THE GENUS OF A QUADRATIC FORM

JOHN CONWAY

Our basic problem is to answer the question : when are two quadratic forms equivalent by a rational or integral change of basis? We shall temporarily suppose that all our forms are non-degenerate (i.e., have non-zero determinant), although degenerate forms really give no trouble,

The answer in the rational case is given by the celebrated Hasse-Minkowski theorem, which is usually stated in the form:

Two rational forms are equivalent over the rationals just if they are equivalent over the reals, and over the p-adic rationals for each positive prime number p.

This at first sounds like gobbledigook, because it seems to demand that you must first understand "p-adic", which really ain't so. Indeed, Minkowski, who understood the situation very well, did not have the notion of p-adic rational number.

The point really is, that there is a simple invariant for each p, and two rational quadratic forms of the same non-zero determinant and dimension are equivalent if and only if they are equivalent over the reals and have the same value of all these invariants.

It is conventional to avoid the exceptional treatment of the reals by regarding them as being the p-adic rationals for a rather special "prime number". If one is working over an algebraic extension of the rationals, there may be more than one of these "special primes", which Hasse (who introduced the idea) correctly called "unit primes." Unfortunately, this nomenclature didn't stick, and they are now usually called "infinite primes".

We're going to stay with the rational case, when there is only one such special prime, usually called "infinity." However, we'll go back to Hasse's way of thinking about things, and call it "-1," which is really much more natural. The "-1-adic" rational or integral numbers will be defined to be the real numbers.

We can now restate the Hasse-Minkowski theorem so as to include -1.

Two forms of the same non-zero determinant are equivalent over the rationals just if they are equivalent of the p-adic rationals for $p =$

$1, 2, 3, 5, \ldots$ (in other words, for all the prime numbers, where -1 is counted as a prime).

This still includes the bogeyman word "p-adic," but I said that p-adic equivalence was determined by a simple invariant. Traditionally, it's been an invariant taking the two values 1 and -1, and called THE "Hasse-Minkowski invariant." However, the definite article is undeserved, because there is no universal agreement on what "the Hasse-Minkowski invariant" means! There are two systems in use, and topologists further confuse the situation by still using an older version, the "Minkowski unit."

I'll describe all these systems later, for those who want to understand the literature. To compute either of the standard "Hasse-Minkowski invariants" in the traditional way, one multiplies a number of "Hilbert norm-residue symbols" that increases as the square of the dimension. This is a process that's complicated, and particularly prone to error, because they all take only 1 and $-l$ as values.

Compare this with my form of the invariant, the p-signature. I shall suppose the form is diagonalized (see the appendix), and since multiplication by non-zero squares does not change its class, that it has shape $Ax^2 + By^2 + \cdots$ where $A, B, C, \ldots$ are integers. Now consider the prime factorization of the typical diagonal term - it is a product of powers of $-1, 2, 3, \ldots$ (note that -1 is a prime!). We'll let $p(A)$ (the p-part of A) be the power of p in the factorization, and $p'(A)$ (the p'-part of A) be $A/p(A)$, which is the product of the powers of the remaining primes.

Then the -1-signature is just

$$-1(A) + -1(B) + -1(C) \ldots,$$

which you will recognize as the traditional signature defined by Sylvester. It is indeed an invariant under real (that is, -1-adic) transformations.

For the other odd primes, we define the p-signature to be

$$p(A) + p(B) + p(C) + \cdots + 4N \pmod 8,$$

where the number N is the number of "p-adic antisquares" among $A, B, C, \ldots$ We define a p-adic antisquare to be a number that fails to be a square for two reasons - on the one hand, its p-part $p(A)$ is an odd power of p (so not a square), while its p'-part $p'(A)$ is not even a square modulo p.

We can see that this does indeed naturally generalize from the -1 case by observing that the $(-1)'$-part of any non-zero number is positive, and so is a square in the real numbers, which makes it natural to say that there are no "-1-adic antisquares".

