

14.4 Completing the Square

Every symmetric matrix over $\mathbb{R}$ can be diagonalized by an orthogonal matrix, which is Chapter 12's spectral theorem. That theorem needs $\mathbb{R}$, an inner product, and the existence of eigenvalues. This section proves a weaker conclusion under far weaker hypotheses: over **any** field of characteristic $\neq 2$, with no inner product, no order, and no eigenvalues available, every symmetric form still becomes diagonal after a change of basis — provided we ask only for congruence, not for similarity. The proof is one algebraic manipulation, completing the square, run by induction; and the induction has a case that a careless proof loses.

Throughout, F is a field with $\text{char } F \neq 2$ (Definition 0.7.2), V is a finite-dimensional vector space over F , β is a **symmetric** bilinear form on V (Definition 14.3.1), and $q(v) = \beta(v, v)$ is its quadratic form (Definition 14.3.2).

14.4.1 Orthogonality without an inner product

Chapter 11 called two vectors orthogonal when their inner product vanished. The word survives the loss of positivity unchanged, because only the vanishing was ever used.

Definition 14.4.1. Orthogonal Basis for a Form

Let β be a bilinear form on V . Vectors $u, v \in V$ are **orthogonal with respect to β** if $\beta(u, v) = 0$. An ordered basis $\mathcal{B} = (v_1, \dots, v_n)$ of V is an **orthogonal basis for β** if

$$\beta(v_i, v_j) = 0 \quad \text{whenever } i \neq j.$$

The definition is engineered to say exactly one thing about matrices: by Definition 14.1.2, $\mathcal{B}$ is an orthogonal basis for β precisely when $[\beta]_{\mathcal{B}}^{\mathcal{B}}$ is a **diagonal** matrix, with $q(v_1), \dots, q(v_n)$ down the diagonal. Two warnings come free. The vectors of such a basis are not required to satisfy $q(v_i) = 1$, and over a general field they usually cannot be rescaled to. And a vector may be orthogonal to itself: $q(v_i) = 0$ is allowed, and for a degenerate form it is unavoidable.

What an orthogonal basis buys is that q becomes a sum of squares with no cross terms. If $v = c_1 v_1 + \dots + c_n v_n$ and $d_i = q(v_i)$, then expanding by bilinearity and deleting the $i \neq j$ terms,

$$q(v) = \sum_{i=1}^n d_i c_i^2. \quad (14.4.1)$$

That is the “sum of squares” a reader has met when completing the square in two variables, and [Eq. 14.4.1](#) is the reason the whole section is called what it is.

14.4.2 The theorem, and the case that breaks it

Here is the naive argument, and it is worth seeing it fail. To make $q(\mathbf{v}) = ax_1^2 + 2bx_1x_2 + cx_2^2$ into a sum of squares, write

$$q = a\left(x_1 + \frac{b}{a}x_2\right)^2 + \left(c - \frac{b^2}{a}\right)x_2^2,$$

which is exactly a change of variable. The step divides by $a = q(\mathbf{e}_1)$. If $a = 0$ there is nothing to complete, and one may hope to start with x_2 instead — but $q(\mathbf{x}) = 2x_1x_2$ has $q(\mathbf{e}_1) = q(\mathbf{e}_2) = 0$,

and neither variable offers a foothold. The repair is to change the vector, not the variable: $q(\mathbf{e}_1 + \mathbf{e}_2) = 2 \neq 0$. That repair is a lemma, and it is where $\text{char } F \neq 2$ is spent.

Lemma 14.4.1. A Non-Zero Form Is Non-Zero Somewhere on the Diagonal

Let $\text{char } F \neq 2$ and let β be a symmetric bilinear form on V with $\beta \neq 0$. Then there exists $v \in V$ with $q(v) \neq 0$.

Proof. Since $\beta \neq 0$, there are $u, w \in V$ with $a = \beta(u, w) \neq 0$. If $q(u) \neq 0$ or $q(w) \neq 0$ we are done. So suppose $q(u) = q(w) = 0$. Expanding by bilinearity and using symmetry,

$$q(u + w) = q(u) + 2\beta(u, w) + q(w) = (1 + 1)a.$$

Since $\text{char } F \neq 2$, the element $1 + 1$ is nonzero, and a product of two nonzero elements of a field is nonzero, so $q(u + w) \neq 0$. This proves the lemma. ■

Contrapositively: if q vanishes identically then $\beta = 0$. That is the case the induction must handle separately, and the lemma is what lets it be handled in one line.

