Sci. Rep. Kanazawa Univ.
Vol. 37, No. 1 pp. 1-22
July 1992

Gaussian composition of congruence classes

Yoshiomi FURUTA

Department of Mathemtics, Faculty of science, Kanazawa University
(received : March 25, 1992)

Abstruct. Gaussian composition of binary quadratic forms is recalled in some convenient forms and the composition of integral quadratic forms is generalized in the case of congruence classes.

Introduction

In [3], Gauss has defined a composition of quadratic forms, and shown that the copmposition induces a group structure of the unimodular equivalence classes of quadratic forms. It is well-known now that there is an isomorphism between the group of the unimodular equivalence classes of quadratic forms and the group of the absolute ideal classes of a quadratic field.

The purpose of the present paper is to reformulate Gaussian composition in some convenient forms and to generalize the above isomorphism to the case of congruence class groups.

At first in Section 1, we recall the composition in [3] and reformulate them in some convenient forms. In Section 2, we shall show a duplication formula by direct calculation implied from the Gaussian compostion treated in Section 1, which has been implied from a syzygy in our previous paper [2]. Its ternary form representation will be shown in Section 3.

In Section 4 we have a correspondence between equivalence classes of quadratic forms modulo the congruence subgroup $\Gamma_0(m)$ and congruence ideal classes mod m, and in Section 5 an isomorphism between them as groups by means of concordant forms in [1, Chap. 14]. Its ternary form representation mod m in explicit forms will be given in Section 6.

§1. Gaussian composition of quadratic forms

Let R be an integral domain. We denote by $f = [a, b, c]$ a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ over R, and set $[f] = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$, that is, $f(x, y) = [x, y][f]\,{}^t[x, y]$.

We recall the Gaussian composition in [3] arranging by means of matrices. Let $f_1 = [a_1, b_1, c_1]$ and $f_2 = [a_2, b_2, c_2]$ be two binary quadratic forms. We call a binary quadratic form $F = [A, B, C]$ a *Gaussian composition* of f_1 and f_2, when there are square matrices P and Q of degree 2 such that

$$X = [x_1, y_1]\, P\, {}^t[x_2, y_2], \quad Y = [x_1, y_1]\, Q\, {}^t[x_2, y_2]$$

and

$$F(X,Y) = f_1(x_1,y_1)f_2(x_2,y_2).$$

When $P = \begin{bmatrix} p_1 & p_2 \\ p_2' & p_3 \end{bmatrix}$ and $Q = \begin{bmatrix} q_1 & q_2 \\ q_2' & q_3 \end{bmatrix}$, F is called a Gaussian composition of f_1 and f_2 by P and Q, or by $[p_1, p_2, p_2', p_3]$ and $[q_1, q_2, q_2', q_3]$.

The following proposition is implied from [3, Art. 235] by use of matrices and changing some of letters.

PROPOSITION 1.1([3, ART. 235]). *Let*

$$(1.2)\quad \begin{cases} P = \begin{bmatrix} p_1 & p_2 \\ p_2' & p_3 \end{bmatrix}, \quad Q = \begin{bmatrix} q_1 & q_2 \\ q_2' & q_3 \end{bmatrix}, \\ P_1 = \begin{bmatrix} p_1 & p_2 \\ q_2' & q_3 \end{bmatrix}, \quad Q_1 = \begin{bmatrix} q_1 & q_2 \\ p_2' & p_3 \end{bmatrix}, \\ E_1 = \begin{bmatrix} p_1 & p_2 \\ q_1 & q_2 \end{bmatrix}, F_1 = \begin{bmatrix} p_1 & p_3 \\ q_1 & q_3 \end{bmatrix}, G_1 = \begin{bmatrix} p_2' & p_3 \\ q_2' & q_3 \end{bmatrix}, \\ E_2 = \begin{bmatrix} p_1 & p_2' \\ q_1 & q_2' \end{bmatrix}, F_2 = \begin{bmatrix} p_2 & p_2' \\ q_2 & q_2' \end{bmatrix}, G_2 = \begin{bmatrix} p_2 & p_3 \\ q_2 & q_3 \end{bmatrix}. \end{cases}$$

Let further

$$(1.3)\quad \begin{cases} A = -|Q|, & B = |P_1| + |Q_1|, & C = -|P|, \\ a_1 = |E_1|, & b_1 = |F_1| - |F_2|, & c_1 = |G_1|, \\ a_2 = |E_2|, & b_2 = |F_1| + |F_2|, & c_2 = |G_2|, \end{cases}$$

and

$$f_1 = [a_1, b_1, c_1],\ f_2 = [a_2, b_2, c_2],\ F = [A, B, C].$$

Then F is a Gaussian composition of f_1 and f_2 by P and Q, that is, we have

$$(1.4)\qquad F(X,Y) = f_1(x_1,y_1)f_2(x_2,y_2),$$

where

$$(1.5)\qquad X = [x_1, y_1]\, P\, {}^t[x_2, y_2], \quad Y = [x_1, y_1]\, Q\, {}^t[x_2, y_2].$$

The discriminants of f_1, f_2 and F are all coincide.

This is verified by direct calculation when the result has given. Gauss has found it by analyzing the condition of (1.5) to be satisfied (1.4), which implies the converse statement of Proposition 1.1 as follows by modifying Gauss's method.

PROPOSITION 1.6 ([3, ART. 235]). *Let $f_1 = [a_1, b_1, c_1]$, $f_2 = [a_2, b_2, c_2]$, and $F = [A, B, C]$ be quadratic forms of same discriminant D. Suppose that F is a Gaussian composition of f_1 and f_2 by $[p_1, p_2, p_2', p_3]$ and $[q_1, q_2, q_2', q_3]$, that is, they satisfy (1.4) and (1.5). Then the coefficients of f_1, f_2 and F are determined by P and Q and the relations (1.2) and (1.3) exept trivial change of signs of the coefficients.*

Proof. Let $P = \begin{bmatrix} p_1 & p_2 \\ p_2' & p_3 \end{bmatrix}$ and $Q = \begin{bmatrix} q_1 & q_2 \\ q_2' & q_3 \end{bmatrix}$. Define a matrix $M_2(x_2, y_2)$ by

$$M_2(x_2, y_2) = [P\,{}^t[x_2, y_2], Q\,{}^t[x_2, y_2]]. \tag{1.7}$$

Then $[X, Y] = [x_1, y_1]M(x_2, y_2)$ and for fixed values of x_2, y_2, we have

$$\begin{aligned}[x_1, y_1]M_2(x_2, y_2)[F]\,{}^tM_2(x_2, y_2)\,{}^t[x_1, y_1] \\ = [x_1, y_1]f_2(x_2, y_2)[f_1]\,{}^t[x_1, y_1].\end{aligned} \tag{1.8}$$

This implies

$$M_2(x_2, y_2)[F]\,{}^tM_2(x_2, y_2) = f_2(x_2, y_2)[f_1], \tag{1.9}$$

and by taking their determinants, we have

$$|M_2(x_2, y_2)|^2 = f_2(x_2, y_2)^2. \tag{1.10}$$

Now it follows from (1.7) and (1.10) that

$$a_2^2 = f_2(1, 0)^2 = |M_2(1, 0)|^2 = |E_2|^2, \tag{1.11}$$

$$c_2^2 = f_2(0, 1)^2 = |M_2(0, 1)|^2 = |G_2|^2, \tag{1.12}$$

It is further easy to see by direct calculation that

$$|M_2(1, 1)| = |E_2| + |F_2| + |F_1| + |G_2|,$$

$$|M_2(1, -1)| = |E_2| - |F_2| - |F_1| + |G_2|.$$

Thus (1.10) implies $(a_2 + b_2 + c_2)^2 = |E_2| + |F_2| + |F_1| + |G_2|$, $(a_2 - b_2 + c_2)^2 = |E_2| - |F_2| - |F_1| + |G_2|$, and hence

