VIGRE Algebra QR Review, September 29, 2003

These sessions will be primarily driven by questions from those attending. If there are not enough questions at a given session, I will go through the materials that I used in the Review that I did in Fall, 2002.

A question was raised about Sylvester's theorem. I have included at the end here some relevant discussion from last Fall's Review (Session of November 4, 2002).

Here is a briefer discussion. A real symmetric $n \times n$ matrix A represents a symmetric bilinear form B on $\mathbb{R}^n$ (thought of as column vectors) where $B(u, v)$ is the unique entry of $u^{\mathrm{tr}}Av$; here, $^{\mathrm{tr}}$ indicates transpose. There is also a quadratic form Q associated with A (and with B) that is defined by some authors as $Q(v) = B(v, v)$ and by others as $Q(v) = \frac{1}{2}B(v, v)$. The convention used does not affect the discussion below. The effect of a change of basis by an invertible matrix P (suppose that left multiplication by P converts the new coordinates to the original coordinates) is to replace A by $P^{\mathrm{tr}}AP$, for if u, v are the new coordinates, the value of B on this pair of vectors is $B((Pu)^{\mathrm{tr}}, Pv) = (Pu)^{\mathrm{tr}}APv = u^{\mathrm{tr}}(P^{\mathrm{tr}}AP)v$, so that when works with the new coordinates, one should use the matrix $P^{\mathrm{tr}}AP$ instead of A. One gets an equivalence relation called *cogredience* or *congruence*. We will use the former term. Sylvester's theorem asserts that every symmetric matrix is cogredient to a diagonal matrix, and that the number p of positive entries, the number q of negative entries, and the number r of 0 entries are invariants of the cogredience class and determine it uniquely. Then (p, q, r) is called the *signature* of the matrix or associated form. Some authors call $p - q$ the signature. The rank of the matrix will be $p + q$. From the rank $p + q$, the signature $p - q$, and the size $n = p + q + r$, one can recover the three numbers p, q, r. It is also a theorem that a real symmetric matrix is conjugate by a real orthogonal matrix N (this means that $N^{\mathrm{tr}} = N^{-1}$) to a diagonal matrix. This is an instance of cogredience as well as of conjugacy, and so the cogredience class of a real symmetric matrix is determined by its eigenvalues. The bilinear form and the quadratic form are called *non-degenerate* if the rank is n, i.e., if $r = 0$. The matrix or form is called *positive definite* if $p = n$ and *positive semi-definite* if $q = 0$. The notions of *negative definite* (resp., *semi-definite*) are defined similarly: $q = n$ or $p = 0$, resp.

To determine (p, q, r) it is easiest to do row and column operations to bring the matrix to diagonal form, but whenever one does a row operation, one must also do the corresponding column operation, and vice versa. Doing only row operations will not preserve the signature.

For example, suppose one wants to determine the possible signatures (p, q, r) of the real symmetric matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ 3 & 7 & x \end{pmatrix}$$

as x varies in the real numbers. Subtract twice the first row from the second and **also** subtract twice the first column from the second to get first

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 3 & 7 & x \end{pmatrix}$$

and then

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 1 \\ 3 & 1 & x \end{pmatrix}.$$

Next subtract three times the first row from the third and then three times the first column from the third to get first

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 1 \\ 0 & 1 & x-9 \end{pmatrix}$$

and then

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & x-9 \end{pmatrix}.$$

Finally, subtract first the second row from the third and then the second column from the third to get first

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & x-10 \end{pmatrix}$$

and then

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x-10 \end{pmatrix}.$$

Now one can see that one has a non-degenerate form precisely when $x \neq 10$. If $x > 10$ the form is positive definite and the signature is $(3, 0, 0)$. If $x = 10$ the form is positive semi-definite and the signature is $(2, 0, 1)$. If $x < 10$ the form is not definite or semidefinite, and the signature is $(2, 1, 0)$. While it is possible to determine the signature of a specific matrix by looking for eigenvalues, it is almost always easier to use the method of this problem. But keep in mind that the diagonal entries of the matrix found in this way need not be eigenvalues of the original matrix: they have the same signs as the eigenvalues of the original matrix, suitably ordered.

The question was raised, is every element that commutes with an n-cycle, say $h = (1\ 2\ \cdots\ n)$ in S_n necessarily a power of it. Now, g commutes with h iff $ghg^{-1} = h$, and when an element is written as a product of disjoint cycles the effect of conjugating by g may be calculated by simply applying g inside the parentheses of the various cycles to the individual elements. The reason is that if h maps a to a' and $g(a) = b$ while $g(a') = b'$ then $ghg^{-1}(b) = gh(a) = g(a') = b'$.