Theorem 14.4.2. Diagonalization of a Symmetric Form

Let F be a field with $\text{char } F \neq 2$, let V be a finite-dimensional vector space over F , and let β be a symmetric bilinear form on V . Then V has an orthogonal basis for β .

Equivalently: every symmetric $\mathbf{A} \in M_n(F)$ is congruent to a diagonal matrix, that is, there is an invertible $\mathbf{P} \in M_n(F)$ with $\mathbf{P}^\top \mathbf{A} \mathbf{P}$ diagonal.

Idea. Induction on $\dim V$. The step wants to peel off one basis vector and recurse on a complement, exactly as “peel off an eigenvector” does in Chapter 9 — but the complement here is the set of vectors orthogonal to the chosen one, not an invariant subspace, and it is available only if the chosen v_1 has $q(v_1) \neq 0$. So the proof splits into two steps: ① if q vanishes everywhere, the form is zero and **every** basis is orthogonal; ② otherwise [Lemma 14.4.1](#) supplies a v_1 with $q(v_1) \neq 0$, the linear functional $w \mapsto \beta(v_1, w)$ is nonzero, its kernel W is a hyperplane meeting $\text{span}(v_1)$ trivially, and the induction hypothesis applies to β restricted to W . Step ① is not a formality: without it the argument has no base for the recursion when the form degenerates, and the word “equivalently” in the statement would be unearned.

Proof. We induct on $n = \dim V$. If $n = 0$ the empty basis is orthogonal, vacuously; if $n = 1$ any basis (v_1) is orthogonal, since there is no pair $i \neq j$. Let $n \geq 2$ and suppose the result holds for all spaces of dimension $n - 1$ over F .

Step 1: the form vanishes on the diagonal. Suppose $q(v) = 0$ for every $v \in V$. By [Lemma 14.4.1](#), read contrapositively, $\beta = 0$. Then $\beta(v_i, v_j) = 0$ for every pair of vectors whatsoever, so **any** basis of V is an orthogonal basis for β , and its matrix is $\mathbf{O}$, which is diagonal.

Step 2: the form does not vanish on the diagonal. Otherwise there is $v_1 \in V$ with $c = q(v_1) \neq 0$; in particular $v_1 \neq 0$. Define

$$\varphi: V \rightarrow F, \quad \varphi(w) = \beta(v_1, w).$$

Then φ is linear, because β is linear in its second argument, and $\varphi(v_1) = c \neq 0$, so $\varphi \neq 0$. A nonzero functional is surjective onto F (Proposition 5.1.2), so $\text{rank } \varphi = 1$ and, by the Rank–Nullity Theorem (Theorem 2.3.1), $W = \ker \varphi$ has $\dim W = n - 1$.

Moreover $\text{span}(v_1) \cap W = \{0\}$: if $av_1 \in W$ then $0 = \varphi(av_1) = ac$, and $c \neq 0$ forces $a = 0$. So the sum $\text{span}(v_1) + W$ is direct, and $\dim(\text{span}(v_1) + W) = 1 + (n - 1) = n$, both by Theorem 1.7.4. A subspace of V of dimension $\dim V$ is all of V (Theorem 1.6.8), so

$$V = \text{span}(v_1) \oplus W.$$

The restriction of β to $W \times W$ is a bilinear form on W , and it is symmetric because β is. As $\dim W = n - 1$, the induction hypothesis provides an orthogonal basis $(v_2, \dots, v_n)$ of W for that restriction.

Concatenating bases of the summands of a direct sum gives a basis of it (Theorem 1.7.5, (a) $\Leftrightarrow$ (d)), so $\mathcal{B} = (v_1, v_2, \dots, v_n)$ is a basis of V . It is orthogonal for β : for $j \geq 2$ we have $v_j \in W = \ker \varphi$, so $\beta(v_1, v_j) = \varphi(v_j) = 0$, and $\beta(v_j, v_1) = 0$ by symmetry; and for $2 \leq i \neq j$ the value $\beta(v_i, v_j)$ is 0 by the choice of the basis of W . This completes the induction.