$$b_2^2 = (|F_1| + |F_2|)^2. \tag{1.13}$$

In the same way as above, let

$$M_1(x_1,y_1)=[[x_1,y_1]P,[x_1,y_1]Q]. \tag{1.14}$$

Then

$$[X,Y]=M_1(x_1,y_1)\,{}^t[x_2,y_2]=[x_2,y_2]\,{}^tM(x_1,y_1), \tag{1.15}$$

$$M_1(x_1,y_1)[F]\,{}^tM_1(x_1,y_1)=f_1(x_1,y_1)[f_1], \tag{1.16}$$

$$|M_1(x_1,y_1)|^2=f_1(x_1,y_1)^2. \tag{1.17}$$

Then we have

$$a_1^2=f_1(1,0)^2=|M_1(1,0)|^2=|E_1|^2, \tag{1.18}$$

$$c_1^2=f_1(0,1)^2=|M_1(0,1)|^2=|G_1|^2, \tag{1.19}$$

and further

$$|M_1(1,1)|=|E_1|+|F_1|-|F_2|+|G_1|,$$
$$|M_1(1,-1)|=|E_1|-|F_1|+|F_2|+|G_1|.$$

Hence

$$b_1^2=(|F_1|-|F_2|)^2. \tag{1.20}$$

Now, we claim that the left hand side of (1.4) is unique by given f_1, f_2, P and Q. To see this, it is enough to show that $[X^2, XY, Y^2]$ gives three independent vectors by suitable values of x_1, x_2, y_1, y_2, and this is easily seen because of infinitely many possibities of the values of each of x_1, x_2, y_1, y_2. Thus, if the coefficients of f_1 and f_2 satisfy (1.3), then the coefficients of F must also satisfy (1.3). This is realy the possible case by Proposition 1.1, and the following other cases are trivially possible: (i) $F=(-f_1)(-f_2)$, (ii) $(-F)=(-f_1)(f_2)$, (iii) $(-F)=f_1(-f_2)$. There is no other case than the above. because, $D=B^2-4AC=b_1^2-4a_1c_1=b_2^2-4a_2c_2$ by assumption of the proposition. Hence the signs of a_1, c_1 must be follow suit by $4a_1c_1=(|F_1|-|F_2|)^2-D$, and the signs of a_2, c_2 by $4a_2c_2=(|F_1|+|F_2|)^2-D$. The case changing sign of only b_1 or b_2 is never happen. Because, if it happen, say the case of $-b_1$, then it is easy for instance by replacing $-y_1$ instead of y_1 to see that (1.16) holds if the sign of

p_2 and p_2' are changed. But this contradicts to the uniquness of the left hand side as already seen above.

Remark 1.21. We define $\beta_f(U)$ for a quadratic form $f = [a, b, c]$ and a square matrix $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$ by

$$\beta_f(U) = 2au_1u_2 + b(u_1u_4 + u_2u_3) + 2cu_3u_4. \tag{1.22}$$

Then

$${}^tU \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} U = \begin{bmatrix} f(u_1, u_3) & \beta_f(U)/2 \\ \beta_f(U)/2 & f(u_2, u_4) \end{bmatrix}, \tag{1.23}$$

and the forms [1] to [8] of [3, Art. 235] are followed from (1.9) and (1.16). The form [9] coincides with $\beta_F(F_1) + \beta_F(F_2) = 2b_1b_2$, which is followed from (1.4) by direct calculation.

Gauss has given a method to obtain a composition of given quadratic forms f_1 and f_2 as follows.

Proposition 1.24 [3, Art. 236]. *Let $f_1 = [a_1, b_1, c_1]$, $f_2 = [a_2, b_2, c_2]$ be primitive quadratic forms of same discriminant. Set*

$$S = \begin{bmatrix} 0 & a_1 & a_2 & \frac{b_1 + b_2}{2} \\ -a_1 & 0 & -\frac{b_1 - b_2}{2} & c_2 \\ -a_2 & \frac{b_1 - b_2}{2} & 0 & c_1 \\ -\frac{b_1 + b_2}{2} & -c_2 & -c_1 & 0 \end{bmatrix}.$$

Choose elements $[r], [q], [s]$ and $[p]$ in R^4 as follows:

$$S\,{}^t[r] \neq 0, \qquad S\,{}^t[r] = {}^t[q],$$

$$[s]\,{}^t[q] = 1, \qquad {}^t[p] = S\,{}^t[s].$$

Let matrices P, Q, P_1 amd Q_1 be the same as in Proposition 1.1 by the componens of $[p]$ and $[q]$. Let further A, B, C and $F = [A, B, C]$ be also as in Proposition 1.1 .

Then F is the Gaussian composition of f_1 and f_2.

Proof. We can recall Gauss's proof as follows. Let

$$T = \begin{bmatrix} 0 & c_1 & -c_2 & -\dfrac{b_1 - b_2}{2} \\ c_1 & 0 & -\dfrac{b_1 + b_2}{2} & a_2 \\ c_2 & -\dfrac{b_1 + b_2}{2} & 0 & a_1 \\ -\dfrac{b_1 - b_2}{2} & -a_2 & a_1 & 0 \end{bmatrix}.$$

Then by the assumption $a_2^2 - 4a_1a_3 = b_2^2 - 4b_1b_3$, we have $TS = 0$. This implies $T\,{}^t[q] = TS\,{}^t[r] = 0$. Hence it follows from $S\,{}^t[s] = {}^t[p]$ and $[s]\,{}^t[q] = 1$ that $a_1, a_2, a_3, b_1, b_2, b_3$ satisfy the condition of Proposition 1.1 by the components of $[p]$ and $[q]$. For instance, $|E_1| = p_1q_2 - p_2q_1 = (a_1s_2 + a_2s_3 + (b_1 + b_2)s_4/2)q_2 - (-a_1s_1 - (b_1 - b_2)s_3/2 + c_2s_4)q_1 = a_1(s_1q_1 + s_2q_2) - s_3(-(b_1 - b_2)q_1/2 - a_2q_2) - s_4(c_2q_1 - (b_1 - b_2)q_2/2) = a_1(s_1q_1 + s_2q_2 + s_3q_3 + s_4q_4) - s_3(-(b_1 - b_2)q_1/2 - a_2q_2 + a_1q_3) - s_4(c_2q_1 - (b_1 - b_2)q_2/2 + a_1q_4) = a_1$, since $[s]\,{}^t[q] = 1$ and $T\,{}^t[q] = 0$. In the same way, we have $a_2 = |F_1| - |F_2|$, etc. by $E_1, F_1, G_1, E_2, F_2, G_2$ in the same forms of Proposition 1.1. Then Propsition 1.1 implies that F is the composition of f_1 and f_2 by $[p]$ and $[q]$.

For a binary quadratic form $f(x, y)$ and a square matrix U of degree 2 , define f^U by

$$f^U(x, y) = f([x, y]\,{}^tU). \tag{1.25}$$

PROPOSITION 1.26. *Let f_1 and f_2 be two primitive forms of same discriminant. Let $f_1' = f_1^{U_1}$ and $f_2' = f_2^{U_2}$ by $U_1, U_2 \in SL_2(R)$. Let f_3 be the Gaussian composition of f_1 and f_2 by matrices P and Q. Then f_3 is the Gaussian composition of f_1' and f_2' by ${}^tU_1PU_2$ and ${}^tU_1QU_2$.*

Proof. By assumption, $f_3(X, Y) = f_1(x_1, y_1)f_2(x_2, y_2)$, where

$$X = [x_1, y_1]P\,{}^t[x_2, y_2] \quad \text{and} \quad Y = [x_1, y_1]Q\,{}^t[x_2, y_2].$$

Let

$$P_1 = {}^tU_1PU_2,\ Q_1 = {}^tU_1QU_2,$$
$$[x_1', y_1'] = [x_1, y_1]\,{}^tU_1^{-1},\ \ [x_2', y_2'] = [x_2, y_2]\,{}^tU_2^{-1}.$$

Then

$$X = [x_1, y_1]\,{}^tU_1^{-1}\,{}^tU_1PU_2U_2^{-1}\,{}^t[x_2, y_2] = [x_1', y_1']P_1\,{}^t[x_2', y_2'],$$

$$Y = [x_1, y_1]\,{}^tU_1^{-1}\,{}^tU_1QU_2U_2^{-1}\,{}^t[x_2, y_2] = [x'_1, y'_1]Q_1\,{}^t[x'_2, y'_2],$$
$$f_1(x_1, y_1) = f'_1(x'_1, y'_1),\ f_2(x_2, y_2) = f'_2(x'_2, y'_2),$$

and

$$f_3(X, Y) = f'_1(x'_1, y'_1)f'_2(x'_2, y'_2),$$

which proves the Proposition.

