}\}$) is simple (assuming $|\mathbb{F}|>3$, $n\geq 3$, and B isotropic). But the proof is more complicated and we refer to [op. cit.]. For $\mathbb{F}=\mathbb{C}$, the derived group $D(\mathrm{O}(V,B))$ is just $\mathrm{SO}_n(\mathbb{C})$.