15

On the Classification of Integral Quadratic Forms

J. H. Conway and N. J. A. Sloane

This chapter gives an account of the classification of integral quadratic forms. It is particularly designed for readers who wish to be able to do explicit calculations. Novel features include an elementary system of rational invariants (defined without using the Hilbert norm residue symbol), an improved notation for the genus of a form, an efficient way to compute the number of spinor genera in a genus, and some conditions which imply that there is only one class in a genus. We give tables of the binary forms with $-100 \leqslant \det \leqslant 50$, the indecomposable ternary forms with $|\det| \leqslant 50$, the genera of forms with $|\det| \leqslant 11$, the genera of p-elementary forms for all p, and the positive definite forms with determinant 2 up to dimension 18 and determinant 3 up to dimension 17.

1. Introduction

The project of classifying integral quadratic forms has a long history, to which many mathematicians have contributed. The binary (or two-dimensional) forms were comprehensively discussed by Gauss. Gauss and later workers also made substantial inroads into the problem of ternary and higher-dimensional forms. The greatest advances since then have been the beautiful development of the theory of rational quadratic forms (Minkowski, Hasse, Witt), and Eichler's complete classification of indefinite forms in dimension 3 or higher in terms of the notion of spinor genus.

Definite forms correspond to lattices in Euclidean space. For small dimensions they can be classified using Minkowski's generalization of Gauss's notion of reduced form, but this method rapidly becomes impracticable when the dimension reaches 6 or 7. However there is a geometric method used by Witt and Kneser which (after the work of Niemeier) is effective roughly until the sum of the dimension and the

$(\text{determinant})^{1/2}$ exceeds 24, beyond which point it seems that the forms are inherently unclassifiable. The situation is summarized in Fig. 15.1.

There are several novel features of this chapter.

(1) We present (in §5) an elementary system of rational invariants for quadratic forms, defined without using the Hilbert norm residue symbol, and whose values are certain integers modulo 8. The modulo-8 version of the 2-adic invariant seems to have first arisen in topological investigations (see [Cas1], [Hir4]). Practitioners in the subject know that the effect of the "product formula" is to yield congruence conditions modulo 8 on the signature. With the invariants we use these congruences emerge immediately rather than at the end of a long calculation (see Eqs. (15) and (16)).

(2) We also give a simply described system of p-adic invariants for integral forms that yields a handy notation for the genus of a quadratic form (§7).

(3) In terms of this new notation we enumerate (in §8.1 and Table 15.4) all genera of quadratic forms having determinant of magnitude less than 12, and

(4) classify the genera of p-elementary forms for all p (§8.2).

In view of Eichler's theory of spinor genera (see Theorem 14), these results actually give the integral equivalence classes in the case of indefinite forms of dimension $\geqslant 3$.

(5) We also give a simple description of the spinor genus, including a notation for the various spinor genera in the genus of a given form, and an easy computational way of finding their number (§9).

Dimension	Definite	Indefinite
1	Trivial	Trivial
2	Gauss: reduced forms.	Gauss: cycles of reduced forms.
3	Minkowski:	
.	reduced	
.	forms	
.	...	
7		Eichler:
.	Kneser-	spinor
.	Niemeier	genus
.	gluing	
.	method.	
24	...	
.		
.	Impracticable.	

Figure 15.1 How quadratic forms are classified.

(6) We include some theorems giving conditions under which a genus contains just one class (Theorem 20 and its Corollaries). In particular we show that, if f is an indefinite form of dimension n and determinant d, and there is more than one class in the genus of f, then

$$4^{[\frac{n}{2}]} d \quad \text{is divisible by } k^{\binom{n}{2}} \tag{1}$$

for some nonsquare natural number $k \equiv 0$ or $1 \pmod 4$).
(7) We also give a number of tables:
— reduced binary quadratic forms whose determinant d satisfies $|d| \leqslant 50$ for definite forms, $|d| \leqslant 100$ for indefinite forms (Tables 15.1, 15.2),
— indecomposable ternary forms with $|d| \leqslant 50$ for definite forms and $|d| \leqslant 100$ for indefinite forms (Tables 15.6, 15.7),
— genera of quadratic forms with $|d| < 12$ (Table 15.4),
— definite quadratic forms of determinant 2 and dimension $\leqslant 18$ (15.8),
— definite quadratic forms of determinant 3 and dimension $\leqslant 17$ (15.9).

Our treatment is addressed to a reader who wishes to be able to do explicit calculations while gaining some understanding of the general theory. The chapter is arranged as follows. §§2 and 4 contain definitions and other mathematical preliminaries. §3 deals with binary forms. §§5,6 treat the classification of forms over the rational numbers, and §7 the classification over the p-adic integers and the associated notion of the genus of a form. §8 gives some applications of the results of §7. The spinor genus of a form and the classification of indefinite forms are dealt with in §9, and definite forms in §10. The final section discusses the computational complexity of the classification problem.

2. Definitions

2.1 Quadratic forms. Let x be the row vector (x_1, x_2) and A the symmetric matrix $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$. Then the expression

$$f(x) = xAx^{tr} = ax_1^2 + 2bx_1x_2 + cx_2^2 \tag{2}$$

is called the *binary quadratic form* with matrix A. Calculations with this form often involve the associated *bilinear form*

$$f(x, y) = xAy^{tr} = ax_1y_1 + bx_1y_2 + bx_2y_1 + cx_2y_2 .$$

Replacing A by a symmetric matrix of arbitrary dimension n we obtain the notion of an *n-ary quadratic form* and of an *n-ary symmetric bilinear form* (see §2.2 of Chap. 2). From the very large number of references on quadratic forms let us mention in particular [Bor5], [Cas3], [Cas4], [Coh5], [Dav2a], [Dic2], [Dic3], [Eic1], [Gau1], [Hsi1]-[Hsi9], [Jon3], [Kne1]-[Kne9], [Lam1], [Mil7], [Min0]-[Min3], [O'Me1]-[O'Me4], [Orz1], [Ran3], [Ran5], [Ran5a], [Rie1], [Rys1]-[Rys14], [Sch0]-[Sch2], [Sch13], [Sch14], [Ser1], [Smi5], [Smi6], [Tau2], [Wae5], [Wat3]-[Wat22], [Wit1], [Zag1].

We are concerned with the classification of integral quadratic forms under integral equivalence. There are two definitions of integrality for a quadratic form. The binary form (2) is *integral as a quadratic form* if a, $2b$ and c belong to $\mathbf{Z}$, and *integral as a symmetric bilinear form* if its matrix entries a, b, c belong to $\mathbf{Z}$. The latter is the definition used by Gauss [Gau1]; Cassels [Cas3] calls such a form *classically integral*. Although some authors hold strong opinions about which definition of integrality should be used (Watson [Wat3] refers to "Gauss's mistake of introducing binomial coefficients into the notation"), it makes very little difference for the classification theory. The two definitions are not really rivals but collaborators. For if f is integral in either sense then $2f$ is integral in the other sense, and f is equivalent to g if and only if $2f$ is equivalent to $2g$. Since for algebraic purposes a form is usually most conveniently specified by its matrix entries, we prefer the second definition, and so in this book we call f an *integral form* if and only if its matrix entries are integers (i.e. if and only if it is classically integral, or integral as a symmetric bilinear form).

2.2 Forms and lattices; integral equivalence. Some geometric ideas are appropriate. We consider a rational vector space V with inner product $(\ ,\ )$ and refer to (x, x) as the *norm* of x. If V is 2-dimensional, and spanned by vectors e_1 and e_2 with

$$(e_1, e_1) = a, \quad (e_1, e_2) = b, \quad (e_2, e_2) = c\ ,$$

then the norm of the vector $x = x_1e_1 + x_2e_2$ is just $f(x)$, and its inner product with the vector $y = y_1e_1 + y_2e_2$ is $f(x, y)$.

The vectors $x = x_1e_1 + x_2e_2$ for which x_1 and x_2 are integers form a *lattice* in V, and e_1, e_2 is an *integral basis* for this lattice. The other integral bases for this lattice have the form $\alpha e_1 + \beta e_2$, $\gamma e_1 + \delta e_2$, where $\alpha, \beta, \gamma, \delta$ are integers with $\alpha\delta - \beta\gamma = \pm 1$. We shall therefore call two binary forms f and g with matrices A and B *integrally equivalent*, or say they are in the same *class*, and write $f \sim g$, if there exists a matrix

$$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \qquad (3)$$

with integer entries and determinant ± 1 for which $B = MAM^{tr}$. Geometrically, f and g refer to the same lattice with different integral bases. The equivalence is *proper* if $\det M = +1$, *improper* if $\det M = -1$.

The general case is exactly similar (§2.2 of Chap. 2). A symmetric matrix $A = (a_{ij})$ with integer entries determines a (classically) integral form f, whose values are the norms of the members of a lattice Λ (in an n-dimensional vector space) that has an integral basis $e_1, \ldots, e_n$ with $(e_i, e_j) = a_{ij}$. If $M = (m_{ij})$ has integer entries then the vectors $e_1{}' = \Sigma m_{1j}e_j$, ..., $e_n{}' = \Sigma m_{nj}e_j$ will generate a sublattice of Λ, and this will be all of Λ if and only if M^{-1} has integer entries; this happens if and only if $\det M = \pm 1$.

We therefore say that two n-ary forms f and g with matrices A and B are (*properly* or *improperly*) *integrally equivalent* if their matrices are related by

$$B = M A M^{tr} \tag{4}$$

for some M with integer entries and determinant $+1$ or -1 respectively.

It is clear that the number $d = \det A$ is an invariant of f for integral equivalence (i.e. if f and g are integrally equivalent, $\det A = \det B$), and we shall call d the *determinant* of f. The reader should be aware that many authors use the term *discriminant* for this number multiplied by certain powers of 2 and -1 that depend on the dimension (and the author).

In practice, when transforming f into an equivalent form, we derive the matrix B from A by performing elementary row operations (multiplying a row by a unit or adding multiples of one row to another), followed by the exactly corresponding column operations.

These notions can be immediately generalized to arbitrary rings R (with 1). A form f is defined over R if it is represented by a matrix A with entries from R, and two forms f and g are equivalent over R if (4) holds for some M with entries from R and with a determinant which is a unit of R (i.e. an element of R with an inverse in R). For example, taking R to be the rational numbers $\mathbf{Q}$, we see that the forms $x^2 + y^2$, $2z^2 + 2t^2$, although not integrally equivalent, are rationally equivalent, as shown by the formulae

$$x = z + t, \ z = ½ (x + y) ,$$
$$y = z - t, \ t = ½ (x - y) .$$

If f and g are rationally equivalent, the ratio of their determinants is the square of a nonzero rational number.

3. The classification of binary quadratic forms

Almost everything one can say about the classification of binary quadratic forms was already said by Gauss in his *Disquisitiones arithmeticae* [Gau1]. The complete classification in the indefinite binary case uses cycles of reduced forms, and is totally unlike Eichler's complete classification of indefinite forms in dimensions $\geqslant 3$. A very clear account has recently been given by Edwards [Edw1], who also discusses the connections with the ideal theory of quadratic number rings, and so here we shall only present the results, together with a brief indication of these connections. Other treatments of the binary case may be found in [Cas3], [Dav1], [Jon3], [LeV1], [Wat3], [Zag1], etc.

3.1 Cycles of reduced forms

Theorem 1 (Quoted with changes in notation from [Edw1, p. 325].)

Let $\begin{bmatrix} a_0 & b_0 \\ b_0 & a_1 \end{bmatrix}$ *(abbreviated* $a_0 {}^{b_0} a_1$*) be an integral binary quadratic form of* *determinant* $d = a_0 a_1 - b_0^2$, *and suppose that* $-d$ *is not a square. We define a sequence*

$$\begin{bmatrix} a_0 & b_0 \\ b_0 & a_1 \end{bmatrix}, \begin{bmatrix} a_1 & b_1 \\ b_1 & a_2 \end{bmatrix}, \ldots, \begin{bmatrix} a_i & b_i \\ b_i & a_{i+1} \end{bmatrix}, \ldots \tag{5}$$

(*abbreviated*

$$a_0 \overset{b_0}{} a_1 \overset{b_1}{} a_2 \ldots a_i \overset{b_i}{} a_{i+1} \ldots)$$

of binary forms of determinant d *by the rules*:

a_i *and* b_i *determine* a_{i+1} *as* $\dfrac{b_i^2+d}{a_i}$,

b_i *and* a_{i+1} *determine* b_{i+1} *as the largest solution of*

$$b_i + b_{i+1} \equiv 0 \pmod{a_{i+1}} \tag{6}$$

for which

$$b_{i+1}^2 + d < 0 \tag{7}$$

if such solutions exist, and otherwise as the smallest solution of (6) *in absolute value, taking* b_{i+1} *positive in case of a tie.*

Then the sequence of forms derived in this way from the given form is ultimately periodic, the forms in the period being called a cycle of reduced forms. *Furthermore two binary forms are properly equivalent if and only if they lead to the same cycle of reduced forms.*

The condition that $-d$ be not a square implies that the a_i are nonzero, and so a_{i+1} and b_{i+1} are well-defined. Only minor modifications are required when $-d$ is a square — see §3.3.

As an example, the sequence of forms arising from $x^2 - 67y^2$ is

$$\begin{array}{ccccccccccccccccccccccccccc} & 0 & & 0 & & 8 & & 7 & & 5 & & 2 & & 7 & & 7 & & 2 & & 5 & & 7 & & 8 & & 8 & \\ +1 & & -67 & & +1 & & -3 & & +6 & & -7 & & +9 & & -2 & & +9 & & -7 & & +6 & & -3 & & +1 & & -3\ldots \end{array} \tag{8}$$

There are ten reduced forms in the cycle. On the other hand $-x^2 + 67y^2$ leads to the disjoint sequence obtained by changing the signs of the lower terms in (8) (the a_i's), and is therefore an inequivalent form.

3.2 Definite binary forms. In the case of a definite (say positive definite) binary form, it follows from Theorem 1 that the cycle contains either a single form

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix}, \quad \text{with } b = 0 \text{ or } 2b = |a|\,, \tag{9}$$

or else two forms

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}, \begin{bmatrix} c & -b \\ -b & a \end{bmatrix}. \tag{10}$$

The term reduced is normally applied only to the single form (9) or to whichever of the pair (10) satisfies

$$(1,1) \text{ entry} < (2,2) \text{ entry} , \text{ or } a = c \text{ and } b > 0 .$$

It is not difficult to show that a positive definite form $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ is reduced in this sense if and only if it satisfies

$$-a < 2b \leqslant a \leqslant c, \text{ with } b \geqslant 0 \text{ if } a = c \qquad (11)$$

[Dic3, Theorem 99], [Jon3, Theorem 76]. Furthermore every positive definite form is properly equivalent to a unique such reduced form. Since (11) implies $b^2 \leqslant d/3$, all reduced forms are easily enumerated: for each b with $|b| \leqslant \sqrt{d/3}$ we factor $d+b^2 = ac$ in all possible ways consistent with (11) (see Table 15.1).

The reduction condition (11) expresses the fact that

a is the absolutely smallest value taken (at a vector e_1 say) by the form, and

c is the absolutely smallest value that can be taken by the form at a vector e_2 independent of e_1.

An appropriate generalization of these conditions to higher dimensions leads to the notion of a Minkowski reduced form (see §10.1).

(11) is also equivalent to the assertion that the root $z = x/y$ of $f(x,y) = 0$ in the upper half plane lies in the region $|z| \geqslant 1$, $-\frac{1}{2} \leqslant \operatorname{Re} z \leqslant \frac{1}{2}$ shaded in Fig. 15.2. As the form undergoes unimodular transformations

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbf{Z}) ,$$

i.e. with $\alpha, \beta, \gamma, \delta \in \mathbf{Z}$ and $\alpha\beta - \gamma\delta = 1$, this root transforms into $\dfrac{\alpha z+\beta}{\gamma z+\delta}$,

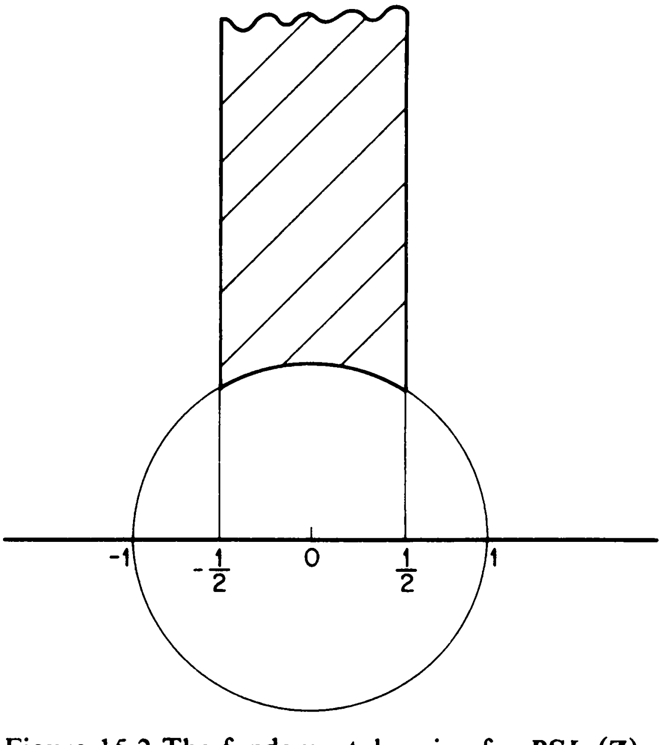

Figure 15.2 The fundamental region for $PSL_2(\mathbf{Z})$.

and the region mentioned is a fundamental region for the action of $SL_2(\mathbb{Z})$ on the upper half plane (see for example [LeV1, Vol. 1, Chap. 1]). This notion also generalizes to higher dimensions, and it is an important theorem that in the generalization the fundamental region has only finitely many walls (which correspond to inequalities on the matrix entries of the form).

3.3 Indefinite binary forms. In the indefinite case, supposing that $-d$ is not a square, it can be shown from Theorem 1 that the reduced forms (those in the cycle) are precisely the ones satisfying

$$0 < b < \sqrt{-d} < \min\{\, b+|a|,\ b+|c| \,\} \tag{12}$$

[Gau1, §183]. Again the reduced forms are easily found: for each positive integer $b < \sqrt{-d}$ we factor $d+b^2 = ac$ in all possible ways satisfying (12).