Thus, for g to commute with h it must permute $1, \ldots, n$ in such a way as to produce an n-cycle that is the same as h, and these have the form

$$(k \;\; k+1 \;\; \cdots \;\; n \;\; 1 \;\; 2 \;\; \cdots \;\; k-1)$$

for some choice of k. From this it follows that the only permutations that commute with h are the powers of h.

A question was asked about an old QR problem: V is a real vector space of dimension n. One part of the problem is to show that if $f = f_1$ is not 0 in V then every element of $V \otimes_{\mathbb{R}} V$ can be expressed in the form $f_1 \otimes g_1 + \cdots + f_n \otimes g_n$ for suitable elements f_i, g_i in V. To do this, extend f to a basis $f = f_1, \ldots, f_n$ for V, and let $v_1, \ldots, v_n$ be another basis. The then every element of $V \otimes V$ can be written as a linear combination of elements $f_i \otimes v_j$, say as $\sum_{ij} c_{ij} f_i \otimes v_j$. But this can be rewritten as $\sum_i f_i \otimes (\sum_j c_{ij} v_j)$ which has the required form.

Another part of the problem required showing that there is some element of $V \otimes V$ that cannot be written as the sum of $n-1$ terms of the form $f_i \otimes g_j$. Here is one way to do this. Pick a basis $v_1, \ldots, v_n$ for V, and a possibly different basis $w_1, \ldots, w_n$ as well. Then every element of $V \otimes V$ can be written uniquely in the form $\sum_{ij} c_{ij} v_i \otimes v_j$. This give a vector space isomorphism between $V \otimes V$ and $n \times n$ matrices (c_{ij}). An element of the form $f \otimes g$ can be written as $(\sum_i a_i v_i) \otimes \sum_j b_j w_j) = \sum_{i,j} (a_i b_j) v_i \otimes w_j$ so that the corresponding matrix $(a_i b_j)$ is the product of the $n \times 1$ column with entries a_i and the $1 \times n$ row with entries b_j. This implies that the matrix corresponding to $f \otimes g$ has rank at most one. The rank of the sum of two matrices is at most the sum of their ranks, since the column space of the sum is contained in the sum of the column spaces of the two matrices. Thus, the matrix corresponding to the sum of $n-1$ elements $f_i \otimes g_i$ has rank at most $n-1$. It follows that a element of $V \otimes V$ whose corresponding matrix has rank n, such as $v_1 \otimes w_1 + \cdots + v_n \otimes w_n$, which corresponds to the identity matrix, cannot be a sum of $n-1$ elements of the form $f_i \otimes g_i$.

Another question dealt with a QR problem which asked one to classify all groups of order $1996 = 4 \cdot 499$. Before attempting this, we first recall some facts about semi-direct products. The following is taken from material prepared for last Fall's review.

A surjective group homomorphism $f : G \to H$ is called *split* if it has a right inverse $g : H \to G$ that is a group homomorphism: thus $f \circ g = \mathbf{1}_H$. This implies that $g(H)$ is isomorphic with H, is disjoint from the kernel N, and that $g(H)$ and N generate G. Conversely, if H is a subgroup of G disjoint from a normal subgroup N and H, N together generate G, then $G = NH$ and $G/N \equiv H$. Each element of G can be written uniquely in the form hn with $h \in H$ and $n \in N$, for if $h_1 n_1 = h_2 n_2$ then $h_2^{-1} h_1 = n_2 n_1^{-1} \in H \cap N = \{e\}$, and this implies both $h_2 = h_1$ and $n_2 = n_1$.

In this situation the group structure of G is determined by knowing one additional piece of information, namely, how H acts on N by conjugation. The action of H on N by conjugation gives a homomorphism $\phi : H \to \operatorname{Aut} N$ (the value of $\phi(h)$ on n is hnh^{-1}). If we know ϕ, then we can recover the multiplication in G: $(nh)(n'h') = \big(n(hn'h^{-1})\big)(hh') = (n\phi(h)(n'))(hh')$.