For the matrix statement, let $\mathbf{A} \in M_n(F)$ be symmetric and let $\beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top \mathbf{A} \mathbf{y}$ on $V = F^n$, which is symmetric by Proposition 14.3.1 and has $[\beta]_{\mathcal{E}}^{\mathcal{E}} = \mathbf{A}$ in the standard basis $\mathcal{E}$. Take an orthogonal basis $\mathcal{B}$ as above and let $\mathbf{P} = [\text{id}]_{\mathcal{B}}^{\mathcal{E}}$, the matrix whose columns are the vectors of $\mathcal{B}$, which is invertible. By Theorem 14.2.1, $[\beta]_{\mathcal{B}}^{\mathcal{B}} = \mathbf{P}^\top \mathbf{A} \mathbf{P}$, and this matrix is diagonal. This proves the theorem. ■

Two hypotheses did visible work. Symmetry was used twice: to make $\beta(v_j, v_1)$ vanish along with $\beta(v_1, v_j)$, and to keep the restriction to W symmetric so the induction could run. The characteristic hypothesis was used exactly once, inside [Lemma 14.4.1](#) — and that single use is essential: Exercise C2 below exhibits a symmetric matrix over $\mathbb{F}_2$ that is congruent to no diagonal matrix at all.

Warning. **Diagonal does not mean “the diagonal entries are eigenvalues”.** The matrix $\mathbf{P}^\top \mathbf{A} \mathbf{P}$ of [Theorem 14.4.2](#) is congruent to $\mathbf{A}$, not similar to it, and its entries are the values $q(v_i)$ at whatever basis the algorithm happened to produce. Over $\mathbb{R}$ they can be scaled at will: replacing v_i by tv_i replaces d_i by $t^2 d_i$. There is no canonical list of numbers here. The next section finds what there *is*.

Quick check. In [Theorem 14.4.2](#), how many of the diagonal entries d_i are zero?

Solution. Exactly $n - \text{rank } \mathbf{A}$ of them. A diagonal matrix has rank equal to its number of nonzero entries, and congruence preserves rank (Theorem 14.2.3), so the count is the same for every orthogonal basis even though the individual d_i are not. In the language of Section 1,

those v_i with $d_i = 0$ span the radical $\text{rad}(\beta)$ of Definition 14.1.3, since in an orthogonal basis such a v_i pairs to zero with every basis vector; and β is nondegenerate (Definition 14.1.4) exactly when no d_i is zero.

14.4.3 The algorithm: symmetric row and column operations

The proof is constructive, but running it by hand means chasing kernels of functionals. There is a bookkeeping device that does the same work on the matrix directly, and it is the practical content of this section.

The key observation is that a congruence by an elementary matrix is a **pair** of operations. Let $\mathbf{E}$ be an elementary matrix (Definition 3.4.1). Right multiplication $\mathbf{A}\mathbf{E}$ performs a column operation, and left multiplication $\mathbf{E}^\top\mathbf{A}$ performs the corresponding row operation. So $\mathbf{A} \mapsto \mathbf{E}^\top\mathbf{A}\mathbf{E}$ performs both, and the result is congruent to $\mathbf{A}$ and again symmetric. Doing the operations in pairs is exactly what keeps the matrix symmetric, and that is the whole idea.

Algorithm. To diagonalize a symmetric $\mathbf{A} \in M_n(F)$ by congruence, write $\mathbf{A}$ and $\mathbf{I}_n$ side by side and repeat, for $i = 1, 2, \dots, n$ in turn:

- **If $a_{ii} = 0$ but some $a_{jj} \neq 0$ with $j > i$** , swap rows i, j and then columns i, j .
- **If $a_{ii} = 0$ and every $a_{jj} = 0$ for $j \geq i$** , look for an entry $a_{ij} \neq 0$ with $j > i$. If there is none, then row i and column i are already zero in every position, so move on to $i + 1$. If there is one, add row j to row i , then column j to column i ; the new a_{ii} is $2a_{ij} \neq 0$.
- **Now $a_{ii} \neq 0$.** For each $j > i$ with $a_{ij} \neq 0$, subtract (a_{ij}/a_{ii}) times row i from row j , then (a_{ij}/a_{ii}) times column i from column j .