When $-d$ is a square, Theorem 1 must be modified slightly, and in particular the inequality in (7) must be replaced by $\leqslant$. Then the process of Theorem 1 terminates in a form $\begin{bmatrix} a & b \\ b & 0 \end{bmatrix}$ with $b = \sqrt{-d}$. If the process is extended *backwards* it terminates in a form $\begin{bmatrix} 0 & b \\ b & c \end{bmatrix}$. Gauss [Gau1, §§206-210] proved that two forms $\begin{bmatrix} a & b \\ b & 0 \end{bmatrix}$, $\begin{bmatrix} a' & b \\ b & 0 \end{bmatrix}$ are properly equivalent if and only if $a \equiv a' \pmod{2b}$, and are improperly equivalent if and only if

$$aa' \equiv \gcd(a,b)^2 \pmod{2b\gcd(a,b)}\ .$$

We therefore extend the notion of reduced form in this case to include, besides the forms satisfying (12), all forms of the shape

$$0\ {}^{b}\ a \quad \text{or} \quad a\ {}^{b}\ 0 \quad (-b < a \leqslant b)\ .$$

Then the "cycle" of reduced forms becomes a finite sequence

$$0\ {}^{b_0}\ a_1\ {}^{b_1}\ a_2\ {}^{b_2} \ldots\ a_k\ {}^{b_0}\ 0\ .$$

Gauss declared that tables of binary quadratic forms should not be published, since they are so easily computed [Leh1, p. 69]. Nevertheless we feel the usefulness of our paper is enhanced by Tables 15.1 and 15.2, which enumerate *all* reduced binary quadratic forms with $-100 \leqslant d \leqslant 50$. The notation is that introduced in Theorem 1. Table 15.1 gives the positive definite forms with $d \leqslant 50$, and Table 15.2 the cycles of reduced indefinite forms. In Table 15.2 four related cycles

$$\ldots +a\ {}^{b} -c\ {}^{d} +e\ {}^{f} -g\ {}^{h} \ldots$$
$$\ldots -a\ {}^{b} +c\ {}^{d} -e\ {}^{f} +g\ {}^{h} \ldots$$
$$\ldots {}^{h} +g\ {}^{f} -e\ {}^{d} +c\ {}^{b} -a \ldots$$
$$\ldots {}^{h} -g\ {}^{f} +e\ {}^{d} -c\ {}^{b} +a \ldots$$

Table 15.1. **Reduced positive definite binary forms.**

d	Forms
1	$1^{0}1$
2	$1^{0}2$
3	$1^{0}3$, $2^{1}2$
4	$1^{0}4$, $2^{0}2$
5	$1^{0}5$, $2^{1}3$
6	$1^{0}6$, $2^{0}3$
7	$1^{0}7$, $2^{1}4$
8	$1^{0}8$, $2^{0}4$, $3^{1}3$
9	$1^{0}9$, $3^{0}3$, $2^{1}5$
10	$1^{0}10$, $2^{0}5$
11	$1^{0}11$, $2^{1}6$, $3^{\pm1}4$
12	$1^{0}12$, $2^{0}6$, $3^{0}4$, $4^{2}4$
13	$1^{0}13$, $2^{1}7$
14	$1^{0}14$, $2^{0}7$, $3^{\pm1}5$
15	$1^{0}15$, $3^{0}5$, $2^{1}8$, $4^{1}4$
16	$1^{0}16$, $2^{0}8$, $4^{0}4$, $4^{2}5$
17	$1^{0}17$, $2^{1}9$, $3^{\pm1}6$
18	$1^{0}18$, $2^{0}9$, $3^{0}6$
19	$1^{0}19$, $2^{1}10$, $4^{\pm1}5$
20	$1^{0}20$, $2^{0}10$, $4^{0}5$, $3^{\pm1}7$, $4^{2}6$
21	$1^{0}21$, $3^{0}7$, $2^{1}11$, $5^{2}5$
22	$1^{0}22$, $2^{0}11$
23	$1^{0}23$, $2^{1}12$, $3^{\pm1}8$, $4^{\pm1}6$
24	$1^{0}24$, $2^{0}12$, $3^{0}8$, $4^{0}6$, $5^{1}5$, $4^{2}7$
25	$1^{0}25$, $5^{0}5$, $2^{1}13$
26	$1^{0}26$, $2^{0}13$, $3^{\pm1}9$, $5^{\pm2}6$
27	$1^{0}27$, $3^{0}9$, $2^{1}14$, $4^{\pm1}7$, $6^{3}6$
28	$1^{0}28$, $2^{0}14$, $4^{0}7$, $4^{2}8$
29	$1^{0}29$, $2^{1}15$, $3^{\pm1}10$, $5^{\pm1}6$
30	$1^{0}30$, $2^{0}15$, $3^{0}10$, $5^{0}6$
31	$1^{0}31$, $2^{1}16$, $4^{\pm1}8$, $5^{\pm2}7$
32	$1^{0}32$, $2^{0}16$, $4^{0}8$, $3^{\pm1}11$, $4^{2}9$, $6^{2}6$
33	$1^{0}33$, $3^{0}11$, $2^{1}17$, $6^{3}7$
34	$1^{0}34$, $2^{0}17$, $5^{\pm1}7$
35	$1^{0}35$, $5^{0}7$, $2^{1}18$, $3^{\pm1}12$, $4^{\pm1}9$, $6^{1}6$
36	$1^{0}36$, $2^{0}18$, $3^{0}12$, $4^{0}9$, $6^{0}6$, $4^{2}10$, $5^{\pm2}8$
37	$1^{0}37$, $2^{1}19$
38	$1^{0}38$, $2^{0}19$, $3^{\pm1}13$, $6^{\pm2}7$
39	$1^{0}39$, $3^{0}13$, $2^{1}20$, $4^{\pm1}10$, $5^{\pm1}8$, $6^{3}8$
40	$1^{0}40$, $2^{0}20$, $4^{0}10$, $5^{0}8$, $4^{2}11$, $7^{3}7$
41	$1^{0}41$, $2^{1}21$, $3^{\pm1}14$, $6^{\pm1}7$, $5^{\pm2}9$
42	$1^{0}42$, $2^{0}21$, $3^{0}14$, $6^{0}7$
43	$1^{0}43$, $2^{1}22$, $4^{\pm1}11$
44	$1^{0}44$, $2^{0}22$, $4^{0}11$, $3^{\pm1}15$, $5^{\pm1}9$, $4^{2}12$, $6^{\pm2}8$
45	$1^{0}45$, $3^{0}15$, $5^{0}9$, $2^{1}23$, $7^{2}7$, $6^{3}9$
46	$1^{0}46$, $2^{0}23$, $5^{\pm2}10$
47	$1^{0}47$, $2^{1}24$, $3^{\pm1}16$, $4^{\pm1}12$, $6^{\pm1}8$, $7^{\pm3}8$
48	$1^{0}48$, $2^{0}24$, $3^{0}16$, $4^{0}12$, $6^{0}8$, $7^{1}7$, $4^{2}13$, $8^{4}8$
49	$1^{0}49$, $7^{0}7$, $2^{1}25$, $5^{\pm1}10$
50	$1^{0}50$, $2^{0}25$, $5^{0}10$, $3^{\pm1}17$, $6^{\pm2}9$

are all represented in the table by a single entry

$$\dots a\,{}^{b}\,c\,{}^{d}\,e\,{}^{f}\,g\,{}^{h}\ \dots .$$

In restoring the signs it is helpful to note that the lower digits alternate in sign. Some care is needed in recovering the original cycles, because some of the four cycles just mentioned may coincide, and so an entry in the table may represent one, two or four cycles. We have used ordinary parentheses ( ) and curly brackets { } to further reduce the size of the table. Entries bounded by parentheses indicate whole or half periods. Thus for $d = -99$ the entry

$$(5\,{}^{8}\,7\,{}^{6}\,9\,{}^{3}\,10\,{}^{7})$$

represents the four distinct cycles

$$\dots 5\,{}^{8}\,{-7}\,{}^{6}\,9\,{}^{3}\,{-10}\,{}^{7}\,5\,{}^{8}\,{-7} \dots$$

$$\dots {-5}\,{}^{8}\,7\,{}^{6}\,{-9}\,{}^{3}\,10\,{}^{7}\,{-5}\,{}^{8}\,7 \dots$$

$$\dots 7\,{}^{8}\,{-5}\,{}^{7}\,10\,{}^{3}\,{-9}\,{}^{6}\,7\,{}^{8}\,{-5} \dots$$

$$\dots {-7}\,{}^{8}\,5\,{}^{7}\,{-10}\,{}^{3}\,9\,{}^{6}\,{-7}\,{}^{8}\,5 \dots$$

However, the entry

$$(3\,{}^{5}\,4\,{}^{3}\,7\,{}^{4})$$

for $d = -37$ yields only two inequivalent cycles, namely

$$\dots 3\,{}^{5}\,{-4}\,{}^{3}\,7\,{}^{4}\,{-3}\,{}^{5}\,4\,{}^{3}\,{-7}\,{}^{4}\,3\,{}^{5}\,{-4} \dots$$

and its reversal. Most entries in the table are contained within curly brackets, which indicate reflections about the outermost digits. Thus for $d = -13$ the entry

$$\{1\,{}^{3}\,4\,{}^{1}\,3\,{}^{2}\}$$

represents the single cycle

$$\dots 1\,{}^{3}\,{-4}\,{}^{1}\,3\,{}^{2}\,{-3}\,{}^{1}\,4\,{}^{3}\,{-1}\,{}^{3}\,4\,{}^{1}\,{-3}\,{}^{2}\,3\,{}^{1}\,{-4}\,{}^{1}\,1\,{}^{3}\,{-4} \dots$$

while for $d = -14$,

$$\{1\,{}^{3}\,5\,{}^{2}\,2\}$$

represents the two cycles

$$\dots 1\,{}^{3}\,{-5}\,{}^{2}\,2\,{}^{2}\,{-5}\,{}^{3}\,1\,{}^{3}\,{-5} \dots$$

and

$$\dots {-1}\,{}^{3}\,5\,{}^{2}\,{-2}\,{}^{2}\,5\,{}^{3}\,{-1}\,{}^{3}\,5 \dots .$$

Table 15.2a. Reduced indefinite binary forms.

d	Forms
−1	$0^{1}\}$, $0^{1}1\}$
−2	$\{1^{1}\}$
−3	$\{1^{1}2\}$
−4	$0^{2}\}$, $0^{2}1\}$, $0^{2}2\}$
−5	$\{1^{2}\}$, $\{2^{1}\}$
−6	$\{1^{2}2\}$
−7	$\{1^{2}3^{1}2\}$
−8	$\{1^{2}4\}$, $\{2^{2}\}$
−9	$0^{3}\}$, $0^{3}1\}$, $0^{3}2\}$, $0^{3}3\}$
−10	$\{1^{3}\}$, $\{2^{2}3^{1}\}$
−11	$\{1^{3}2\}$
−12	$\{1^{3}3\}$, $\{2^{2}4\}$
−13	$\{1^{3}4^{1}3^{2}\}$, $\{2^{3}\}$
−14	$\{1^{3}5^{2}2\}$
−15	$\{1^{3}6\}$, $\{2^{3}3\}$
−16	$0^{4}\}$, $0^{4}1\}$, $0^{4}2\}$, $0^{4}3^{2}4\}$, $0^{4}4\}$
−17	$\{1^{4}\}$, $\{2^{3}4\}$
−18	$\{1^{4}2\}$, $\{3^{3}\}$
−19	$\{1^{4}3^{2}5^{3}2\}$
−20	$\{1^{4}4\}$, $\{2^{4}\}$, $\{4^{2}\}$
−21	$\{1^{4}5^{1}4^{3}3\}$, $\{2^{3}6\}$
−22	$\{1^{4}6^{2}3^{4}2\}$
−23	$\{1^{4}7^{3}2\}$
−24	$\{1^{4}8\}$, $\{2^{4}4\}$, $\{3^{3}5^{2}4\}$
−25	$0^{5}\}$, $0^{5}1\}$, $0^{5}2\}$, $0^{5}3^{4}\}$, $0^{5}4^{3}\}$, $0^{5}5\}$
−26	$\{1^{5}\}$, $\{2^{4}5^{1}\}$
−27	$\{1^{5}2\}$, $\{3^{3}6\}$
−28	$\{1^{5}3^{4}4\}$, $\{2^{4}6^{2}4\}$
−29	$\{1^{5}4^{3}5^{2}\}$, $\{2^{5}\}$
−30	$\{1^{5}5\}$, $\{2^{4}7^{3}3\}$
−31	$\{1^{5}6^{1}5^{4}3^{5}2\}$
−32	$\{1^{5}7^{2}4\}$, $\{2^{4}8\}$, $\{4^{4}\}$
−33	$\{1^{5}8^{3}3\}$, $\{2^{5}4^{3}6\}$
−34	$\{1^{5}9^{4}2\}$, $\{^{5}3^{4}6^{2}5^{3}\}$
−35	$\{1^{5}10\}$, $\{2^{5}5\}$
−36	$0^{6}\}$, $0^{6}1\}$, $0^{6}2\}$, $0^{6}3\}$, $0^{6}4\}$, $0^{6}5^{4}4\}$, $0^{6}6\}$
−37	$\{1^{6}\}$, $\{2^{5}6^{1}\}$, $(3^{5}4^{3}7^{4})$
−38	$\{1^{6}2\}$
−39	$\{1^{6}3\}$, $\{2^{5}7^{2}5^{3}6\}$
−40	$\{1^{6}4\}$, $\{2^{6}\}$, $\{5^{5}3^{4}8\}$, $\{4^{4}6^{2}\}$
−41	$\{1^{6}5^{4}\}$, $\{2^{5}8^{3}4^{5}\}$
−42	$\{1^{6}6\}$, $\{2^{6}3\}$
−43	$\{1^{6}7^{1}6^{5}3^{4}9^{5}2\}$
−44	$\{1^{6}8^{2}5^{3}7^{4}4\}$, $\{2^{6}4\}$
−45	$\{1^{6}9^{3}4^{5}5\}$, $\{2^{5}10\}$, $\{3^{6}\}$, $\{6^{3}\}$
−46	$\{1^{6}10^{4}3^{5}7^{2}6^{4}5^{6}2\}$
−47	$\{1^{6}11^{5}2\}$
−48	$\{1^{6}12\}$, $\{2^{6}6\}$, $\{3^{6}4\}$, $\{4^{4}8\}$
−49	$0^{7}\}$, $0^{7}1\}$, $0^{7}2\}$, $0^{7}3^{5}8^{3}5^{7}0$, $0^{7}4^{5}6^{7}0$, $0^{7}7\}$
−50	$\{1^{7}\}$, $\{2^{6}7^{1}\}$, $\{5^{5}\}$

Table 15.2b. Reduced indefinite binary forms.

d	Forms
−51	$\{1^{7}2\}, \{3^{6}5^{4}7^{3}6\}$
−52	$\{1^{7}3^{5}9^{4}4\}, \{2^{6}8^{2}6^{4}\}. \{4^{6}\}$
−53	$\{1^{7}4^{5}7^{2}\}. \{2^{7}\}$
−54	$\{1^{7}5^{3}9^{6}2\}, \{3^{6}6\}$
−55	$\{1^{7}6^{5}5\}. \{2^{7}3^{5}10\}$
−56	$\{1^{7}7\}. \{2^{6}10^{4}4\}, \{4^{6}5^{4}8\}$
−57	$\{1^{7}8^{1}7^{6}3\}. \{2^{7}4^{5}8^{3}6\}$
−58	$\{1^{7}9^{2}6^{4}7^{3}\}, \{2^{6}11^{5}3^{7}\}$
−59	$\{1^{7}10^{3}5^{7}2\}$
−60	$\{1^{7}11^{4}4\}, \{2^{6}12\}, \{3^{6}8^{2}7^{5}5\}, \{4^{6}6\}$
−61	$\{1^{7}12^{5}3^{7}4^{5}9^{4}5^{6}\}, \{2^{7}6^{5}\}$
−62	$\{1^{7}13^{6}2\}$
−63	$\{1^{7}14\}, \{2^{7}7\}, \{3^{6}9^{3}6\}$
−64	$0^{8}\}. 0^{8}1\}, 0^{8}2\}, 0^{8}3^{7}5^{8}0, 0^{8}4\}. 0^{8}6^{4}8\}, 0^{8}7^{6}4\}, 0^{8}8\}$
−65	$\{1^{8}\}, \{2^{7}8^{1}\}, \{{}^{7}4^{5}10\}. \{5^{5}8^{3}7^{4}\}$
−66	$\{1^{8}2\}, \{3^{6}10^{4}5^{6}6\}$
−67	$\{1^{8}3^{7}6^{5}7^{2}9^{7}2\}$
−68	$\{1^{8}4\}, \{2^{8}\}, \{4^{6}8^{2}\}$
−69	$\{1^{8}5^{7}4^{5}11^{6}3\}, \{2^{7}10^{3}6\}$
−70	$\{1^{8}6^{4}9^{5}5\}, \{2^{8}3^{7}7\}$
−71	$\{1^{8}7^{6}5^{4}11^{7}2\}$
−72	$\{1^{8}8\}, \{2^{8}4\}, \{3^{6}12\}, \{4^{6}9^{3}7^{4}8\}, \{6^{6}\}$
−73	$\{1^{8}9^{1}8^{7}3^{8}\}, \{2^{7}12^{5}4^{7}6^{5}8^{3}\}$
−74	$\{1^{8}10^{2}7^{5}\}, \{2^{8}5^{7}\}$
−75	$\{1^{8}11^{3}6\}. \{2^{7}13^{6}3\}, \{5^{5}10\}$
−76	$\{1^{8}12^{4}5^{6}8^{2}9^{7}3^{8}4\}. \{2^{8}6^{4}10^{6}4\}$
−77	$\{1^{8}13^{5}4^{7}7\}, \{2^{7}14\}$
−78	$\{1^{8}14^{6}3\}. \{2^{8}7^{6}6\}$
−79	$\{1^{8}15^{7}2\}, (3^{8}5^{7}6^{5}9^{4}7^{3}10^{7})$
−80	$\{1^{8}16\}. \{2^{8}8\}, \{4^{6}11^{5}5\}, \{4^{8}\}, \{8^{4}\}$
−81	$0^{9}\}. 0^{9}1\}. 0^{9}2\}. 0^{9}3\}. 0^{9}4^{7}8^{9}0. 0^{9}5^{6}9^{3}8^{5}7^{9}0, 0^{9}6\}. 0^{9}9\}$
−82	$\{1^{9}\}. \{2^{8}9^{1}\}, (3^{7}11^{4}6^{8})$
−83	$\{1^{9}2\}$
−84	$\{1^{9}3\}. \{2^{8}10^{2}8^{6}\}, \{4^{6}12\}. \{4^{8}7^{5}\}$
−85	$\{1^{9}4^{7}9^{2}\}. \{2^{9}\}, \{5^{5}12^{7}3^{8}7^{6}\}. \{\text{"''}^{7}6^{5}10\}$
−86	$\{1^{9}5^{6}10^{4}7^{3}11^{8}2\}$
−87	$\{1^{9}6\}, \{2^{9}3\}$
−88	$\{1^{9}7^{5}9^{4}8\}, \{2^{8}12^{4}6^{8}4\}. \{4^{6}13^{7}3^{8}8\}, \{4^{8}6\}$
−89	$\{1^{9}8^{7}5^{8}\}. \{2^{9}4^{7}10^{3}8^{5}\}$
−90	$\{1^{9}9\}. \{3^{9}\}. \{2^{8}13^{5}5\}. \{6^{9}9^{3}\}$
−91	$\{1^{9}10^{1}9^{8}3^{7}14\}, \{2^{9}5^{6}11^{5}6^{7}7\}$
−92	$\{1^{9}11^{2}8^{6}7^{8}4\}, \{2^{8}14^{6}4\}$
−93	$\{1^{9}12^{3}7^{4}11^{7}4^{9}3\}, \{2^{9}6\}$
−94	$\{1^{9}13^{4}6^{8}5^{7}9^{2}10^{8}3^{7}15^{8}2\}$
−95	$\{1^{9}14^{5}5\}. \{2^{9}7^{5}10\}$
−96	$\{1^{9}15^{6}4\}, \{3^{9}5^{6}12\}, \{2^{8}16\}, \{4^{8}8\}, \{6^{6}10^{4}8\}$
−97	$\{1^{9}16^{7}3^{8}11^{3}8^{5}9^{4}\}. \{2^{9}8^{7}6^{5}12^{7}4^{9}\}$
−98	$\{1^{9}17^{8}2\}. \{7^{7}\}$
−99	$\{1^{9}18\}, \{2^{9}9\}, \{3^{9}6\}, (5^{8}7^{6}9^{3}10^{7})$
−100	$0^{10}\}, 0^{10}1\}, 0^{10}2\}. 0^{10}3^{8}12^{4}7^{10}0, 0^{10}4\}. 0^{10}5\}. 0^{10}6^{8}\},$

When $-d$ is a perfect square, the cycles become chains terminated by 0's. Thus for $d = -16$,

$$0^{4}3^{2}4\}$$

represents

$$0^{4}3^{2}-4^{2}3^{4}0$$

and

$$0^{4}-3^{2}4^{2}-3^{4}0\,.$$

Numerous other tables exist in the literature (see [Bra1], [Cas3, p. 357], [Edw1, p. 333], [Inc1], [Jon1], [Leg1], [Leh1, pp. 68-72], [Som2]), but most of these omit some classes of forms (for example the imprimitive forms, or those with $-d$ a square, or indefinite forms).

