

§1. Gauss sums and equivalence of quadratic forms

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **35 (1989)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **11.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

§ 1. GAUSS SUMS AND EQUIVALENCE OF QUADRATIC FORMS

We summarize in this section some classical criteria, essentially due to Minkowski (cf. [8]), for \mathbf{Z}_p -equivalence of quadratic forms in terms of Gauss sums.

In general, if f and g are two integral quadratic forms in k variables over a ring Λ , and A and B are the symmetric matrices with entries in Λ such that $f(x) = x^T A x$, $g(x) = x^T B x$, we will say that f and g are Λ -equivalent, (resp. of the same Λ -type) if there exist $P, Q \in GL(k, \Lambda)$ such that $B = P^T A P$ (resp. $B = Q A P$). In the first case we shall write " $f \sim g$, over Λ ".

Let p be a prime, $t \geq 1$ an integer and let $\Lambda = \mathbf{Z}/p^t \mathbf{Z}$ with discrete topology. Let dn be the Haar measure of Λ normalized by $dn(\Lambda) = p^t$ and take $\phi = 1$. The representation mass (0.1) of $n \in \Lambda$ by a quadratic form f over Λ is the ordinary number of representations

$$r(n, f, p^t) := \# f^{-1}(n).$$

Its Fourier transform is given by

$$\theta(m, f, p^t) := \sum_{n=1}^{p^t} r(n, f, p^t) \exp(2\pi i n m p^{-t}).$$

It clearly coincides with the Gauss-Weil transform (0.3), which in this case is the ordinary Gauss sum:

$$\theta(m, f, p^t) = \sum_{x \in \Lambda^k} \exp(2\pi i m f(x) p^{-t}).$$

By the Fourier inversion formula we have, moreover,

$$(1.1) \quad r(n, f, p^t) = p^{-t} \sum_{m=1}^{p^t} \theta(m, f, p^t) \exp(-2\pi i m n p^{-t}).$$

As is well known, any integral p -adic form is \mathbf{Z}_p -equivalent to an orthogonal sum of 1-dimensional forms if $p > 2$, and 1-dimensional and 2-dimensional forms if $p = 2$. Since, on the other hand, given two integral p -adic forms f and g we have for every $t \geq 1$

$$\theta(\cdot, f \perp g, p^t) = \theta(\cdot, f, p^t) \theta(\cdot, g, p^t),$$

the θ values of f can be deduced from the next proposition.

PROPOSITION 1.1. i) Let $u, v \in \mathbf{Z}_p, p \nmid uv$ and $s, t \in \mathbf{Z}, s \geq 0, t \geq 1$. Then

$$\theta(u, p^s v X^2, p^t) = \begin{cases} p^t & \text{if } t \leq s \\ p^{(t+s)/2} \left(\frac{uv}{p}\right)^{t+s} \varepsilon_p^{(t+s)^2} & \text{if } t > s, p > 2 \\ 0 & \text{if } t = s + 1, p = 2 \\ 2^{(t+s+1)/2} \left(\frac{2}{uv}\right)^{t+s+1} \exp(2\pi i uv/8) & \text{if } t > s + 1, p = 2. \end{cases}$$

where $\varepsilon_p = 1$ or i , according to $p \equiv 1$ or $3 \pmod{4}$.

ii) Let $F(X, Y) = vX^2 + 2wXY + zY^2, 2 \nmid (v, w, z)$ be a 2-adic non-diagonalizable integral quadratic form. Then if $t \geq 1$ and $u \in \mathbf{Z}_2$ is odd

$$\theta(u, 2^s F, 2^t) = \begin{cases} 2^{2t} & \text{if } t \leq s. \\ 2^{t+s+1} \left(\frac{2}{d}\right)^{t+s+1} & \text{if } t > s, \end{cases}$$

where $d = vz - w^2$.

Proof. From the definition of θ it is clear that

$$\theta(u, p^s v f, p^t) = \theta(p^s uv, f, p^t) = \begin{cases} p^{tk} & \text{if } t \leq s, \\ p^{sk} \theta(uv, f, p^{t-s}) & \text{if } t > s, \end{cases}$$

for any integral p -adic form f and u, v, s, t as in i). Hence the assertion of i) follows from the well-known values of the Gauss sums $\theta(\cdot, X^2, p^t)$ (cf. [3], Ch. 7, Thms. 5.6 and 5.7).