For two matrices M_1, M_2 of degree 2, we define $[M_1, M_2] \in \mathbf{Z}^6$ by

$$(1.27)\qquad [M_1, M_2] = [|E_1(M_1, M_2)|, |F_1(M_1, M_2)|, |G_1(M_1, M_2)|,$$
$$|E_2(M_1, M_2)|, |F_2(M_1, M_2)|, |G_2(M_1, M_2)|],$$

where $E_j(M_1, M_2), F_j(M_1, M_2), G_j(M_1, M_2)$ $(j = 1, 2)$ be as in Proposition1.1 replaced their matrices P, Q by M_1, M_2. It is easy to see that $[M_1, M_2] = -[M_2, M_1]$.

By Gauss [3, Art. 239], we have the following relation of two compositions obtained by two pair of matrices $\{P, Q\}$ and $\{R, S\}$ respectively.

Proposition 1.28([3, Art. 239]). *Let $f_1 = [a_1, b_1, c_1]$, $f_2 = [a_2, b_2, c_2]$ be two primitive integral forms. Let F be a composition of f_1 and f_2 by P and Q, and $\bar{F}$ be a composition f_1 and f_2 by R and S, where*

$$P = \begin{bmatrix} p_1 & p_2 \\ p'_2 & p_3 \end{bmatrix},\quad Q = \begin{bmatrix} q_1 & q_2 \\ q'_2 & q_3 \end{bmatrix},\quad R = \begin{bmatrix} r_1 & r_2 \\ r'_2 & r_3 \end{bmatrix},\quad S = \begin{bmatrix} s_1 & s_2 \\ s'_2 & s_3 \end{bmatrix}.$$

Suppose that f_1 is primitive and let $[\lambda] = [\lambda_1, \cdots \lambda_6]$ be an element of $\mathbf{Z}^6$ such that $[\lambda]\,{}^t[P, Q] = 1$.

Set

$$T = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix},$$

where

$$\alpha = [\lambda]\,{}^t[R, Q],\quad \beta = [\lambda]\,{}^t[P, R],\quad \gamma = [\lambda]\,{}^t[S, Q],\quad \delta = [\lambda]\,{}^t[P, S].$$

Then we have $|T| = 1$, and further for $j = 1, 2$ we have

$$E_j(P, Q)T = E_j(R, S),\ F_j(P, Q)T = F_j(R, S),\ G_j(P, Q)T = G_j(R, S).$$

Moreover

$$T[\bar{F}]\,{}^tT = [F].$$

Proof. We can recall Gauss's proof as follows. For instance, (1,1)-entry of $E_1(P,Q)T$ is equal to $\alpha p_1 + \beta q_1 = [\lambda]\,{}^t[R,Q]p_1 + [\lambda]\,{}^t[P,R]q_1 = [\lambda]\,{}^t([Rp_1,Q] - [Rq_1,P])$

$$= \lambda_1 \left(\begin{vmatrix} r_1 & r_2 \\ q_1 & q_2 \end{vmatrix} p_1 + \begin{vmatrix} r_1 & r_2 \\ p_1 & p_2 \end{vmatrix} q_1 \right) + \lambda_2 \left(\begin{vmatrix} r_1 & r_3 \\ q_1 & q_3 \end{vmatrix} p_1 + \begin{vmatrix} r_1 & r_3 \\ p_1 & p_3 \end{vmatrix} q_1 \right) \cdots$$

$$= \lambda_1 r_1 \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix} + \lambda_2 r_1 \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix} + \cdots = r_1[\lambda]\,{}^t[P,Q] = r_1.$$

§2. Duplication

Suppose that $p_2 = p_2'$ and $q_2 = q_2'$ in Proposition 1.1. Then $E_1 = E_2$, $G_1 = G_2$ and $|F_2| = 0$. Thus we have the following proposition of duplication.

PROPOSITION 2.1. *Let*

$$a = \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}, \; b = \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix}, \; c = \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix},$$

$$A = -\begin{vmatrix} q_1 & q_2 \\ q_2 & q_3 \end{vmatrix}, \; B = \begin{vmatrix} p_1 & p_2 \\ q_2 & q_3 \end{vmatrix} + \begin{vmatrix} q_1 & q_2 \\ p_2 & p_3 \end{vmatrix}, \; C = -\begin{vmatrix} p_1 & p_2 \\ p_2 & p_3 \end{vmatrix}.$$

Let further

$$X = [x_1, y_1] \begin{bmatrix} p_1 & p_2 \\ p_2 & p_3 \end{bmatrix} {}^t[x_2, y_2],$$

$$Y = [x_1, y_1] \begin{bmatrix} q_1 & q_2 \\ q_2 & q_3 \end{bmatrix} {}^t[x_2, y_2].$$

Then

$$AX^2 + BXY + CY^2 = (ax_1^2 + bx_1y_1 + cy_1^2)(ax_2^2 + bx_2y_2 + cy_2^2).$$

The converse statement holds as in Proposition 1.1.

In our previous paper [2, Theorem 2.3], we have a duplication formula of a unimodular equivalence class of quadratic foms, which will be implied from the above Proposition 2.1 as seen below.

Let $\mathbf{Z}^3 = \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}$. For an element $\alpha = [a_1, a_2, a_3]$ of $\mathbf{Z}^3$, we set

$$[\alpha] = \begin{bmatrix} a_1 & a_2/2 \\ a_2/2 & a_3 \end{bmatrix}$$

and

$$\alpha[x] = [x]\,[\alpha]\,{}^t[x] = a_1x_1^2 + a_2x_1x_2 + a_3x_2^2,$$

where $[x] = [x_1, x_2]$. Note that we take quadratic forms with in the non-classical definition, in contrast to [2]. Owing to the non-classical definition of forms, we define $\psi, \wedge$, and μ, which correspond to $\phi, *$ and ν of [2] as follows.

Let $\alpha = [a_1, a_2, a_3]$, $\beta = [b_1, b_2, b_3]$ and $\gamma = [c_1, c_2, c_3]$ be elements of $\mathbf{Z}^3$. Set

(2.2) $$\psi(\alpha, \beta) = a_2b_2 - 2(a_1b_3 + a_3b_1),$$

(2.3) $$\psi(\alpha) = \psi(\alpha, \alpha) = a_2^2 - 4a_1a_3,$$

(2.4) $$\alpha \wedge \beta = [a_1b_2 - a_2b_1,\ 2(a_1b_3 - a_3b_1),\ a_2b_3 - a_3b_2]$$

$$= \left[\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, 2\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}\right],$$

(2.5) $$\mu_{\alpha,\beta} = [\psi(\beta),\ -2\psi(\alpha, \beta),\ \psi(\alpha)].$$

Remark 2.6. Denote $\alpha' = [a_3, 2a_2, a_1]$ for $\alpha = [a_1, a_2, a_3]$. Then $\alpha \wedge \beta = 2(\alpha' \times \beta')$, where $\times$ stands for the usual outer product.

The following equalities are immediately obtained by partly using the above Remark.