3.4 Composition of binary forms. For binary forms, under suitable restrictions, there is a notion of *composition* found by Gauss, that gives the forms a group structure ([Gau1, §234], [Cas3, Chap. 4], [Dic2, Chap. 3], [Edw1, §8.6], [Jon3, §4.4]). There is no generalization to dimensions $\geqslant 3$. Composition is best understood in terms of the multiplication of ideal classes in the corresponding quadratic number rings.

For simplicity we shall suppose that $-d$ is a square-free number not congruent to 1 (mod 4), since then the set $\mathbf{Z}[\sqrt{-d}\,]$ of algebraic integers in $\mathbf{Q}\,(\sqrt{-d})$ is precisely the set of numbers of the form $r+s\sqrt{-d}$ for $r, s \in \mathbf{Z}$. It is also natural to restrict attention to *properly primitive* quadratic forms $f(x,y) = ax^2 + 2bxy + cy^2$ (those for which the numbers a, $2b$, c have no common factor) of determinant $ac - b^2 = d$.

Any ideal $\mathscr{J}$ in $\mathbf{Z}\,[\sqrt{-d}\,]$ has a two-member basis (over $\mathbf{Z}$), so that

$$\mathscr{J} = <r + s\sqrt{-d}\ ,\ t + u\sqrt{-d}>\ ,$$

and its *norm* is usually taken to be the positive integer $|ru - st|$ [Rei1, pp. 293, 330]. A *principal* ideal has a single generator $r + s\sqrt{-d}$ (say) over $\mathbf{Z}\,[\sqrt{-d}\,]$, while over $\mathbf{Z}$ it is generated by $r + s\sqrt{-d}$ and $\sqrt{-d}\ (r + s\sqrt{-d})$. This ideal has norm $r^2 + s^2d$, and will be denoted by

$$<r + s\sqrt{-d}>\,.$$

To get the proper correspondence between Gauss's group of forms under composition and the group of ideal classes we must introduce the notion of a *normed* or *oriented* ideal, an ideal $\mathscr{J}$ of norm N corresponding to two normed ideals $\mathscr{J}_N$ and $\mathscr{J}_{-N}$. A *principal normed ideal* is

$$<r + s\sqrt{-d}>_{r^2+s^2d}\ ,$$

rather than

$$<r + s\sqrt{-d}>_{-(r^2+s^2d)}\,.$$

Multiplication of normed ideals is defined by

$$\mathscr{I}_N \cdot \mathscr{J}_M = \mathscr{I}\mathscr{J}_{NM} \,. \tag{13}$$

Two (normed) ideals $\mathscr{I}$ and $\mathscr{J}$ are said to be in the same (normed) *ideal class* if and only if there exist principal (normed) ideals $\mathscr{P}$ and $\mathscr{Q}$ for which $\mathscr{I}\mathscr{P} = \mathscr{J}\mathscr{Q}$, and under composition these ideal classes form a group, the (normed) *ideal class group.*

The proper (i.e. determinant $+1$) equivalence classes of properly primitive forms of determinant d correspond to classes of normed ideals as follows. (We remind the reader that we are supposing $-d$ to be square-free and not congruent to 1 mod 4). One solution of the equation $f(x, y) = ax^2+2bxy+cy^2 = 0$ is

$$\frac{x}{y} = \frac{-b+\sqrt{-d}}{a} \,,$$

and we shall say that the normed ideal

$$< a, -b+\sqrt{-d} >_a$$

corresponds to f.

Composition may now be defined as follows. To compose two quadratic forms we first pass to the corresponding normed ideals, multiply them using (13), and then, working modulo principal normed ideals, convert the product to a normed ideal of shape

$$< a, \; -b+\sqrt{-d} >_a \,,$$

and reduce the corresponding quadratic form $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ of determinant d by the cycle method of Theorem 1.

For example, the quadratic form $\begin{bmatrix} 3 & 2 \\ 2 & -1 \end{bmatrix}$, which belongs to the reduced cycle

$$\begin{array}{ccccccccc} & 2 & & 2 & & 1 & & 1 & \\ 3 & & -1 & & 3 & & -2 & & 3 \end{array}$$

corresponds to the normed ideal

$$< 3, \; -2+\sqrt{7} >_3 \,.$$

The square of this is the normed ideal of norm 9 whose ideal part is generated by

$$3^2 = 9, \;\; 3(-2+\sqrt{7}) = -6+3\sqrt{7}, \;\; (-2+\sqrt{7})^2 = 11-4\sqrt{7} \,,$$

and this is easily seen to be the same as the ideal $<9, \; -5+\sqrt{7}>_9$ corresponding to the form $\begin{bmatrix} 9 & 5 \\ 5 & 2 \end{bmatrix}$, which gives the reduction sequence

$$\begin{array}{ccccccccccccc} & 5 & & 1 & & 2 & & 2 & & 1 & & 1 & \\ 9 & & 2 & & -3 & & 1 & & -3 & & 2 & & -3 \cdots \end{array}$$

Thus the composition of the equivalence class containing $\begin{bmatrix} 3 & 2 \\ 2 & -1 \end{bmatrix}$ with itself yields the class containing $\begin{bmatrix} 2 & 1 \\ 1 & -3 \end{bmatrix}$. In fact every form of determinant -7 is in one of these two classes, and so the group is cyclic of order 2.

It is perhaps worthwhile to mention that the forms improperly equivalent to f belong to the inverse class in the group (see [Cas3, Chap. 14, Theorem 2.1]). Thus the inverse class is represented by either $\begin{bmatrix} c & b \\ b & a \end{bmatrix}$ or $\begin{bmatrix} a & -b \\ -b & c \end{bmatrix}$. A form improperly equivalent to itself is usually called an *ambiguous* form. Edwards [Edw1, Chaps. 7, 8] gives a clear account of the group structure in the general case, with many examples. He works, however, with an axiomatically defined notion of *divisor*, in place of our normed ideals.

3.5 Genera and spinor genera for binary forms. The theory of genera (§7) was originally developed by Gauss only for the binary case, where it presents special features and is intimately connected with the group of forms under composition. In fact two forms are in the same genus if and only if their quotient is a square in this group. The genus of a binary quadratic form is usually indicated by certain "characters" which can be computed from the numbers represented by the form. We shall not describe the easy conversion from this notation into the one used in §7.

The theory of spinor genera described in §9 assumes throughout that the dimension is at least three, and in the binary case there are several differences. Our treatment is no longer appropriate since there do not exist spinor operators corresponding to all sequences $(r_{-1}, r_2, r_3, \ldots)$ of p-adic unit square classes. Estes and Pall [Est1] have given a full investigation of spinor genera in the binary case and have shown in particular that two forms are in the same spinor genus if and only if their quotient is a fourth power in the group.

4. The p-adic numbers

We now return to the general case of a quadratic form of arbitrary dimension. The notion of integral equivalence (defined in §2) is a very subtle one, which is best approached by studying the weaker notions of equivalence over the larger rings

$\mathbf{Q}$, the rational numbers,

$\mathbf{Q}_p$, the p-adic rational numbers, and

$\mathbf{Z}_p$, the p-adic integral numbers,

where p ranges over the "primes" $-1, 2, 3, 5, \ldots$. The multiplicative group of nonzero rational numbers is a direct product of its cyclic subgroups generated by -1 and the positive prime numbers $2, 3, 5, \ldots$. In this chapter we shall refer to -1 as a prime number, although it presents several special features which arise from the fact that the subgroup it generates is cyclic of order 2 rather than of infinite order. By convention

$\mathbf{Q}_{-1}$ and $\mathbf{Z}_{-1}$ are both equal to the ring $\mathbf{R}$ of real numbers. The number theory of $\mathbf{Q}$ or $\mathbf{Z}$ involves an infinity of prime numbers; by passing to $\mathbf{Q}_p$ or $\mathbf{Z}_p$ we concentrate on just one prime at a time.

4.1 The p-adic numbers. We give a brief description of the main properties of the p-adic numbers that will be needed later. Further information is readily available in a number of books [Bac1], [Bor5], [Cas3], [Kob1], [Mah4], [O'Me1].

Any real number is the limit of a Cauchy sequence of rationals in the ordinary metric

$$d_{-1}(x, y) = |x-y| .$$

If p is any positive prime, we can also equip the rationals with the *p-adic metric*

$$d_p(x, y) = \frac{1}{p^k} ,$$

where p^k is the exact power of p in the factorization of $x-y$. For instance

$$d_5\,(2, 52) = \frac{1}{5^2} = \frac{1}{25} ,$$

$$d_3(\frac{1}{27}, 0) = \frac{1}{3^{-3}} = 27 .$$

We note that for $x \neq y$ the product of $d_p(x,y)$ over all primes p (including -1) is $+1$.

The *p-adic rational numbers* $\mathbf{Q}_p$ are the limit points of Cauchy sequences of ordinary rational numbers with respect to the p-adic metric. The *p-adic integers* (or *rational p-adic integers*) $\mathbf{Z}_p$ are obtained by requiring the terms in the sequence to be ordinary integers.

For example, the difference between the nth and any later term in the sequence 4, 34, 334, 3334, ... is divisible by 5^n (in fact by 10^n), and so this sequence is 5-adically convergent to a 5-adic integer a say. In this case a is actually a rational number. For $3a$ is the limit of the sequence 12, 102, 1002, 10002, ... which 5-adically converges to 2, since its nth term differs from 2 by a multiple of 5^n. Thus $a = 2/3$.

In a similar way we see that any rational number whose denominator is not divisible by p is a p-adic integer.

4.2 p-adic square classes. As another example, we see that 6 has a square root among the 5-adic integers, since $1^2 \equiv 6 \pmod 5$, $(-9)^2 \equiv 6 \pmod{25}$, $(16)^2 \equiv 6 \pmod{125}$, $(-109)^2 \equiv 6 \pmod{625}$, ... , the sequence $1, -9, 16, -109$, ... being capable of being continued indefinitely in such a way that the n-th term is congruent to all later terms modulo 5^n. It is therefore a 5-adic Cauchy sequence whose limit is a square root of 6. Similarly, for any positive odd prime p, an integer not divisible by p that is a quadratic residue modulo p is a p-adic square [Bac1, p. 59].

Two p-adic rational numbers are said to be in the same *p-adic square class* if their ratio is a p-adic rational square. The square classes for the various values of p may be described as follows (cf. [Bac1, pp. 59-60], [Cas3, p. 40], [Wat3, p. 33]):

$$+u,\ -u \quad \text{for } p = -1 \ ,$$

$$u_1,\ u_3,\ u_5,\ u_7,\ 2u_1,\ 2u_3,\ 2u_5,\ 2u_7 \quad \text{for } p = 2 \ ,$$

$$u_+,\ u_-,\ pu_+,\ pu_- \quad \text{for } p \geqslant 3 \ ,$$

where

for $p = -1$, u is any positive real number (a (-1)-adic unit),

for $p = 2$, u_i represents any 2-adic unit congruent to i (mod 8),

for $p \geqslant 3$, u_+ (resp. u_-) is any p-adic unit that is a quadratic residue (nonresidue) mod p.

4.3 An extended Jacobi-Legendre symbol. In agreement with our policy of regarding -1 as a prime, it is natural to define the greatest common divisor of two integers

$$n = (-1)^a 2^b 3^c \ldots \ , \quad \nu = (-1)^\alpha 2^\beta 3^\gamma \ldots \tag{14}$$

with $a = 0$ or 1, $\alpha = 0$ or 1, and b, β, c, γ, ... $= 0, 1, 2, \ldots$ to be

$$(n, \nu) = (-1)^{\min(a,\alpha)} 2^{\min(b,\beta)} 3^{\min(c,\gamma)} \ldots \ .$$

Note that this implies that two negative numbers cannot have $(n, \nu) = 1$ and so will not be counted as coprime. We can define the Jacobi-Legendre symbol $\left(\frac{\nu}{n}\right)$ in all cases where $(n, \nu) = 1$ as follows:

$$\left(\frac{\nu}{p}\right) = \begin{array}{l} \pm 1 \text{ for a prime } p \geqslant 3, \text{ according as } \nu \text{ is or is not} \\ \text{congruent to a square mod } p \ . \end{array}$$

$$\left(\frac{\nu}{-1}\right) = 1 \qquad \text{(since in this case } \nu > 0) \ , \text{ and}$$

$$\left(\frac{\nu}{2}\right) = 1 \text{ if } \nu \equiv \pm 1 \pmod 8 \ , \ -1 \text{ if } \nu \equiv \pm 3 \pmod 8 \ .$$

(Note that $\left(\frac{\nu}{p}\right)$ is equally well defined if ν is a p-adic integer not divisible by p, since every p-adic integer is congruent modulo p to a rational integer.) The symbol $\left(\frac{\nu}{n}\right)$ for n given by (14) is then defined to be

$$\left(\frac{\nu}{-1}\right)^a \left(\frac{\nu}{2}\right)^b \left(\frac{\nu}{3}\right)^c \cdots \ .$$

With this definition the law of quadratic reciprocity asserts that

$$\left(\frac{\nu}{n}\right) = \left(\frac{n}{\nu}\right),$$

whenever either symbol is defined, unless n and ν are both congruent to -1 (mod 4), when

$$\left(\frac{\nu}{n}\right) = -\left(\frac{n}{\nu}\right).$$

4.4 Diagonalization of quadratic forms. It is well-known that any quadratic form over a field of characteristic $\neq 2$ (for example $\mathbf{Q}$ or $\mathbf{Q}_p$) may be diagonalized, and in fact any vector at which the form takes a nonzero value may be taken as the first term of a diagonal basis (see for example [Jon3, Theorem 2]).

Furthermore for $p \neq 2$ any form can be diagonalized over $\mathbf{Z}_p$. For $p = -1$ this is covered by the previous assertion. Otherwise we proceed as follows. We first find a matrix entry that is divisible by the lowest power of p. If this is a diagonal entry, say a_{11}, then we can start the diagonalization by subtracting multiples of the first row from the others so as to clear the rest of the first column, following this by the corresponding column operations to clear the rest of the first row. On the other hand if a nondiagonal entry, say a_{12}, is divisible by the least power of p, and all diagonal entries are divisible by a higher power, we can reduce to the first case by adding the second row to the first and then the second column to the first. This replaces a_{11} by $a_{11}+2a_{12}+a_{22}$, which, since $p \neq 2$, is now divisible by the lowest power of p to occur in any entry.

The same method works if $p = 2$ unless we arrive at a stage when some off-diagonal entry a_{12} say is divisible by the least possible power $q = 2^k$, while all diagonal entries are divisible by 2^{k+1}. In this case the leading 2×2 submatrix has the form

$$\begin{pmatrix} qa & qb \\ qb & qc \end{pmatrix},$$

where a and c are divisible by 2 but b is not, so that $d = ac-b^2$ is not divisible by 2. This implies that any pair of integers (x, y) is a 2-adically integral linear combination of (a, b) and (b, c), so that (since all entries are divisible by q) we can subtract suitable multiples of the first two rows from the others (followed by the corresponding column operations), so as to remove $\begin{pmatrix} qa & qb \\ qb & qc \end{pmatrix}$ as a direct summand. Thus we have proved the following result.

Theorem 2. *For $p \neq 2$ any p-adically integral form can be diagonalized by a p-adically integral transformation. For $p = 2$ there is a p-adically* *integral transformation expressing the form as a direct sum of forms with matrices*

$$(qx)\ ,\quad \begin{bmatrix} qa & qb \\ qb & qc \end{bmatrix}\ ,$$

where q is a power of 2, a and c are divisible by 2, but x, b and $d = ac - b^2$ are not.

Note. The reader who consults other works on quadratic forms will notice that what we call the prime -1 is usually given the name ∞. Over more general algebraic number rings there will be several such "primes", corresponding to different archimedean valuations, and in Hasse's original publications they were given symbols such as $1', 1'', \ldots$. The most appropriate name for them is "unit primes", since they arise from properties of the group of units of the underlying ring. Unfortunately the pernicious habit has grown up of calling them "infinite primes" instead. When we started to write this chapter we hesitated between the notations ∞ and -1 for the archimedean prime in our case, but eventually found that the unconventional name -1 made things so much more simple that its omission would be indefensible.

5. Rational invariants of quadratic forms

In §§5 and 6 we shall investigate when two integral quadratic forms are equivalent over the rational numbers; the main results are stated in Theorems 3, 4 and 5. Rational invariants for quadratic forms are usually defined via the Hilbert norm residue symbol ([Cas3, Chap. 6], [Jon3, Chap. 3], [Wat3, Chap. 3]). Our treatment avoids the use of this symbol and furthermore transforms the standard "product formula" into the readily usable sum formula (15) or "oddity formula" (16). Since we are working over $\mathbf{Q}$ we may assume that the form has already been diagonalized (cf. §4.4).