In fact, given any two groups N, H, together with a homomorphism from $\phi : H \to \operatorname{Aut} N$ one can construct a group G with H and N as disjoint subgroups that generate G such that N is normal and the action of H on N by conjugation is given by ϕ. Moreover, the discussion of the paragraphs above shows that there is only one possible candidate for G: introduce a group structure on $N \times H$ by letting the multiplication be given by the rule $(n, h) * (n', h') = (n\phi(h)n', hh')$. It is easy to check that (e, e) is an identity (to be more precise, one might write (e_N, e_H)), that multiplication is associative, and that (n, h) has inverse (what is it?). It is easy to check that the set of elements of the form (e, h) for $h \in H$ is a subgroup isomorphic with H, and that the set of elements of the form (n, e) for $n \in N$ is a normal subgroup, disjoint from it, isomorphic with n. The group $N \times H$ with multiplication $*$ is called the *semi-direct product* of N by H. The term *normal product* is also used.[1]

We now return to the classification of groups of order 1996. In fact, we shall classify groups of order $4p$, where $p > 3$ is prime and $p \equiv 3 \bmod 4$. The number of Sylow p-subgroups divides 4 and is congruent to 1 mod p. It follows that there is only one Sylow p-subgroup, and it must be normal. Call it N. Of course, $N \cong \mathbb{Z}/pZ$. Choose a Sylow 2-subgroup $H \subseteq G$ which must be either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now G/N will have order four and H cannot meet N, since their orders are relatively prime. Thus, H injects into G/N, and this must be an isomorphism since both have order 4. It follows that any group of order $4p$ is a semidirect product and is determined by the map of H into $\operatorname{Aut}(N)$ that will correspond to conjugation on N by an element of H.

The automorphisms of $\mathbb{Z}/n\mathbb{Z}$ are given by multiplication by a unit in of the ring $\mathbb{Z}/nZ$. In the case where $n = p$ is prime, this is a cycle group of order $p-1$, and if $p = 4k+3$ then $p - 1 = 2(2k+1)$, and the only elements whose orders are powers of 2 are $\{1, -1\}$. This is a copy of $\mathbb{Z}_2$. This means that G is a completely determined by the choice of H and a homomorphism of H to $\mathbb{Z}/2Z$.

If $H = \mathbb{Z}/4\mathbb{Z}$, there are two choices: one can send the generator of H to the identity in $\mathbb{Z}_2$, or to the generator of $\mathbb{Z}_2$. This yields two non-isomorphic groups: one is abelian, and is $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/4p\mathbb{Z}$, and the other is non-abelian with Sylow 2-subgroup $\mathbb{Z}/4\mathbb{Z}$.

If $H = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then we may think of both H and the copy of $\mathbb{Z}/2\mathbb{Z}$ to which we are mapping H as vector spaces over $\mathbb{Z}/2\mathbb{Z}$. The map is either trivial, or surjective. In the first case we get a direct sum, and this is the abelian group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/2Z \oplus \mathbb{Z}/2p\mathbb{Z}$. In the second case, we can choose a basis for H over $\mathbb{Z}/2\mathbb{Z}$ such that one basis element maps to the generator of $\mathbb{Z}/2\mathbb{Z}$ and the other to zero. This determines the isomorphism class of G, and gives a non-abelian group that has $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as its Sylow 2-subgroup. Thus, there are, up to isomorphism, four groups of order $4p$.

[1] Authors who favor right actions will prefer to describe such groups using the right action of H on N by conjugation. The point is that in the situation of the first paragraph, G is also HN, and one has $(h'n')(hn) == (h'h)(h^{-1}n'hn)$. The details of this formulation are left to the reader.

In general it may be difficult to determine whether two semi-direct products of H and N are isomorphic or not, but if α is an automorphism of H and one changes the map $\phi : H \to \mathrm{Aut}\,(N)$ by replacing it with $\phi \circ \alpha$, the groups obtained are isomorphic.

The following are problems distributed at last Monday's session: we may discuss them next time, but I will give preference to answering questions from the participants.

1. Let H be a subgroup of G of index 3. Prove that either H is normal, or that H has a subgroup N of index 2 in H such that N is normal in G.

2. Say that a group G has the TFF property if there is a normal subgroup N which is torsion-free and has finite index. Prove that if G has the TFF property then so does any subgroup of G.

3. Let G be a finite group with with a normal subgroup H such that both G/H' and H are nilpotent. Prove that G is nilpotent. Here H' denotes the derived (or commutator) subgroup of H.

4. Find all finite groups G with at most 3 conjugacy classes.

5. Let G be a group with $|G| = 30$.

(i) Prove that either G has a normal Sylow 3-subgroup or a normal Sylow 5-subgroup.