Over a field where division is inconvenient — $\mathbb{Q}$ or $\mathbb{Z}$ -valued data by hand — the clearing step may instead be done as row $j \mapsto a_{ii}$ row $j - a_{ij}$ row i , with the matching column operation. That is the same move composed with scaling row and column j by $a_{ii} \neq 0$, which is itself a congruence, so it is legitimate; it keeps the entries integral and changes the diagonal result only by square factors. The worked example below takes this route.

Perform only the **column** half of each operation on the matrix standing to the right. When $\mathbf{A}$ has become diagonal, that matrix is $\mathbf{P}$, and $\mathbf{P}^\top\mathbf{A}\mathbf{P}$ is the diagonal result.

The second bullet is [Lemma 14.4.1](#) made mechanical, and the factor $2 = 1 + 1$ in it is where the algorithm would stop in characteristic 2. The right-hand matrix works because applying the column operations $\mathbf{E}_1, \mathbf{E}_2, \dots, \mathbf{E}_k$ in order turns $\mathbf{I}$ into $\mathbf{E}_1\mathbf{E}_2 \cdots \mathbf{E}_k$, which is the product whose transpose and self sandwich $\mathbf{A}$.

Example. Diagonalizing a symmetric matrix with zero diagonal

Over $\mathbb{Q}$, diagonalize

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

by congruence, producing an invertible $\mathbf{P}$ with $\mathbf{P}^\top\mathbf{A}\mathbf{P}$ diagonal.

Solution. The form is $q(\mathbf{x}) = 2x_1x_2 + 2x_1x_3 + 2x_2x_3$: every diagonal entry is 0, so there is no square to complete yet, and the second bullet applies.

Step 1 (create a pivot). Add row 2 to row 1, then column 2 to column 1. The matrix becomes

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix},$$

the left matrix after the row operation and the right one after the matching column operation. The new corner entry is $q(\mathbf{e}_1 + \mathbf{e}_2) = 2$.

Step 2 (clear the first row and column, in two paired moves). Rather than divide by 2, use the operation “row 2 $\mapsto 2 \cdot$ row 2 – row 1”, which is a scaling followed by an addition, hence a congruence by a product of two elementary matrices, and legitimate because $2 \neq 0$ in $\mathbb{Q}$. Apply it and its column partner. This keeps every entry an integer:

$$\begin{pmatrix} 2 & 1 & 2 \\ 0 & -1 & 0 \\ 2 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 2 \\ 0 & -2 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

Then “row 3 $\mapsto$ row 3 – row 1” and its column partner:

$$\begin{pmatrix} 2 & 0 & 2 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

The transforming matrix. Applying the three **column** operations to $\mathbf{I}_3$ in the same order gives

$$\mathbf{I}_3 \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 & -1 \\ 1 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{P}.$$

Here $\det \mathbf{P} = 2 \neq 0$, so $\mathbf{P}$ is invertible, and

$$\mathbf{P}^\top \mathbf{A} \mathbf{P} = \text{diag}(2, -2, -2).$$

The check is one column at a time: with $\mathbf{p}_1 = (1, 1, 0)$, $\mathbf{p}_2 = (-1, 1, 0)$, and $\mathbf{p}_3 = (-1, -1, 1)$, we get $q(\mathbf{p}_1) = 2$, $q(\mathbf{p}_2) = -2$, and $q(\mathbf{p}_3) = 2 - 2 - 2 = -2$, while $\beta(\mathbf{p}_1, \mathbf{p}_2) = \mathbf{p}_1^\top \mathbf{A} \mathbf{p}_2 = (1, 1, 0) \cdot (1, -1, 0) = 0$ and similarly for the other two pairs.

