Invent. math. 97, 219–235 (1989)

Inventiones mathematicae
© Springer-Verlag 1989

Binary forms and orders of algebraic number fields*

Jin Nakagawa
Department of Mathematics, Joetsu University of Education, Joetsu 943, Japan

0. Introduction

0.0. The class numbers of binary forms of degree greater than three has been scarcely studied. It seems that the finiteness of class numbers proved by Birch and Merriman is the only general result. In the case of binary cubic forms, Davenport obtained asymptotic formulae for certain sums of class numbers. Shintani studied deeply binary cubic forms using the theory of prehomogeneous vector spaces (see [9]). Recently Wright extended Shintani's work to arbitrary algebraic number fields (see [11]). In this paper, we go back to Davenport's work, since the space of binary forms of degree $n > 3$ is no longer a prehomogeneous vector space. We observe that the Hessian of a binary cubic form played an essential role in Davenport [3]. Our main idea is to define a suitable analogue of 'Hessian'. We shall use it to obtain a lower estimate for a certain sum of class numbers of totally real binary forms of degree $n > 3$. We shall also apply our method to the problem of counting orders of totally real algebraic number fields of degree $n > 3$. Further, we shall prove that there exist infinitely many real quadratic fields having an A_n-extension which is unramified at all primes including the infinite primes (see Uchida [10], Yamamoto [12], Yamamura [13]).

Acknowledgements. The author wishes to express his gratitude to Professor Yasuo Morita for his valuable advice and continuous encouragement.

0.1 Notation and statement of the results

Throughout this paper, we denote by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the ring of rational integers, the rational number field, the real number field and the complex number field, respectively. For a Galois extension K over a finite algebraic number field F, we denote by $\mathrm{Gal}(K/F)$ the Galois group of K/F. We say that K/F is a *weakly unramified G-extension* if K/F is unramified at all finite primes and $\mathrm{Gal}(K/F) = G$. We say that K/F is a *strictly unramified G-extension* if K/F is

* This research was partially supported by Grant-in-Aid for Scientific Research (No. 62740021), Ministry of Education, Science and Culture

unramified at all primes including the infinite primes and $\mathrm{Gal}(K/F)=G$. For a natural number n, we denote by S_n, and A_n the symmetric group of degree n and the alternating group of degree$n$, respectively. We say that a binary form of degree n is *totally real* if it is decomposed into n distinct linear factors over $\mathbb{R}$. Let $\Gamma=\mathrm{GL}_2(\mathbb{Z})$. For $\gamma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma$ and a binary form $f(x, y)$, we define $\gamma\cdot f$ by $(\gamma\cdot f)(x, y)=f(ax+cy, bx+dy)$. We say that $\gamma\cdot f$ is *Γ-equivalent* to f and write $f\underset{\Gamma}{\sim}\gamma\cdot f$. We say that a binary form is *integral* if its coefficients are in $\mathbb{Z}$. We say that an integral binary form is *irreducible* if it is irreducible over $\mathbb{Q}$. For a given positive integer D, we denote by $h_n^+(D)$ the number of Γ-equivalence classes of integral, irreducible, totally real binary forms of degree n with discriminant D.

Theorem 1. *Let $n\geqq 4$ and put $\kappa=(n+1)/(2n-2)$. Then there exists a positive constant C_n such that*

$$\liminf_{X\to\infty}\frac{\sum_{0<D\leqq X} h_n^+(D)}{X^\kappa}\geqq C_n.$$

Let K be an algebraic number field of degree n over $\mathbb{Q}$. We say that a subring $\mathcal{O}$ of K is an order if it is a free $\mathbb{Z}$-module of rank n and it contains $\mathbb{Z}$. We note that the quotient field of $\mathcal{O}$ is K. We denote by $N_n^+(X)$ the number of orders $\mathcal{O}$ with discriminant $D(\mathcal{O})\leqq X$ whose quotient fields are totally real algebraic number fields of degree n over $\mathbb{Q}$. Further, we denote by $\tilde{N}_n^+(X)$ the number of orders $\mathcal{O}$ with discriminant $D(\mathcal{O})\leqq X$ satisfying the following condition $(*)$:

$(*)$ (i) the quotient field K of $\mathcal{O}$ is a totally real algebraic number field of degree n over $\mathbb{Q}$,

(ii) if we denote by L the normal closure of K over $\mathbb{Q}$, then $\mathrm{Gal}(L/\mathbb{Q})=S_n$ and $L/\mathbb{Q}(\sqrt{D_K})$ is a strictly unramified A_n-extension.

Theorem 2. *Let the notation and assumptions be as in Theorem 1. Then we have*

$$\liminf_{X\to\infty}\frac{N_n^+(X)}{X^\kappa}\geqq C_n.$$

Theorem 3. *Let the notation and assumptions be as in Theorem 1. Then there exists a positive constant C_n' such that*

$$\liminf_{X\to\infty}\frac{\tilde{N}_n^+(X)}{X^\kappa}\geqq C_n'.$$

Theorem 4. *For any integer $n\geqq 4$, there exist infinitely many real quadratic fields having a strictly unramified A_n-extension.*

1. Quadratic forms of $n-1$ variables associated with binary forms of degree n

Let n be a natural number with $n \geqq 3$ and let

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n \quad (a_j \in \mathbb{Z})$$

be an integral irreducible binary form of degree n. Let θ be a root of the equation $f(x, 1) = 0$ and put $K_f = \mathbb{Q}(\theta)$. So K_f is an algebraic number field of degree n over $\mathbb{Q}$. Put

$$\xi_0 = 1, \qquad \xi_j = \sum_{k=0}^{j-1} a_k \theta^{j-k} \quad (1 \leqq j \leqq n-1)$$

and let $\mathcal{O}_f$ denote the lattice in K_f generated by ξ_j's over $\mathbb{Z}$. This lattice is the one used in Birch and Merriman [1]. Our first fundamental result is

Proposition 1.1. *Notation and assumptions being as above, the following four assertions hold:*

(i) *$\mathcal{O}_f$ is an order of K_f and the discriminant $D(\mathcal{O}_f)$ coincides with the discriminant $D(f)$ of f.*

(ii) *If we put $\xi_n = -a_n$, then*

$$\xi_i \xi_j = \sum a_{i+j-k} \xi_k - \sum a_{i+j-k} \xi_k \quad (1 \leqq i \leqq j \leqq n-1).$$

The first sum is taken for all k with $j < k \leqq \mathrm{Min}(i+j, n)$ and the second one is taken for all k with $\mathrm{Max}(i+j-n, 1) \leqq k \leqq i$.

(iii) $\mathrm{Tr}(\xi_0) = n$, $\mathrm{Tr}(\xi_j) = -j a_j$ $(1 \leqq j \leqq n-1)$, *where* Tr *is the trace map of K_f to $\mathbb{Q}$.*

(iv) $\mathrm{Tr}(\xi_i \xi_j) = i a_i a_j + \sum_k (2k - i - j) a_k a_{i+j-k}$ $(1 \leqq i \leqq j \leqq n-1)$. *The sum is taken for all k with* $\mathrm{Max}(i+j-n, 0) \leqq k < i$.