(ii) Prove that G is isomorphic with a semidirect product of $\mathbb{Z}_{15}$ by $\mathbb{Z}_2$. (This is equivalent to showing that G has a normal subgroup that is cyclic of order 15 and a subgroup that is cyclic of order 2 meeting it only in the identity element.)

6. Find all groups of order 21, up to isomorphism.

7. Prove that a finite simple group of even order is generated by elements of order 2.

8. Let G be a group with center Z. Suppose that G/Z is cyclic. Prove that there exists an element x of G such that every element of G can be written in the form $x^n z$ for some integer n and some $z \in Z$. From this, prove that G is abelian.

9. Let I and J be ideals of a commutative ring with identity R such that $I + J = R$. Prove that for any two positive integers m, n, $I^m + J^n = R$. (The ideal I^m is generated by all products of m elements of I.)

10. (Not a QR problem.) Consider a deck with $2N$ cards, where N is a positive integer. Call the cards $1, 2, \ldots, 2N$, so that the top card has the label "1". Consider a shuffle that first divides the deck in half, reverses the order of the cards in the top half, and then interlaces the two halves with the cards alternating so that the original top card winds up on the bottom. The new positions are then $N+1$, N, $N+2$, $N-1$, $\ldots$, $2N-1$, 2, $2N$, 1. Suppose that $2N = 2^n$, where n is a positive integer. Show that $n+1$ of these shuffles restore the deck to its original order.

Following is some material from the review session of November 4, 2002.

Bilinear maps, quadratic forms, and (skew-)symmetric matrices

Let U, V and W be vector spaces over a field k. A *bilinear* map $B : U \times V \to W$ is a function that is linear in each coordinate separately when the other is held fixed. Thus, for all $u, u' \in U$ and $v, v' \in V$ and all scalars $a, a' \in k$,

$$B(au + a'u', v) = aB(u, v) + a'B(u', v) \quad \text{and} \quad B(u, av + a'v') = aB(u, v) + a'B(u, v').$$

Repeated application shows that

$$B(\sum_{i=1}^{m} a_i u_i, \sum_{j=1}^{n} b_j v_j) = \sum_{i,j} a_i b_j B(u_i, v_j).$$

If one has a basis u_i for U and a basis v_j for V then there is a unique bilinear map to W taking specified values w_{ij} on the pairs (u_i, v_j) as i and j run independently through the index sets for the two bases. This is correct even when the bases are infinite.

A bilinear form B on a k-vector space V is a bilinear map $V \times V \to k$. If one chooses an ordered basis v_i for V, and uses it for both copies of V, then B is uniquely determined by the scalars a_{ij} which are its values on the pairs (v_i, v_j). If the basis is finite with n elements, then we can place these values into an $n \times n$ matrix $A = (a_{ij})$. We use the superscript $^{\rm tr}$ to denote the transpose of a matrix. If we use coordinates in K^n (written as column vectors) with respect to the chosen ordered basis, then on (u, v) is $u^{\rm tr}Av$ (thought of as a scalar rather than as a 1×1 matrix). Thus, once a basis is fixed, there is a bijection between bilinear forms on the n-dimensional vector space V and and $n \times n$ matrices. The bilinear form is called *non-degenerate* if its matrix is invertible. The rank of bilinear form is the rank of its matrix. Non-degenerate forms have maximum rank.

If one changes basis, and C is the invertible matrix such that multiplying by C converts coordinates in the new basis to coordinates in the original basis, then the matrix of B with respect to the new basis is clearly $C^{\rm tr}AC$. Two $n \times n$ matrices A, A' are called *cogredient* (or *congruent*) if there is an $n \times n$ invertible matrix C such that $C^{\rm tr}AC = A'$. This is an equivalence relation, and the equivalence classes classify bilinear forms.

A bilinear form B is called *symmetric* if $B(u, v) = B(v, u)$ for all choices of u and v, and this is equivalent to having a symmetric matrix in the finite-dimensional case. A bilinear form B is called *alternate* if $B(v, v) = 0$ for all $v \in V$. Then

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

and so $B(u, v) = -B(v, u)$ is implied. Any bilinear form that satisfies $B(u, v) = -B(v, u)$ for all u, v is alternate provided the base field has characteristic different from 2: $B(u, u) = -B(u, u)$ implies $B(u, u) = 0$ except in characteristic 2. A bilinear form is alternate if and only if its matrix satisfies $A^{\rm tr} = -A$ and the main diagonal consists entirely of 0's: the latter condition is automatic if the characteristic is not 2. We shall call such matrices *alternate*. Except in characteristic 2, this condition is equivalent to skew-symmetry (i.e., $A^{\rm tr} = -A$).