Two observations about that example. The determinants are $\det \mathbf{A} = 2$ and $\det(\mathbf{P}^\top \mathbf{A} \mathbf{P}) = 8$, and they differ by $(\det \mathbf{P})^2 = 4$: a congruence multiplies the determinant by a square, which is the discriminant statement of Section 2. And the eigenvalues of $\mathbf{A}$ are $2, -1, -1$, whose signs are $+, -, -$ — the same pattern of signs as $2, -2, -2$, with none of the same numbers. That coincidence is Section 5.

14.4.4 Over the complex numbers, and over a general field

The diagonal entries produced by the algorithm are not canonical, but there is a precise statement of how much freedom remains.

Proposition 14.4.3. Diagonal Entries Are Defined Only up to Squares

Let $\mathcal{B} = (v_1, \dots, v_n)$ be an orthogonal basis for β with $d_i = q(v_i)$, and let $t_1, \dots, t_n \in F$ be nonzero. Then $(t_1 v_1, \dots, t_n v_n)$ is again an orthogonal basis for β , with diagonal entries $t_i^2 d_i$.

Proof. Scaling basis vectors by nonzero scalars again gives a basis. For $i \neq j$, bilinearity gives $\beta(t_i v_i, t_j v_j) = t_i t_j \beta(v_i, v_j) = 0$, so the new basis is orthogonal; and $q(t_i v_i) = t_i^2 q(v_i) = t_i^2 d_i$. ■

So each nonzero d_i can be changed to any other element of its coset in the group $F^\times / (F^\times)^2$ of **square classes**, and no further, by this move. How much that costs depends entirely on the arithmetic of F :

- Over $\mathbb{C}$, every element is a square, so there is exactly one nonzero square class and every nonzero d_i can be turned into 1.
- Over $\mathbb{R}$, the squares are the positive numbers, so there are two classes and every nonzero d_i can be turned into 1 or -1 , according to its sign — the subject of the next section.
- Over $\mathbb{Q}$ there are infinitely many classes ($2, 3, 5, \dots$ are pairwise inequivalent), so the 1-dimensional forms $q(x) = x^2$ and $q(x) = 2x^2$ are already noncongruent.
- Over $\mathbb{F}_p$ with p odd there are exactly two classes, as for $\mathbb{R}$, but “which class” is not a matter of sign.

The complex case collapses completely.

Corollary 14.4.4. Classification of Complex Symmetric Matrices by Rank

Let $\mathbf{A} \in M_n(\mathbb{C})$ be symmetric of rank r . Then $\mathbf{A}$ is congruent to

$$\mathbf{I}_r \oplus \mathbf{O}_{n-r} = \text{diag}(\underbrace{1, \dots, 1}_r, 0, \dots, 0).$$

Consequently two symmetric matrices in $M_n(\mathbb{C})$ are congruent if and only if they have the same rank, and there are exactly $n + 1$ congruence classes.

Proof. By Theorem 14.4.2 (with $\text{char } \mathbb{C} = 0$) there is an invertible $\mathbf{P}_1$ with $\mathbf{P}_1^\top \mathbf{A} \mathbf{P}_1 = \mathbf{D} = \text{diag}(d_1, \dots, d_n)$ diagonal. Congruence preserves rank (Theorem 14.2.3), and the rank of a diagonal matrix is its number of nonzero entries, so exactly r of the d_i are nonzero. Permuting the basis vectors is a congruence by a permutation matrix $\mathbf{P}_2$, so we may assume $d_1, \dots, d_r \neq 0$ and $d_{r+1} = \dots = d_n = 0$.

Every nonzero complex number has a square root, so choose $s_i \in \mathbb{C}$ with $s_i^2 = d_i$ for $i \leq r$, and set $t_i = 1/s_i$ for $i \leq r$ and $t_i = 1$ otherwise. By Proposition 14.4.3 the congruence

by $\mathbf{P}_3 = \text{diag}(t_1, \dots, t_n)$ replaces d_i by $t_i^2 d_i$, which is 1 for $i \leq r$ and 0 otherwise. So $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \mathbf{I}_r \oplus \mathbf{O}_{n-r}$ with $\mathbf{P} = \mathbf{P}_1 \mathbf{P}_2 \mathbf{P}_3$.