(2.7) $$4\psi(\alpha \wedge \beta) = \psi(\mu_{\alpha,\beta}),$$

(2.8) $$\mu_{\alpha,\beta}(x, y) = \psi(\beta x - \alpha y).$$

Moreover we have the following relations similarly to [2, §1]:

$$\alpha \wedge \alpha = 0, \quad \alpha \wedge \beta = -\beta \wedge \alpha, \quad \alpha \wedge (\beta + \gamma) = \alpha \wedge \beta + \alpha \wedge \gamma,$$

$$\alpha \wedge (\beta \wedge \gamma) + \beta \wedge (\gamma \wedge \alpha) + \gamma \wedge (\alpha \wedge \beta) = 0,$$

$$\psi(\alpha \wedge \beta, \alpha) = \psi(\alpha, \alpha \wedge \beta) = 0.$$

We have further

$$\alpha \wedge (\beta \wedge \gamma) = \psi(\alpha, \beta)\gamma - \psi(\alpha, \gamma)\beta, \tag{2.9}$$

$$\psi(\alpha \wedge \beta, \gamma \wedge \delta) = \psi(\alpha, \delta)\psi(\gamma, \beta) - \psi(\alpha, \gamma)\psi(\beta, \delta), \tag{2.10}$$

$$\psi(\alpha \wedge \beta, \gamma) = \psi(\beta, \gamma \wedge \alpha) = -2 \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}. \tag{2.11}$$

Now, the following proposition of duplication is implied immediately from Proposition 2.1, by taking $2a_1$, a_2,$2a_3$, $2b_1$,b_2, $2b_3$ instead of $p_1, p_2, p_3, q_1, q_2, q_3$ respectively.

PROPOSITION 2.12. *Let f be a binary quadratic form. Then except trivial chsange of signs, the qudratic form f has an expression $f = \alpha \wedge \beta$ by α and β of $\mathbf{Q}^3$ if and only if*

$$\mu_{\alpha,\beta}(\xi_1, \xi_2) = f(x_1, y_1)\, f(x_2, y_2),$$

where $\xi_1 = [x_1, y_1]\,[\alpha]\,{}^t[x_2, y_2]$ *and* $\xi_2 = [x_1, y_1]\,[\beta]\,{}^t[x_2, y_2]$.

Remark 2.13. We note that for any integral binary quadratic form f, there are quadratic forms α and β such that $f = \alpha \wedge \beta$. In fact, let $f = [a, b, c] \in \mathbf{Z}^3$, and let $e = \text{g.c.d.}(a, c)$. Take $r, s \in \mathbf{Z}$ so that $ar + cs = e$. Then

$$f = \alpha \wedge \beta, \tag{2.14}$$

where

$$\alpha = \left[\frac{a}{e}, 0, \frac{-c}{e}\right], \quad \beta = \left[\frac{bs}{2}, e, \frac{br}{2}\right]. \tag{2.15}$$

Note that β is in $\frac{\mathbf{Z}}{2} \oplus \mathbf{Z} \oplus \frac{\mathbf{Z}}{2}$, not necessarily in $\mathbf{Z}^3$ in general, but $\mu_{\alpha,\beta}$ is integral as follows

$$\mu_{\alpha,\beta}(\xi_1, \xi_2) = (e^2 - b^2 rs)\xi_1^2 + \frac{2}{e}(abr - bcs)\xi_1\xi_2 + 4\frac{ac}{e^2}\xi_2^2. \tag{2.16}$$

Remark 2.17 Let $x = x_1 = x_2$ and $y = y_1 = y_2$ in Proposition 2.12. Then $\xi_1 = \alpha(x, y)$ and $\xi_2 = \beta(x, y)$, and we have

$$\psi(\beta)\alpha(x,y)^2 - 2\psi(\alpha,\beta)\alpha(x,y)\beta(x,y) + \psi(\alpha)\beta(x,y)^2 = (\alpha \wedge \beta)(x,y)^2.$$

This is one of syzygy in classical invariant theory(Cf. [2, (1.5)]).

§3. Ternary form representation of duplication

We shall show that the quadratic form $\mu_{\alpha,\beta}$ obtained in Proposition 2.12 as a duplication of f is further transformed to a ternary quadratic form whose expression does not contain α or β.

At first, let $f = \alpha \wedge \beta$ with $\alpha, \beta \in \mathbf{Z}^3$. Let $\mathbf{x} = [x_1, x_2, x_3] \in \mathbf{Z}^3$. Then (2.9) implies $f \wedge \mathbf{x} = (\alpha \wedge \beta) \wedge \mathbf{x} = -\mathbf{x} \wedge (\alpha \wedge \beta) = \psi(\mathbf{x}, \beta)\alpha - \psi(\mathbf{x}, \alpha)\beta$, and (2.8) implies

$$\mu_{\alpha,\beta}(\eta_1, \eta_2) = \psi(f \wedge \mathbf{x}), \tag{3.1}$$

where $\eta_1 = \psi(\mathbf{x}, \alpha)$ and $\eta_2 = \psi(\mathbf{x}, \beta)$.

Note that the right hand side of the above formula is a ternary quadratic form and determined by f withought using α or β, which is explicitly given as follows:

$$\psi(f \wedge \mathbf{x}) = 4(c^2 x_1^2 + ac x_2^2 + a^2 x_3^2 - bc x_1 x_2 - ab x_2 x_3 + (b^2 - 2ac) x_1 x_3). \tag{3.2}$$

We shall further transform it to another form as follows.

Let $f = [a, b, c]$ and $\mathbf{x} = [x_1, x_2, x_3]$ be as above. Then by (2.11) and (2.4),

$$\psi(f \wedge \mathbf{x}) = \psi(f \wedge \mathbf{x}, f \wedge \mathbf{x}) = -2 \begin{vmatrix} a & b & c \\ x_1 & x_2 & x_3 \\ \begin{vmatrix} a & b \\ x_1 & x_2 \end{vmatrix} & 2\begin{vmatrix} a & c \\ x_1 & x_3 \end{vmatrix} & \begin{vmatrix} b & c \\ x_2 & x_3 \end{vmatrix} \end{vmatrix}$$

$$= 4\left(\begin{vmatrix} a & c \\ x_1 & x_3 \end{vmatrix}^2 - \begin{vmatrix} a & b \\ x_1 & x_2 \end{vmatrix} \begin{vmatrix} b & c \\ x_2 & x_3 \end{vmatrix} \right).$$

Set

$$T = \begin{bmatrix} 0 & 0 & -1/2 \\ 0 & 1 & 0 \\ -1/2 & 0 & 0 \end{bmatrix}. \tag{3.3}$$

For any $f = [a, b, c]$, let

$$\mathfrak{T}(f) = \begin{bmatrix} 0 & c & -b \\ -c & 0 & a \\ b & -a & 0 \end{bmatrix}. \tag{3.4}$$

Let further

$$[X_1, X_2, X_3] = [x_1, x_2, x_3]\,\mathfrak{T}(f).$$

Then since $\psi(f \wedge \mathbf{x}) = 4(X_2^2 - X_3X_1) = 4[X_1, X_2, X_3]\,T\,{}^t[X_1, X_2, X_3]$, we have

$$\psi(f \wedge \mathbf{x}) = 4\mathbf{x}\,\mathfrak{T}(f)\,T\,{}^t\mathfrak{T}(f)\,{}^t\mathbf{x}. \tag{3.5}$$

Remark 3.6. It is well-known that $\mathfrak{T}$ gives an isomorphism between the Lie ring of the orthogonal group $O(3)$ by means of the usual Lie product and the Lie ring of $\mathbf{R}^3$ by means of the vector product. If we define a product $[A, B]_T$ for matrices A, B of degree 3 by

$$[A, B]_T = ATB - BTA,$$

where T is as in (3.3), then we have

$$[A, B]_T = \mathfrak{T}\left(\frac{\alpha \wedge \beta}{2}\right),$$

where α and β are elements of $\mathbf{Z}^3$ such that $A = \mathfrak{T}(\alpha)$ and $B = \mathfrak{T}(\beta)$.

Remark 3.7. For any $\alpha = [a_1, a_2, a_3] \in \mathbf{Z}^3$, let $[\alpha] = \begin{bmatrix} a_1 & a_2/2 \\ a_2/2 & a_3 \end{bmatrix}$ as before. If $[\alpha] \equiv [\beta] \bmod SL_2(\mathbf{Z})$, then we have

$$\mathfrak{T}(\beta)\,T\,{}^t\mathfrak{T}(\beta) \equiv \mathfrak{T}(\alpha)T\,{}^t\mathfrak{T}(\alpha) \mod SL_3(\mathbf{Z}).$$

In fact, for $[\beta] = {}^tU\,[\alpha]\,U$ by $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix} \in SL_2(\mathbf{Z})$, let

$$U_1 = \begin{bmatrix} u_4^2 & -2u_3u_4 & u_3^2 \\ -u_2u_4 & 2u_2u_3 + 1 & -2u_1u_3 \\ u_2^2 & -2u_1u_2 & u_1^2 \end{bmatrix}.$$

Then $U_1 \in SL_3(\mathbf{Z})$, and $\mathfrak{T}(\beta)T\,{}^t\mathfrak{T}(\beta) = {}^tU_1\,\mathfrak{T}(\alpha)T\,{}^t\mathfrak{T}(\alpha)U_1$.