In the rest of this discussion the bilinear form will be assumed to be either symmetric or alternate. In these cases we say the $u \perp v$ if $B(u, v) = 0$. Under our hypothesis that the form is symmetric or alternate, this relation is symmetric. Note that a non-zero vector can be perpendicular to itself. The usual inner product on $\mathbb{R}^n$ is the bilinear form corresponding to the identity matrix, and is, of course, symmetric.

For every alternate bilinear form B there is a basis such that the matrix of B is the direct sum of 2×2 blocks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and 1×1 blocks that are (0). Thus, every alternate matrix is cogredient to a matrix of this form. Two alternate matrices are cogredient if and only if they have the same rank, which must be even. The determinant of an alternate matrix must be a perfect square in the field, because cogredience preserves determinants up to multiplication by a nonzero square in the field.

Exercises

(1) Prove that if A is a skew-symmetric or a symmetric matrix over $\mathbb{R}^n$ that maps a subspace V into itself, then A also maps the orthogonal complement of V, with respect to the usual inner product, into itself. (Note that u is orthogonal, in the usual inner product, to the value of A on v iff $u^{\mathrm{tr}}Av = 0$ iff $(u^{\mathrm{tr}}Av)^{\mathrm{tr}} = 0$ iff $v^{\mathrm{tr}}A^{\mathrm{tr}}u = 0$ iff $\pm v^{\mathrm{tr}}Au = 0$ iff v is orthogonal, in the usual inner product, to the value of A on u.)

(2) Recall that, by a previous problem, every real square matrix maps either a one-dimensional or a two-dimensional subspace of $\mathbb{R}^n$ into itself (this was Problem 7. from the session of October 21: one uses the existence of complex eigenvalue and eigenvector). Show that A as in part (1) is orthogonally conjugate (since, when C is orthogonal, $C^{-1} = C^{\mathrm{tr}}$, this also gives cogredience) to a direct sum of matrices, each of which has the same kind of symmetry as A, and each of which is either 2×2 or 1×1. Thus, in the skew-symmetric case, each block is either $\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}$ for some real number c or (0), while in the symmetric case each block is either of the form $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ or is 1×1.

(3) Show that a two by two symmetric matrix over $\mathbb{R}$ always has a real eigenvalue, and, hence, can be diagonalized orthogonally. Conclude that every real symmetric matrix is orthogonally conjugate to a diagonal matrix. In particular, a real symmetric matrix of arbitrary size has real eigenvalues.

(4) Use the result of (2) to show that every real skew-symmetric matrix has pure imaginary eigenvalues ($0 = 0i$ is included among the pure imaginary numbers.)

(5) An orthogonal matrix over the real numbers also has the property that if it maps a subspace V of $\mathbb{R}^n$ into itself, then it maps the orthogonal complement of V into itself as well. Using this and the fact stated at the beginning of (2), show that every orthogonal matrix over $\mathbb{R}$ is a direct sum of orthogonal matrices each of which is either a 2×2 block or a 1×1 block, (± 1).

(6) One can define an inner product on $\mathbb{C}^n$ by letting the product (u, v) of $u = (u_j)$ and $v = (v_j)$ be $\sum_{j=1}^{n} u_j \overline{v_j}$, where the bar indicates complex conjugation. This inner product is not bilinear: it is linear in the first coordinate, but conjugate linear in the second, i.e., $(u, cv) = \overline{c}(u, v)$. This gives a notion of orthogonality and a norm. Every subspace of $\mathbb{C}^n$ has a unitary basis, i.e., a basis of mutually orthogonal vectors of length 1. Denote by

A^* the conjugate of the transpose of the $n \times n$ matrix A. Then the columns of A form a unitary basis for $\mathbb{C}^n$ iff $A^*A = I$ iff $AA^* = I$. Such a matrix is called *unitary.* A matrix A is called *Hermitian* if $A^* = A$. A real unitary matrix is orthogonal. A real Hermitian matrix is symmetric. Show that every Hermitian matrix is conjugate, by a unitary matrix, to a diagonal matrix with real eigenvalues. Show that every unitary matrix is conjugate, by a unitary matrix, to a diagonal matrix whose eigenvalues have absolute value 1. (Imitate the argument in (2) for the Hermitian case and the argument in (5) for the unitary case. In a way, matters are simpler over $\mathbb{C}$, because every square matrix has an eigenvalue.)