Let $F(X, Y)$ be as in ii). Being primitive, F is diagonalizable if and only if it represents some odd integer, and this is equivalent to v or z being odd. Suppose that $t > s$ and v and z even. One computes easily by hand that

$$\theta(u, F, 2) = 4, \quad \theta(u, F, 4) = 8 \left(\frac{2}{d}\right).$$

If $t \geq 3$, we get ii) from the equality

$$\theta(u, F, 2^t) = 4\theta(u, F, 2^{t-2}). \quad \square$$

THEOREM 1.2. *Let f, g be two non-singular integral p -adic quadratic forms in k variables. If $p = 2$, assume that they are of the same type. The following conditions are equivalent:*

- i) $f \sim g$ over \mathbf{Z}_p ,
- ii) $r(\cdot, f, p^t) = r(\cdot, g, p^t)$ for all $t \geq 1$,
- iii) $\theta(\cdot, f, p^t) = \theta(\cdot, g, p^t)$ for all $t \geq 1$.

Two \mathbf{Z}_p -equivalent forms are, in particular, $\mathbf{Z}/p^t\mathbf{Z}$ -equivalent for all $t \geq 1$, hence they have the same representation numbers $r(n, f, p^t)$ for all $t \geq 1, n \in \mathbf{Z}_p$. Since $r(\cdot, f, p^t)$ and $\theta(\cdot, f, p^t)$ are Fourier transforms over $\mathbf{Z}/p^t\mathbf{Z}$ one of each other, ii) and iii) are clearly equivalent. Therefore, the proof of Theorem 1.2 is reduced to showing that Gauss sums determine \mathbf{Z}_p -equivalence. This is easy if $p > 2$:

Proof of Theorem 1.2 for $p > 2$. We proceed by induction on k . Let $f(X) = p^s v X^2, g(X) = p^{s'} v' X^2, p \nmid vv'$. By Proposition 1.1, the equality $\theta(1, f, p^t) = \theta(1, g, p^t)$ for $t = s + 1, s + 2$ implies that $s = s'$ and $\left(\frac{v}{p}\right) = \left(\frac{v'}{p}\right)$, thus $f \sim g$ over \mathbf{Z}_p . Let $f = p^s f_0, g = p^{s'} g_0$ be two forms in k variables with f_0, g_0 primitive. If they have the same Gauss sums, then $s = s'$, otherwise, if $s < s'$ by Proposition 1.1 we would have

$$|\theta(1, f, p^{s'})| < \theta(1, g, p^{s'}) = p^{s'k},$$

a contradiction. Since f_0 and g_0 will have the same Gauss sums, we can suppose that f and g are both primitive. Let u be a p -adic unit represented by f and g . It is well known that, over \mathbf{Z}_p , we have splittings

$$f \sim \langle u \rangle \perp f_1, \quad g \sim \langle u \rangle \perp \langle g_1 \rangle.$$

Since $\theta(\cdot, uX^2, p^t)$ never vanishes and \mathbf{Z}_p -equivalent forms have the same Gauss sums, we will have

$$\theta(\cdot, f_1, p^t) = \frac{\theta(\cdot, f, p^t)}{\theta(\cdot, uX^2, p^t)} = \frac{\theta(\cdot, g, p^t)}{\theta(\cdot, uX^2, p^t)} = \theta(\cdot, g_1, p^t),$$

for all t . By the induction hypothesis this implies $f_1 \sim g_1$, hence $f \sim g$ over \mathbf{Z}_p . \square

The proof of Theorem 1.2 for $p = 2$ is much more delicate, due to the fact that Gauss sums can vanish in this case. We need a few properties of 2-adic forms which we sum up in Lemma 1.3 below.

We recall that a primitive 2-adic integral quadratic form is called *properly primitive* if it represents some odd integer, otherwise it is called *improperly primitive*. Clearly a 2-dimensional primitive form is properly primitive if and only if it is diagonalizable over \mathbf{Z}_2 .