§4. Correspondence between quadratic forms and ideals mod m

Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field, where d is a square free rational integer, and D be the discriminant of K. We call a rational integer D a *discriminant integer* when D is a discriminant of some quadratic field, namely D satisfies either one of the following conditions: (i) D is square free and $D \equiv 1 \mod 4$, (ii) $D = 4d, d$ is a square free and $d \not\equiv 1 \mod 4$.

Denote by $\mathbf{N}$ the absolute norm to the rational number field $\mathbf{Q}$. Let

$$\omega = \begin{cases} \dfrac{1+\sqrt{D}}{2} = \dfrac{1+\sqrt{d}}{2} & \text{when} \quad d \equiv 1 \mod 4, \\ \dfrac{\sqrt{D}}{2} = \sqrt{d} & \text{when} \quad d \not\equiv 1 \mod 4 \end{cases}$$

Then $\{1, \omega\}$ forms a $\mathbf{Z}$-basis of O_K, the ring of integers of K. Let $\mathfrak{a}$ be a fractional ideal of K. Then we can choose $\{ra, r(b+\omega)\}$ as a $\mathbf{Z}$-basis of $\mathfrak{a}$, where $r \in \mathbf{Q}$; $a, b \in \mathbf{Z}$; and $r > 0, a > 0$. We denote it by $\mathfrak{a} = r[a, b+\omega]$, and the basis is called a *canonical basis* of $\mathfrak{a}$. It is uniquly determined by $\mathfrak{a}$, and called the *reduced canonical basis* , when $0 \leq b < a$. An integral ideal $\mathfrak{a}$ is called *primitive* if $r = 1$.

Denote by Δ_0 the following sugroup of $SL_2(\mathbf{Z})$:

$$\Delta_0 = \left\{ \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}; \quad u \in \mathbf{Z} \right\}.$$

For any rational integer m, denote by $\Gamma_0(m)$ the following subgroup of $SL_2(\mathbf{Z})$:

$$\Gamma_0(m) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z})\,;\, a \equiv 1,\, c \equiv 0 \mod m \right\}.$$

For a binary quadratic form $f(x, y)$ and a square matrix U of degree 2 , the form f^U is defined by $f^U(x, y) = f([x, y]\,{}^tU) = [x, y]\,{}^tU[f]U\,{}^t[x, y]$ as in (1.25), and we have easily the following

LEMMA 4.1. *Let* $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$ *be an integral matrix. Then*

$$f^U(1, 0) = f(u_1, u_3), \qquad f^U(0, 1) = f(u_2, u_4).$$

If g.c.d $(u_1, u_3) = 1$, *then there is* U *in* $SL_2(\mathbf{Z})$ *such that* $f(u_1, u_3) = f^U(1, 0)$.
If g.c.d $(u_2, u_4) = 1$, *then there is* U *in* $SL_2(\mathbf{Z})$ *such that* $f(u_2, u_4) = f^U(0, 1)$.

For rational binary quadratic forms f_1 and f_2, define

(4.2) $$f_1 \equiv f_2 \mod \Gamma_0(m) \quad \text{or} \quad \mod \Delta_0$$

if $f_2 = f_1^U$ by $U \in \Gamma_0(m)$ or by $U \in \Delta_0$ respectively.

Let D be a discriminant integer, and m be any rational integer. We classify the primitive integral binary quadratic forms of discriminant D mod $\Gamma_0(m)$, and call its class an *equivalence class* mod m of quadratic forms of discriminant D.

Any fractional ideal $\mathfrak{a}$ is written by $\mathfrak{a} = (r)\mathfrak{a}_0$, where $r \in \mathbf{Q}$ and $\mathfrak{a}_0$ is primitive. If $r[a, b+\omega]$ is a canonical basis of $\mathfrak{a}$, then

$$\mathrm{N}\mathfrak{a} = r^2 a. \tag{4.3}$$

Now we define mappings Φ and Ψ between fractional ideals of K and rational binary quadratic forms as follows:

For a fractional ideal $\mathfrak{a}$ of K with a cannonial basis $r[a, b+\omega]$, define Φ as follows.

$$\Phi(r[a, b+\omega]) = \frac{r}{a} N(ax + (b+\omega)y) = r[a, b', c], \tag{4.4}$$

where $b' = 2b+1$ or $= 2b$ according as $d \equiv 1 \mod 4$ or not, and $D = (b')^2 - 4ac$. The last form determins an integer c by $\mathrm{N}(b+\omega) \equiv 0 \bmod a$, since $[a, b+\omega]$ is an ideal basis. The image of Φ of an ideal is depend on the choice of its canonical basis, but is unique mod Δ_0.

Conversely let $f = r[a, b, c]$, where [a,b,c] is primitive . Then we define Ψ by

$$\Psi(f) = r\left[a, \frac{b+\sqrt{D}}{2}\right], \tag{4.5}$$

where $D = b^2 - 4ac$. The image of Ψ is a canonical basis of an ideal, since D is a discriminant integer.

PROPOSITION 4.6. *Let D be a discriminant integer. Then primitive binary quadratic forms of discriminant D mod Δ_0 and primitive ideals of the quadratic field $K = \mathbf{Q}(\sqrt{D})$ correspond one another by Φ and Ψ inversely.*

Proof. Let $\mathfrak{a} = [a, b+\omega]$ be a primitive integral ideal, and $\Phi([a, b+\omega]) = [a, b', c]$, where $D = (b')^2 - 4ac$ as in (4.4). Note that the class of $\Phi([a, b+\omega])$ mod Δ_0 is not depend on the choice of canonical basis of $\mathfrak{a}$. We have $\Psi([a, b', c]) = \left[a, \frac{b'+\sqrt{D}}{2}\right] = \left[a, b + \frac{1+\sqrt{D}}{2}\right]$ or $= \left[a, b + \frac{\sqrt{D}}{2}\right]$ acording as $d \equiv 1 \mod 4$ or not. Hence $\Psi(\Phi(\mathfrak{a})) = [a, b+\omega] = \mathfrak{a}$.

Conversely let $f = [a, b, c]$ and $D = b^2 - 4ac$. Then we have $\Psi(f) = \left[a, \frac{b+\sqrt{D}}{2}\right] = [a, b_1 + \omega]$, where $b_1 = (b-1)/2$ or $= b/2$ according as $D \equiv 1$ mod 4 or not. Hence $\Phi(\Psi(f)) = [a, b_1', c] = [a, b, c]$.

PROPOSITION 4.7. *Let $\mathfrak{a}_1, \mathfrak{a}_2$ be primitive ideals of a quadratic field $K = \mathbf{Q}(\sqrt{d})$, and let $[a_1, b_1 + \omega], [a_2, b_2 + \omega]$ be their canonical basis respectively. Suppose $\mathfrak{a}_1 = \lambda \mathfrak{a}_2$ by $\lambda = (r + m(s + t\omega))/w$, where $r, s, t, w \in \mathbf{Z}$, $\mathrm{N}\lambda > 0$ and g.c.d.$(w, m) = 1$. Then there is $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix} \in SL_2(\mathbf{Z})$ such that $ru_1 \equiv w$, $u_3 \equiv 0$ mod m and*

$$[a_1, b_1 + \omega]U = \lambda[a_2, b_2 + \omega].$$

Proof. Let $A_1 = s - b_2 t$, $A_2 = a_2 t$, $A_3 = (\frac{d-1}{4} - b_2)t$ or $= b_2 t$, and $A_4 = s + t + b_2 t$ or $= s + b_2 t$ according as $d \equiv 1$ mod 4 or not. Then since $\omega^2 = \omega + \frac{d-1}{4}$ or $= d$ according as $d \equiv 1$ mod 4 or not , we have $w\lambda[a_2, b_2 + \omega] = [a_2, b_2 + \omega]V$, where $V = \begin{bmatrix} r + mA_1 & mA_3 \\ mA_2 & r + mA_4 \end{bmatrix}$. On the other hand since $\mathfrak{a}_1 = \lambda \mathfrak{a}_2$ and $\mathrm{N}\lambda > 0$, there is U in $SL_2(\mathbf{Z})$ such that $\lambda[a_2, b_2+\omega] = [a_1, b_1+\omega]U$. Hence $\begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix} V = w \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} U$, which implies

$$VU^{-1} = w \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}. \tag{4.8}$$

Let $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$. Then $mA_2 u_4 - (r + mA_4)u_3 = 0$ and $-mA_2 u_2 + (r + mA_4)u_1 = w$. Hence we have $u_3 \equiv 0$, $ru_1 \equiv w$ mod m, which proves the proposition.