Proof. It was shown in [1] that $D(\mathcal{O}_f) = D(f)$. By the definition of θ and ξ_j's, we have

$$\begin{aligned} \xi_1 \xi_j &= a_0 \theta (a_0 \theta^j + a_1 \theta^{j-1} + \ldots + a_{j-1} \theta) \\ &= a_0 (a_0 \theta^{j+1} + a_1 \theta^j + \ldots + a_{j-1} \theta^2 + a_j \theta - a_j \theta) \\ &= a_0 \xi_{j+1} - a_j \xi_1 \quad (1 \leqq j \leqq n-2). \end{aligned}$$

Since $f(\theta, 1) = 0$ and $\xi_n = -a_n$, this is also valid for $j = n-1$. Similarly for $2 \leqq i \leqq j \leqq n-2$, we have

$$\begin{aligned} \xi_i \xi_j &= (\xi_{i-1} + a_{i-1})(\xi_{j+1} - a_j \theta) \\ &= \xi_{i-1} \xi_{j+1} + a_{i-1} \xi_{j+1} - (a_j / a_0)(\xi_1 \xi_{i-1} + a_{i-1} \xi_1) \\ &= \xi_{i-1} \xi_{j+1} + a_{i-1} \xi_{j+1} - a_j \xi_i. \end{aligned}$$

Using this equation, the assertion (ii) follows by induction on i. Hence $\mathcal{O}_f$ is an order of K_f. Let $\sigma\colon \mathcal{O}_f \to \mathrm{GL}_n(\mathbb{Z})$ be the regular representation of the ring

$\mathcal{O}_f$ with respect to the basis (ξ_i), i.e. $\alpha\xi_i = \sum_{k=0}^{n-1} \sigma(\alpha)_{ik}\xi_k$ for $\alpha \in \mathcal{O}_f$. If $j \geqq 1$, then it follows from (ii) that

$$\sigma(\xi_j)_{ii} = \begin{cases} -a_j & \text{if } 1 \leqq i \leqq j, \\ 0 & \text{otherwise.} \end{cases}$$

Hence we have $\mathrm{Tr}(\xi_j) = \mathrm{Tr}\,\sigma(\xi_j) = -j\,a_j$. The assertion (iv) follows from (ii) and (iii). q.e.d.

Now we define the quadratic form $\Psi(f)$ of $n-1$ variables $x_1, \ldots, x_{n-1}$ associated with the binary form f of degree n:

$$\Psi(f)(x_1, \ldots, x_{n-1}) = \sum_{i,j=1}^{n-1} [n\,\mathrm{Tr}(\xi_i\xi_j) - \mathrm{Tr}(\xi_i)\,\mathrm{Tr}(\xi_j)]\,x_i x_j.$$

We remark that $\Psi(f)$ is a constant multiple of the restriction of the quadratic form $\mathrm{Tr}(x^2)$ $(x \in \mathcal{O}_f)$ to the hyperplane defined by $\mathrm{Tr}(x) = 0$. Indeed, if we put

$$x = \sum_{j=0}^{n-1} x_j \xi_j \qquad (x_j \in \mathbb{Z}),$$

then we have

$$n\,\mathrm{Tr}(x^2) = \Psi(f)(x_1, \ldots, x_{n-1}) + \mathrm{Tr}(x)^2.$$

Applying the linear transformation

$$y_0 = \mathrm{Tr}(x) = n\,x_0 + \sum_{j=1}^{n-1} \mathrm{Tr}(\xi_j)\,x_j, \qquad y_i = x_i \quad (1 \leqq i \leqq n-1),$$

we have

$${}^t(y_j) \begin{pmatrix} n & & & \\ * & 1 & & \\ \vdots & & \ddots & \\ * & & & 1 \end{pmatrix}^{-1} (n\,\mathrm{Tr}(\xi_i\xi_j)) \begin{pmatrix} n & * & \ldots & * \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}^{-1} (y_j) = y_0^2 + \Psi(f)(y_1, \ldots, y_{n-1}).$$

By this equation, we see that $\det \Psi(f) = n^{n-2} \det(\mathrm{Tr}(\xi_i\xi_j))$. Hence by the definition of the discriminant $D(\mathcal{O}_f)$ and (i) of Proposition 1.1, we have

$$\det \Psi(f) = n^{n-2} D(f). \tag{1.1}$$

If we write $\Psi(f)(x_1, \ldots, x_{n-1}) = \sum_{i,j=1}^{n-1} h_{ij} x_i x_j$ $(h_{ij} = h_{ji})$, then it follows from (iii) and (iv) of Proposition 1.1 that

$$h_{ij} = i(n-j)\,a_i a_j + \sum_k n(2k - i - j)\,a_k a_{i+j-k} \qquad (i \leqq j), \tag{1.2}$$

where the sum is taken for all k with $\mathrm{Max}(i+j-n, 0) \leqq k < i$.

Remark. For $n=3$, we have

$$2^{-1}\Psi(f)(x_1,x_2)=(a_1^2-3a_0a_2)x_1^2+(a_1a_2-9a_0a_3)x_1x_2+(a_2^2-3a_1a_3)x_2^2.$$

This is a constant multiple of the Hessian of the binary cubic form f and played a significant role in the work of Davenport [3].

Let V be the $\mathbb{R}$-vector space of binary forms of degree n and let W be that of quadratic forms of $n-1$ variables:

$$V=\{f(x,y)=a_0x^n+a_1x^{n-1}y+\ldots+a_ny^n;\,(a_i)\in\mathbb{R}^{n+1}\},$$

$$W=\left\{H(x_1,\ldots,x_{n-1})=\sum_{i,j=1}^{n-1}h_{ij}x_ix_j;\,(h_{ij})_{1\leqq i\leqq j\leqq n-1}\in\mathbb{R}^N\right\},$$

where $h_{ji}=h_{ij}$ and $N=n(n-1)/2$. We denote by $V_{\mathbb{Z}}$ the set of integral binary forms of degree n. Further, we denote by $V_{\mathbb{Z}}^{\text{irr}}$ (resp. $V_{\mathbb{Z}}^{\text{red}}$) be the set of integral irreducible (resp. reducible) binary forms of degree n. We extend Ψ to a mapping of V to W by the quadratic equations (1.2). We note that the Eq. (1.1) is valid for all $f\in V$ by Hilbert's irreducibility theorem (cf. Lang [6]).

Now we are going to prove two basic properties of the mapping Ψ. The first one states that the action of $\mathrm{GL}_{n-1}(\mathbb{R})$ on W is compatible with that of $\mathrm{GL}_2(\mathbb{R})$ on V under Ψ. The second one states that if $n\geqq 4$, then the mapping Ψ is injective on an open subset of V. Before we state the results, we recall that the group action of $\mathrm{GL}_m(\mathbb{R})$ on the space of forms of m variables is defined by the linear transformation of variables: For a form $g(x_1,\ldots,x_m)$ of m variables and $\gamma\in\mathrm{GL}_m(\mathbb{R})$, we define $\gamma\cdot g$ by $(\gamma\cdot g)(x_1,\ldots,x_m)=g(x_1',\ldots,x_m')$, where $(x_1',\ldots,x_m')=(x_1,\ldots,x_m)\gamma$.