5.1 The invariants and the oddity formula. Any rational or p-adic integer A can be written uniquely in the form $A = p^\alpha a$ where a is prime to p (meaning that a is positive if $p = -1$, cf. §4.3). Then $p(A) = p^\alpha$ is called the *p-part* of A, and $p'(A) = a$ is the *p'-part*. We shall introduce the term *p-adic antisquare* to mean a number of the form $p^{\text{odd}} \cdot u_-$ when $p \geqslant 3$, and $2^{\text{odd}} \cdot u_{\pm 3}$ for $p = 2$, since both the p- and p'-parts of such a number are non-squares. (There are no (-1)-adic antisquares.) In terms of our extended Jacobi-Legendre symbol, $p^\alpha a$ is a p-adic antisquare if and only if

$$p^\alpha \text{ is not a square and } \left(\frac{a}{p}\right) = -1\ .$$

The *p-signature* of the integral quadratic form $f = \operatorname{diag}\{p^\alpha a, p^\beta b, p^\gamma c, \ldots\}$ is defined to be

$$\begin{aligned} &p^\alpha + p^\beta + p^\gamma + \cdots + 4m \quad (p \neq 2) , \\ &a + b + c + \cdots + 4m \qquad (p = 2) , \end{aligned}$$

where m is the number of p-adic antisquares among $p^\alpha a$, $p^\beta b$, $p^\gamma c$, ... Thus the (-1)-signature of f is just its ordinary signature, which (by Sylvester's law of inertia, §6.2) is an invariant for real equivalence. For $p \geqslant 2$ the p-signature is only to be regarded as defined modulo 8, and we shall see that the p-signature is an invariant for rational equivalence. The 2-signature, which often behaves specially, is also called the *oddity* of f.

What is usually termed the product formula relating the different p-adic invariants [Cas3, p. 76], [Jon3, Th. 29] becomes in this notation the sum formula

$$\text{2-signature} - \text{dimension} \equiv \sum_{\text{odd } p} p\text{-signature} - \text{dimension} \pmod 8 \quad (15)$$

or

$$\sum_{\text{all } p} p\text{-excess } (f) \equiv 0 \pmod 8 ,$$

where we define the *p-excess* to be

$$\begin{aligned} &p\text{-signature} - \text{dimension} , \quad (p \neq 2) , \\ &\text{dimension} - p\text{-signature} , \quad (p = 2) . \end{aligned}$$

For practical calculations it is better to treat the contributions from $p = -1$ and 2 separately, leading to the *oddity formula*:

$$\text{signature } (f) + \sum_{p \geqslant 3} p\text{-excess } (f) \equiv \text{oddity } (f) \pmod 8 . \quad (16)$$

Example. For the form $f = \text{diag } \{1, 3, -3\}$ we compute:

for $p = -1$, the signature $= 1+1-1 = 1$,
for $p = 3$, the 3-excess $= 0+2+2+4 = 8$

(since -3 is a 3-adic antisquare), and

for $p \geqslant 5$, the p-excess $= 0+0+0 = 0$,

while

for $p = 2$, the oddity $= 1+3-3 = 1$,

so that (16) reads

$$1+8+0+0+ \cdots \equiv 1 \pmod 8 .$$

Then our first main theorem, the proof of which will be given in §6, is the following.

Theorem 3. *Two nonsingular forms of the same dimension are equivalent over the rationals if and only if*
(i) *the quotient of their determinants is a rational square, and*
(ii) *for each p they have the same p-excess.*
Condition (ii) *may be replaced by the equivalent condition*:
(ii)$'$ *they have the same signature, the same oddity, and, for all $p \geqslant 3$, the same p-excesses modulo* 8.

It is obvious that if two forms are equivalent over the rationals then they must be equivalent over $\mathbf{Q}_p$ for all p. Since on the other hand the invariants used in Theorem 3 are p-adic invariants, this theorem can be restated as follows.

Theorem 4 (The weak Hasse principle). *A necessary and sufficient condition for two rational forms to be equivalent over* $\mathbf{Q}$ *is that they be equivalent over $\mathbf{Q}_p$ for all p.*

5.2 Existence of rational forms with prescribed invariants. The next theorem states that the oddity formula is essentially the only relation between the p-adic invariants for all p.

Theorem 5 (The strong Hasse principle). *If for each p we are given a p-adic form $f^{(p)}$ of determinant d, satisfying*

$$\textit{signature}\ (f^{(-1)}) + \sum_{p \geqslant 3} p\text{-excess}\ (f^{(p)}) \equiv \textit{oddity}\ (f^{(2)}) \pmod 8 ,$$

then there exists a rational form f which is equivalent to $f^{(p)}$ over $\mathbf{Q}_p$ for each p.
By Theorem 4, if such a form exists it is unique up to equivalence.

Sketch of proof. (For further details see for example [Cas3, Chap. 6, Theorem 1.3] or [Jon3, Theorem 29].) The theorem is first reduced to the case when f is a binary form. Then we wish to find a rational form $f = \operatorname{diag}\{A, B\}$ of prescribed determinant d and with a given signature and non-trivial p-excesses for finitely many primes p. The idea is to choose a large prime q and to take $f = \operatorname{diag}\{p_1 p_2 \cdots q, p_1 p_2 \cdots qd\}$, where the p_i are chosen from these primes and the divisors of $2d$. The value of the p-excess for each prime p dividing d is controlled by the residue class of q modulo p, or if $p = 2$ by the residue class of q modulo 8. All these values may therefore be simultaneously adjusted by requiring q to be in a suitable arithmetic progression modulo $4d$. The existence of such primes q is guaranteed by Dirichlet's theorem (1837) on primes in arithmetic progressions (see for example [Apo1]). For primes $p \neq q$ that do not divide d, the p-excess is trivial, while for q itself the q-excess must be correct by the oddity formula.

Remarks. (1) This proof essentially dates back to Legendre, at a time when Dirichlet's theorem was an unproved conjecture. Gauss later eliminated the dependence on that conjecture by finding a proof using the genera of integral binary quadratic forms (see [Cas3, Chap. 14, §5).

(2) The possible values of a given p-adic invariant for an n-dimensional form can be computed from its possible values for 1-dimensional forms,

which are easily listed. For instance, p-excesses are always even, and are divisible by 4 if $p \equiv 1 \pmod 4$.

5.3 The conventional form of the Hasse-Minkowski invariant. In the literature on quadratic forms the subtle part of the p-adic invariant for a form is usually expressed as a number equal to ± 1, called the Hasse-Minkowski invariant (rather than our p-excess). There are several different conventions, but a common one [Cas3, p. 55] is that the Hasse-Minkowski invariant for $f = \operatorname{diag}\{A_1, A_2, \ldots, A_n\}$ is

$$(f)_p = (A_1, A_2, \ldots, A_n)_p = \prod_{1 \leqslant i < j \leqslant n} (A_i, A_j)_p \tag{17}$$

where $(x, y)_p$ is the so-called Hilbert norm residue symbol. This invariant can be recovered from the p-excess as follows. $(f)_p$ is equal to

$$+1 \qquad \text{or} \qquad -1$$

according as the p-excess of f is or is not congruent modulo 8 to that of

$$f_0 = \operatorname{diag}\{A_1 A_2 \ldots A_n, 1, 1, \ldots, 1\},$$

the "standard" form having the same determinant and dimension as f.

6. The invariance and completeness of the rational invariants

This section is devoted to proving Theorem 3.

6.1 The p-adic invariants for binary forms. The equivalence class of a *binary* form over a field is completely determined by its determinant d (modulo squares) and by any nonzero number a that it represents. For if $f(e_1) = a$, we can take e_1 to be the first vector of a diagonal basis, with respect to which we must have $f = \operatorname{diag}\{a, d/a\}$.

For the p-adic rationals there are only finitely many square classes, and we can enumerate all possible forms (see Table 15.3), and thereby check that two forms have the same determinant and p-adic invariants (signature, p-excess, and oddity) if and only if they are equivalent. As an example we consider the 2-adic forms of determinant $2u_3$. Each such form is equivalent to one of

$$\operatorname{diag}\{u_1, 2u_3\}, \qquad \operatorname{diag}\{u_3, 2u_1\}, \qquad \operatorname{diag}\{u_5, 2u_7\}, \qquad \operatorname{diag}\{u_7, 2u_5\}$$

for which the oddities are respectively

$$1{+}3{+}4 \equiv 0, \qquad 3{+}1 \equiv 4, \qquad 5{+}7 \equiv 4, \qquad 7{+}5{+}4 \equiv 0$$

Table 15.3. Correspondence between the p-adic invariants and the numbers represented by binary forms.

p	Det	Square classes represented	Signature
-1	$+u$	$+u$	2
		$-u$	-2
	$-u$	$+u, -u$	0
p	Det	Square classes represented	Oddity
2	u_1	$u_1, u_5, 2u_1, 2u_5$	2
		$u_3, u_7, 2u_3, 2u_7$	6
	u_3	u_1, u_3, u_5, u_7	4
		$2u_1, 2u_3, 2u_5, 2u_7$	0
	u_5	$u_1, u_5, 2u_3, 2u_7$	6
		$u_3, u_7, 2u_1, 2u_5$	2
	u_7	all	0
	$2u_1$	$u_1, u_3, 2u_1, 2u_3$	2
		$u_5, u_7, 2u_5, 2u_7$	6
	$2u_3$	$u_1, u_7, 2u_3, 2u_5$	0
		$u_3, u_5, 2u_1, 2u_7$	4
	$2u_5$	$u_1, u_3, 2u_5, 2u_7$	2
		$u_5, u_7, 2u_1, 2u_3$	6
	$2u_7$	$u_1, u_7, 2u_1, 2u_7$	0
		$u_3, u_5, 2u_3, 2u_5$	4

p	Det	Square classes represented	p-excess, for p (mod 8) $\equiv$			
			1	3	5	7
$\geqslant 3$	u_+	all	0	—	0	—
		u_+, u_-	—	0	—	0
		pu_+, pu_-	—	4	—	4
	u_-	all	—	0	—	0
		u_+, u_-	0	—	0	—
		pu_+, pu_-	4	—	4	—
	pu_+	u_+, pu_+	0	2	4	6
		u_-, pu_-	4	6	0	2
	pu_-	u_+, pu_-	4	6	0	2
		u_-, pu_+	0	2	4	6

(mod 8). Since x^2+6y^2 (the first form) represents 7, it is equivalent to the fourth form, and similarly the second and third forms are equivalent. But an easy calculation reveals that x^2+6y^2 does not represent any number of the form $4^m(8k+3)$, and so these two pairs of forms are not equivalent. Thus there are two distinct 2-adic binary forms of determinant $2u_3$. The first has oddity 0 and represents the numbers u_1, u_7, $2u_3$ and $2u_5$, while the second has oddity 4 and represents the numbers u_3, u_5, $2u_1$ and $2u_7$. This explains the entries for $p = 2$, det $= 2u_3$ in Table 15.3.

After a similar discussion for all the cases with $p = 2$ in Table 15.3 we conclude that the oddity is a 2-adic invariant, and together with the determinant is a complete invariant for 2-adic rational equivalence. Similarly for the other primes. This completes the proof of the "only if" part of Theorem 3 for binary forms.

The reader will notice that there is, for each p, one form that represents all nonzero numbers. This is the *isotropic* form diag $\{A, -A\}$, of determinant -1, so called because it also represents zero nontrivially.

6.2 The p-adic invariants for n-ary forms. It is easy to extend the above remarks to show that our invariants really are invariants for forms of all dimensions. The proof reduces to showing that any equivalence between diagonal forms can be broken down into a chain of *binary* equivalences (i.e. ones effecting just two diagonal terms).

To see this, note that for

$$f = \text{diag}\ \{a,b,c, \ldots\}, \quad f' = \text{diag}\ \{a',b', c', \ldots\}$$

to be equivalent, a' must be representable by f. We choose a representation involving the smallest number of terms, say

$$a' = ax^2 + by^2 + cz^2 + dt^2\ ,$$

and then we have the binary equivalences

$$\text{diag}\ \{a,b,c,d,e, \ldots\} \sim \text{diag}\ \{a_2,b^*,c,d,e, \ldots\}$$
$$\sim \text{diag}\ \{a_3,b^*,c^*,d,e, \ldots\} \sim \text{diag}\ \{a_4,b^*,c^*,d^*,e, \ldots\}\ ,$$

where $a_2 = ax^2 + by^2$, $a_3 = ax^2 + by^2 + cz^2$, $a_4 = \cdots$ are nonzero. These show that f and f' are equivalent to diag $\{a',b^*,c^*, \ldots\}$, and so by Witt's cancellation theorem (which we shall prove in a moment) the forms diag $\{b,c,d, \ldots\}$ and diag $\{b^*,c^*,d^*,\ldots\}$ are equivalent. Since by induction the latter equivalence reduces to a chain of binary ones, we deduce the same for the equivalence of f and f'.

The remainder of this section will be devoted to the proof that two forms having the same p-adic invariants for all p (including -1) are equivalent over the rationals.

Let f and g be two rational quadratic forms with the same nonzero determinant (modulo a square factor), and the same signature, oddity and

p-excess for all $p \geqslant 3$. Then we shall prove that for a suitable nonsingular form h, $f \oplus h$ is equivalent to $g \oplus h$ and will deduce that f is equivalent to g by repeated application of Witt's cancellation theorem.

Theorem 6 (Witt's cancellation theorem [Wit1], [Cas3, p. 21], [Sch0, p. 22], [Sch2, Chap. 1]). *Over any field of characteristic* $\neq 2$, *if* diag $\{a, b, c, \ldots\} \sim$ diag $\{a, b', c', \ldots\}$ *and* $a \neq 0$, *then* diag $\{b, c, \ldots\} \sim$ diag $\{b', c', \ldots\}$.

Proof. This is equivalent to the following geometrical assertion. Let V be a vector space over the field, equipped with the bilinear form $f(x, y) = ax_1y_1 + bx_2y_2 + cx_3y_3 + \cdots$. Then if vectors v and w in V have the same nonzero norm a, there is an automorphism of V fixing f and taking v to w. Now for any $r \in V$ of nonzero norm, the reflection

$$x \rightarrow x - 2\frac{f(x, r)}{f(r, r)}r \tag{18}$$

is an automorphism of V preserving f. Not both the vectors $r = v \pm w$ can have zero norm, and so one of the corresponding reflections exists and takes v to $\pm w$, and can be followed by negation if necessary. This establishes the theorem.

Remark. Sylvester's law of inertia (the invariance of signature under real equivalence [Jon3, Theorem 2]) follows immediately from Theorem 6, since if

$$\text{diag }\{(+1)^{r+k}, (-1)^s\} \sim \text{diag }\{(+1)^r, (-1)^{s+k}\}$$

over the reals, then we can deduce that

$$\text{diag }\{(+1)^k\} \sim \text{diag }\{(-1)^k\},$$

implying $k = 0$ (since one form is positive definite, the other negative definite).

We shall say that a form has *trivial invariants* if all its p-excesses are congruent to zero modulo 8 and its determinant is a perfect square. Then the desired result will follow from:

Theorem 7. *If F has trivial invariants then F is equivalent over the rationals to a form of the shape*

$$\text{diag }\{\pm 1, \pm 1, \ldots, \pm 1\}.$$

To see that the result we want is a consequence of Theorem 7 we argue as follows. Since p-excesses are always even, if f and g have the same invariants then

$$f \oplus f \oplus f \oplus f \quad \text{and} \quad g \oplus f \oplus f \oplus f \tag{19}$$

will both have (the same) trivial invariants, and by Theorem 7 will be equivalent to forms of the shape diag $\{\pm 1, \pm 1, \ldots\}$. Since signature (f)

= signature (g), the numbers of positive and negative terms agree, and the two forms (19) are equivalent. By Witt cancellation (Theorem 6) we deduce that $f \sim g$.

6.3 The proof of Theorem 7. We shall suppose throughout that F is a diagonal form with square-free integer entries and with trivial invariants, and will actually show that, for a sufficiently large N,

$$F \oplus \operatorname{diag}\{(+1)^N, (-1)^N\} \sim \operatorname{diag}\{\pm 1, \pm 1, ...\}$$

over the rationals. We shall do this by gradually reducing the primes appearing in the entries of F. Let p be the largest such prime, and call the entries of F divisible by p the *p-terms*. Note that any p-term has the form $pq_1q_2...q_k$ where $-1 \leqslant q_i < p$ for all i. We suppose first that $p \geqslant 3$.

Theorem 8. (The replacement lemma). *Assume $p \geqslant 3$. If $-1 \leqslant a, b < p$, and ab is congruent to a square (mod p), then we may replace any p-term "pat" by "pbt" without introducing any prime larger than p.*

Note. The replacement process involves adjoining more direct summands ± 1 to F.

Proof. (Based on [Con8, p. 401].) We can write $ab = x^2 - py$, with $|x| < ½p$, and so $|y| < p$. Then the identity

$$pat(b/p)^2 - pbt(x/p)^2 = -ybt$$

shows that the form diag $\{pat, -pbt\}$ represents $-ybt$, and therefore, by the observation at the beginning of §6.1, is equivalent to diag $\{yat, -ybt\}$. Also $x^2 - y^2 =$ diag $\{1, -1\}$ represents all numbers, in particular $-pbt$, and so

$$\operatorname{diag}\{1, -1\} \sim \operatorname{diag}\{-pbt, pbt\} .$$

Then we have

$$\operatorname{diag}\{pat, 1, -1\} \sim \operatorname{diag}\{pat, -pbt, pbt\} \sim \operatorname{diag}\{yat, -ybt, pbt\} ,$$

which is the desired replacement. This completes the proof of Theorem 8.

We now suppose $p > 2$. By repeated use of the replacement lemma we can replace each p-term by pu^k, and so by p or pu, where $u = r + 1$ is the least positive non-residue modulo p. But also diag$\{p, pr\}$ represents pu, and so is equivalent to diag$\{pu, pur\}$. We may therefore replace

$$p, p \text{ by } p, pr, \text{ then } pu, pur, \text{ then } pu, pu \ , \qquad (20)$$

or vice versa, so that the first of two or more p-terms may be chosen arbitrarily.

The determinant condition tells us there exist evenly many p-terms. We may replace the first one by $-p$ and the second by p or pu (and definitely by p if there are more than two p-terms). If the second is p we can now eliminate the first two p-terms using

$$\text{diag}\,\{-p,p\} \sim \text{diag}\,\{-1,\ 1\}\ . \tag{21}$$

If not, the *only* p-terms are $-p,pu$, and the p-excess differs by 4 from that of diag$\{-p,p\}$ (which is zero), and so is non-trivial, contradicting the supposition.