Define $\mathfrak{S}'_K(m)$ by

$$\mathfrak{S}'_K(m) = \{(\lambda); \lambda \in K^\times; \lambda \equiv 1 \quad \mathrm{mod}^\times m, \mathrm{N}\lambda > 0\}. \tag{4.9}$$

THEOREM 4.10. *Let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic field of discriminant D and m be any rational integer. Then the ideal classes mod $\mathfrak{S}'_K(m)$ of K and the equivalence classes mod $\Gamma_0(m)$ of primitive binary quadratic forms $f(x, y)$ of discriminant D such that $f(1, 0)$ is prime to m correspond by Φ and Ψ one another inversely.*

Proof. In the same way as the case of $m = 1$, we can prove the theorem as follows.

(i) Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be primitive ideals of K prime to m, and suppose that $\mathfrak{a}_1 \equiv \mathfrak{a}_2 \bmod \mathfrak{S}'_K(m)$. Let $\mathfrak{a}_1 = (\lambda)\mathfrak{a}_2$, where $\lambda \in \mathfrak{S}'_K(m)$. Let $[a_1, b_1 + \omega]$ and $[a_2, b_2 + \omega]$ be canonical basis of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ respectively. Then by Proposition

4.7, there is U in $\Gamma_0(m)$ such that $[a_1, b_1+\omega]U = \lambda[a_2, b_2+\omega]$, and (4.4) and (4.3) impliy

$$\Phi(\mathfrak{a}_1) = \frac{1}{a_1}\mathrm{N}(a_1x + (b_1+\omega)y) = \frac{1}{a_1}\mathrm{N}([a_1, b_1+\omega]\,{}^t[x,y])$$

$$\equiv \frac{1}{a_1}\mathrm{N}([a_1, b_1+\omega]U\,{}^t[x,y]) = \frac{1}{a_1}\mathrm{N}(\lambda[a_2, b_2+\omega]\,{}^t[x,y])$$

$$= \frac{\mathrm{N}\lambda}{a_1}a_2\Phi(\mathfrak{a}_2) = \Phi(\mathfrak{a}_2) \mod \Gamma_0(m).$$

(ii) Conversely let f_1, f_2 be primitive quadratic forms of discriminant D, and $f_1(x,y) = f_2([x,y]\,{}^tU)$ by $U = \begin{bmatrix} u_1 & u_2 \\ mu_3 & u_4 \end{bmatrix} \in \Gamma_0(m)$. Let $\Psi(f_1) = \mathfrak{a}_1 = [a_1, b_1+\omega]$, $\Psi(f_2) = \mathfrak{a}_2 = [a_2, b_2+\omega]$ in expression of canonical basis. Then (4.4), (4.5) and Proposition 4.6 implies

$$f_1(x,y) \equiv \Phi\Psi(f_1(x,y)) \tag{4.11}$$

$$= \frac{1}{a_1}\mathrm{N}(a_1x + (b_1+\omega)y) = \frac{1}{a_1}\mathrm{N}([a_1, b_1+\omega]\,{}^t[x,y]) \qquad \mathrm{mod.}\ \Delta_0.$$

By assumption and adjusting U by Δ_0 if necessary, we have

$$f_1(x,y) = f_2([x,y]\,{}^tU) = \frac{1}{a_2}\mathrm{N}([a_2, b_2+\omega]U\,{}^t[x,y]) \tag{4.12}$$

$$= \frac{1}{a_2}\mathrm{N}([u_1a_2 + mu_3(b_2+\omega), u_2a_2 + u_4(b_2+\omega)]\,{}^t[x,y]).$$

Now let σ be the non-trivial automorphism of $K/\mathbf{Q}$. Then by (4.11) the roots of $f_1(x,1)$ are $-\dfrac{b_1+\omega}{a_1}$ and $-\dfrac{b_1+\omega^\sigma}{a_1}$. Compaired with (4.12), there is an element λ of K such that

$$\begin{cases} u_1a_2 + mu_3(b_2+\omega) = a_1\lambda, \\ u_2a_2 + u_4(b_2+\omega) = (b_1+\omega)\lambda \quad \text{or} \quad = (b_1+\omega^\sigma)\lambda. \end{cases} \tag{4.13.}$$

However the latter of the second equality in (4.13) does not happen. Because (4.12) implies

$$f_1(x,y) = \frac{1}{a_2}\mathrm{N}(a_1\lambda x + (b_1+\omega^\sigma)\lambda y) = \frac{\mathrm{N}\lambda}{a_2}\mathrm{N}(a_1x + (b_1+\omega^\sigma)y) = \frac{\mathrm{N}\lambda}{a_2}a_1f_1(x,y).$$

Hence

$$\mathrm{N}\lambda = \frac{a_2}{a_1} > 0. \tag{4.14}$$

On the other hand, the second case of (4.13) implies

$$\begin{vmatrix} a_2 & b_2+\omega \\ a_2 & b_2+\omega^\sigma \end{vmatrix} |U| = \begin{vmatrix} a_1\lambda & (b_1+\omega^\sigma)\lambda \\ a_1\lambda^\sigma & (b_1+\omega)\lambda^\sigma \end{vmatrix} = -\mathrm{N}\lambda \begin{vmatrix} a_1 & b_1+\omega \\ a_1 & b_1+\omega^\sigma \end{vmatrix}.$$

Then by $a_1 > 0$ and $a_2 > 0$, we have $\mathrm{N}\lambda < 0$, which contradict to (4.14).

Now let $\lambda = (s+t\omega)/r$, where $r, s, t \in \mathbf{Z}$ and g.c.d.$(s,t) = 1$. Then the first of (4.13) implies $a_2 \equiv a_1 s/r$, $a_1 t/r \equiv 0 \bmod m$. Hence $t \equiv 0 \bmod m$. Moreover (4.14) implies $a_2 = a_1 N\lambda \equiv a_1 s^2/r^2 \bmod m$. Hence $s^2 \equiv rs \bmod m$. Thus $s \equiv r \bmod m$. Hence $\lambda \equiv 1 \bmod m$, and (4.13) implies $[a_2, b_2+\omega]\, U = \lambda[a_1, b_1+\omega]$. Since $N\lambda > 0$ by (4.14), we have $\mathfrak{a}_2 \equiv \mathfrak{a}_1 \bmod \mathfrak{S}'_K(m)$.

§5. Class composition of quadratic forms mod m

In this section, let m be an integer such that $m \equiv 0 \quad \bmod 4$ when m is even. For a rational quadratic form $f(x,y) = ax^2 + bxy + cy^2$ and a square matrix $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$, let $f^U(x,y) = f([x,y]\,{}^tU)$ as in (1.25).

Let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic field of discriminant D. In order to show that the correspondence Φ and Ψ defined in Section 2 give an isomorphism between the class group of ideals mod $\mathfrak{S}'_K(m)$ of K and the equivalence class group mod $\Gamma_0(m)$ of binary quadratic forms of discriminant D, we shall refer a part of [1, Chapter 14] modifying by means of equivalence mod $\Gamma_0(m)$.

Let us call an integral quadratic form $f(x,y)$ *represents* an integer s mod $\Gamma_0(m)$, when there is a matrix U in $\Gamma_0(m)$ such that $s = f^U(1,0)$. This is equivalent that there are rational integers x, y such that $x \equiv 1 \bmod m$, g.c.d.$(x,y) = 1$, and $f(x, my) = s$.