We denote by ρ_r the matrix representation of $\mathrm{GL}_2(\mathbb{R})$ on the space of binary forms of degree r with respect to the standard basis. Hence if $g(x,y)=\sum_{0\leqq j\leqq r}b_jx^{r-j}y^j\ (b_j\in\mathbb{R})$ and $(\gamma\cdot g)(x,y)=\sum_{0\leqq j\leqq r}c_jx^{r-j}y^j\ (\gamma\in\mathrm{GL}_2(\mathbb{R}))$, then

$$\begin{pmatrix}c_0\\c_1\\\cdots\\c_r\end{pmatrix}=\rho_r(\gamma)\begin{pmatrix}b_0\\b_1\\\cdots\\b_r\end{pmatrix}.$$

Proposition 1.2. *For* $\gamma\in\mathrm{GL}_2(\mathbb{R})$, *put*

$$\psi(\gamma)=\det(\gamma)\,\rho_{n-2}(\gamma)(\in\mathrm{GL}_{n-1}(\mathbb{R})).$$

Then ψ *defines a homomorphism of* $\mathrm{GL}_2(\mathbb{R})$ *into* $\mathrm{GL}_{n-1}(\mathbb{R})$ *with the following properties:*

$$\operatorname{Ker}\psi=\begin{cases}\{\pm 1\} & \textit{if } n \textit{ is even},\\ \{1\} & \textit{if } n \textit{ is odd},\end{cases}$$

$$\Psi(\gamma\cdot f)=\psi(\gamma)\cdot\Psi(f)\qquad \textit{for all } \gamma\in\mathrm{GL}_2(\mathbb{R}),\ f\in V.$$

Proof. It is obvious that ψ is a homomorphism and it is easy to see that Ker ψ is $\{\pm 1\}$ or trivial according as n is even or odd. To prove the last formula, for $f \in V$, let $\mathscr{A}_f$ denote the commutative $\mathbb{R}$-algebra with basis $\xi_0 = 1$, ξ_j $(1 \leqq j \leqq n-1)$ whose ring structure is defined by the equations in (ii) of Proposition 1.1. If $f \in V_{\mathbb{Z}}^{\mathrm{irr}}$, then $\mathscr{A}_f \cong \mathcal{O}_f \underset{\mathbb{Z}}{\otimes} \mathbb{R}$ is a commutative associative $\mathbb{R}$-algebra. Hence $\mathscr{A}_f$ is a commutative associative $\mathbb{R}$-algebra for all $f \in V$ by Hilbert's irreducibility theorem. Since $\mathrm{GL}_2(\mathbb{R})$ is generated by $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ $(a, c, d \in \mathbb{R}, \mathrm{ad} \neq 0)$, we may assume that γ is one of the above three matrices. Put $g = \gamma \cdot f$ and let η_j denote the ξ_j for $\mathscr{A}_g$. Let $a_0, \ldots, a_n$ and $b_0, \ldots, b_n$ be the coefficients of f and g respectively. We shall show that there exists an algebra isomorphism σ of $\mathscr{A}_g$ onto $\mathscr{A}_f$ defined in the form

$$(\sigma(\eta_j)) = \begin{pmatrix} 1 & 0 \ldots 0 \\ * & \\ \vdots & \psi(\gamma) \\ * & \end{pmatrix} (\xi_j).$$

Case 1. $\gamma = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. Then we have $b_i = a^{n-i} d^i a_i$ $(0 \leqq i \leqq n)$. Let σ be the linear isomorphism of $\mathscr{A}_g$ onto $\mathscr{A}_f$ defined by

$$\sigma(\eta_0) = \xi_0, \qquad \sigma(\eta_i) = a^{n-i} d^i \xi_i \qquad (1 \leqq i \leqq n-1).$$

By the definition of the ring structures of $\mathscr{A}_f$ and $\mathscr{A}_g$, we have

$$\begin{aligned} \sigma(\eta_i)\,\sigma(\eta_j) &= a^{2n-i-j} d^{i+j} \xi_i \xi_j \\ &= a^{2n-i-j} d^{i+j} \{\textstyle\sum a_{i+j-k} \xi_k - \sum a_{i+j-k} \xi_k\} \\ &= \textstyle\sum b_{i+j-k}\, \sigma(\eta_k) - \sum b_{i+j-k}\, \sigma(\eta_k) \\ &= \sigma(\eta_i \eta_j) \qquad (1 \leqq i \leqq j \leqq n-1). \end{aligned}$$

In the above equation, the first sum is taken for all k with $j < k < \mathrm{Min}(i+j, n)$ and the second one is taken for all k with $\mathrm{Max}(i+j-n, 1) \leqq k \leqq i$.

Case 2. $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then we have $b_i = a_{n-i}$ $(0 \leqq i \leqq n)$. Let σ be the linear isomorphism of $\mathscr{A}_g$ onto $\mathscr{A}_f$ defined by

$$\sigma(\eta_0) = \xi_0, \qquad \sigma(\eta_i) = -a_{n-i} \xi_0 - \xi_{n-i} \qquad (1 \leqq i \leqq n-1).$$

To prove $\sigma(\eta_i)\,\sigma(\eta_j) = \sigma(\eta_i \eta_j)$ $(1 \leqq i \leqq j \leqq n-1)$, we may assume that $a_n \neq 0$ since a polynomial function which is zero on an non-empty Zarisky open subset of V is identically zero. We use induction on i. For $1 \leqq j \leqq n-1$, we have

$$\begin{aligned} \sigma(\eta_1)\,\sigma(\eta_j) &= (b_1 \xi_0 + \xi_{n-1})(b_j \xi_0 + \xi_{n-j}) \\ &= b_1 b_j \xi_0 + b_1 \xi_{n-j} + b_j \xi_{n-1} + \xi_{n-j} \xi_{n-1} \\ &= -b_1 b_j \xi_0 - b_1 \sigma(\eta_j) - b_j \sigma(\eta_1) + \xi_{n-j} \xi_{n-1} \,. \end{aligned}$$

By the definition of the ring structure of $\mathscr{A}_f$,

$$\xi_{n-j}\,\xi_{n-1}=\begin{cases}-a_{n-j-1}\,a_n\,\xi_0-a_n\,\xi_{n-j-1}-a_{n-1}\,\xi_{n-j} & \text{if } 1\leqq j\leqq n-2,\\ -a_0\,a_n\,\xi_0-a_{n-1}\,\xi_1 & \text{if } j=n-1.\end{cases}$$

If we put $\eta_n=-b_n\,\eta_0$, then we have

$$\xi_{n-j}\,\xi_{n-1}=b_0\,\sigma(\eta_{j+1})+b_1\,\sigma(\eta_j)+b_1\,b_j\,\xi_0 \qquad (1\leqq j\leqq n-1).$$

Hence we have $\sigma(\eta_1)\,\sigma(\eta_j)=b_0\,\sigma(\eta_{j+1})-b_j\,\sigma(\eta_1)=\sigma(\eta_1\,\eta_j)$. Let $2\leqq i\leqq n-1$ and assume that $\sigma(\eta_{i-1})\,\sigma(\eta_j)=\sigma(\eta_{i-1}\,\eta_j)$ $(i-1\leqq j\leqq n-1)$. Let $i\leqq j\leqq n-1$. Since $(\sigma(\eta_1)\,\sigma(\eta_{i-1}))\,\sigma(\eta_j)=\sigma(\eta_{i-1})\,(\sigma(\eta_1)\,\sigma(\eta_j))$, we have

$$\{b_0\,\sigma(\eta_i)-b_{i-1}\,\sigma(\eta_1)\}\,\sigma(\eta_j)=\sigma(\eta_{i-1})\{b_0\,\sigma(\eta_{j+1})-b_j\,\sigma(\eta_1)\}.$$