I won't define the 2-signature just yet, because I don't need to - since it can in fact be recovered from the p-signatures for odd p. So we have an easy statement of the H-M theorem:

Two rational quadratic forms of the same non-zero determinant are equivalent if and only if they have the same p-signatures for all the odd primes (incluing -1).

I'll postpone the proof for now (even though it's not particularly difficult). The way I propose to handle the discussion (in both the rational and integral cases) is

(i) to show how to compute the appropriate invariants
(ii) to say what relations there are between the invariants
(iii) to prove the said relations
(iv) to say to what extent the invariants are complete.
(v) to prove the completeness assertions (if any)
(vi) to prove they actually are invariants.

This seems a rather peculiar order, so I'll say a few words in its defence. My first aim is to empower you to do actual computations and to understand just what's true. Proving that what's true is true is not so important. In fact, this is the way I first learned the theory myself - with some pain I learned what was true without being able to understand why. Some readers may find it interesting to follow the history of my own interaction with quadratic forms, given in the next section.

0.1. **My life with quadratic forms.** There's no special reason for all readers to be interested in this. If you're not, by all means go on to the more substantive sections that follow.

My first introduction to quadratic forms came from knot theory, since some of the invariants of a knot are derived from an integral quadratic form, so it was an important problem to be able to say when two forms should be counted the same.

Later on I had another reason to be interested in quadratic forms, since the simple group I discovered was in fact the automorphism group of the 24-dimensional quadratic form, modulo its center.

In those two applications, I was only a user of the theory, and made no attempt to understand it. But then a paper of Kneser's taught me that for knot-theoretical purposes, what matters about a quadratic form is precisely its genus, so I looked up the two nearly simultaneous papers that characterized the genus. In fact the only difficulty was to understand the 2-adic component of the genus.

They did this in two different ways. One, by Gordon Pall, did so by means of a rather complicated system of invariants. The other, by

Burton W. Jones, instead gave rules for finding a canonical version of a given form. I found a system of invariants that was simpler than Pall's, but still had no hope of understanding what was going on.

Indeed the only way I could prove that my putative invariants actually were invariant was to derive them from Pall's, and the only way I could prove them complete was to show how they sufficed to define Burton Jones's canonical form. So presuming that Pall and Jones had both solved the problem correctly (which I had no idea how to prove), I did indeed have a complete set of invariants, and a characterization of the genus that was simpler than those of both Pall and Jones.

Later on it become still simpler when Cassels told me of a German discovery that the trace of a diagonal form of odd determinant was a 2-adic invariant. This enabled be to give a still simpler system of invariants, though I was still unable to see just why they were invariant.

Still later, Peter Doyle educated me about the solution to the old problem that Mark Kac famously encapsulated in his question "Can you hear the shape of a drum?". This led to the notion of "audible invariant", which for a quadratic form means one whose values can be computed if you know how often each number is represented by the form.

It turned out that nearly all the invariants of quadratic forms were audible, and that the only exceptions were clearly invariant. Moreover, the proof that they were audible was easy (much easier than the old proofs of Pall and Jones).

So after some decades I had managed to understand what was going on. That's why I wrote my book, "THE SENSUAL (quadratic) FORM," and (I suppose) why I was invited to talk to you here.

0.2. **The Connection with Quadratic Reciprocity.** I recall Legendre's definition of his symbol $(a\,|\,p)$ (usually written vertically with a above p). It is defined for odd positive prime p, and a prime to p, and takes the value $+1$ if a is a square modulo p, and -1 otherwise. Jacobi extended this to the case when the "denominator" is a product of odd primes by defining $(a\,|\,pqr\ldots)$, when a is prime to $pqr\ldots$, to be $(a\,|\,p)(a\,|\,q)(a\,|\,r)\cdots$, a somewhat unilluminating definition that we'll stick with for now.