So when $p > 2$ we have been able to reduce the size of p by repeated application of the replacement lemma. If $p = 2$ all p-terms are ± 2, and there are an even number of them since the determinant is a square. They can then be eliminated using the equivalences diag $\{2,\ 2\} \sim$ diag $\{1,\ 1\}$, diag $\{2,\ -2\} \sim$ diag $\{1,\ -1\}$, diag $\{-2,\ -2\} \sim$ diag $\{-1,\ -1\}$. This completes the proofs of Theorems 7 and 3.

7. The genus and its invariants

Two integral quadratic forms are said to be in the same *genus* if they are equivalent over the p-adic integers for all primes p (including -1). As we shall see in §9, for indefinite forms of dimension $n \geqslant 3$, there is usually only one equivalence class of forms in a genus. In fact this holds whenever $|\det f| < 128$, and when it fails $4^{[n/2]}\det f$ must be divisible by $k^{\binom{n}{2}}$ for some nonsquare natural number $k \equiv 0$ or $1 \pmod 4$.

In this section we give a complete system of invariants for p-adic integral equivalence for each p, and then show how to combine them to obtain a handy characterization of the genus.

No proofs will be offered. For $p \neq 2$ several accounts are readily available (e.g. Cassels [Cas3]), and all cases are handled by O'Meara [O'Me1], who gives the invariants for forms over arbitrary number fields. The correctness of the simple system of invariants and transformation rules for $p = 2$ given here was originally verified (by J.H.C.) by showing that they suffice to put every form into B. W. Jones' canonical form [Jon2], yet are consistent with G. Pall's complete system of invariants [Pal1]. A direct verification has now been given by K. Bartels [Bar19].

We remark that much of the importance of the genus — for instance in topological investigations — arises from the fact that two forms f and g are in the same genus if and only if $f \oplus \begin{bmatrix}01\\10\end{bmatrix}$ and $g \oplus \begin{bmatrix}01\\10\end{bmatrix}$ are integrally equivalent. This follows from properties of the spinor genus.

7.1 p-adic invariants. As we saw in Theorem 2, any form can be decomposed over the p-adic integers as a direct sum

$$f = f_1 \oplus pf_p \oplus p^2f_{p^2} \oplus \cdots \oplus qf_q \oplus \cdots \tag{22}$$

in which each f_q is a p-adic *unit form*, meaning a p-adic integral form whose determinant is prime to p (if $p \geqslant 2$) or a positive definite form (if $p = -1$). The summands qf_q in (22) are called *Jordan constituents* of f, and (22) itself is a *Jordan decomposition* of f. We call q the *scale* of the constituent qf_q. Note that, when $p = -1$, (22) is the familiar result that any form can be written as a sum of definite forms:

$$f = 1 \cdot f_1 \oplus (-1) f_{-1} ,$$

where f_1 and f_{-1} are positive definite.

For $p \neq 2$ the set of values of q occurring in (22), together with the *dimensions* $n_q = \dim f_q$ and *signs*

$$\epsilon_q = \left(\frac{\det f_q}{p} \right) ,$$

form a complete set of invariants for f (see Theorem 9). The case $p = 2$ presents additional complexities and will be discussed in §§7.3-7.6. In the case $p = -1$, $\epsilon_q = +1$ since $\det f_q$ is positive, and so n_{+1} and n_{-1} are the only invariants (this is Sylvester's law of inertia, §6.2). By convention, $+1$ and -1 will usually be abbreviated to $+$ and $-$, and so we write n_+ for n_{+1}, n_- for n_{-1}.

7.2 The p-adic symbol for a form. For $p = -1$ we express the fact that $n_+ = a$ and $n_- = b$ by the *(-1)-adic symbol*

$$+^a \, -^b \, .$$

For other odd p we shall use a *p-adic symbol* which is a formal product of the "factors"

$$q^{\epsilon_q n_q} .$$

For example if $p = 3$, the symbol

$$1^{-2} \, 3^{+5} \, 9^{+1} \, 27^{-3} \tag{23}$$

represents a form

$$f = f_1 \oplus 3f_3 \oplus 9f_9 \oplus 27f_{27}$$

with $\dim f_1 = 2$, $\dim f_3 = 5$, $\dim f_9 = 1$, $\dim f_{27} = 3$, where the determinants of f_3, f_9 are quadratic residues modulo 3 and those of f_1, f_{27} are nonresidues.

In these symbols we may adopt certain obvious abbreviations, such as replacing (23) by $1^{-2} \, 3^5 \, 9 \, 27^{-3}$.

Theorem 9. *For $p \neq 2$, two quadratic forms f and g are equivalent over the p-adic integers if and only if they have the same invariants n_q, ϵ_q for each power q of p, or equivalently if and only if they have the same p-adic symbol.*

The proofs of Theorems 9 and 10 are omitted (see the remarks at the beginning of this section). Theorem 9 makes two assertions. First, q, ϵ_q, n_q are a complete set of invariants for the Jordan constituents qf_q, and second, the invariants of the Jordan constituents are invariants of f. Both assertions must be modified when $p = 2$.

7.3 2-adic invariants. Let the 2-adic Jordan decomposition of f be

$$f = f_1 \oplus 2f_2 \oplus 4f_4 \oplus \cdots \oplus qf_q \oplus \cdots . \tag{24}$$

Then the invariants of qf_q are the quantities
q, the *scale* of qf_q,
S_q = I or II (see below), the *type* of f_q, which is the *scaled type* of qf_q,
$n_q = \dim f_q$ (the *dimension* of f_q or qf_q),
$\epsilon_q = \left(\frac{\det f_q}{2}\right)$ (the *sign* of f_q or qf_q), and
t_q, the *oddity* of f_q (see §5.1).

We define S_q to be I if qf_q represents an odd multiple of q, and otherwise II (compare §2.4 of Chap. 2). Equivalently, S_q is I if and only if there is an odd entry on the main diagonal of the matrix representing f_q, and otherwise II. If f_q (of type I) has been diagonalized, then t_q is its trace, read modulo 8. If f_q has type II, $t_q = 0$.

7.4 The 2-adic symbol. The 2-adic symbol representing a given Jordan decomposition (24) of f is a formal product of factors

$$q_{t_q}^{\epsilon_q n_q} \quad \text{or} \quad q^{\epsilon_q n_q} ,$$

where the former indicates a constituent qf_q for which f_q has type I and

$$\left(\frac{\det f_q}{2}\right) = \epsilon_q , \quad \dim f_q = n_q , \quad \text{oddity } (f_q) = t_q ,$$

while the latter indicates a constituent qf_q for which f_q has type II and

$$\left(\frac{\det f_q}{2}\right) = \epsilon_q , \quad \dim f_q = n_q , \quad \text{oddity } (f_q) = 0 .$$

We shall sometimes write

$$q_{\mathrm{I}}^{\epsilon_q n_q} \text{ for } q_{t_q}^{\epsilon_q n_q} , \; q_{\mathrm{II}}{}^{\epsilon_q n_q} \text{ for } q^{\epsilon_q n_q}$$

(The value of t_q is often unimportant).

For example $1^{-2}2_5^{+3}4_3^{-1}8^{+4}$ (or $1_{\mathrm{II}}^{-2}\, 2_5^{+3}\, 4_3^{-1}\, 8_{\mathrm{II}}^{+4}$) represents a form having a Jordan decomposition

$$f_1 \oplus 2f_2 \oplus 4f_4 \oplus 8f_8 ,$$

in which f_1, f_2, f_4, f_8 have dimensions 2, 3, 1, 4 and determinants congruent to ± 3, ± 1, ± 3, ± 1 (mod 8) respectively, f_1 and f_8 have type II, while f_2 and f_4 are of type I and can be put into diagonal form with traces congruent to 5 and 3 (mod 8) respectively.

7.5 Equivalences between Jordan decompositions. So far we have described the invariants for a *Jordan constituent* qf_q. Unfortunately a form may have several essentially different Jordan decompositions, and so can have several different 2-adic symbols. The precise rule giving all such equivalences is as follows.

Theorem 10. *Two forms f and f' with respective invariants*

$$n_q, S_q, \epsilon_q, t_q \quad \text{and} \quad n'_q, S'_q, \epsilon'_q, t'_q$$

are 2-adically equivalent just if
(i) $n_q = n'_q$, $S_q = S'_q$ *for all q, and*
(ii) *for each integer m (including negative integers) for which f_{2^m} has type* II, *we have*

$$\sum_{q<2^m} (t_q - t'_q) \equiv 4(\min(a,m) + \min(b,m) + \cdots) \pmod 8$$

where $2^a, 2^b, \ldots$ are the values of q for which $\epsilon_q \neq \epsilon'_q$.

Although Theorem 10 completely describes all the 2-adic equivalences, it is often simpler to use the following ideas.

Compartments and trains. Suppose f has a Jordan decomposition (24). By an *interval* of forms we mean all the forms qf_q, even those of zero dimension, for which $q_1 \leqslant q \leqslant q_2$, where q_1, q_2 are powers of 2. A *compartment* is a maximal interval in which all forms are of scaled type I, and a *train* is a maximal interval having the property that for each pair of adjacent forms at least one is of scaled type I. Thus in

$$1^{+2}[2_6^{-2}\, 4_5^{+3}]8^{+0}[16_1^{+1}]32^{+2}\colon\ 64^{-2}\colon\ 128^{-4}[256_3^{-1}]512^{+0} \qquad (25)$$

the square brackets enclose the compartments and the trains are separated by colons. Notice that here one train has two compartments, while another train has none.

There are two ways in which such symbols may be altered and yet still represent 2-adically equivalent forms.

(i) **Oddity fusion**. Two 2-adic symbols represent the same form if the only change is that the oddities have been altered in a way that does not affect their total sum over any compartment.

So we may replace the individual oddity markers in a compartment by their total (modulo 8), written as a subscript to the entire compartment. For example we may replace $[2_6^{-2}\, 4_5^{+3}]$ in (25) by $[2^{-2}\, 4^{+3}]_3$.

(ii) **Sign walking**. A form is unaltered if the signs ϵ_q of any two terms in a train are simultaneously changed, provided certain oddities are altered by 4. Let $\epsilon_{q_1}, \epsilon_{q_2}, q_1 < q_2$, be the signs we wish to change. We imagine walking along the train from the term for q_1 to that for q_2. Our walk consists of a number of steps between adjacent forms f_q and f_{2q}, and each such step involves just one compartment, since at least one of f_q, f_{2q} is of type I, and if they are both of type I they are in the same compartment. Then the rule is that the total oddity of a compartment must be changed by 4 modulo 8, precisely when the number of steps that involve that compartment is odd.

Suppose for example we wish to change the signs corresponding to f_2 and f_{16} in the train

$$1^2\,[2^{-2}\,4^3]_3\,8^0\,[16^1]_1\,32^2\,. \tag{26}$$

The walk has three steps, from f_2 to f_4, f_4 to f_8, and f_8 to f_{16}. The first two steps affect the first compartment and the third step affects the second compartment. The resulting symbol is therefore

$$1^2\,[2^2\,4^3]_3\,8^0[16^{-1}]_5\,32^2 \tag{27}$$

Alternatively, a walk of just one step from f_2 to f_4 in (26) would lead to

$$1^2[2^2\,4^{-3}]_7\,8^0\,[16^1]_1\,32^2\,. \tag{28}$$

All of (26), (27), (28) represent equivalent forms.

The effect of the three-step walk could also be achieved by three separate one-step walks, except that at an intermediate stage the symbol would contain a factor 8^{-0}, corresponding to an impossible Jordan constituent. Transformations involving such impossible constituents are quite legal provided the end results are meaningful.

7.6 A canonical 2-adic symbol. Using these rules we can arrange that there is at most one minus sign per train, which can be attached to any form of nonzero dimension. One convenient rule is to put this sign on the earliest nonzero dimensional form of a train. If this convention is adopted and only the total oddities of the compartments are given, the resulting symbol is absolutely unique and may be taken as a canonical symbol for the form. Thus for (25) the canonical symbol is

$$1^{-2}[2^{+2}4^{+3}]_7\,8^{+0}[16^{+1}]_1\,32^{+2}\!:\;64^{-2}\!:\;128^{+4}[256^{+1}]_7\,512^{+0}\,,$$

which would be further abbreviated in practice to

$$1^{-2}[2^2\,4^3]_7\,[16]_1\,32^2\!:\;64^{-2}\!:\;128^4\,[256]_7\,.$$

Then two forms are 2-adically equivalent if and only if their canonical symbols are identical.

7.7 Existence of forms with prescribed invariants. It is important to specify exactly which conceivable systems of invariants actually correspond to quadratic forms. There are three sets of conditions.

The determinant conditions for each p. The p-adic square classes of the determinant as computed from the p-adic symbols must agree with its known value. In other words the product of all the signs ϵ_q in the p-adic symbol must be $\left(\frac{a}{p}\right)$ (29)

where $\det(f) = p^\alpha a$ and $(a, p) = 1$.

The oddity condition, relating all p. From the p-adic symbols we can compute the invariants appearing in the oddity formula. Thus for $p = -1$,

$$\text{signature } (f) = r-s \ ,$$

if the (-1)-adic symbol is $+^r -^s$; and for $p \geqslant 3$,

$$p\text{-excess } (f) \equiv \sum_q n_q(q-1) + 4k_p \quad (\text{mod } 8) \ ,$$

where the n_q are the dimensions of the Jordan constituents and k_p is the number of *antisquare terms* (i.e. q not a square and $\epsilon_q = -1$) in the p-adic symbol; and for $p = 2$,

$$\text{oddity } (f) \equiv \sum_q t_q + 4k_2 \quad (\text{mod } 8) \ ,$$

from the 2-adic symbol. Then these quantities must be related by the oddity formula

$$\text{signature } (f) + \sum_{p \geqslant 3} p\text{-excess } (f) \equiv \text{oddity } (f) \quad (\text{mod } 8) \ . \qquad (30)$$

The existence condition for each Jordan constituent. Each term in the p-adic symbol must correspond to an existing form. If $p \neq 2$, for each Jordan constituent qf_q of dimension n and sign ϵ we must have

$$\text{if } n = 0 \text{ or } p = -1 \text{ then } \epsilon = + \ . \qquad (31)$$

For $p = 2$ the following must hold:

$$\text{for } n = 0, \quad \text{type} = \text{II and } \epsilon = + \ , \qquad (32)$$

$$\text{for } n = 1, \begin{cases} \epsilon = + \Rightarrow t \equiv \pm 1 \pmod 8 \ , \\ \epsilon = - \Rightarrow t \equiv \pm 3 \pmod 8 \ , \end{cases} \qquad (33)$$

$$\begin{matrix}\text{for } n = 2 \\ \text{and type I}\end{matrix} \begin{cases} \epsilon = + \Rightarrow t \equiv 0 \text{ or } \pm 2 \pmod 8 \ , \\ \epsilon = - \Rightarrow t \equiv 4 \text{ or } \pm 2 \pmod 8 \ , \end{cases} \qquad (34)$$

while for general n we have $t \equiv n \pmod 2$, and

$$t \equiv 0 \pmod 8 \text{ for type II, so that } n \text{ odd} \Rightarrow \text{type I}. \qquad (35)$$

Theorem 11. *If a system of putative p-adic symbols for each p satisfies the determinant, oddity and p-adic existence conditions* (29)–(35), *then there exists an integral quadratic form with these p-adic symbols.*

When working with the abbreviated form of a 2-adic symbol, it is helpful to know that the only existence condition on a compartment containing two or more Jordan constituents is that its total oddity must have the same parity as its total dimension.

7.8 A symbol for the genus. We can combine the significant portions of our p-adic symbols to give a handy notation for the entire genus (that happily generalizes some notation we have used elsewhere [Con13], [Con33], [Con34]). This symbol has the form

$$\mathrm{I}_{r,s}(\cdots) \quad \text{or} \quad \mathrm{II}_{r,s}(\cdots) \ ,$$

where the Roman numeral is the type of the entire form, i.e. the type of its 2-adic Jordan constituent f_1; the subscripts indicate the (-1)-adic symbol $+^r-^s$; and the parenthesis contains the usual symbols

$$q^{\pm m},\ q_t^{\pm m},\ q_{\mathrm{I}}^{\pm m},\ q_{\mathrm{II}}^{\pm m}$$

for the powers $q > 1$ of all primes 2, 3, ... The subscripts t, I or II may be omitted when their values can be deduced from the oddness of m or the oddity formula (30).

The symbols

$$1^{\pm m},\ 1_t^{\pm m}\ (\text{or}\ \ 1_{\mathrm{I}}^{\pm m})$$

corresponding to the constituents f_1 in each p-adic Jordan decomposition have been omitted. However

the sign ± can be recovered from $\det f$,
the number m can be recovered from $\dim f = r+s$,
the type I or II (for $p = 2$) is displayed, and
the oddity t (when relevant) can be computed from the oddity formula (30).

For example $\mathrm{I}_{r,s}(2)$ has determinant $(-1)^s 2$, and so its p-excess is 0 for $p \geqslant 3$. From (30) the oddity is $r-s$, and therefore the 2-adic symbol is

$$1_{\mathrm{I}}^{\pm(r+s-1)}\, 2_{\mathrm{I}}^{1} = [1^{+(r+s-1)}\, 2^1]_{r-s}\ ,$$

using (29). Similarly $\mathrm{II}_{r,s}(3)$ (whose determinant is $(-1)^s 3 = \pm 3$) has 3-adic symbol $1^{\pm(r+s-1)}3^1$ (with the same ±), yielding a 3-excess of 2, and 2-adic symbol $1_{\mathrm{II}}^{-(r+s)}$, since $\det f \equiv \pm 3 \pmod 8$. The 2-adic symbol for $\mathrm{I}_{r,s}(3)$ would be $1_{r-s+2}^{-(r+s)}$.

A variant of this notation indicates the total dimension $r+s$ explicitly and treats -1 like any other prime, thus writing

$$\mathrm{I}_{r+s}(-^s X) \quad \text{or} \quad \mathrm{II}_{r+s}(-^s X)$$

for

$$\mathrm{I}_{r,s}(X) \quad \text{or} \quad \mathrm{II}_{r,s}(X)$$

respectively.

8. Classification of forms of small determinant and of p-elementary forms

8.1 Forms of small determinant. Using the notation introduced in the previous section, the distinct genera of forms of any given determinant can be classified in a systematic way. One first writes down all possible p-adic symbols for $p = -1, 2$ and all p dividing the determinant (it is best to handle $p = 2$ last). The determinant condition (29) and the rules for manipulating trains (§7.5) are used to control the signs. Then the oddity formula (30) and the existence conditions (§7.7) lead to congruences (modulo 8) relating the signature to the oddity parameters. We illustrate this process by classifying the genera of forms with determinants ± 1 and ± 3.