Hence

$$\begin{aligned}b_0\,\sigma(\eta_i)\,\sigma(\eta_j)&=b_{i-1}\,\sigma(\eta_1)\,\sigma(\eta_j)+b_0\,\sigma(\eta_{i-1})\,\sigma(\eta_{j+1})-b_j\,\sigma(\eta_1)\,\sigma(\eta_{i-1})\\&=b_0\,\sigma(\eta_{i-1})\,\sigma(\eta_{j+1})+b_{i-1}\{b_0\,\sigma(\eta_{j+1})-b_j\,\sigma(\eta_1)\}\\&\quad-b_j\{b_0\,\sigma(\eta_i)-b_{i-1}\,\sigma(\eta_1)\}\\&=b_0\{\sigma(\eta_{i-1}\,\eta_{j+1})+b_{i-1}\,\sigma(\eta_{j+1})-b_j\,\sigma(\eta_i)\}.\end{aligned}$$

By the definition of the ring structure of $\mathscr{A}_g$, the right hand side of the above equation coincides with $b_0\,\sigma(\eta_i\eta_j)$. Since $b_0=a_n\neq 0$, we have $\sigma(\eta_i)\,\sigma(\eta_j)=\sigma(\eta_i\eta_j)$.

Case 3. $\gamma=\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$. Then we have $b_i=\sum_{k=0}^{i}\binom{n-k}{i-k}c^{i-k}a_k$, where $\binom{n}{i}$ is the binomial coefficient. Let σ be the linear isomorphism of $\mathscr{A}_g$ onto $\mathscr{A}_f$ defined by

$$\sigma(\eta_0)=\xi_0,$$

$$\sigma(\eta_i)=\sum_{k=1}^{i}\binom{n-k-1}{i-k}c^{i-k}\,\xi_k-\left\{\sum_{k=0}^{i-1}\binom{n-k-1}{i-k-1}c^{i-k}\,a_k\right\}\xi_0 \qquad (1\leqq i\leqq n-1).$$

We may assume that $a_0\neq 0$ by the same reason as in Case 2. Let $1\leqq j\leqq n-1$. Then we have

$$\begin{aligned}&\sigma(\eta_1)\,\sigma(\eta_j)-\sigma(\eta_1\,\eta_j)\\&\quad=\sigma(\eta_1)\,\sigma(\eta_j)-b_0\,\sigma(\eta_{j+1})+b_j\,\sigma(\eta_1)\\&\quad=\sigma(\eta_1)(\sigma(\eta_j)+b_j\,\xi_0)-b_0\,\sigma(\eta_{j+1})\\&\quad=(\xi_1-c\,a_0\,\xi_0)\left\{\sum_{k=1}^{j}\binom{n-k-1}{j-k}c^{j-k}(\xi_k+a_k\,\xi_0)\right\}-a_0\,\sigma(\eta_{j+1}).\end{aligned}$$

Using the equations $\xi_1(\xi_k + a_k \xi_0) = a_0 \xi_{k+1}$, $\binom{n-k}{j+1-k} - \binom{n-k-1}{j-k} = \binom{n-k-1}{j+1-k}$, we see that the right hand side of the above equation coincides with zero. By induction on i, we have $\sigma(\eta_i)\,\sigma(\eta_j) = \sigma(\eta_i \eta_j)$.

Using the algebra isomorphism σ, the desired formula follows immediately from the definition of the quadratic forms $\Psi(f)$ and $\Psi(g)$. q.e.d.

Corollary. (i) $\psi(\Gamma) \subset \mathrm{GL}_{n-1}(\mathbb{Z})$.

(ii) $\mathcal{O}_{\gamma \cdot f} = \mathcal{O}_f$ *for* $f \in V_{\mathbb{Z}}^{\mathrm{irr}}$, $\gamma \in \Gamma$.

Lemma 1.1. *Let* $n \geqq 4$ *and put*

$$\Delta(f) = (n-2)\, h_{11}[(n-3)\, h_{22} + 2n\, h_{13}] - 2(n-1)(n-3)\, h_{12}^2,$$

$$\mathcal{S}_0 = \{f \in V;\, h_{11}\, \Delta(f) = 0\},$$

$$V^+ = \{f \in V;\, a_0 > 0\},$$

where $(h_{ij}) = \Psi(f)$. *Then the mapping* Ψ *is injective on the open subset* $V^+ - \mathcal{S}_0$ *of* V.

Proof. Put $A_j = a_j n^{-1} a_0^{-1}$ and $H_{ij} = h_{ij} n^{-2} a_0^{-2}$. In view of (1.2), we have

$$(j+1) A_{j+1} = (n-j) A_1 A_j - H_{1j} \qquad (1 \leqq j \leqq n-1), \tag{1.3}$$

$$2(n-j) A_2 A_j - (j+1)(n-1) A_1 A_{j+1} = H_{2j} - H_{1,j+1} \qquad (2 \leqq j \leqq n-1). \tag{1.4}$$

Here we put $H_{1n} = 0$. By (1.3) and (1.4), we have

$$(n-j) H_{11} A_j - (n-1) H_{1j} A_1 = H_{1,j+1} - H_{2j} \qquad (2 \leqq j \leqq n-1). \tag{1.5}$$

Hence we see by (1.3) and (1.5) that A_1 satisfies an algebraic equation of degree j. It follows from the equations of degrees two and three that

$$\Delta(f) A_1 = \Delta'(f), \tag{1.6}$$

where $\Delta'(f) = 3(n-2)\, h_{11}(h_{23} - h_{14}) - 2(n-3)\, h_{12}(h_{22} - h_{13})$.

On $V^+ - \mathcal{S}_0$ we have $\Delta(f) \neq 0$ and so we can determine A_1 by

$$A_1 = \Delta'(f)/\Delta(f). \tag{1.7}$$

We observe that the right hand side of (1.7) is a rational function of h_{ij}. By (1.7) we have

$$(n-2) H_{11}^2 = (n-1)(n-2) H_{11} A_1^2 - 2(n-1) H_{12} A_1 + 2 H_{22} - 2 H_{13}. \tag{1.8}$$

On $V^+ - \mathcal{S}_0$ we have $h_{11} \neq 0$ and hence

$$a_0^2 = (n-2)\, n^{-2}\, h_{11}^2\, [(n-1)(n-2)\, h_{11} A_1^2 - 2(n-1)\, h_{12} A_1 + 2(h_{22} - h_{13})]^{-1}. \tag{1.9}$$

In view of (1.7) and (1.9), $a_0 > 0$ is uniquely determined by (h_{ij}). Since $A_j = A_j n^{-1} a_0^{-1}$ and A_j is a polynomial in A_1 with coefficients in $\mathbb{Q}[H_{ij}]$, a_j is also uniquely determined by (h_{ij}). q.e.d.