The values of both these symbols lie in the standard multiplicative group of order 2, namely $\{1,-1\}$. When working with p-signatures, which usually take values modulo 8, it is convenient to change this value set to the additive group $\{0,4\}$ of numbers modulo 8. So I'll define the linear Legendre and Jacobi symbols by $[a\,|\,p]$ or $[a\,|\,pqr...]$ to be 0 or 4 $\pmod 8$ according as $(a\,|\,p)$ or $(a\,|\,pqr\ldots)$ is 1 or -1.

In this notation, the original statement of quadratic reciprocity takes the form

$$[p \,|\, q] + [q \,|\, p] = (p-1)(q-1)$$

where p and q are distinct positive odd primes, but we can generalize it, first trivially to include -1 as a prime, and later to replace p and q by disjoint sets of odd primes.

Now any non-zero number A is a product of powers of primes, where we are including -1 as a prime. I define $p(A)$, the p-part of A, to be the power of p in this, and $p'(A)$, the p'-part of A, to be $A/p(A)$, the product of the powers of the remaining primes. Notice that the linear Jacobi symbol $[p'(A) \,|\, p(A)]$ take the value $4 \pmod 8$ just when A is a p-adic antisquare, and $0 \pmod 8$ otherwise.

This means that our definition of the p-signature for positive odd p can be recast in the form

$$p(A) + [p'(A) \,|\, p(A)] + p(B) + [p'(B) \,|\, p(B)] + \cdots,$$

which works also for $p = -1$ when we define $[x \,|\, -1]$ to be 0 for positive x as is natural because positive numbers are squares in the reals (i.e., in "the -1-adic numbers").

It is convenient to define also the p-excess of f to be its p-signature minus its dimension, which can be written

$$p(A) - 1 + [p'(A) \,|\, p(A)] + p(B) - 1 + [p'(B) \,|\, p(B)] + \cdots$$

All of these notions can be generalized by replacing p by any set PI of odd primes. So the PI-excess is

$$PI(A) - 1 + [PI'(A) \,|\, PI(A)] + PI(B) - 1 + [PI'(B) \,|\, PI(B)] + \cdots$$

Now quadratic reciprocity tells us that this is an additive function of the set PI of odd primes! It suffices to prove this for a 1-dimensional form, say Ax^2. To see this, if PI and QI are disjoint sets of odd primes, let $A = PQR$, where $P = PI(A)$ and $Q = QI(A)$. Then the PI-excess of the form Ax^2 is

$$P - 1 + [QR \,|\, P] = P - 1 + [Q \,|\, P] + [R \,|\, P]$$

while the QI-excess is

$$Q - 1 + [PR \,|\, Q] = Q - 1 + [P \,|\, Q] + [R \,|\, Q].$$

We shall show that the sum of these is the $(PI \cup QI)$-excess, namely

$$PQ - 1 + [R \,|\, PQ] = PQ - 1 + [R \,|\, P] + [R \,|\, Q].$$

For, the difference between this expression and the sum of the first two is $(P-1)(Q-1) - [Q \,|\, P] - [P \,|\, Q]$, which vanishes by quadratic reciprocity.

This establishes the additivity result that the sum of the excesses for any two disjoint sets of odd primes is the excess for their union. We can extend this additivity to sets that may include 2, simply by defining the PI-excess for such a PI form to be the negative of the PI'-excess, where PI' is the complementary set of (necessarily odd) primes!

This may seem like cheating, but let us examine the 2-excess for the form Ax^2, where A is an odd number (say d) times a power of 2 (say 2^n). It is obtained by subtracting

$$d + n[d\,|\,2]$$

from 1. Now the conventional Jacobi symbol $(d\,|\,2)$ is 1 or -1 according as d has the form $8k \pm 1$ or $8k \pm 3$. So if we call A a 2-adic antisquare just when n is odd and d has form $8k \pm 3$ we see that $d + n[d\,|\,2]$ is what was called the oddity of the form Ax^2 in the SqF, which was a 2-adic invariant. Adding this result for $A, B, C, \ldots$ we see that the 2-excess of an arbitrary form $Ax^2 + By^2 + \cdots$ is its dimension minus its oddity.