Lemma 5.1 [1, Chap.14, Lemma 2.1]. *Let $f = [a,b,c]$ be a primitive form and let M be any integer prime to m. Then there is an integer prime to M which is represented by f mod $\Gamma_0(m)$.*

Proof. This is shown in the same way as in [1] by taking $f(x,my)$ such that $x \equiv 1 \bmod m$ and g.c.d.$(x,y) = 1$ instead of $f(x,y)$. Namely let p be a prime dividing M. We consider three cases

(i) $p \nmid a$. if $p \nmid x$ and $p \mid y$ then $f(x,my)$ is prime to p.

(ii) $p \nmid c$. Similar.

(iii) $p \mid a, p \mid c$, so $p \nmid b$. Then $p \nmid x, p \nmid y$ ensures that $f(x,my)$ is prime to p.

Lemma 5.2 [1, Chap.14, Lemma 2.2]. *Suppose that two primitive forms with the same middle coefficient $[a_1, b, c_1]$ and $[a_2, b, c_2]$ are equivalent mod*

$\Gamma_0(m)$. *Let l be an integer such that $l \mid c_1, l \mid c_2$ and g.c.d.$(a_1, a_2, l) = 1$. Then $[la_1, b, l^{-1}c_1]$ and $[la_2, b, l^{-1}c_2]$ are equivalent mod $\Gamma_0(m)$.*

This is proved in the same way as in [1] taking t divisible by m.

Two primitive forms

$$f_j = [a_j,\, b_j,\, c_j] \qquad (j = 1, 2)$$

of discriminant D are called *concordant* or *united* if (i) $a_1 a_2 \neq 0$, (ii) the two middle coefficients are the same, say $b_1 = b_2 = b$ and (iii) the form

$$f_3 = [a_1 a_2,\, b,\, *] \tag{5.3}$$

of discriminant D is integral. Then f_3 is necessarily primitive. Moreover f_3 coincides with a Gaussian composition of f_1 and f_2, which will be shown later in Proposition 3.10.

Let us call the above f_3 the *concordant composition* of f_1 and f_2.

Remark 5.4. When g.c.d.$(a_1, a_2) = 1$, the condition (iii) follows from (i) and (ii)([1, Chap.14, Note before Lemma 2.3]), and we have $\Psi(f_1)\Psi(f_2) = \Psi(f_3)$ since $[a_1, b+\omega][a_2, b+\omega] = [a_1 a_2, b+\omega]$ when g.c.d.$(a_1, a_2) = 1$.

Remark 5.5. If $b_1^2 - 4a_1c_1 = b^2 - 4a_1c$ and $b \equiv b_1 \bmod 2a_1$, then for any integer m we have

$$[a_1,\, b_1,\, c_1] \equiv [a_1,\, b,\, c] \mod \Gamma_0(m).$$

In fact, let $U = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$, where $b = b_1 + 2a_1 t$. Then

$$^tU \begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{bmatrix} U = \begin{bmatrix} a_1 & b/2 \\ b/2 & c \end{bmatrix}.$$

LEMMA 5.6 [1, CHAP.14, LEMMA 2.3]. *Let $\mathrm{C}_1, \mathrm{C}_2$ be two classes mod $\Gamma_0(m)$ of primitive forms of discriminant $D \neq 0$. Then there are concordant forms $f_j = [a_j, b, *] \in \mathrm{C}_j\ (j = 1, 2)$. Further, they may be chosen so that a_1, a_2 are prime to one another and to any integer M given in advance.*

Proof. This is proved by slight modification of the proof of [1] as follows. By Lemma 5.1 , the class C_1 represents some integer a_1 prime to M and C_2 represents some integer a_2 prime to $a_1 M$. Hence there are forms

$$[a_j, b_j, *] \in \mathrm{C}_j \qquad (j = 1, 2).$$

Let b be an integer such that

$$b \equiv b_j \mod 2a_j \qquad (j = 1, 2),$$

whose existence follows from that a_1 and a_2 are prime to one another and $b_j^2 \equiv D \mod 4a_j$. Let $U_j = \begin{bmatrix} 1 & t_j \\ 0 & 1 \end{bmatrix} \in \Gamma_0(m)$, where $b = b_j + 2a_j t_j$. Then by Remark 5.5, integers c'_j are determined by

$${}^tU_j \begin{bmatrix} a_j & b_j/2 \\ b_j/2 & c_j \end{bmatrix} U_j = \begin{bmatrix} a_j & b/2 \\ b/2 & c'_j \end{bmatrix}.$$

Now $f_j = [a_j, b, c'_j]$ is to be required.

LEMMA 5.7 [1, CHAP.14, LEMMA 2.4]. *Let $\mathbf{C}_1, \mathbf{C}_2$ be two classes mod $\Gamma_0(m)$ of primitive forms of discriminant $D \neq 0$. Then there is a class $\mathbf{C}$ such that the concordant composition of $f_j \in \mathbf{C}_j (j = 1, 2)$ always lies in $\mathbf{C}$.*

This is proved in the same way as in [1] by taking the equivalence mod $\Gamma_0(m)$ for the equivalence $\sim$.

Now, we can define a product of two classes mod m of quadratic forms by the concordant composition of representatives of the classes. The following theorem is implied from Theorem 4.10 and Remark 5.4.

THEOREM 5.8. *Let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic field of discriminant D. Then Φ and Ψ give an isomorphism between the group of ideal classes of K mod $\mathfrak{S}'_K(m)$ and the group of equivalent classes mod $\Gamma_0(m)$ of binary quadratic forms of discriminant D.*

For a primitive quadratic form f, denote by $C_m(f)$ the class of f mod $\Gamma_0(m)$. We call a form f_3 a *composition* of two primitive forms f_1 and f_2 mod m, when $C_m(f_3) = C_m(f_1)C_m(f_2)$, in other words, there are $U_i \in \Gamma_0(m)\, (i = 1, 2, 3)$ such that $f_1^{U_1}$ and $f_2^{U_2}$ are concordant and $f_3^{U_3}$ is a concordant composition of $f_1^{U_1}$ and $f_2^{U_2}$.

PROPOSITION 5.9. *Let $f_1 = [a_1, b_1, c_1]$ and $f_2 = [a_2, b_2, c_2]$ be two primitive forms of discriminant D. Suppose that g.c.d.$(a_1, a_2) = 1$, and let $u_1, u_2 \in \mathbf{Z}$ such that $a_1u_1 + a_2u_2 = 1$. Let $\bar{b} = a_1u_1b_2 + a_2u_2b_1, \bar{c} = (\bar{b}^2 - D)/(4a_1a_2)$ and $f_3 = [a_1a_2, \bar{b}, \bar{c}]$. Then f_3 is a composition of f_1 and f_2 mod m for any integer m. Let $t_1 = (b_2 - b_1)u_1/2, t_2 = (b_1 - b_2)u_2/2$. Then $\bar{b} = b_1 + 2a_1t_1 = b_2 + 2a_2t_2$.*

Proof. It is easy to see $\bar{b} = b_1 + 2a_1t_1 = b_2 + 2a_2t_2$. Let $V_1 = \begin{bmatrix} 1 & t_1 \\ 0 & 1 \end{bmatrix}, V_2 = \begin{bmatrix} 1 & t_2 \\ 0 & 1 \end{bmatrix}$, and let $\bar{f}_1 = f^{V_1}$ and $\bar{f}_2 = f^{V_2}$. Then the forms $\bar{f}_1$ and $\bar{f}_2$ are concordant forms with the middle coeficient $\bar{b}$, and we have the proposition by definition of concordant composition.