Proposition 1.3. *Let the notation be as in Lemma 1.1. Put $\mathcal{S}=\bigcap g\cdot\mathcal{S}_0$, where g runs over all elements of* $\mathrm{GL}_2(\mathbb{R})$. *Then $\mathcal{S}$ is an invariant closed subset of V, and the mapping Ψ is injective on the open subset $V^+-\mathcal{S}$ of V.*

Proof. Let $f_1, f_2\in V^+-\mathcal{S}$. By Proposition 1.2 and Lemma 1.1, it suffices to show that there exists an element g of $\mathrm{GL}_2(\mathbb{R})$ such that $g\cdot f_1$, $g\cdot f_2\in V^+-\mathcal{S}_0$. Put $H_i=\{g\in\mathrm{GL}_2(\mathbb{R});\ g\cdot f_i\in\mathcal{S}_0\}$ $(i=1, 2)$. Then H_i's are hypersurfaces in $\mathrm{GL}_2(\mathbb{R})$. Since f_i's are in V^+, we can take an open neighborhood U of the identity such that $U\cdot f_i\subset V^+$ $(i=1, 2)$. Since $\dim U>\dim H_i$, we have $U\not\subset H_1\cup H_2$. Hence there exists an element $g\in U$ such that $g\cdot f_1, g\cdot f_2\in V^+-\mathcal{S}_0$. q.e.d.

2. Binary forms whose splitting fields are unramified A_n-extensions over quadratic fields

First, we refer to the following result in Nakagawa [7, Theorem 1] which is an extension of Yamamura [13, Proposition] and Osada [8, Theorem 5].

Proposition 2.1. *Let $n\geqq 3$ and let K be an algebraic number field of degree n over $\mathbb{Q}$. Let L be the normal closure of K over $\mathbb{Q}$. If the discriminant D_K of K is square free, then* $\mathrm{Gal}(L/\mathbb{Q})=S_n$ *and $L/\mathbb{Q}(\sqrt{D_K})$ is a weakly unramified A_n-extension.*

Let f be an integral irreducible binary form of degree n. In the previous section, we have constructed an order $\mathcal{O}_f$ in K_f with discriminant $D(f)$. If $D(f)$ is square free, then $\mathcal{O}_f$ coincides with the ring of integers in K_f and the discriminant of K_f coincides with $D(f)$. Hence $\mathcal{O}_f$ satisfies the condition $(*)$ in the introduction by the above proposition. In the following, we shall obtain a weaker sufficient condition for $\mathcal{O}_f$ to satisfy $(*)$.

Let p be a prime number and let n be a natural number with $n\geqq 2$. Let $\mathbb{Z}_p$, $\mathbb{Q}_p$ and $\mathbb{F}_p$ denote the ring of p-adic integers, the field of p-adic numbers and the finite field of p elements, respectively. Further, let ord_p denote the additive p-adic valuation of $\mathbb{Q}_p$ which is normalized by $\mathrm{ord}_p(p)=1$. For $p\neq 2$, let $U_n(p)$ denote the set of all binary forms $f(x, y)$ of degree n with coefficients in $\mathbb{F}_p$ satisfying the following condition (U):

(U) $f(x, y)$ has at most one multiple factor, which is of multiplicity two.

Further for $p=2$, let $U_n(2)$ be the set of all binary forms $f(x, y)$ of degree n with coefficients in $\mathbb{F}_2$ such that $D(f)\neq 0$. Applying Hensel's lemma, we have

Lemma 2.1. *Let $f(x, y)\in\mathbb{Z}[x, y]$ be a binary form of degree n which is irreducible over $\mathbb{Q}$. Put $K=K_f$. If p is an odd prime number and $f \bmod p\in U_n(p)$, then* $\mathrm{ord}_p D_K\leqq 1$.

By Lemma 2.1 and Proposition 2.1, we have

Proposition 2.2. *Let $f(x, y)\in\mathbb{Z}[x, y]$ be a binary form of degree $n\geqq 3$ which is irreducible over $\mathbb{Q}$. If $f \bmod p\in U_n(p)$ for all prime numbers p, then the normal closure of K_f is a weakly unramified A_n-extension of the quadratic field $\mathbb{Q}(\sqrt{D(f)})$.*

For a finite set A, let $\# A$ denote the cardinality of A. To count $\# U_n(p)$, put $S_n(p)=\{f(x)\in\mathbb{F}_p[x];\, f(x)$ is monic of degree n and has no multiple factors$\}$, $T_n(p)=\{f(x)\in\mathbb{F}_p[x];\, f(x)$ is monic of degree n and has just one multiple factor, which is of multiplicity two$\}$.

Lemma 2.2. *$\# S_n(p)=p^n-p^{n-1}$ for $n\geqq 2$.*

Proof. Put $s_0=1$, $s_1=p$ and $s_n=\# S_n(p)$ $(n\geqq 2)$. If $f(x)\in\mathbb{F}_p[x]$ is a monic polynomial with $D(f)=0$, then it is uniquely written in the form $f(x)=g(x)\,h(x)^2$, where $g(x)$ and $h(x)$ are monic, $\deg h(x)\geqq 1$ and $D(g)\neq 0$. Hence we obtain

$$p^n-s_n=\sum_{j=1}^{[n/2]} s_{n-2j}p^j.$$

Using this equation, the lemma follows immediately by induction on n. q.e.d.

Lemma 2.3.

$$\# T_n(p)=\begin{cases} p(p-1)\displaystyle\sum_{0\leqq j\leqq n-3}(-1)^{n-3-j}p^j & \text{if } n\geqq 3,\\ p & \text{if } n=2.\end{cases}$$

Proof. For $c\in\mathbb{F}_p$, put $s_n(c)=\#\{g(x)\in S_n(p);\, g(c)=0\}$. Using the transformation $x\to x-c$, we see that $s_n(c)$ does not depend on c. Since $f(x)\,(\in T_n(p))$ is written in the form $f(x)=(x-c)\,g(x)$, where $g(x)\in S_{n-1}(p)$ and $g(c)=0$. Hence we obtain $\# T_n(p)=ps_{n-1}(0)$. On the other hand, it is obvious that $s_{n-1}(0)=s_{n-2}-s_{n-2}(0)(s_n=\# S_n(p))$. Hence we obtain $\# T_n(p)=p\sum_{k=0}^{n-2}(-1)^k s_{n-2-k}$. Now the lemma follows from Lemma 2.2. q.e.d.

By Lemmas 2.2 and 2.3, we have

Proposition 2.3. (i) *For $p\neq 2$,*

$$\# U_n(p)=\begin{cases} p^{n-3}(p^2-1)^2 & \text{if } n\geqq 4,\\ p^2(p^2-1) & \text{if } n=3.\end{cases}$$

(ii) $\# U_n(2)=3\cdot 2^{n-2}$.

Corollary.

$$\prod_{p:\,\text{prime}}[\# U_n(p)]\,p^{-n-1}=\begin{cases} 24\pi^{-4} & \text{if } n\geqq 4,\\ 3\pi^{-2} & \text{if } n=3.\end{cases}$$

We shall use the convergence of the above infinite product in the proof of Theorem 3.

3. A lemma on lattice points

Let $\mathscr{D}\subset\mathbb{R}^N$ be a bounded open subset whose boundary $\partial\mathscr{D}$ is $(N-1)$-Lipschitz parametrizable, i.e. there exist finitely many mappings of $[0,1]^{N-1}$ to $\mathbb{R}^N$ satisfying Lipschitz's condition such that the images cover $\partial\mathscr{D}$. Put $L_0=\mathbb{Z}^N\subset\mathbb{R}^N$. For a natural number m, a lattice point $a\in L_0$ and a positive real number t, put $\lambda(m, a, t)=\#[t\mathscr{D}\cap(mL_0+a)]$, where $t\mathscr{D}=\{tx\in\mathbb{R}^N; x\in\mathscr{D}\}$ and $mL_0+a=\{ml+a\in L_0; l\in L_0\}$. We use the order notation O of Landau. The following lemma is a modified version of Lang [5, Chap. 6, Theorem 2] and is proved by the same argument.