I summarize what our definitions have achieved for those who are getting a bit lost. The oddity of an arbitrary form $Ax^2 + By^2 + \cdots$ is the sum of the odd parts $2'(A), 2'(B), \ldots$ minus 4 times the number of 2-adic antisquares among them. It is a 2-adic invariant, and the 2-excess of a form is its dimension minus its oddity. The sum of the p-excesses over all the primes in some set PI is the PI-excess, which is 0 (mod 8) when PI is the set of all primes (including -1 and 2). This result equivalent to quadratic reciprocity.

So much for the facts in the rational case. We now turn to the problem of describing the invariants of a quadratic form under integral equivalents. Once again again, these are "p-adic", but this time they are invariants of the form under p-adic integral transformations.

The rational and integral cases are in one way similar, namely that in either case each of our invariants is actually a p-adic invariant for some prime p (possibly -1). They fundamentally differ in that the p-adic invariants are a complete system of invariants for rational equivalence, whereas for integral equivalence we have only the result that there are only finitely many forms having the same invariants as a given one. These forms comprise what is termed a genus.

Once again, we can define them without actually needing to understand the bogeyman word "p-adic". We concentrate first on the case when p is odd. Then (see the Appendix) it is in fact possible to diagonalize the form without ever needing to divide by 2. (This is "a rational p-adic diagonalization.")

Now sort the diagonal terms according to the power of p that they contain, say as

$$[a_1, a_2, \ldots] + p[b_1, b_2, b_3, \ldots] + \cdots + q[c_1, c_2, c_3, \ldots] + \cdots$$

where q ranges over all the distinct powers of p, and none of the numbers

$$a_1, \ldots, b_1, \ldots, \ldots, c_1, \ldots, \ldots$$

has denominator divisible by p. We'll write this as

$$1.f1 + p.fp + \cdots + q.fq + \cdots$$

and call the forms $q.fq$ the Jordan constituents of f.

In the general case when p is a positive odd prime there are infinitely many distinct powers of p, and so most of the Jordan constituents will have dimension 0. These 0-dimensional forms are called "love forms" (think of tennis!) and have determinant 1.

In the case $p = -1$, there are only two distinct powers of p, (namely 1 and -1, which we abbreviate just to $+$ and $-$), so the Jordan decomposition has only two terms, and we write it $f + -f-$. Moreover, in this case we interpret "A is divisible by p" as meaning "A is negative", so that $f+$ and $f-$ are positive-definite forms.

The p-adic invariants are easily read from the Jordan decomposition. They are, for each power q of p, what we call "the q-dimension", namely $nq = \dim(fq)$, and what we call "the q-sign", which is the Legendre symbol $sq = (\det(fq)\,|\,p)$. We combine all these into a single symbol, which when p is a positive odd prime takes the form

$$1^{n1s1} \cdot p^{npsp} \cdot \cdots \cdot q^{nqsq} \cdot \cdots$$

When $p = -1$, the determinants of $f+$ and $f-$ are positive, and so are squares in the "-1-adic integers". This means that we should consider both signs $s+$ and $s-$ to be 1, and the symbol simplifies just to

$$+^{n+}.\ -^{n-}\ .$$

Let's consider the form $\text{diag}[-1, 2, -3, 4, -5, 6, -7, 8, -9]$ as an example. For $p = -1$, the Jordan decomposition is

$$+\,\text{diag}[2, 4, 6, 8] - \text{diag}[1, 3, 5, 7, 9]$$

and so the -1-symbol is $+^4.-^5$.