LEMMA 1.3. (cf. [1, Ch. 8]). Let $H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $H' = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Then

i) Every improperly primitive form over \mathbf{Z}_2 is \mathbf{Z}_2 -equivalent to one of the following two:

$$H \perp \dots \perp H \perp H \quad \text{or} \quad H \perp \dots \perp H \perp H'.$$

ii) For any 2-adic unit u we have splittings over \mathbf{Z}_2 :

$$\langle u \rangle \perp H \sim \langle u, 1, -1 \rangle,$$

$$\langle u \rangle \perp H' \sim \langle u-2, u+2, (2u+3)(u+2)^{-1} \rangle,$$

$$\langle 2u \rangle \perp H \sim \langle 2u+8 \rangle \perp H'.$$

Proof of Theorem 1.2 for $p = 2$. By induction on k . Let $f(X) = 2^s v X^2$, $g(X) = 2^{s'} v' X^2$, $2 \nmid v v'$. By Proposition 1.1, $\theta(1, f, 2^t) = \theta(1, g, 2^t)$ for $t = s + 2, s + 3$ implies that $s = s'$ and $v \equiv v' \pmod{8}$, hence $f \sim g$ over \mathbf{Z}_2 . Let f and g be two forms in k variables, $k \geq 2$, of the same type. We consider the splittings over \mathbf{Z}_2 :

$$f \sim 2^{s_1} f_1 \perp \dots \perp 2^{s_r} f_r,$$

$$g \sim 2^{s_1} g_1 \perp \dots \perp 2^{s_r} g_r, \quad 0 \leq s_1 < s_2 < \dots < s_r,$$

f_i, g_i with unit determinant and the same number of variables, k_i , for all i . Without restriction we can suppose that f and g are primitive, that is $s_1 = 0$. If f and g have the same Gauss sums, then for each i , f_i and g_i are both properly or improperly primitive since, by Proposition 1.1, this is equivalent to the vanishing or not of $\theta(1, f, 2^{s_i+1})$. The proof proceeds in a different way according to whether f_1, g_1 are properly or improperly primitive.

Suppose that f_1 and g_1 are improperly primitive. If $k_1 > 2$, by i) of Lemma 1.3 we have, over \mathbf{Z}_2 ,

$$f \sim H \perp F, \quad g \sim H \perp G,$$

and, since $\theta(\cdot, H, 2^t)$ never vanishes, we have

$$\theta(\cdot, F, 2^t) = \frac{\theta(\cdot, f, 2^t)}{\theta(\cdot, H, 2^t)} = \theta(\cdot, G, 2^t),$$

for all t . By the induction hypothesis $F \sim G$, hence $f \sim g$ over \mathbf{Z}_2 . If $k_1 = 2$ and $f_1 \sim g_1$ over \mathbf{Z}_2 , we can proceed as above. Suppose that $k_1 = 2$ and

$$\begin{aligned} f &\sim H \perp 2^{s_2} f_2 \perp \dots \perp 2^{s_r} f_r, \\ g &\sim H' \perp 2^{s_2} g_2 \perp \dots \perp 2^{s_r} g_r. \end{aligned}$$

If $s_2 > 1$ (or $k = k_1 = 2$) or f_2, g_2 are improperly primitive we have

$$\theta(1, f, 4) = 2^{3+2(k-2)} = -\theta(1, g, 4),$$

a contradiction. Hence $s_2 = 1$ and f_2, g_2 are diagonalizable. By ii) of Lemma 1.3, $g \sim H \perp 2^{s_2} g'_2 \perp \dots$, over \mathbf{Z}_2 , and we can proceed as above.