Lemma 3.1. *$\lambda(m, a, t)=\mathrm{vol}(\mathscr{D})(t/m)^N+O((t/m)^{N-1})$ as $t\to\infty$, where the constant in O depends only on N and Lipschitz's constants of the mappings for $\partial\mathscr{D}$.*

4. Reducible polynomials

In this section, we shall give an estimate for the number of reducible polynomials. Let $n\geqq 3$. For positive real numbers $t_j>0$ $(0\leqq j\leqq n)$, put

$$\mathrm{Pol}_{n,t}=\left\{f(x)=\sum_{j=0}^{n} a_j x^{n-j}\in\mathbb{Z}[x];\ |a_j|\leqq t_j\ (0\leqq j\leqq n),\ a_0>0\right\},$$

$$\mathrm{Red}_{n,t}=\{f(x)\in\mathrm{Pol}_{n,t};\ f(x)\ \mathrm{is reducible}\}$$

$(t=(t_0, \ldots, t_n))$. Then we have

Proposition 4.1. *If $t_{n-1}\geqq 1$ and $t_n\geqq 1$ then we have*

$$\frac{\#(\mathrm{Red}_{n,t})}{\#(\mathrm{Pol}_{n,t})}\geqq\frac{2^{n-1}(1+\log t_0)(1+\log t_n)}{t_{n-1}}+\frac{1}{t_n}.$$

To prove this, we need the following lemma.

Lemma 4.1. *Let κ be an algebraically closed field. Suppose n elements $a_1, \ldots, a_{n-2}$, $a_n\neq 0$, $b\neq 0$ of κ are given. For $\lambda\in\kappa$, put $f_\lambda(x)=x^n+a_1x^{n-1}+\ldots+a_{n-2}x^2+\lambda x+a_n$. Then there exist at most $\binom{n-2}{m-1}$ values of λ such that $f_\lambda(x)$ is a multiple of a monic polynomial of degree m with constant term b.*

Proof. Let $\alpha_1, \ldots, \alpha_n\in\kappa$ be the roots of $f_\lambda(x)$. Put $\Omega=\{1, 2, \ldots, n\}$. For each subset $I\subset\Omega$ with $\#I=m$, put $\beta_I=(-1)^m\prod_{i\in I}\alpha_i$. Further put $F_\lambda(x)=\prod_I(x-\beta_I)$, where I runs over all subsets of Ω with $\#I=m$. Then we see that $f_\lambda(x)$ is a multiple of a monic polynomial of degree m with constant term b if and only if $F_\lambda(b)=0$. Hence it suffices to prove that $F_\lambda(b)$ is a polynomial in λ of degree $\binom{n-2}{m-1}$. We write $F_\lambda(x)=x^N+A_1x^{N-1}+\ldots+A_N$, $N=\binom{n}{m}$. Put $c=\binom{n-2}{m-1}$, $k_0=\binom{n-1}{m}$. Since $b\neq 0$, it suffices to show that $\deg_\lambda A_k\leqq c$ for all k and the equality holds if and only if $k=k_0$. If we define the weight of a_j to be j and that of λ to be $n-1$, then A_k is a polynomial in a_j and λ of weight km. If $k<k_0$, then it is obvious that

$$(n-1)\deg_\lambda A_k \leqq km < k_0 m = (n-1)c.$$

Hence $\deg_\lambda A_k < c$ for $k<k_0$. Next suppose $k>k_0$. Take k distinct subsets $I_1, \ldots, I_k$ of Ω with $\# I_j = m$. For each $\nu \in \Omega$, let e_ν denote the number of I_j containing ν. Then there exist at least $k-e_\nu$ distinct subsets of $\Omega-\{\nu\}$ consisting of m elements. Hence we obtain $k-e_\nu \leqq \binom{n-1}{m}$, i.e. $e_\nu \geqq k-k_0>0$. Since $\beta_{I_1}\ldots\beta_{I_k} = (-1)^{km}\prod_{\nu=1}^{n} \alpha_\nu^{e_\nu}$, we see that A_k is a multiple of a_n^r, where $r=k-k_0$. Since A_k is of weight km, we have

$$(n-1)\deg_\lambda A_k \leqq km - nr = nk_0 - k(n-m) < mk_0 = (n-1)c,$$

i.e. $\deg_\lambda A_k < c$ for $k>k_0$. Finally, suppose $k=k_0$. Put $S=(-1)^k \sum \beta_{I_1}\ldots\beta_{I_k}$, where the sum is taken for all k distinct subsets $I_1, \ldots, I_k \subset \Omega$ with $\bigcup I_j = \Omega$, $\# I_j = m$. Further, put $T=A_k - S$. Then it is obvious that S is a polynomial in $a_1, \ldots, a_{n-2}$, a_n and λ of weight km. Moreover, S is a multiple of a_n. Hence we have $\deg_\lambda S<c$. Since $k=k_0=\binom{n-1}{m}$, for each $\nu \in \Omega$, there exists only one set of k distinct subsets $I_1, \ldots, I_k$ with $\bigcup I_j \subset \Omega - \{\nu\}$, $\# I_j = m$. Further, for each $\mu \in \Omega - \{\nu\}$, there exist exactly c j's such that $\mu \in I_j$. Hence $T=(-1)^k \sum_{\nu=1}^{n} (-1)^{km} \prod_{j \neq \nu} \alpha_j^c$. Now it is easy to see that $\deg_\lambda T = c$. Hence $\deg_\lambda A_{k_0} = c$. q.e.d.

Proof of Proposition 4.1. It is clear that $\#(\mathrm{Pol}_{n,t}) = [t_0] \prod_{i=1}^{n} (2[t_i]+1)$. It is also clear that the number of $f(x) \in \mathrm{Red}_{n,t}$ with $a_n=0$ is $[t_0]\prod_{i=1}^{n-1}(2[t_i]+1)$. Now we consider $f(x) \in \mathrm{Red}_{n,t}$ with $a_n \neq 0$. If $g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$ $(b_i \in \mathbb{Z}, b_0>0)$ is a divisor of $f(x)$, then b_0 and b_m are divisors of a_0 and a_n, respectively. Hence by Lemma 4.1, if $a_0, a_1, \ldots, a_{n-2}, a_n$ are given integers, then there exist at most $2d(a_0)\,d(a_n)\binom{n-2}{m-1}$ values of a_{n-1} such that f has a divisor of degree m. Here $d(k)$ denotes the number of positive divisors of an integer k. Hence the number of $f(x) \in \mathrm{Red}_{n,t}$ with $a_n \neq 0$ is at most

$$2\prod_{i=1}^{n-2}(2[t_i]+1) \sum_{0<a_0\leqq t_0} d(a_0) \sum_{0<|a_n|\leqq t_n} d(a_n) \sum_{m=1}^{[n/2]} \binom{n-2}{m-1}.$$

Since $\sum_{0<k\leqq x} d(k) \leqq [x](1+\log[x])$, the proposition follows. q.e.d.

5. Proof of the theorems

In this section, we prove the theorems. We note that our argument is based on that of Davenport [3] and Davenport and Heilbronn [4]. We use the same notation as in the previous sections without further comment. First we prove some lemmas.