PROPOSITION 5.10. *Let $f_1 = [a_1, b, c_1]$ and $f_2 = [a_2, b, c_2]$ be concordant primitive forms of discriminant D such that g.c.d.$(a_1, a_2) = 1$. Let $f_3 = [a_1a_2, b, *]$ be the the concordant composition of f_1 and f_2. Take $u_1, u_2 \in \mathbb{Z}$ so that $a_1u_1 + a_2u_2 = 1$, and let $w = c_1u_2 + c_2u_1$. Then f_3 coincides with the Gaussian composition obtained from $[p] = [1, 0, 0, -w]$ and $[q] = [0, a_1, a_2, b]$.*

Proof. In order to obtain the Gaussian composition, we apply Proposition 1.24. Since $b_1 = b_2 = b$ in the present case, the matrix S in Proposition 1.24 is as follows.

$$S = \begin{bmatrix} 0 & a_1 & a_2 & b \\ -a_1 & 0 & 0 & c_2 \\ -a_2 & 0 & 0 & c_1 \\ -b & -c_2 & -c_1 & 0 \end{bmatrix}.$$

Let $[r] = [-1, 0, 0, 0]$. Then since $S\,{}^t[r] = {}^t[0, a_1, a_2, b]$, we can take $[q] = [0, a_1, a_2, b]$ and $[s] = [0, u_1, u_2, 0]$ in Proposition 1.24. Moreover since $S\,{}^t[s] = {}^t[a_1u_1 + a_2u_2, 0, 0 - c_2u_1 - c_1u_2]$, we have $[p] = [1, 0, 0, -w]$, $A = -|Q| = a_1a_2$, $B = |P_1| + |Q_1| = b$, and $C = -|P| = w$. Hence Proposition 1.24 implies $f_3 = [A, B, C]$, the Gaussian composition of f_1 and f_2 obtained from $[p]$ and $[q]$.

A Gaussian composition obtained in Proposition 1.1 is a representative of the composition of the unimodular equivalence class but not necesarily of the class mod m in the case $m > 1$. Now by Proposition 1.26, the proof of Proposition 5.9 and Proposition 5.10, we have a Gaussian composition of equivalence classes mod m as follows.

THEOREM 5.11. *Let $f_1 = [a_1, b_1, c_1]$ and $f_2 = [a_2, b_2, c_2]$ be two primitive forms of discriminant D such that g.c.d.$(a_1, a_2) = 1$. Take $u_1, u_2 \in \mathbb{Z}$ so that $a_1u_1 + a_2u_2 = 1$, and let $t_1 = (b_2 - b_1)u_1/2$, $t_2 = (b_1 - b_2)u_2/2$ and $w = c_1u_2 + c_2u_1$. Let further*

$$V_1 = \begin{bmatrix} 1 & t_1 \\ 0 & 1 \end{bmatrix}, \qquad V_2 = \begin{bmatrix} 1 & t_2 \\ 0 & 1 \end{bmatrix},$$

$$P = {}^tV_1^{-1} \begin{bmatrix} 1 & 0 \\ 0 & -w \end{bmatrix} V_1^{-1}, \qquad Q = {}^tV_2^{-1} \begin{bmatrix} 0 & a_1 \\ a_2 & \bar{b} \end{bmatrix} V_2^{-1},$$

and F be the Gaussian composition of f_1 and f_2 by P and Q. Then F is a concordant composition, and hence a composition mod m for any m:

$$C_m(F) = C_m(f_1)C_m(f_2).$$

Moreover, let P_1 and Q_1 be obtained from P and Q as in Proposition 1.1. Then F is given by $F = [A, B, C]$, where $A = -|Q| = a_1a_2$, $B = |P_1| + |Q_1|$, and $C = -|P| = w$.

§6. Duplication mod m

Let m be an integer, and $f = [a, b, c]$ be an integral binary quadratic form such that g.c.d.$(a, m) = 1$. Denote by $C_m(f)$ the class of f mod m. The purpose of this section is to construct a duplication F of f mod m, i.e., a form F such that

$$C_m(f)^2 = C_m(F) \tag{6.1}$$

for a given form $f = [a, b, c]$.

Remark 6.2. A duplication obtained from Proposition 2.12 is a representative of the duplication of the unimodular equivalence class but not necesarily of the class mod m in the case $m > 1$.

Now in order to have a duplication of f mod m, we choose a form $f_1 = f^{U_1} = [a_1, b_1, c_1]$ such that $U_1 \in \Gamma_0(m)$ and g.c.d.$(a, a_1) = 1$. Then a duplication of f mod m is obtained by definition as a concordant composition of f and f_1.

LEMMA 6.3. *Let $f = [a, b, c]$ be a primitive form, and suppose that g.c.d.$(a, m) = 1$. Let $f_1 = f^{U_1} = [a_1, b_1, c_1]$ by $U_1 = \begin{bmatrix} u_1 & u_2 \\ m & u_4 \end{bmatrix} \in \Gamma_0(m)$. Then*

$$a_1 = f(u_1, m) = au_1^2 + bu_1m + cm^2. \tag{6.4}$$

and there is u_1 such that g.c.d.$(a_1, am) = 1$.

Proof. The formula (6.4) is followed from Lemma 4.1immediately. We can choose u_1 for instance as follows. Let $a = a_0h$, where g.c.d.$(a_0, c) = 1$ and prime divisors of h and c coincide. Let $u_1 = a_0^e \equiv 1 \bmod m$ by some integer e. Then g.c.d.$(a_1, m) = 1$. Moreover g.c.d.$(a_1, a) = 1$. In fact, if $p \mid h$, then $p \mid c, p \nmid u_1, p \nmid m$ and $p \nmid b$ owing to primitivity of f. Hence $p \nmid a_1$. If $p \mid a_0$, then $p \mid u_1$, $p \nmid m$ and $p \nmid c$. Hence $p \nmid a_1$.

Let $f = [a, b, c]$ be as above a primitive form of discriminant D, and g.c.d.$(a, m) = 1$. Let $f_1 = [a_1, b_1, c_1]$ be a form obtained as in Lemma 6.3. Choose $r, s \in \mathbf{Z}$ so that $ar + a_1s = 1$, and let

$$\bar{b} = arb_1 + a_1sb. \tag{6.5}$$

Let

$$t_0 = (b_1 - b)r/2, \quad t_1 = (b - b_1)s/2, \tag{6.6}$$

$$V_0 = \begin{bmatrix} 1 & t_0 \\ 0 & 1 \end{bmatrix}, \quad V_1 = \begin{bmatrix} 1 & t_1 \\ 0 & 1 \end{bmatrix}, \tag{6.7}$$

and

$$\bar{f}_0 = f^{V_0}, \quad \bar{f}_1 = f_1^{V_1} = f^{U_1 V_1}. \tag{6.8}$$

Then since $\bar{b} = b + 2at_0 = b_1 + 2a_1t_1$, the forms $\bar{f}_0$ and $\bar{f}_1$ are concordant, i.e., $\bar{f}_0 = [a, \bar{b}, \bar{c}_0]$ and $\bar{f}_1 = [a_1, \bar{b}, \bar{c}_1]$, where $\bar{c}_0 = (\bar{b}^2 - D)/4a$, $\bar{c}_1 = (\bar{b}^2 - D)/4a_1$. Let $F = [aa_1, \bar{b}, \bar{c}]$ be the concordant composition of $\bar{f}_0$ and $\bar{f}_1$, where $\bar{c} = (\bar{b}^2 - D)/4aa_1$. Then F satisfies (6.1), and we have

THEOREM 6.9. *Let $f = [a, b, c]$ be an integral quadratic form of discriminant D, and $F = [aa_1, \bar{b}, \bar{c}]$ be an integral quadratic form determined by the following data:*

$a_1 = au_1^2 + bmu_1 + cm^2$, where u_1 is an integer such that $u_1 \equiv 1 \bmod m$ and g.c.d.$(u_1, c) = 1$.

$\bar{b} = arb_1 + a_1sb$, where $b_1^2 \equiv D \bmod 4a_1$, $ar + a_1s = 1$

$\bar{c} = (\bar{b}^2 - D)/(4aa_1)$.

Then F is a duplication of f mod m, i.e., $C_m(F) = C_m(f)^2$.

References

[1] J. W. S. Cassels, *Rational quadratic forms*, Academic Press, 1978.

[2] Y. Furuta, Gauss's ternary form reduction and its application to a prime decomposition symbol, Nagoya Math. J., 98 (1985), 77-86.

[3] C. F. Gauss, *Disquitiones arithmeticae*, translation to german by H. Haser, Chelsea 1889.