Determinant ± 1. Let the (-1)-adic symbol be $+^r -^s$, with $r+s = n$. Since the determinant is $\equiv \pm 1 \pmod 8$, the possible 2-adic symbols are

$$1_t^{+(r+s)} \quad \text{and} \quad 1^{+(r+s)},$$

for which the respective oddity conditions read

$$r-s \equiv t \quad \text{and} \quad r-s \equiv 0 \quad (\text{mod } 8).$$

The former determines t and corresponds to the genus symbol $\mathrm{I}_{r,s} = \mathrm{I}_{r,s}(1)$, which exists for all possible signatures except $r = s = 0$. The latter gives $\mathrm{II}_{r,s} = \mathrm{II}_{r,s}(1)$, which exists only for signatures divisible by 8. (The existence conditions are trivially satisfied.) This explains lines 1 and 2 of Table 15.4 below.

Determinant ± 3. The possible p-adic symbols for

$p =$	-1	3	2

are

$\mathrm{I}_{r,s}(3)$:	$+^r -^s$	$1^{\pm(r+s-1)}3^1$	$1_t^{-(r+s)}$
$\mathrm{I}_{r,s}(3^{-1})$:	$+^r -^s$	$1^{\mp(r+s-1)}3^{-1}$	$1_t^{-(r+s)}$
$\mathrm{II}_{r,s}(3)$:	$+^r -^s$	$1^{\pm(r+s-1)}3^1$	$1^{-(r+s)}$
$\mathrm{II}_{r,s}(3^{-1})$:	$+^r -^s$	$1^{\mp(r+s-1)}3^{-1}$	$1^{-(r+s)}$,

where the ambiguous sign ± is $-^s$, and the 2-adic sign is $-$ since the determinant is $\equiv \pm 3 \pmod 8$. These lead to the respective oddity conditions

$$r-s+2 \equiv t,$$

$$r-s+6 \equiv t,$$

$$r-s+2 \equiv 0,$$

$$r-s+6 \equiv 0,$$

the first two of which determine t, while the last two give conditions on the signature. The existence conditions on the Jordan constituents are automatically satisfied except for small n, when they are best handled by consideration of all pairs (r, s) with $r+s = n$. Thus in the case $\mathrm{I}_{r,s}(3)$ and for (r,s) equal to

$$(0,0), \qquad (1,0), \qquad (0,1), \qquad (2,0), \qquad (1,1), \qquad (0,2)$$

we find the 2-adic symbol to be

$$1_2^{-0}, \qquad 1_3^{-1}, \qquad 1_1^{-1}, \qquad 1_4^{-2}, \qquad 1_2^{-2}, \qquad 1_0^{-2}$$

respectively, for which the existence condition holds in only three cases:

$$\times \qquad \surd \qquad \times \qquad \surd \qquad \surd \qquad \times$$

The three failures are classified as $n_{r-s} = 0,\ 1_{-1},\ 2_{-2}$ in Table 15.4.

Similar arguments lead to the following theorem.

Theorem 12. *All genera of forms with* $|determinant| \leqslant 11$ *are as indicated in Table* 15.4.

The theory of spinor genera (see Corollary 21 below) shows that for indefinite cases of dimension $\geqslant 3$ these are also the integral equivalence classes.

In Table 15.4 we have used the convention that all ambiguous signs in any row of the table are linked. The last column lists the exceptions, if any, in the form n_σ, where n is the dimension and σ the forbidden signature. If all signatures of dimension n are excluded the subscript is omitted. The asterisk * towards the end of the table indicates that when $n = 1$, this genus must be interpreted as $\mathrm{II}_{r,s}(2^{-1} \times 5^{-1})$.

8.2 p-elementary forms. The same methods enable as to classify the so-called *p-elementary* forms, that is, forms for which L^*/L is a nontrivial elementary abelian p-group, where L is the lattice of the form and L^* is the dual lattice. These forms were partially classified by Rudakov and Shafarevich [Rud1], [Rud2], and the results used by Nikulin in [Nik1]-[Nik6] (see also [Dol1]).

Theorem 13. (a) *For* $p \geqslant 3$ *the distinct genera of p-elementary forms are*

$$\mathrm{I}_{r,s}(p^{\pm k}) \quad \textit{for all signatures} \quad r-s\ ,$$

and

$$\mathrm{II}_{r,s}(p^{\pm k}) \quad \textit{for} \quad r-s \equiv \pm 2-2-(p-1)k \pmod 8\ ,$$

except that in either case when $k = n$ $(= r+s)$ *the sign must be* $\left(\frac{-1}{p}\right)^s$.

Table 15.4. All genera of forms with |det| ≤ 11.

|Det|	Genus	Signature (mod 8)	Exceptions n_{r-s}
1	$\mathrm{I}_{r,s}$	all	0
1	$\mathrm{II}_{r,s}$	0	none
2	$\mathrm{I}_{r,s}(2)$	all	0,1
2	$\mathrm{II}_{r,s}(2)$	± 1	none
3	$\mathrm{I}_{r,s}(3^{\pm 1})$	all	$0, 1_{\mp 1}, 2_{\mp 2}$
3	$\mathrm{II}_{r,s}(3^{\pm 1})$	∓2	none
4	$\mathrm{I}_{r,s}(4_{\pm 1})$	all	$0, 1, 2_{\mp 2}, 3_{\mp 3}$
4	$\mathrm{II}_{r,s}(4^{1})$	± 1	none
4	$\mathrm{II}_{r,s}(4^{-1})$	± 3	none
4	$\mathrm{I}_{r,s}(2_{\mathrm{I}}^{2})$	all	0,1,2
4	$\mathrm{II}_{r,s}(2_{\mathrm{I}}^{2})$	0, ± 2	0
4	$\mathrm{I}_{r,s}(2_{\mathrm{II}}^{2})$	all	$0, 1, 2, 3_{\pm 3}, 4_{\pm 4}$
4	$\mathrm{II}_{r,s}(2_{\mathrm{II}}^{2})$	0	0
4	$\mathrm{II}_{r,s}(2_{\mathrm{II}}^{-2})$	4	none
5	$\mathrm{I}_{r,s}(5)$	all	0
5	$\mathrm{I}_{r,s}(5^{-1})$	all	$0, 1, 2_{0}$
5	$\mathrm{II}_{r,s}(5)$	4	none
5	$\mathrm{II}_{r,s}(5^{-1})$	0	0
6	$\mathrm{I}_{r,s}(2 \times 3^{\pm 1})$	all	0,1
6	$\mathrm{II}_{r,s}(2 \times 3^{\pm 1})$	odd	$1_{\pm 1}$
7	$\mathrm{I}_{r,s}(7^{\pm 1})$	all	$0, 1_{\mp 1}, 2_{\mp 2}$
7	$\mathrm{II}_{r,s}(7^{\pm 1})$	± 2	none
8	$\mathrm{I}_{r,s}(8_{\pm 1})$	all	$0, 1, 2_{\mp 2}, 3_{\mp 3}$
8	$\mathrm{I}_{r,s}(8_{\pm 3}^{-1})$	all	$0, 1, 2_{0}, 2_{\mp 2}, 3_{\mp 1}$
8	$\mathrm{II}_{r,s}(8)$	± 1	none
8	$\mathrm{II}_{r,s}(8^{-1})$	± 1	1
8	$\mathrm{I}_{r,s}(2 \times 4)$	all	0,1,2
8	$\mathrm{II}_{r,s}(2 \times 4)$	even	0
8	$\mathrm{I}_{r,s}(2^{3})$	all	0,1,2,3
8	$\mathrm{II}_{r,s}(2^{3})$	odd	1
9	$\mathrm{I}_{r,s}(9^{\pm 1})$	all	$0, 1_{\mp 1}$
9	$\mathrm{II}_{r,s}(9^{\pm 1})$	0	0
9	$\mathrm{I}_{r,s}(3^{2})$	all	$0, 1, 2_{0}$
9	$\mathrm{I}_{r,s}(3^{-2})$	all	$0, 1, 2_{\pm 2}$
9	$\mathrm{II}_{r,s}(3^{2})$	4	none
9	$\mathrm{II}_{r,s}(3^{-2})$	0	0
10	$\mathrm{I}_{r,s}(2 \times 5^{\pm 1})$	all	0,1
10	$\mathrm{II}_{r,s}(2 \times 5)$	± 3	none
10	$\mathrm{II}_{r,s}(2 \times 5^{-1})$	± 1	none*
11	$\mathrm{I}_{r,s}(11^{\pm 1})$	all	$0, 1_{\mp 1}, 2_{\mp 2}$
11	$\mathrm{II}_{r,s}(11^{\pm 1})$	∓ 2	none

Table 15.5. The 2-elementary forms.

$\mathrm{I}_{r,s}(2_{\mathrm{I}}^{k})$,	$0 < k < n$;

$\mathrm{I}_{r,s}(2_{\mathrm{II}}^{k})$,	k even $< n$, and
	if $k = n-1$ then $r-s \equiv \pm 1 \pmod 8$,
	if $k = n-2$ then $r-s \not\equiv 4 \pmod 8$;

$\mathrm{II}_{r,s}(2_{\mathrm{I}}^{k})$,	$0 < k \equiv n \pmod 2$, and
	if $k = 1$ then $r-s \equiv \pm 1 \pmod 8$,
	if $k = 2$ then $r-s \not\equiv 4 \pmod 8$;

$\mathrm{II}_{r,s}(2_{\mathrm{II}}^{k})$,	n and k even, $r-s \equiv 0 \pmod 8$;
$\mathrm{II}_{r,s}(2_{\mathrm{II}}^{-k})$,	n and k even, $0 < k < n$, $r-s \equiv 4 \pmod 8$.

When these forms are indefinite of dimension $\geqslant 3$, *each genus contains just one spinor genus, and so, by Theorem* 14, *just one class.*

(b) *The distinct genera of* 2*-elementary forms are as shown in Table* 15.5. *In all indefinite cases these genera again contain just one class.*

9. The spinor genus

9.1 Introduction. The spinor genus, introduced by Eichler ([Eic1]; see also [Ear1], [Ear3]-[Ear5], [Hsi2]), is a refinement of the notion of genus, and its importance stems from the following remarkable result.

Theorem 14. (Eichler [Eic1]; see also [Cas3, Chap. 11, Theorem 1.4], [Wat3, Theorem 63]). *For indefinite forms of dimension at least* 3, *a spinor genus contains exactly one integral equivalence class of forms.*

The current use of the term differs slightly from Eichler's (by replacing the orthogonal group by the special orthogonal group in some places). The description given here is in essence due to Watson [Wat3], although since Watson's description is rather complicated our treatment is based on the version given by Cassels [Cas3], which we recommend to the reader who would like to see the proofs. Cassels does not however give quite enough information about spinor norms to justify the claim that the spinor genus is a practicably computable invariant. We have therefore quoted from the relevant theorem of Watson, and have taken some pains to produce a mechanical rule for computing the spinor kernel.

The invariants we described in the previous section are invariants of the genus. If two forms are in the same genus we can find a rational transformation relating them whose denominator can be made relatively prime to any given integer. If this transformation is integral (i.e. if the denominator is 1) the forms are in the same class. The concept of spinor genus arises when we apply local arguments to this rational transformation to see what obstruction there is to making it an integral one.

Each genus is partitioned into a number of spinor genera (the number is always a power of 2). There is a group of *spinor operators* acting transitively on the spinor genera, so that we can obtain any spinor genus in the genus from a fixed one by applying a suitable spinor operator. Thus the division into spinor genera is determined once we name the spinor operators and are able to decide when a given spinor operator acts trivially, i.e. is in the *spinor kernel.* Our Theorems 15-17 serve as operational definitions for the notions of spinor operator and spinor kernel.

The computations depend on the calculation of the spinor norms of operations in certain orthogonal groups. Excellent references are Kneser [Kne3], Hsia [Hsi1], Earnest and Hsia [Ear2]. These references have the additional merit of discussing the problem over more general rings and of giving the best possible conditions on the indices of prime divisors of the discriminant to ensure that an indefinite genus contains just one class.

9.2 The spinor genus. If f and g are forms of determinant d in the same genus, then they are rationally equivalent by some transformation whose denominator is prime to $2d$ [Cas3, Chap. 9], [Wat3, p. 78]. Hence we can find corresponding lattices L and M for which

$$[L:\ L\cap M] = [M:\ L\cap M] = r \quad \text{(say)}\ , \tag{36}$$

for some number r which is prime to $2d$. We may paraphrase Watson's redefinition of spinor genus by saying that f and g are in the same spinor genus if and only if r is an automorphous number (as defined below).

Theorem 15. (Obtained from Theorem 70 of [Wat3].) (a) *The spinor genus of g (or M) is determined by that of f (or L) together with the number r. Using SG to denote spinor genus we shall write*

$$SG(g) = SG(f) * \Delta(r)\ ,$$

$$SG(M) = SG(L) * \Delta(r)\ .$$

and call "$\Delta(r)$" a spinor operator.
(b) *Furthermore, if the dimension is at least* 3, *then $SG(f) * \Delta(r)$ is defined for every natural number r prime to* $2d$.

To complete the definition we need to know how to find the r's for which $\Delta(r)$ is in the spinor kernel, i.e. $\Delta(r)$ fixes every spinor genus. This is done in the next section.

Remarks. (i) Part (b) of Theorem 15 fails for dimension 2. (ii) The theorem is usually applied to indefinite forms of dimension $\geqslant 3$, in which case by Theorem 14 we need not distinguish between the spinor genus of a form and the form itself.

9.3 Identifying the spinor kernel. Any element of the orthogonal group of f, over a field not of characteristic 2, can be written as a product of reflections in certain vectors $v_1, v_2, \dots, v_k$. The *spinor norm* (defined only up to multiplication by square factors) of this operation is $f(v_1) \cdots f(v_k)$. This operation is *proper* (i.e. of determinant 1) or *improper* (determinant -1) according as k is even or odd. The proper operations form the *special orthogonal group* of the form. Only some elements of the orthogonal group of f have integral matrix entries: these are the *integral automorphisms* of f.

We call $r \in \mathbf{Q}$ *automorphous* if it is the spinor norm of a proper integral automorphism of f. Similarly a p-adic number $A = p^\alpha a \in \mathbf{Q}_p$ is *p-adically automorphous* if it is the spinor norm of a proper p-adic integral automorphism of f.

The following theorems are due to Eichler [Eic1] and Watson [Wat3]. We have obtained them by translating Cassels's versions into our notation — see in particular Theorem 3.1 of Cassels [Cas3, Chap. 11] and its corollary.

Theorem 16. *The spinor kernel consists of the spinor operators $\Delta(r)$ for which the positive integer r is an automorphous number not divisible by any prime divisor of $2d$.*

It is important that we can compute the spinor kernel "locally", in fact by performing a simple calculation for each prime in a certain finite set Π. In the terminology of the next section we have:

Theorem 17. *The spinor kernel is generated by the spinor operators $\Delta_p(A)$ for which $p \in \Pi$ and A is a p-adically automorphous number.*

9.4 Naming the spinor operators for the genus of f. Let Π be any finite set of primes that contains -1, 2 and all primes dividing $d = \det f$, where f is some form in the genus. (We shall see later that often some primes can be removed from Π with no loss of information).

Since the spinor operators depend only on the square class of r, we can name them by sequences $(\dots, r_p, \dots)_{p \in \Pi}$, in which each r_p is a p-adic unit square class. In this notation the group operation is componentwise multiplication. Rational or p-adic integers can be regarded as spinor operators in the following way.

(i) To any rational integer r not divisible by any $p \in \Pi$ there corresponds the spinor operator whose p-coordinate is the p-adic square class of r for each p. We shall write this as

$$\Delta(r) = (r, r, \dots) \tag{37}$$

(the square class being understood).

(ii) To each p-adic integer $A = p^{\alpha}a$ there corresponds the spinor operator $\Delta_p(A)$ whose p_1-coordinate (for $p_1 \neq p$) is the p_1-adic square class of p^{α}, and whose p-coordinate is the p-adic square class of a:

$$\Delta_p(A) = (p^{\alpha}, p^{\alpha}, ..., p^{\alpha}, a, p^{\alpha}, ...) . \tag{38}$$

9.5 Computing the spinor kernel from the p-adic symbols. In view of Theorem 17 the spinor kernel is determined once we know the p-adically automorphous numbers. A vector v is called a *p-adic root vector* for f if and only if the reflection in v is a p-adically integral automorphism of f. Of course this reflection has determinant -1.

Theorem 18. (Based on Theorem 81 of [Wat3]). *A p-adic number is p-adically automorphous for f if and only if it is the product of an even number of norms of p-adic root vectors for f.*

Remark. For odd p it follows from [Cas3, p. 115, Corollary 1] that every p-adically integral automorphism is the product of p-adically integral reflections. For $p = 2$ this is usually true but not always [O'Me4].

An algorithm for finding the p-adically automorphous numbers for a form.

In the rest of this section we describe a mechanical rule for finding the p-adically automorphous numbers, that can be justified using Theorem 18. §9.6 contains some examples and simplifications.

The algorithm is rather complicated to state, but is completely mechanical and very easy to apply. If $p \neq 2$ we first diagonalize f, or if $p = 2$ we express f as a direct sum of forms of the shapes

$$(qx) \quad \text{and} \quad \begin{bmatrix} qa & qb \\ qb & qc \end{bmatrix} ,$$

where q is a power of 2, a and c are divisible by 2, but x, b and $ac-b^2$ are not (see Theorem 2). We now prepare a list in two parts:

(I) If $p \neq 2$, all the diagonal entries, or if $p = 2$ the diagonal entries qx. (These numbers are not yet to be interpreted modulo squares, and of course the list may contain repeated entries.)

(II) Only if $p = 2$: the numbers $2qu_1$, $2qu_3$, $2qu_5$, $2qu_7$ for every direct summand $\begin{bmatrix} qa & qb \\ qb & qc \end{bmatrix}$.

Then the group of p-adically automorphous numbers is generated by the p-adic square classes of the ratios (or products) of all pairs of numbers from the total list, supplemented by:

(i) all p-adic units if

either $p \geqslant 3$ and f_q has dimension $\geqslant 2$ for any q,
or $p = 2$ and $f_q \oplus f_{2q} \oplus f_{4q} \oplus f_{8q}$ has dimension $\geqslant 3$ for any q,

and

(ii) the square classes

$$2u_1, \qquad 2u_3, \qquad u_5, \qquad u_3, \qquad u_7,$$

whenever $p = 2$ and part (I) of the list contains two entries whose ratio has the form

$$u_1, \qquad u_5, \qquad (1 \text{ or } 4 \text{ or } 16)u_{\text{odd}}, \qquad (2 \text{ or } 8)u_{1 \text{ or } 5}, \qquad (2 \text{ or } 8)u_{3 \text{ or } 7}$$

respectively.

Example. For the form $f = \text{diag}\,\{3, 16\}$ and the prime $p = 2$, part (I) of the list consists of $\{3 = u_3, 16 = 16u_1\}$ and part (II) is empty. Since the ratio of 16 to 3 has the form $16u_3$, we supplement the total list by u_5, according to (ii). Thus the 2-adically automorphous numbers are generated by the square classes of $\{16u_1, u_3, u_5\}$, i.e. are $\{u_1, u_3, u_5, u_7\}$.