For the classification: congruent matrices have equal rank by Theorem 14.2.3, and matrices of equal rank are both congruent to the same normal form, hence to each other by Proposition 14.2.2. The possible ranks are $0, 1, \dots, n$, giving $n + 1$ classes. This proves the corollary. ■

Contrast this with similarity, where complex symmetric matrices are not classified by anything so simple: the matrix $\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$ is symmetric, nonzero, and satisfies $\mathbf{A}^2 = \mathbf{O}$, so it is not even diagonalizable as an operator. Congruence is a coarser relation than similarity on symmetric matrices, and over $\mathbb{C}$ it is coarse enough to be finite.

14.4.5 Exercises

14.4.5.1 A. Check your understanding

Exercise. A1

- Define what it means for an ordered basis to be an **orthogonal basis for a bilinear form** β , and say what that means about $[\beta]_{\mathcal{B}}$.
- State [Theorem 14.4.2](#) with all of its hypotheses.
- Which step of the proof uses $\text{char } F \neq 2$, and what exactly is divided by?
- Determine whether the following statement is correct, and justify your answer: if $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \text{diag}(d_1, \dots, d_n)$, then the d_i are the eigenvalues of $\mathbf{A}$.
- Describe the pair of operations that a congruence by an elementary matrix performs.

Solution.

- $\mathcal{B} = (v_1, \dots, v_n)$ is orthogonal for β if $\beta(v_i, v_j) = 0$ whenever $i \neq j$. Equivalently $[\beta]_{\mathcal{B}}$ is diagonal, with entries $q(v_i)$.
- If $\text{char } F \neq 2$, V is finite-dimensional over F and β is a symmetric bilinear form on V , then V has an orthogonal basis for β ; equivalently every symmetric $\mathbf{A} \in M_n(F)$ is congruent to a diagonal matrix.
- [Lemma 14.4.1](#), inside Step 2 of the proof. It produces $q(u + w) = (1 + 1)\beta(u, w)$ and needs $1 + 1 \neq 0$ to conclude that this is nonzero. Equivalently, the algorithm's repair move multiplies by 2, so it needs $2 \neq 0$.
- Incorrect. The relation is congruence, not similarity. In [Example \(Diagonalizing a symmetric matrix with zero diagonal\)](#) the diagonal entries are $2, -2, -2$ while the eigenvalues are $2, -1, -1$. Only the signs matched there, and Section 5 explains why.
- A column operation and the matching row operation: $\mathbf{A} \mapsto \mathbf{E}^\top \mathbf{A} \mathbf{E}$. Performing both keeps the matrix symmetric and keeps it in the same congruence class.

14.4.5.2 B. Practice

Exercise. B1: Symmetric elimination

Over $\mathbb{Q}$, let

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

Diagonalize $\mathbf{A}$ by paired row and column operations, exhibiting $\mathbf{P}$ and $\mathbf{P}^\top \mathbf{A} \mathbf{P}$.

Solution. Here $a_{11} = 1 \neq 0$, so the pivot is already available.

Clear the first row and column. Subtract $2 \times$ row 1 from row 2, then $2 \times$ column 1 from column 2. The entry a_{13} is already 0, so nothing else is needed in this round:

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & -3 & 3 \\ 0 & 3 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 3 \\ 0 & 3 & 1 \end{pmatrix}.$$

Clear the second row and column. The pivot is -3 , and $a_{23} = 3$, so add row 2 to row 3 and then column 2 to column 3:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 3 \\ 0 & 0 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

The transforming matrix. Applying the two column operations to $\mathbf{I}_3$ gives

$$\mathbf{P} = \begin{pmatrix} 1 & -2 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{P}^\top \mathbf{A} \mathbf{P} = \text{diag}(1, -3, 4).$$

As a check, $\det \mathbf{P} = 1$ and $\det \mathbf{A} = -12 = \det \text{diag}(1, -3, 4)$.

Exercise. B2: No pivot on the diagonal

Over $\mathbb{Q}$, let $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $q(\mathbf{x}) = 2x_1x_2$.

- Find a vector $\mathbf{v}$ with $q(\mathbf{v}) \neq 0$, as in [Lemma 14.4.1](#).
- Diagonalize $\mathbf{A}$ by paired operations and exhibit $\mathbf{P}$.
- Write q as a difference of two squares in the new coordinates.