We now continue with a summary of the theory of symmetric bilinear forms (without proofs). A symmetric bilinear form B always has an orthogonal basis, i.e., a basis consisting of vectors v_j such that $B(v_i, v_j) = 0$ if $v_i \neq v_j$. This means that it has a matrix that is diagonal, and for a suitable ordering of the basis the nonzero diagonal entries will precede the diagonal entries. Over an algebraically closed field, the nonzero diagonal entries can all be chosen to be 1. Over the real numbers, they call all be chosen to be 1 or -1.

A symmetric bilinear form over $\mathbb{R}$ is called *positive definite* if $B(u, u) > 0$ unless $u = 0$ and *negative definite* if $B(u, u) < 0$ unless $u = 0$. The form is called positive (resp., negative) *semidefinite* if $B(u, u) \geq 0$ (resp., ≤ 0) for all u. What do these conditions say about the eigenvalues?

Over the real numbers, every symmetric bilinear form B has a unique matrix that is diagonal, and such that the diagonal entries consist of a string of 1's, a string of -1's, and then a string of 0's. Some of these strings may be empty. This is called Sylvester's theorem. Thus, every real symmetric matrix is cogredient to a matrix of the type described. Let p, q, and r be the numbers of 1's, -1's, and 0's on the diagonal in such a matrix. The rank of the matrix is $p + q$. Some authors call $p - q$ the *signature* of the matrix. The rank and signature determine the cogredience class (assuming that one knows the size). Other authors refer to (p, q, r) as the signature, which certainly determines the cogredience class. Here p represents the dimension of the maximum subspace on which the restriction of the form is positive definite, q represents the dimension of the maximum subspace on which the restriction of the form is negative definite, and r represents the dimension of the subspace of all vectors that are perpendicular under B to every other vector (there may be a larger subspace on which the form is identically 0).

A quadratic form on a vector space V over k is a function $Q : V \to k$ which, when represented in coordinates, is given by a homogeneous polynomial of degree 2 in the coordinates. Thus, if $x_1, \ldots, x_n$ represent the variable coordinates, there is a formula for the function of the form $Q(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} c_{ij} x_i x_j$, where the c_{ij} are scalars in k. If one uses a different basis, there is a linear change of coordinates, but the function is still represented by a homogeneous polynomial of degree 2. If B with matrix (a_{ij}) is a bilinear form on k, then $Q(x) = B(x, x)$ is a quadratic form with $Q(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$. Note that the coefficient of $x_i x_j$ for $i < j$ (after one combines terms) is $a_{ij} + a_{ji}$, while the coefficient of x_i^2 is a_{ii}.

For the rest of this discussion we assume that the field k does not have characteristic 2. We want to show that every quadratic form arises from a unique bilinear form. Given a quadratic form with coefficients c_{ij} as above, let $a_{ii} = c_{ii}$ for every i, but let $a_{ij} = a_{ji} = \frac{1}{2}c_{ij}$ for all $i < j$. The matrix $A = (a_{ij})$ gives a symmetric bilinear form B, and one calculates that $B(x, x) = x^{\mathrm{tr}}Ax = Q(x)$, noting that $\frac{1}{2}a_{ij}x_ix_j + \frac{1}{2}a_{ij}x_jx_i = a_{ij}x_ix_j$. But one can recover B from Q as follows:

$$Q(u+v) = B(u+v, u+v) = B(u, u)+B(u, v)+B(v, u)+B(v, v) = Q(u)+2B(u, v)+Q(v),$$

and so $B(u, v) = \frac{1}{2}\big(Q(u + v) - Q(u, u) - Q(v, v)\big)$. Thus, over a field of characteristic different from 2, there is a bijection between bilinear forms and quadratic forms.[2] The effect of change of basis is captured by the notion of cogredience of matrices, and the classification of quadratic forms is equivalent to the classification of symmetric matrices. In particular, for every quadratic form there is a basis for which it is a linear combination of squares of variables. Over an algebraically closed field the coefficients may all be taken to be 1 or 0. Over the reals, the coefficients may all be taken to be -1, 1, or 0. Over the reals one may even choose an orthonormal basis such that the form is a linear combination of squares of variables (but the coefficients might be any real numbers). All the terminology of bilinear forms (rank, signature, positive and negative definiteness, etc.) immediately transfers to quadratic forms.

[2] Because it makes sense even in characteristic 2, many authors define the bilinear form associated with a quadratic form Q to be $B(u, v) = Q(u+v, u+v) - Q(u, u) - Q(v, v)$. If one does this, then $Q(u) = \frac{1}{2}B(u, u)$.