Suppose now that f_1 and g_1 are properly primitive. Let u be a 2-adic unit represented by f and g . We have splittings over \mathbf{Z}_2 :

$$(1.2) \quad f \sim \langle u \rangle \perp F, \quad g \sim \langle u \rangle \perp G.$$

Since $\theta(\cdot, uX^2, 2^t) \neq 0$ for $t \neq 1$, we get $\theta(\cdot, F, 2^t) = \theta(\cdot, G, 2^t)$ for all $t \neq 1$. We have only to prove that $\theta(\cdot, F, 2) = \theta(\cdot, G, 2)$ and the claim will follow from the induction hypothesis. If $k_1 = 1$ or F and G are both properly or improperly primitive we are done. Assume that F is properly and G improperly primitive. This is possible indeed (see ii) of Lemma 1.3). By ii) of Lemma 1.3 we can always find a \mathbf{Z}_2 -splitting $g \sim \langle u \rangle \perp G'$, with G' properly primitive except for the case that over \mathbf{Z}_2

$$g \sim \langle u \rangle \perp H' \perp 2^{s_2} g_2 \perp \dots,$$

with $k_1 = 3$ and $s_2 > 1$ (or $k = 3$) or g_2 improperly primitive. Let us assume in this case that over \mathbf{Z}_2

$$f \sim \langle u, v, w \rangle \perp 2^{s_2} f_2 \perp \dots.$$

From $\theta(1, f, 4) = \theta(1, g, 4)$ we get

$$\exp(2\pi i(v+w)/8) = -\left(\frac{2}{vw}\right),$$

or, equivalently, $vw \equiv 3 \pmod{8}$. This implies that either v or w are congruent (mod 8) to any of $u - 2, u + 2$; hence, changing u by v or w we get a splitting (1.2) with F and G both properly primitive. \square

Remark. For $p = 2$ and $k \leq 4$ we could remove in the theorem the condition of f and g being of the same type. For $k \geq 5$ this is not

possible anymore, as the following example shows: By Proposition 1.1 the diagonal forms $f = \langle 1, 2, 2, 2, 4 \rangle$, $g = \langle 1, 1, 2, 4, 4 \rangle$ have the same Gauss sums $\theta(\cdot, f, 2^t) = \theta(\cdot, g, 2^t)$ for all $t \geq 1$, however they are obviously not \mathbf{Z}_2 -equivalent.

The theory of Minkowski reproduced in this section was extended by O'Meara to integral quadratic forms over local fields.

§ 2. LOCAL REPRESENTATION MASSES AND \mathbf{Z}_p -EQUIVALENCE OF FORMS

We identify \mathbf{Q}_p with its topological dual by defining $\langle n, m \rangle = \chi_p(nm)$, where χ_p is Tate's character:

$$\chi_p(a) = \exp\left(2\pi i \sum_{s < 0} a_s p^s\right),$$

if $a = \sum_{s \geq s_0} a_s p^s$. Let dn be the Haar measure of \mathbf{Q}_p normalized by $dn(\mathbf{Z}_p) = 1$. As is well-known, dn is selfdual. Let dx be the Haar measure of \mathbf{Q}_p naturally induced by dn .

Let f be a non-singular integral p -adic quadratic form in $k \geq 1$ variables. We shall deal in this section with the representation mass function given by (0.1) for $\phi = 1_{(\mathbf{Z}_p)^k}$. That is, we define for all $n_o \in \mathbf{Q}_p$:

$$r(n_o, f, \mathbf{Z}_p) = \lim_{U \rightarrow \{n_o\}} (dx(f^{-1}(U) \cap \mathbf{Z}_p^k) / dnU),$$

whenever this limit exists. Clearly r has support contained in \mathbf{Z}_p . We can also consider the Gauss-Weil transform of $1_{(\mathbf{Z}_p)^k}$ by f given by

$$\theta(m, f, \mathbf{Q}_p) = \int_{\mathbf{Z}_p^k} \langle f(x), m \rangle dx.$$

The relationship between these representation masses and the ones introduced in the preceding section is given in the following

LEMMA 2.1. i) Let $n \in \mathbf{Z}_p$, $n \neq 0$, and $t > v_p(4n)$. Then

$$r(n, f, \mathbf{Z}_p) = \lim_{s \rightarrow \infty} p^{(1-k)s} r(n, f, p^s) = p^{(1-k)t} r(n, f, p^t).$$

ii) Let $m \in \mathbf{Z}_p$ and $u \in \mathbf{Z}_p$, $t \geq 1$ be chosen arbitrarily satisfying $m = up^{-t}$. Then

$$\theta(m, f, \mathbf{Q}_p) = p^{-kt} \theta(u, f, p^t).$$