Lemma 5.1. *The image of the mapping Ψ is not contained in any hyperplane of W through the origin.*

Proof. Suppose that the image of Ψ is contained in the hyperplane $\sum_{i\leqq j} c_{ij}h_{ij}=0$. Substituting h_{ij} by the right hand side of (1.2), we obtain an identity in a_j's. We define the weight of a_j to be j. Taking the homogeneous part of weight k, we obtain $\sum_{i\leqq j, i+j=k} c_{ij}h_{ij}=0$. Assume that $k=2m$. In view of (1.2), we see that a_m^2 is contained only in h_{mm}. Hence $c_{mm}=0$. Among the remaining terms, $a_{m-1}a_{m+1}$ is contained only in $h_{m-1,m+1}$. Hence $c_{m-1,m+1}=0$. Repeating the same argument, we see that c_{ij}'s are all zero. q.e.d.

Lemma 5.2. *There exists a binary form f_0 satisfying the following conditions* (i)–(iv):

(i) $f_0 \in V^+$, (ii) f_0 *is totally real,* (iii) $h_{13}^0<0$, *and* (iv) $\Delta(f_0)<0$, *where* $(h_{ij}^0) = \Psi(f_0)$.

Proof. Put $g_m(x, y)=\prod_{k=1}^{m}(x^2-ky^2)$ and put

$$f_0(x,y)=\begin{cases} g_m(x,y) & \text{if } n=2m, \\ x g_m(x,y) & \text{if } n=2m+1. \end{cases}$$

By direct computations, we see that f_0 satisfies the conditions (i)–(iv). q.e.d.

Lemma 5.3. *Let $f\in V^+$ with $D(f)\neq 0$. If $f(x,1)=0$ has just r_1 real roots and $2r_2$ imaginary roots, then the quadratic form $\Psi(f)$ has signature (r_1+r_2-1, r_2).*

Proof. Let $\mathscr{A}_f$ be the commutative $\mathbb{R}$-algebra in the proof of Proposition 1.2. Then we have $\mathscr{A}_f \cong \mathbb{R}[x]/(f(x,1))$. The lemma follows from the fact that $\mathbb{R}[x]/(f(x,1)) \cong \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$. q.e.d.

Proof of Theorem 1. Let $\mathscr{M}$ be the set of Minkowski reduced positive definite quadratic forms of $n-1$ variables. We note that $\mathscr{M}$ has the following properties (see Cassels [2, Chap. 12]):

(P1) $\mathscr{M}$ is a convex cone in W bounded by a finite number of hyperplanes through the origin.

(P2) $P^0=\bigcup_{T\in \mathrm{GL}_{n-1}(\mathbb{Z})} T\cdot\mathscr{M}$, where P^0 is the set of all positive definite quadratic forms.

(P3) If $T\in \mathrm{GL}_{n-1}(\mathbb{Z})$, $H\in\mathscr{M}^0$ and $T\cdot H\in\mathscr{M}$, then $T\cdot H=H$. Here $\mathscr{M}^0$ is the interior of $\mathscr{M}$.

(P4) If $H=(h_{ij})\in\mathscr{M}$, then

$$0<h_{11}\leqq(4/3)^{(n-2)/2}(\det H)^{1/(n-1)}.$$

Take a binary form f_0 satisfying the conditions (i)–(iv) in Lemma 5.2. Then $\Psi(f_0)$ is positive definite by Lemma 5.3. Hence there exists a matrix $T_0\in\mathrm{GL}_{n-1}(\mathbb{Z})$ such that $T_0\cdot\Psi(f_0)\in\mathscr{M}$. Since the conditions in Lemma 5.2 are open ones, we may assume that $T_0\cdot\Psi(f_0)\in\mathscr{M}^0$ by Lemma 5.1 and the property (P1). Take a small positive number r such that all binary forms in the compact ball $\mathscr{B}_0$ with center at f_0 and radius r satisfy the conditions in Lemma 5.2 and $T_0\cdot\Psi(\mathscr{B}_0)\subset\mathscr{M}^0$. Put

$$\mathscr{F}_0=\{tg\in V;\ g\in\mathscr{B}_0,\ t\in\mathbb{R},\ t>0\}.$$

By the definition of $\mathscr{F}_0$, we have

$$T_0\cdot\Psi(\mathscr{F}_0)\subset\mathscr{M}^0, \tag{5.1}$$

$$\mathscr{F}_0\subset V^+-\mathscr{S}_0. \tag{5.2}$$

For a binary form $f=a_0x^n+\ldots+a_ny^n$, we put $(h_{ij})=\Psi(f)$, $(\tilde{h}_{ij})=T_0\cdot\Psi(f)$. Since $\mathscr{B}_0$ is compact, a_j/a_0, h_{11}/h_{22} and $\tilde{h}_{ij}/\tilde{h}_{11}$ are bounded in $\mathscr{B}_0$. Since Ψ is defined by homogeneous polynomials in a_j's of degree two, we have

$$\sup_{f\in\mathscr{F}_0}|a_j/a_0|=\sup_{f\in\mathscr{B}_0}|a_j/a_0|=\alpha_j\quad(1\leqq j\leqq n), \tag{5.3}$$

$$\sup_{f\in\mathscr{F}_0}|h_{11}/h_{22}|=\sup_{f\in\mathscr{B}_0}|h_{11}/h_{22}|=\beta_0, \tag{5.4}$$

$$\sup_{f\in\mathscr{F}_0}|\tilde{h}_{ij}/\tilde{h}_{11}|=\sup_{f\in\mathscr{B}_0}|\tilde{h}_{ij}/\tilde{h}_{11}|=\tilde{\beta}_{ij}\quad(1\leqq i\leqq j\leqq n-1). \tag{5.5}$$

By (1.2) and the property (P4), we have

$$\begin{aligned}|\tilde{h}_{11}|&=(4/3)^{(n-2)/2}(\det\Psi(f))^{1/(n-1)}\\&=(4/3)^{(n-2)/2}\,n^{(n-2)/(n-1)}D(f)^{1/(n-1)}\quad\text{for } f\in\mathscr{F}_0.\end{aligned} \tag{5.6}$$

If we put $\beta_1=(4/3)^{(n-2)/2}\,n^{(n-2)/(n-1)}\,\mathrm{Max}(\tilde{\beta}_{ij})$, then we have

$$|\tilde{h}_{ij}|\leqq\beta_1 D(f)^{1/(n-1)}\quad(1\leqq i\leqq j\leqq n-1)\ \text{for } f\in\mathscr{F}_0. \tag{5.7}$$

Further if we put $\beta_2=(n-1)\beta_1\,\mathrm{Max}(|t_{ij}|)$, where $(t_{ij})=T_0^{-1}$, then we have

$$|h_{ij}|\leqq\beta_2 D(f)^{1/(n-1)}\quad(1\leqq i\leqq j\leqq n-1)\ \text{for } f\in\mathscr{F}_0. \tag{5.8}$$

In view of (1.2), we have

$$\begin{aligned}\{(n-2)h_{11}\}^2=(n-1)[h_{11}\{(n-2)a_1\}^2-2h_{12}\{n(n-2)a_0a_1\}\\+(h_{22}-h_{13})\{na_0\}^2]+(n-3)(h_{22}-h_{13})\{na_0\}^2.\end{aligned} \tag{5.9}$$