Solution.

- Both $\mathbf{e}_1$ and $\mathbf{e}_2$ give $q = 0$, so take $\mathbf{v} = \mathbf{e}_1 + \mathbf{e}_2$: $q(\mathbf{v}) = 2 \neq 0$.
- Add row 2 to row 1, then column 2 to column 1, reaching $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$. Then apply “row $2 \mapsto 2 \cdot \text{row } 2 - \text{row } 1$ ” and its column partner, reaching $\text{diag}(2, -2)$. Applying the

same two column operations to $\mathbf{I}_2$ gives

$$\mathbf{P} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad \mathbf{P}^\top \mathbf{A} \mathbf{P} = \text{diag}(2, -2).$$

Check directly: $\mathbf{P}^\top \mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and multiplying by $\mathbf{P}$ gives $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$.

- (c) With $\mathbf{x} = \mathbf{P}\mathbf{y}$, that is $x_1 = y_1 - y_2$ and $x_2 = y_1 + y_2$, we get $q = 2(y_1 - y_2)(y_1 + y_2) = 2y_1^2 - 2y_2^2$. This is the familiar identity $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$ read as a change of variable, and it needs 2 to be invertible.

Exercise. B3: Reading off the rank

Let $\mathbf{A} \in M_4(\mathbb{C})$ be symmetric with $\text{rank } \mathbf{A} = 3$. Write down the normal form of $\mathbf{A}$ under congruence, and say how many congruence classes of symmetric matrices there are in $M_4(\mathbb{C})$.

Solution. By Corollary 14.4.4, $\mathbf{A}$ is congruent to $\mathbf{I}_3 \oplus \mathbf{O}_1 = \text{diag}(1, 1, 1, 0)$. Since rank is a complete invariant there, the classes correspond to the possible ranks 0, 1, 2, 3, 4, so there are 5 of them.

14.4.5.3 C. Going deeper

Exercise. C1: Square classes over a finite field

Work over $\mathbb{F}_5$, whose nonzero squares are 1 and 4.

- (a) Prove that the 1×1 matrices (1) and (2) are not congruent over $\mathbb{F}_5$.
- (b) Prove that $\mathbf{I}_2$ and $2\mathbf{I}_2$ are congruent over $\mathbb{F}_5$, by exhibiting a $\mathbf{P}$.
- (c) Explain why (a) and (b) are consistent with Proposition 14.4.3.

Hint: for (b), look for two vectors $\mathbf{p}_1, \mathbf{p}_2$ with $\mathbf{p}_i \cdot \mathbf{p}_i = 2$ and $\mathbf{p}_1 \cdot \mathbf{p}_2 = 0$.

Solution.

- (a) A congruence of 1×1 matrices is $(a) \mapsto (p^2 a)$ with $p \neq 0$. So (1) and (2) are congruent exactly when $2 = p^2$ for some $p \in \mathbb{F}_5^\times$. The squares of 1, 2, 3, 4 are 1, 4, 4, 1, so 2 is not a square and the two are not congruent.
- (b) Take $\mathbf{p}_1 = (1, 1)$ and $\mathbf{p}_2 = (1, 4)$. Then $\mathbf{p}_1 \cdot \mathbf{p}_1 = 2$, $\mathbf{p}_2 \cdot \mathbf{p}_2 = 1 + 16 = 17 = 2$, and $\mathbf{p}_1 \cdot \mathbf{p}_2 = 1 + 4 = 5 = 0$ in $\mathbb{F}_5$. With

$$\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}, \quad \det \mathbf{P} = 4 - 1 = 3 \neq 0,$$

we get $\mathbf{P}^\top \mathbf{I}_2 \mathbf{P} = \mathbf{P}^\top \mathbf{P} = \text{diag}(2, 2) = 2\mathbf{I}_2$.

- (c) Proposition 14.4.3 only says what **rescaling a single basis vector** can do, and that move cannot change a square class. Part (b) does not contradict it, because the congruence there is not diagonal: it mixes the two coordinates, and both diagonal entries change square class at once. What is invariant is the class of their product, the **deter-**

minant: $\det \mathbf{I}_2 = 1$ and $\det(2\mathbf{I}_2) = 4$ differ by $4 = 2^2$, a square.