The supplementation rules correspond to the possibilities for root vectors not necessarily in the basis. Thus e_1+e_2, of norm $2 = 2u_1$, is a 2-adic root vector for $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, illustrating the first rule in (ii).

9.6 Tractable and irrelevant primes

The following considerations may be used to simplify the calculations. If there is a prime p such that, for each p-adic unit u, the spinor operator

$$\Delta_p(u) = (1, 1, \ldots, 1, u, 1, \ldots)_{\ldots, p, \ldots} \qquad (39)$$

lies in the spinor kernel, then plainly the p-coordinate can be deleted, since it conveys no information modulo the spinor kernel. Such p are called *tractable*. For example, -1 is always tractable, as is the prime 2 in the above example.

However, a tractable prime may still have some effect on spinor genus calculations, since if p itself is automorphous, the spinor kernel will contain $\Delta_p(p)$, which has nontrivial values in coordinates other than the p-th. For example, if f is indefinite then -1 is (-1)-adically automorphous, so that $\Delta_{-1}(-1) = (+1, -1, -1, \ldots)_{-1, 2, 3, \ldots}$ is in the spinor kernel.

If the p-adically automorphous numbers are *precisely* the square classes of the p-adic units (as happens when $p \neq -1$ or 2 and $p \nmid \det(f)$), then p is not only tractable but *irrelevant*. Irrelevant primes do not affect the computation of the spinor genus in any way.

Example. We consider the form

$$f = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 18 \end{bmatrix}$$

(discussed in [Wat3, p. 115]). For $p \neq 2$ we can diagonalize f, obtaining diag $\{2, 3/2, 18\}$. To find the spinor kernel we proceed as follows.

$p = -1$: list (I) $= \{2 = u, 3/2 = u, 18 = u\}$, so u is the only (-1)-adically automorphous number.
$p = 2$: list (I) $= \{18 = 2u\}$, list (II) $= \{2u_1, 2u_3, 2u_5, 2u_7\}$, so the 2-adically automorphous numbers are $\{u_1, u_3, u_5, u_7\}$, and 2 is tractable.
$p = 3$: list (I) $= \{2 = u_-, 3/2 = 3u_-, 18 = 9u_-\}$, so the 3-adically automorphous numbers are $\{u_+, 3u_+\}$.

We need retain only the 3-coordinate since 3 is the only intractable prime, and the spinor kernel is generated by

$$\Delta_2(u_1, u_3, u_5 \text{ or } u_7) = (u_+)_3 ,$$
$$\Delta_3(u_+ \text{ or } 3u_+) = (u_+)_3$$

So $(u_-)_3$ is not in the spinor kernel, and therefore the genus of f contains two distinct spinor genera, one containing f, the other containing $f{*}(u_-)_3$. A representative for the second spinor genus is ([Wat3, p. 115])

$$\begin{bmatrix} 6 & 3 & 0 \\ 3 & 6 & 0 \\ 0 & 0 & 2 \end{bmatrix} .$$

9.7 When is there only one class in the genus? In practice one usually finds that all primes are tractable and so the spinor genus coincides with the genus (and therefore, in the case of indefinite forms of dimension at least 3, the genus contains only one class). This section gives some conditions which guarantee that this will happen.

Theorem 19. *If f is indefinite and the genus of f contains more than one class, then for some p (possibly -1), f can be p-adically diagonalized and the diagonal entries all involve distinct powers of p.*

Proof. Suppose the contrary. Then $\dim f \geqslant 3$, since otherwise in the (-1)-adic (real) diagonalization the terms involve distinct powers of -1. We now quote Eichler's theorem (Theorem 14) to see that the class coincides with the spinor genus and there must therefore be an intractable prime p. If $p \geqslant 3$ we know that none of the p-adic Jordan constituents f_q can have dimension $\geqslant 2$ and the result follows. So we may conclude that 2 is the only intractable prime. No nontrivial 2-adic Jordan constituent may have scaled type II, since then all 2-adic units are automorphous. Thus f is 2-adically diagonalizable. If any two of the diagonal terms involve the same power of 2, the algorithm implies that 5 is 2-adically automorphous, and so $(u_5)_2$ is in the spinor kernel. But since -1 is (-1)-adically automorphous, $(u_7)_2$ is also in the spinor kernel, and these generate all the possibilities. Therefore the diagonal entries may only involve distinct powers of 2. This completes the proof.

With a little more care the argument can be refined to give the following result.

Theorem 20. *Suppose f is an indefinite form of dimension n and determinant d.*
(a) *If $p \geqslant 3$ is an intractable prime then*

$$d \text{ is divisible by } p^{\binom{n}{2}} . \tag{40}$$

(b) *A prime $p \equiv 3 (\text{mod } 4)$ cannot be the only intractable prime.*

(c) *If 2 is an intractable prime then*

$$4^{[\frac{n}{2}]} d \text{ is divisible by } 4^{\binom{n}{2}} . \tag{41}$$

(d) *If 2 is the only intractable prime then*

$$4^{[\frac{n}{2}]} d \text{ is divisible by } 8^{\binom{n}{2}} . \tag{42}$$

(We recall that a prime p is tractable if $\Delta_p(u)$ is in the spinor kernel for every p-adic unit u.)

Proof. (a) If an odd prime p is intractable then from part (i) of the algorithm the powers of p in the diagonal terms of f are all distinct, and so, when arranged in increasing order, must be at least $p^0, p^1, p^2,...,$ yielding a product of at least $p^{\binom{n}{2}}$.

(b) If $p \equiv 3 \pmod 4$ is the only intractable prime then every element of the spinor kernel has a name $(u_\pm)_p$. But -1 is (-1)-adically automorphous and is a non-residue modulo p, so $(-1)_p$ is in the spinor kernel. Therefore the spinor kernel has order 2 and p is tractable, a contradiction.

(c) If 2 is intractable then from part (II) of the algorithm there is no type II summand, i.e. the form is diagonalizable. Moreover no three powers of 2 in the diagonal terms can lie in the range 2^t to 2^{t+3} (inclusive), for any t. Therefore, when arranged in increasing order, the powers of 2 must be at least

$$2^0, 2^0, 2^4, 2^4, 2^8, 2^8, \dots .$$

When multiplied by 1, 4, 1, 4, ... this sequence becomes

$$4^0, 4^1, 4^2, 4^3, \dots,$$

which implies (41).

(d) If 2 is the only intractable prime then every element of the spinor kernel has a name $(u_1)_2$, $(u_3)_2$, $(u_5)_2$ or $(u_7)_2$, and since -1 is (-1)-adically automorphous, $(u_7)_2$ is in the spinor kernel. Moreover, if any two powers of 2 in the diagonal terms have ratio 1 or 4 or 16, then by part (ii) of the algorithm $(u_5)_2$ is in the spinor kernel and all possibilities are generated. So the even powers of 2 are at least

$$2^0, 2^6, 2^{12}, \dots ,$$

and the odd powers of 2 are at least

$$2^1, 2^7, 2^{13}, \dots .$$

The least possible values are therefore

$$2^0, 2^1, 2^6, 2^7, 2^{12}, 2^{13}, \ldots ,$$

which on multiplication by 1, 4, 1, 4, ... become

$$8^0, 8^1, 8^2, 8^3, \ldots ,$$

establishing (42).

Theorem 21. *If f is an indefinite form of dimension n and determinant d, with more than one class in its genus, then*

$$4^{[\frac{n}{2}]} d \text{ is divisible by } k^{\binom{n}{2}} \qquad (43)$$

for some nonsquare natural number $k \equiv 0$ or $1 ($mod $4)$.

This is a strengthening of [Wat3, Corollaries 1 and 2 to Theorem 69]. Compare [Kne3], [Hsi1], [Ear2]. Without going into too much detail it is worth mentioning that this result is nearly best possible. If $4^{[n/2]}d$ is divisible by $k^{\binom{n}{2}}$ for such a k, then there is a genus of forms with determinant d or some small multiple of d that contains more than one class.

Proof. If the dimension is 2 the assertion is trivial. For certainly $d \neq \pm 1$, or else there is only one class in the genus. Therefore some prime $p \geqslant 2$ divides d, and (43) holds with $k = 4p$.

For dimensions $n \geq 3$, as in the proof of Theorem 19, there must be at least one intractable prime $p \geq 2$. If some $p \equiv 1 \pmod 4$ is intractable then, from (40), (43) holds with $k = p$. If two primes p and q congruent to 3 (mod 4) are intractable then (43) holds with $k = pq$. If both 2 and $p \equiv 3 \pmod 4$ are intractable then $k = 4p$ will do, from (40) and (41); if 2 is the only intractable prime then $k = 8$ will do, from (42); and by part (b) of Theorem 20 this has exhausted all the possibilities.

Corollary 22. *Suppose f is an indefinite form of dimension n and determinant d, with more than one class in its genus. Then $|d| \geqslant d_0$, where d_0 is given by the following table.*

n	2	3	4,6,8,...	5,7,9,...
d_0	17	128	$5^{\binom{n}{2}}$	$2{\cdot}5^{\binom{n}{2}}$

Proof. For large n, (42) implies that $\det f$ is divisible roughly by $8^{\binom{n}{2}}$, whereas if 5 is intractable then from (40) we need only $5^{\binom{n}{2}} \mid \det f$. The cutoff point turns out to be at $n = 4$, and for $n \geqslant 4$ the smallest determinant (for an indefinite form with more than one class in its genus) is that of the form

$$\begin{pmatrix}2&3\\3&2\end{pmatrix} \oplus 5^2\begin{pmatrix}2&3\\3&2\end{pmatrix} \oplus 5^4\begin{pmatrix}2&3\\3&2\end{pmatrix} \oplus \cdots \oplus 5^{2m}\begin{pmatrix}2&3\\3&2\end{pmatrix} \oplus 5^{2m+2}(2)$$

omitting the final term if n is even. This determinant is

$$5^{\binom{n}{2}} \text{ if } n \text{ is even}\ , \quad 2\cdot 5^{\binom{n}{2}} \text{ if } n \text{ is odd}\ . \tag{44}$$

But (42) is better than (44) when $n = 3$. For $n = 2$, we find from Table 15.2 that the binary forms

$$\begin{bmatrix}2&3\\3&-4\end{bmatrix} \text{ and } \begin{bmatrix}-2&3\\3&4\end{bmatrix}$$

are in distinct classes although both belong to the genus $\mathrm{II}_{1,1}(17)$. The pair of ternary forms with determinant -128 is given at the end of this chapter.

For definite forms the question of when there is only one class in the genus behaves completely differently, and is the subject of a series of papers by Watson [Wat5]-[Wat7], [Wat14]-[Wat22].

10. The classification of positive definite forms

10.1 Minkowski reduction. We shall not say very much about this important notion, since our main interest is in forms of large dimension where it is impracticable. (For further information see the references on reduction algorithms listed in §1.4 of Chap. 2.) Let f be a positive definite n-dimensional form. f is said to be *Minkowski reduced* if it has been expressed in terms of an integral basis $e_1,\ldots, e_n$ such that for each t, $1 \leqslant t \leqslant n$,

$$f(e_t) \leqslant f(v) \quad \text{for all integral vectors } v \text{ for which } e_1,\ldots, e_{t-1}, v$$
$$\text{can be continued to an integral basis.} \tag{45}$$

In other words each successive e_t is chosen so that $f(e_t)$ is as small as is possible. By letting v range over all integral vectors, the condition (45) implies inequalities on the matrix entries a_{ij}. It turns out [Cas3, p. 256, Theorem 1.3] that only finitely many of these inequalities are necessary ("the fundamental region has finitely many walls"), but unfortunately their number tends to infinity very rapidly with the dimension.

Some of these inequalities may be easily written down. (i) It is immediate from (45) that

$$0 < a_{11} \leqslant a_{22} \leqslant \cdots \leqslant a_{nn}\ . \tag{46}$$

(ii) If we let $v = e_t - \sum\limits_{s \in S} \epsilon_s e_s$ (for some set S of subscripts $s < t$ and coefficients $\epsilon_s = \pm 1$) the inequality $f(e_t) \leqslant f(v)$ becomes

$$2\Big| \sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r,s \in S\\ r<s}} \epsilon_r \epsilon_s a_{rs} \Big| \leqslant \sum_{s \in S} a_{ss}\ .$$

The cases $S = \{s\}, \{r, s\}, \{q, r, s\}, \ldots$ lead to

$$2|a_{st}| \leqslant a_{ss} \quad (s < t)\ , \tag{47}$$

$$2|a_{rs} \pm a_{rt} \pm a_{st}| \leqslant a_{rr}+a_{ss} \quad (r < s < t)\ , \tag{48}$$

$$\begin{gathered} 2|\alpha a_{qt}+\beta a_{rt}+\gamma a_{st}-\alpha\beta a_{qr}-\alpha\gamma a_{qs}-\beta\gamma a_{rs}| \\ \leqslant a_{qq}+a_{rr}+a_{ss} \quad (q < r < s < t)\ , \end{gathered} \tag{49}$$

with $\alpha, \beta, \gamma = \pm 1$, etc.

It is a theorem of Minkowski (see for example [Cas3, p. 257, Lemma 1.2]) that for dimension $\leqslant 4$ a reduced form may be defined using vectors v with coefficients equal to 0 or ± 1. In fact the inequalities

(46), (46)-(47), (46)-(48), (46)-(49)

(in which $q, r, s, t \leqslant n$) define a Minkowski reduced form for

$n = 1,$ 2, 3, 4

respectively.

For $n = 5$, 6, 7 and 8, defining systems of inequalities for Minkowski reduced forms have been given by Minkowski, Ryskov, Tammela and Novikova — see [Aff1], [Aff2], [Gru1], [Nov1], [Rys2], [Rys3], [Rys8], [Rys14], [Tam1]-[Tam4]. But the coefficients of v can no longer be restricted to 0 and ± 1.

Many theorems in the geometry of numbers are consequences of the inequalities (45) (see the references mentioned at the beginning of this section). In particular they can be used to show that there are only finitely many classes of forms of any given determinant [Cas1, p. 256, Theorem 1.1] and in some case to enumerate these forms [Wae5]. However, even in dimension 3, the process is tedious for moderately large determinants, and for much higher dimensions it is out of the question.

Tables 15.6 and 15.7 give all indecomposable, reduced, definite ternary forms with determinant $|d| \leqslant 50$ and the indefinite forms with $|d| \leqslant 100$. An entry $a\ _b\ c\ _f\ g\ _h$ represents the form having matrix

$$\begin{bmatrix} a & b & h \\ b & c & f \\ h & f & g \end{bmatrix},$$

and h is omitted when it is zero. Table 15.6 gives the positive definite forms with $d \leqslant 50$, and was computed using the inequalities (46)-(48). Table 15.7 gives the indefinite forms with $|d| \leqslant 100$, and was computed using the theory of spinor genera.

Table 15.6. **Indecomposable positive definite ternary forms.**

d	Forms
4	$2_1 2_1 2$
7	$2_1 2_1 3$
8	$2_1 3_1 2$
10	$2_1 2_1 4$
12	$2_1 4_1 2$, $3_1 2_1 3$
13	$2_1 2_1 5$, $2_1 3_1 3$
16	$2_1 5_1 2$, $2_1 2_1 6$, $3_1 3_1 3_{-1}$
17	$3_1 2_1 4$
18	$2_1 3_1 4$
19	$2_1 2_1 7$, $2_1 4_1 3$
20	$2_1 4_2 4$, $3_1 3_1 3_1$
21	$3_1 3_1 3$
22	$2_1 2_1 8$, $3_1 2_1 5$
23	$2_1 3_1 5$
24	$2_1 7_1 2$, $4_1 2_1 4$, $3_1 3_1 4_{-1}$
25	$2_1 2_1 9$, $2_1 5_1 3$
26	$2_1 4_1 4$
27	$3_1 2_1 6$, $2_1 4_2 5$
28	$2_1 8_1 2$, $2_1 2_1 10$, $2_1 3_1 6$, $2_1 5_2 4$, $3_1 3_1 4_1$
29	$3_1 3_1 4$
30	$3_1 4_1 3$
31	$2_1 2_1 11$, $4_1 2_1 5$
32	$2_1 9_1 2$, $3_1 2_1 7$, $3_1 3_1 5_{-1}$, $3_1 4_2 4$, $4_2 4_2 4$
33	$2_1 3_1 7$, $2_1 4_1 5$
34	$2_1 2_1 12$, $2_1 5_1 4$, $2_1 4_2 6$
35	$3_1 4_1 4_{-1}$
36	$2_1 10_1 2$, $2_1 6_2 4$, $2_1 5_1 5_{-1}$, $3_1 3_1 5_1$, $4_1 4_1 4_{-2}$
37	$2_1 2_1 13$, $2_1 7_1 3$, $3_1 2_1 8$, $2_1 5_2 5$, $3_1 3_1 5$
38	$2_1 3_1 8$, $4_1 2_1 6$
39	$3_1 5_1 3$, $3_1 4_1 4_1$
40	$2_1 11_1 2$, $2_1 2_1 14$, $2_1 4_1 6$, $5_1 2_1 5$, $3_1 3_1 6_{-1}$, $4_1 3_1 4$
41	$2_1 4_2 7$, $3_1 4_1 4$
42	$3_1 2_1 9$
43	$2_1 2_1 15$, $2_1 8_1 3$, $2_1 3_1 9$, $2_1 5_1 5$, $3_1 4_2 5$
44	$2_1 12_1 2$, $2_1 7_2 4$, $3_1 3_1 6_1$, $3_1 5_2 4$, $4_1 4_2 4$, $4_2 4_2 5$
45	$4_1 2_1 7$, $2_1 5_1 6_{-1}$, $3_1 3_1 6$
46	$2_1 2_1 16$, $2_1 5_2 6$, $3_1 4_1 5_{-1}$
47	$3_1 2_1 10$, $2_1 4_1 7$, $2_1 6_2 5$
48	$2_1 13_1 2$, $2_1 3_1 10$, $2_1 4_2 8$, $2_1 6_3 6$, $3_1 6_1 3$, $3_1 3_1 7_{-1}$, $4_1 5_1 4_{-2}$, $4_2 5_2 4$
49	$2_1 2_1 17$, $2_1 9_1 3$, $5_1 2_1 6$, $5_1 3_1 5_{-2}$
50	$2_1 7_1 4$, $3_1 5_1 4_1$, $4_1 4_1 4_{-1}$

Three forms should be added to this table:

$2_1 6_1 2$ at determinant 20, $2_1 6_1 3$ at determinant 31,
and $2_1 6_1 4$ at determinant 42.