For $p = 3$ the decomposition is

$$1.\,\text{diag}[-1, 2, 4, -5, -7, 8] + 3.\,\text{diag}[-1, 2] + 9.\,\text{diag}[-1]$$

whose dimensions are $6, 2$, and 1. Now for

$$a = -1, 2, 4, -5, -7, 8 \quad \text{or} \quad -1, 2 \quad \text{or} \quad -1$$

the Legendre symbol $(a \,|\, 3)$ is respectively

$$- - + + - - \quad \text{or} \quad -, \quad - \quad \text{or} \quad -,$$

and so the 1-sign, 3-sign and 9-sign are the appropriate products of these, namely $+, +$ and $-$. The 3-symbol is therefore

$$1^{6+}.3^{2+}.9^{1-}.$$

The 5-symbol is $1^{8+}.5^{1+}$, and the 7-symbol $1^{8-}.7^{1-}$.

For larger odd p, the symbol takes the form $1^{\mathrm{dim}\,.\,\mathrm{sign}}$, where "dim" is the dimension (so 9 in this example), and the sign is the Legendre symbol of the determinant which is $(-9! \,|\, p)$ here. Things always simplify this way for a positive odd prime that does not divide the determinant, so we usually ignore such primes.

All the "p-symbols" for odd p that we have defined are integral invariants of our form, and they comprise all the p-adic invariants for odd p. The "2-symbol" that we define in the next section, is only an invariant modulo the equivalences we consider there, but taking those into account, is a complete 2-adic invariant for the form.

Taken together, ALL the p-symbols form a complete system of invariants for the genus.

0.3. **The 2-adic invariants. (Advice: omit at first reading!)** We cannot hope to diagonalize every form over the 2-adic integers. But the Appendix shows how to express it as a direct sum of forms of dimension either 1 or 2, each of which is a power of 2 (say q) times a form of odd determinant (say d), and when the dimension is 2, have even diagonal terms.

This still gives us a Jordan decomposition, say

$$1.f1 + 2.f2 + 4.f4 + \cdots$$

where now for the typical constituent $q.fq$ we may need to know not only:

its scale, q its dimension, $nq = \dim(fq)$ its sign, $sq =$ the Jacobi symbol $(2 \,|\, \det(fq))$ but also whether it's an even form (i.e., its diagonal terms are all even) and otherwise (when the form is called odd) also its "oddity" tq (meaning the trace of a diagonalized version, considered modulo 8).

Whether a form is even or odd is called its "parity", and conventionally, we define the diagonal trace to be infinity for an even form, so that all these quantities are conveyable by the single symbol

$$q_{tq}^{nqsq},$$

and when we vary q over all powers of 2, by the "2-symbol" which is the formal product of such expressions for $q = 1, 2, 4, \ldots$

The part of this symbol corresponding to one such q is indeed an invariant of the Jordan constituent $q.fq$ under integral 2-adic equivalence, so the 2-symbol does indeed convey the 2-adic equivalence class.

But the 2-symbol is not actually an invariant of the entire form, because a form can have two 2-adic Jordan decompositions, say

$$1.f1 + 2.f2 + 4.f4 + \cdots \quad \text{and} \quad 1.g1 + 2.g2 + 4.g4 + \cdots$$

in which the individual Jordan consituents $q.fq$ and $q.gq$ fail to be 2-adically equivalent. [Their scales, dimensions and parities of $q.fq$ and $q'gq$ are, however, equal.]

The possible equalities between distinct Jordan decompositions are obtained by combing two "moves", which I call "oddity-fusion" and "sign-walking".

Oddity fusion: If for a consecutive block of powers of 2, all the forms

$$fq, f2q, \ldots, fQ/2, fQ$$

are odd, then we can replace their individual oddities

$$tq, t2q, \ldots, tQ \quad \text{by their sum} \quad tq + t2q + \cdots + tQ$$

without losing any information. We do this by removing the subscripts from the appropriate parts of the 2-symbol, and instead putting their sum as a subscript to a bracket placed around them.

Sign-walking (to be finished later).

Department of Mathematics, Princeton University, Princeton, NJ