Exercise. C2: Is this still true over $\mathbb{F}_2$?

Let $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ over $\mathbb{F}_2$, and let $\beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top \mathbf{A} \mathbf{y}$ on $\mathbb{F}_2^2$.

- (a) Prove that β is alternating.
- (b) Prove that if $\mathbf{P} \in M_2(\mathbb{F}_2)$ is invertible, then every diagonal entry of $\mathbf{P}^\top \mathbf{A} \mathbf{P}$ is 0.
- (c) Deduce that $\mathbf{A}$ is congruent to **no** diagonal matrix except the zero matrix, and hence that [Theorem 14.4.2](#) fails over $\mathbb{F}_2$.

Solution.

- (a) By Proposition 14.3.2 (b): over $\mathbb{F}_2$ we have $-\mathbf{A} = \mathbf{A}$, so $\mathbf{A}^\top = \mathbf{A} = -\mathbf{A}$, and the diagonal entries of $\mathbf{A}$ are 0. (Directly: $\beta(\mathbf{x}, \mathbf{x}) = 2x_1x_2 = 0$.)
- (b) The i -th diagonal entry of $\mathbf{P}^\top \mathbf{A} \mathbf{P}$ is $\mathbf{p}_i^\top \mathbf{A} \mathbf{p}_i = q(\mathbf{p}_i)$, where $\mathbf{p}_i$ is the i -th column of $\mathbf{P}$. By (a), q vanishes identically, so every diagonal entry is 0.
- (c) A diagonal matrix congruent to $\mathbf{A}$ has all diagonal entries 0 by (b), hence is the zero matrix. But congruence preserves rank (Theorem 14.2.3) and $\text{rank } \mathbf{A} = 2 \neq 0 = \text{rank } \mathbf{O}$. So no diagonal matrix is congruent to $\mathbf{A}$. Since $\mathbf{A}$ is symmetric over $\mathbb{F}_2$, the conclusion of [Theorem 14.4.2](#) fails there, and the hypothesis $\text{char } F \neq 2$ cannot be dropped.

Exercise. C3: Diagonalizing the restriction

Let $\text{char } F \neq 2$, let β be a symmetric bilinear form on V , and let $U \subseteq V$ be a subspace.

- (a) Prove that U has an orthogonal basis for the restriction of β to U .
- (b) Give an example, with $\dim V = 2$, in which β is nondegenerate but its restriction to some 1-dimensional U is the zero form.
- (c) Deduce that an orthogonal basis of U cannot always be extended to an orthogonal basis of V by adding vectors of U alone, and say in one sentence what [Theorem 14.4.2](#) does guarantee instead.

Solution.

- (a) The restriction $\beta|_{U \times U}$ is bilinear, since it is the same function on a smaller domain, and symmetric for the same reason. U is finite-dimensional, being a subspace of a finite-dimensional space (Theorem 1.6.7). So [Theorem 14.4.2](#) applies to $(U, \beta|_{U \times U})$ directly.
- (b) Over $\mathbb{Q}$ take $\beta(\mathbf{x}, \mathbf{y}) = x_1y_2 + x_2y_1$ on $\mathbb{Q}^2$, with matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which is invertible, so β is nondegenerate. Put $U = \text{span}(\mathbf{e}_1)$. Then $\beta(a\mathbf{e}_1, b\mathbf{e}_1) = 0$ for all a, b , so the restriction is the zero form even though β is not.
- (c) In (b) the single vector $\mathbf{e}_1$ is an orthogonal basis of U , but no vector of U can be added to it, and any orthogonal basis of V for this β must consist of vectors $\mathbf{v}$ with

$q(\mathbf{v}) \neq 0$ (its matrix is diagonal and invertible), so $\mathbf{e}_1$ belongs to none of them. What the theorem guarantees is only the existence of *some* orthogonal basis of V , built from scratch; it promises nothing about extending a given orthogonal list, and Section 8 is where a correct extension statement finally appears.