Table 15.7. Indecomposable indefinite ternary forms.

d	Forms
∓ 8	$\pm 2 {}_1 \pm 2 {}_1 \mp 2$
∓ 28	$\pm 2 {}_1 \mp 6 {}_1 \pm 2$
∓ 32	$\pm 2 {}_1 \mp 2 {}_1 \pm 6$
∓ 56	$\pm 2 {}_1 \pm 14 {}_1 \mp 2$
∓ 64	$\pm 4 {}_2 \pm 4 {}_2 \mp 4$
∓ 68	$\pm 2 {}_1 \pm 6 {}_1 \mp 6$
∓ 72	$\pm 6 {}_1 \pm 2 {}_1 \mp 6$
∓ 72	$\pm 2 {}_1 \mp 2 {}_1 \pm 14$
∓ 92	$\pm 2 {}_1 \mp 22 {}_1 \pm 2$

10.2 The Kneser gluing method. The integral lattices generated by vectors of norm 1 and 2 are completely classified. Such a lattice can be written as a direct sum of the particular lattices

$$I_n(n \geqslant 1),\quad A_n(n \geqslant 1),\quad D_n(n \geqslant 4),\quad E_6,\quad E_7,\quad E_8.$$

Certain other lattices can be found by *gluing* these (and possibly other) components together. This technique, due to Witt and Kneser [Kne4], is described in §3 of Chap. 4. In Chaps. 16 and 17 we shall describe how, by a combination of gluing and other methods, the unimodular lattices of dimension $n \leqslant 25$ have been enumerated. However it is worth pointing out that the enumerations of unimodular lattices can be used to find lattices of other determinants in a fairly simple way, as the following section will illustrate (cf. [Kne4], [Ple12]).

10.3 Positive definite forms of determinant 2 and 3. By following the method used by Kneser [Kne4], and making use of the results of Chap. 16, in this section we classify the forms of determinant 2 up to dimension 18 and determinant 3 up to dimension 17. This is enough to demonstrate the techniques used, and since beyond this point the tables become unwieldy, is a good place to stop. The results for determinant + dimension $\leqslant 17$ agree with Kneser's.

Theorem 23. *All positive definite forms of determinant* 2 *and dimension* $\leqslant 18$, *or determinant* 3 *and dimension* $\leqslant 17$ *are as shown in Tables* 15.8 *and* 15.9.

Note. The tables explain these lattices in terms of unimodular lattices taken from Chap. 16. As in that chapter a unimodular lattice is specified by its component root lattices.

Outline of proof. Determinant 2. If L_n has determinant 2, then L_n^* / L_n has order 2 and there is a vector $v \in L_n^* \setminus L_n$ with $2v \in L_n$ and

$v \cdot v \equiv \frac{1}{2} \pmod 1$. In the particular case $L_1 = A_1$, write w instead of v, with $w \cdot w = \frac{1}{2}$. Then $L_n \oplus A_1$ can be extended by the glue vector $v+w$ to give a lattice L_{n+1} (say) of determinant 1. Conversely, $L_n = w^{\perp}$ (in L_{n+1}) $= \{x \in L_{n+1} : x \cdot w = 0\}$. Thus all n-dimensional lattices L_n of determinant 2 are uniquely obtained as the orthogonal lattices to norm 2 vectors w in $(n+1)$-dimensional lattices L_{n+1} of determinant 1.

All such L_{n+1} can be found (for $n+1 \leqslant 23$) in Chap. 16. Suppose $L_{n+1} = M_{n+1-k} \oplus \mathrm{I}_k$, where M_{n+1-k} has minimal norm $\geqslant 2$. There are now two possibilities for w.

(a) $w \in \mathrm{I}_k$ (if $k \geqslant 2$), so that $L_n = w^{\perp} = M_{n+1-k} \oplus A_1 \oplus \mathrm{I}_{k-2}$. If L_n has minimal norm 2 then we must have $L_n = M_{n-1} \oplus A_1$. These lattices are shown in column (a) of Table 15.8.

We know from Table 15.4 that there are just two genera with determinant 2, namely $\mathrm{I}_n(2)$ and $\mathrm{II}_n(2)$. $L_n = M_{n-1} \oplus A_1$ is even (i.e. in $\mathrm{II}_n(2)$) exactly when M_{n-1} is. For $n = 17$ there are three lattices in

Table 15.8. Positive definite lattices of determinant 2, minimal norm $\geqslant 2$.

Dim.	(*a*)	(*b*) $<2>^{\perp}$ in	n_{I}	n_{II}	n_{tot}
0	—	—	0	0	0
1	A_1	—	0	1	1
2	—	—	0	0	1
3	—	—	0	0	1
4	—	—	0	0	1
5	—	—	0	0	1
6	—	—	0	0	1
7	—	E_8	0	1	2
8	—	—	0	0	2
9	$E_8 \oplus A_1$	—	0	1	3
10	—	—	0	0	3
11	—	D_{12}	1	0	4
12	—	—	0	0	4
13	$D_{12} \oplus A_1$	E_7^2	2	0	6
14	—	A_{15}	1	0	7
15	$E_7^2 \oplus A_1$	D_{16}, E_8^2, D_8^2	2	2	11
16	$A_{15} \oplus A_1$	$A_{11}E_6$	3	0	14
17	$E_8^2 \oplus A_1$ $D_{16} \oplus A_1$ $D_8^2 \oplus A_1$	$A_{17}A_1$ $D_{10}E_7A_1$ D_6^3 A_9^2	6	4	24
18	$A_{11}E_6 \oplus A_1$	$E_6^3O_1$ $A_{11}D_7O_1$ $A_7^2D_5$	6	0	30

column (a), two of which are even, although the table only indicates their number. The actual components can be found from Chap. 16.

(b) Alternatively we can take w to be any norm 2 vector in a lattice M_{n+1} of determinant 1 and minimal norm 2. For example there are exactly two inequivalent choices for w in the 18-dimensional lattice $A_{11}E_6$. These lattices are shown in column (b) of Table 15.8. In Tables 15.8, 15.9 the symbol $<c>$ denotes a one-dimensional lattice $u\mathbf{Z}$ with $u \cdot u = c$.

The last three columns of Table 15.8 give n_{I} (resp. n_{II}), the number of odd (resp. even) lattices with determinant 2 and minimal norm $\geqslant 2$ in each dimension, and n_t, the number of lattices with determinant 2 and minimal norm $\geqslant 1$.

Determinant 3. If L_n has determinant 3 there is a vector $v \in L_n^* \setminus L_n$ with $3v \in L_n$ and $v \cdot v \equiv \pm 1/3 \pmod 1$. It is easy to see that if $v \cdot v \equiv 1/3 \pmod 1$ then the 3-adic symbol for L_n is $1^{n-1}\, 3^1$, and otherwise it is $1^{n-1}\, 3^{-1}$.

First we consider the case $v \cdot v \equiv 1/3 \pmod 1$. We take A_2 with $w \in A_2^* \setminus A_2$, $w \cdot w = 2/3$ (Chap. 4, Eq. (55)), and extend $L_n \oplus A_2$ by the glue vector $v+w$ to obtain a lattice L_{n+2} of determinant 1. Conversely, $L_n = A_2^{\perp}$ in L_{n+2}. If $L_{n+2} = M_{n+2-k} \oplus \mathrm{I}_k$ there are two possibilities. (a) $A_2 \subset \mathrm{I}_k$, so (if L_n has minimal norm $\geqslant 2$), $L_n = M_{n-1} \oplus <3>$, where M_{n-1} has minimal norm 2 and determinant 1. (b) $A_2 \subset M_{n+2-k}$. For example $A_2^{\perp}$ in E_8 gives $L_6 = E_6$.

Second, consider $v \cdot v \equiv -1/3 \pmod 1$. We take a 1-dimensional lattice M_1 (say) $= <3>$, with generator w of norm 3, and extend $L_n \oplus M_1$ by the glue vector $v + 1/3\, w$ to get a lattice L_{n+1} of determinant 1. Conversely, L_n is the orthogonal lattice to a norm 3 vector w in an $(n+1)$-dimensional lattice L_{n+1} of determinant 1. If $L_{n+1} = M_{n+1-k} \oplus \mathrm{I}_k$ there are now three possibilities to consider. (c) $w \in \mathrm{I}_k$, (d) the projection of w onto M_{n+1-k} has norm 2, while the projection onto I_k has norm 1, and (e) $w \in M_{n+1-k}$.

In case (d), suppose $L_{n+1} = M_n \oplus \mathrm{I}_1$, where M_n has minimal norm 2. Let $w = v+e$ where $v \in M_n$, $v \cdot v = 2$, $e \in \mathrm{I}_1$, $e \cdot e = 1$, and let $K_{n-1} = v^{\perp}$ in M_n, so that $\det K_{n-1} = 2$ (from the first part of the proof). Then $L_n = w^{\perp}$ contains K_{n-1}, and also the vector $u = v-2e$, which generates a 1-dimensional lattice $<6>$ orthogonal to K_{n-1}. In fact L_n is $K_{n-1} \oplus <6>$ extended by a glue vector $t + 1/2\, u$, where t is a nonzero glue vector for $K_{n-1}^* \,/\, K_{n-1}$.

Table 15.9 shows the lattices of minimal norm $\geqslant 2$ in the five cases, and the number of even (n_{II}) and odd (n_{I}) lattices of minimal norm 2 in each dimension. There are four genera of forms of determinant 3 (see Table 15.4), namely $\mathrm{I}_n(3^{\pm 1})$ and $\mathrm{II}_n(3^{\pm 1})$. Columns (a) and (b) belong to either $\mathrm{I}_n(3^1)$ or $\mathrm{II}_n(3^1)$, and columns (c), (d) and (e) to either $\mathrm{I}_n(3^{-1})$ or $\mathrm{II}_n(3^{-1})$. The final column, n_{tot}, gives the number of lattices with determinant 3 and minimal norm $\geqslant 1$.

Table 15.9. Positive definite lattices of determinant 3, minimal norm $\geqslant 2$.

Dim	(a)	(b)	(c)	(d)	(e)	n_I	n_{II}	n_{tot}
		$A_2^\perp$ in		$<3>^\perp$ in	$<3>^\perp$ in			
0	–	–	–	–	–	0	0	0
1	$<3>$	–	–	–	–	1	0	1
2	–	–	A_2	–	–	0	1	2
3	–	–	–	–	–	0	0	2
4	–	–	–	–	–	0	0	2
5	–	–	–	–	–	0	0	2
6	–	E_8	–	–	–	0	1	3
7	–	–	–	–	–	0	0	3
8	–	–	–	$E_8 \oplus I_1$	–	1	0	4
9	$E_8 \oplus <3>$	–	–	–	–	1	0	5
10	–	D_{12}	$E_8 \oplus A_2$	–	–	1	1	7
11	–	–	–	–	D_{12}	1	0	8
12	–	E_7^2	–	$D_{12} \oplus I_1$	–	2	0	10
13	$D_{12} \oplus <3>$	A_{15}	–	–	E_7^2	3	0	13
14	–	D_{16}, E_8^2, D_8^2	$D_{12} \oplus A_2$	$E_7^2 \oplus I_1$	A_{15}	4	2	19
15	$E_7^2 \oplus <3>$	$A_{11}E_6$	–	$A_{15} \oplus I_1$	D_8^2	5	0	24
16	$A_{15} \oplus <3>$	$A_{17}A_1$ $D_{10}E_7A_1$ D_6^3 A_9^2	$E_7^2 \oplus A_2$	$E_8^2 \oplus I_1$ $D_{16} \oplus I_1$ $D_8^2 \oplus I_1$	$A_{11}E_6$	12	0	36
17	$E_8^2 \oplus <3>$ $D_{16} \oplus <3>$ $D_8^2 \oplus <3>$	$E_6^3O_1$ $A_{11}D_7O_1$ $A_7^2D_5$	$A_{15} \oplus A_2$	$A_{11}E_6 \oplus I_1$	$A_{17}A_1$ $D_{10}E_7A_1$ D_6^3 A_9^2	17	0	53

11. Computational complexity

Finally we give a brief discussion of the complexity of the classification problem. (The complexities of other questions connected with lattices are discussed in §1.4 of Chap. 2.) The following are some of the principal questions that we have encountered.

(C1) Find the number of classes of integral quadratic forms of dimension n and determinant d. (C2) Exhibit one form in each class. (C3) Given two forms, determine if they are in the same class. (C4) If they are, find an explicit equivalence. (G1) Find the number of genera of forms of dimension n and determinant d. (G2) Exhibit one form in each genus. (G3) Given two forms, determine if they are in the same genus. (G4) If they are, find an explicit rational equivalence whose denominator is prime to any given number. A closely related problem is to find which numbers are represented by a form. (S) Given a form f of dimension n and determinant d, and an integer k, is there an integral solution to $f(x) = k$? If so, find all solutions.

We shall not say much about (S). For $n = 2$ it was solved by Gauss [Gau1, §§180, 205, 212] (see also [Bor5, p. 142], [Coh5, p. 1], [Edw1, pp. 317, 330], [Lag1], [Lag2], [Mor6]). The complexity of Gauss's solution appears to be dominated by the complexity of factoring k, which is at most $\exp(c\sqrt{\log k \log\log k})$ for some constant c [Mor8], [Pom1]. (Certainly

Gauss's solution is more efficient than the $O(\sqrt{k})$ solutions proposed in [Dij1] and [Bac3] in the case $f = x^2+y^2$.) For general n not much is known. This problem includes the determination of the minimal nonzero norm of a lattice — see §1.4 of Chap. 2.

For problem (C1), in the case $n = 2$ there are explicit formulae for the class number, which can be evaluated in a number of steps that is a polynomial in d [Cas3, p. 371], [Dic2, Chap. VI].

For positive definite forms of fixed dimension n, all of (C1)-(C4) and (G1)-(G4) can be solved by algorithms whose running time is a polynomial in d. (By using Minkowski-reduced forms (§10.1), all entries in the matrices and vectors involved can be bounded by simple functions of d (compare §3.2).) However these polynomials typically behave like d^{n^2}, so the growth as a function of n is likely to be worse than exponential. Furthermore the mass formula (see Chap. 16) shows that the class number for definite forms grows at least as fast as n^{n^2} [Mil7, p. 50]. Since it seems unlikely that one can find the class number for $n > 2$ without determining all the classes, the complexity of (C1) and (C2) for definite forms as a function of n seems to be worse than exponential.

In the remainder of this section we consider indefinite forms. If the determinant is given in factored form, problem (C1) is easy. Using the method of §§7,8, the number of steps required is a polynomial in the number of factors of d. If d is a prime, for example, the answer is given in Theorem 13.

Our invariants for the genus and spinor genus also provide quick (and polynomial-time) solutions to (G1), (G3) and usually (C3). We illustrate with a notorious example. Dickson and Ross in 1930 were unable to decide whether the ternary forms $x^2-3y^2-2yz-23z^2$ and $x^2-7y^2-6yz-11z^2$ were equivalent [Dic3, p. 147]. It is now known that they are equivalent [Ben2], [Cas3, pp. 132, 251], but we shall establish this using our invariants. Replacing the forms by their negatives for convenience, the problem is to decide the integral equivalence of

$$\begin{bmatrix} 3 & 1 & 0 \\ 1 & 23 & 0 \\ 0 & 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 7 & 3 & 0 \\ 3 & 11 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

We first compute the genus in each case. By rational transformations of denominators 3 and 7, respectively, the forms may be diagonalized to

$$\operatorname{diag}\,\{3, \frac{68}{3}, -1\} \quad \text{and} \quad \operatorname{diag}\,\{7, \frac{68}{7}, -1\}\,.$$

Therefore, since 3 and 7 are odd and prime to the determinant -68, we can read off the relevant p-adic symbols

$$\begin{array}{rll} p = -1: & +^2\,- & +^2\,- \\ p = 17: & 1^{-2}\,17^{-1} & 1^{-2}\,17^{-1} \\ p = 2: & 1_2^{-2}\,4_3^{-1} & 1_6^{+2}\,4_7^{+1} \end{array}$$

and since the first 2-adic symbol is converted to the second by a 2-step walk, the forms are indeed in the same genus.

Let us compute the spinor kernel for the first form. Plainly 2 is the only intractable prime, although -1 is still relevant since it tells us that -1 is (-1)-adically automorphous and so $(u_7)_2$ is in the spinor kernel. Since two of the terms in the 2-adic diagonalization have ratio $-3 = u_5$, $(u_5)_2$ is also in the spinor kernel, which therefore includes everything, and so there is only one class in the genus. Thus the two forms are integrally equivalent. In fact the unimodular matrix

$$M = \begin{bmatrix} -3 & 2 & 10 \\ -2 & 3 & 14 \\ -1 & 1 & 5 \end{bmatrix} \tag{50}$$

transforms the first form into the second.

There do not seem to be good algorithms for the remaining problems (C2)-(C4), (G2) and (G4). *Logically* there is no difficulty: the proofs of the theorems on genus and spinor genus (Theorems 9, 10, 14 etc.) are at bottom computationally effective. For example, for problems (C3), (C4) and (G4), if two forms are known to be in the same genus, we can in principle search through all rational matrices until a rational equivalence of denominator r prime to $2d$ is found. The forms are then in the same class if and only if $\Delta(r)$ is in the spinor kernel. If they are in the same class we can continue the search until an integral equivalence is found. (The matrix (50) was essentially found by this procedure, after using the diophantine equations resulting from Eq. (4) to restrict the search.) For problems (C2) and (G2) we search through all integral matrices in turn, applying these techniques, until we have found the correct number of distinct classes or genera of forms of determinant d. But these are only logicians' solutions, and it is not clear to us that in general they can be converted into practical algorithms.

Often there is some convenient artifice. Sometimes one can make use of Gauss's complete theory of binary forms. We illustrate by finding two inequivalent indefinite ternary forms of determinant -128 of the same genus (see Corollary 22). It is easy to see that the genus of $f = \text{diag}\,\{-1, 64, 2\}$, namely $\text{I}_{2,1}(2\times 64)$, contains two spinor genera and hence two classes, namely f and $f * \Delta(3)$. We must find a representative for the second class. Thus we wish to find two lattices L and M in this genus whose intersection has index 3 in each of them. Among the binary forms of determinant -64 we find the form $\begin{bmatrix} -9 & 1 \\ 1 & 7 \end{bmatrix}$, which remains integral when its first row and column are divided by 3 and simultaneously its second row and column are multiplied by 3, yielding $\begin{bmatrix} -1 & 1 \\ 1 & 63 \end{bmatrix}$ So the ternary forms

$$(a)\ \begin{bmatrix} -1 & 1 & 0 \\ 1 & 63 & 0 \\ 0 & 0 & 2 \end{bmatrix} \text{ and } (b)\ \begin{bmatrix} -9 & 1 & 0 \\ 1 & 7 & 0 \\ 0 & 0 & 2 \end{bmatrix} \tag{51}$$

represent lattices L and M for which generators can be chosen in the form e_1, e_2, e_3 for L and $3e_1, e_2/3, e_3$ for M. Now L also possesses the diagonal basis e_1, e_1+e_2, e_3, showing that it corresponds to the original form f. The matrix (51b) is therefore a representative for the second class in this genus.