For $f \in \mathscr{F}_0$, the first term in the right hand side of (5.9) is greater than or equal zero, since (h_{ij}) is positive definite and $h_{13} < 0$. Hence we have

$$\begin{aligned}\{(n-2)h_{11}\}^2 &\geqq (n-3)(h_{22}-h_{13})\{na_0\}^2 \\ &\geqq (n-3)h_{22}\{na_0\}^2 \quad \text{for } f \in \mathscr{F}_0. \end{aligned} \tag{5.10}$$

If we put $\beta_3 = (n-2)n^{-1}\{\beta_0\beta_2/(n-3)\}^{1/2} \operatorname{Max}\{|\alpha_j|, 1\}$, then it follows from (5.3), (5.4), (5.8) and (5.10) that

$$|a_j| \leqq \beta_3 D(f)^{1/2(n-1)} \quad (0 \leqq j \leqq n) \text{ for } f \in \mathscr{F}_0. \tag{5.11}$$

For $X > 0$, put $\mathscr{F}_{0,X} = \{f \in \mathscr{F}_0;\, D(f) \leqq X\}$. Then we have $\mathscr{F}_{0,X} = X^{1/2(n-1)} \cdot \mathscr{F}_{0,1}$, since $D(f)$ is a homogeneous polynomial in a_j's of degree $2(n-1)$. Applying Lemma 3.1, we have

$$\#(\mathscr{F}_{0,X} \cap V_Z) = \operatorname{vol}(\mathscr{F}_{0,1})X^{\kappa} + O(X^{\kappa-\delta}) \quad \text{as } X \to \infty. \tag{5.12}$$

Here we put $\kappa = (n+1)/2(n-1)$, $\delta = 1/2(n-1)$. By (5.11) and Proposition 4.1, we have

$$\#(\mathscr{F}_{0,X} \cap V_{\mathbf{Z}}^{\mathrm{red}}) = O((\log X)^2 X^{\kappa-\delta}) \quad \text{as } X \to \infty. \tag{5.13}$$

Hence we have

$$\#(\mathscr{F}_{0,X} \cap V_{\mathbf{Z}}^{\mathrm{irr}}) = \operatorname{vol}(\mathscr{F}_{0,1})X^{\kappa} + O((\log X)^2 X^{\kappa-\delta}) \quad \text{as } X \to \infty. \tag{5.14}$$

Now we claim that any two distinct binary forms in $\mathscr{F}_0$ are not Γ-equivalent each other. Suppose that $f, g \in \mathscr{F}_0$ and $f \underset{\Gamma}{\sim} g$. Then $g = \gamma \cdot f$ for some $\gamma \in \Gamma$. By Proposition 1.2 and its corollary, we have $\Psi(g) = \psi(\gamma) \cdot \Psi(f)$ and $\psi(\gamma) \in \mathrm{GL}_{n-1}(\mathbf{Z})$. Hence we have $\Psi(f) = \Psi(g)$ by (5.1) and the property (P3). By Proposition 1.3 and (5.2), we have $f = g$. This proves our claim and the assertion of Theorem 1 follows from (5.14). q.e.d.

Proof of Theorem 2. By (5.14), it suffices to show that $\mathcal{O}_f \not\cong \mathcal{O}_g$ for any two distinct integral binary forms $f, g \in \mathscr{F}_0$. Suppose that $\mathcal{O}_f \cong \mathcal{O}_g$. Then we have $\Psi(f) = T \cdot \Psi(g)$ for some $T \in \mathrm{GL}_{n-1}(\mathbf{Z})$. Hence we have $\Psi(f) = \Psi(g)$ by (5.1) and the property (P3). By Proposition 1.3 and (5.2), we have $f = g$. q.e.d.

Proof of Theorem 3. For a prime number p, put $U(p) = \{f \in V_{\mathbf{Z}};\, f \bmod p \in U_n(p)\}$ and $W(p) = \{f \in V_{\mathbf{Z}};\, f \bmod p \notin U_n(p)\}$. Further, put $U = \bigcap_{p:\,\text{prime}} U(p)$. Then for fixed $Y > 0$, we have

$$\lim_{X \to \infty} X^{-\kappa} \#[\mathscr{F}_{0,X} \cap (\bigcap_{p<Y} U(p))] = \operatorname{vol}(\mathscr{F}_{0,1}) \prod_{p<Y} \#[U_n(p)]p^{-n-1} \tag{5.15}$$

by Lemma 3.1 and (5.12). Since $U \subset \bigcap_{p<Y} U(p)$, we have

$$\limsup_{X \to \infty} X^{-\kappa} \#(\mathscr{F}_{0,X} \cap U) \leqq \operatorname{vol}(\mathscr{F}_{0,1}) \prod_{p<Y} \#[U_n(p)]p^{-n-1}. \tag{5.16}$$

As this is true for all $Y>0$, we have

$$\begin{aligned}\limsup_{X\to\infty} X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap U) &\leqq \operatorname{vol}(\mathscr{F}_{0,1})\prod_{p:\,\text{prime}}\#[U_n(p)]p^{-n-1}\\ &=\operatorname{vol}(\mathscr{F}_{0,1})\cdot 24\pi^{-4},\end{aligned}\tag{5.17}$$

by the corollary to Proposition 2.3. To obtain a lower bound for $\#(\mathscr{F}_{0,X}\cap U)$, we observe that $\bigcap_{p<Y} U(p)\subset U\cup(\bigcup_{p\geqq Y} W(p))$. Hence

$$\#[\mathscr{F}_{0,X}\cap(\bigcap_{p<Y} U(p))]\leqq \#(\mathscr{F}_{0,X}\cap U)+\sum_{p\geqq Y}\#(\mathscr{F}_{0,X}\cap W(p)).\tag{5.18}$$

If $p>X$, then $\mathscr{F}_{0,X}\cap W(p)=\emptyset$, since $p\,|\,D(f)$ for $f\in W(p)$. Assume that $p\leqq X$. Then it follows from Lemma 3.1 that

$$\begin{aligned}X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap W(p)) &\leqq [p^{n+1}-\#U_n(p)][\operatorname{vol}(\mathscr{F}_{0,1})p^{-n-1}+CX^{-\delta}p^{-n}]\\ &=p^{n-3}(2p^2-1)[\operatorname{vol}(\mathscr{F}_{0,1})p^{-n-1}+CX^{-\delta}p^{-n}]\\ &\leqq C'p^{-2}+C''p^{-1-\delta}=O(p^{-1-\delta}).\end{aligned}\tag{5.19}$$

Here C, C' and C'' are positive constants which do not depend on p. By (5.15), (5.18) and (5.19), we have

$$\operatorname{vol}(\mathscr{F}_{0,1})\prod_{p<Y}\#[U_n(p)]p^{-n-1}\leqq \liminf_{X\to\infty} X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap U)+O(\sum_{p\geqq Y}p^{-1-\delta}).\tag{5.20}$$

Letting $Y\to\infty$, we obtain

$$\liminf_{X\to\infty} X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap U)\geqq \operatorname{vol}(\mathscr{F}_{0,1})\cdot 24\pi^{-4}.\tag{5.21}$$

Hence we have $\lim_{X\to\infty} X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap U)=\operatorname{vol}(\mathscr{F}_{0,1})\cdot 24\pi^{-4}$. By (5.13),

$$\lim_{X\to\infty} X^{-\kappa}\,\#(\mathscr{F}_{0,X}\cap U\cap V_{\mathbf{Z}}^{\text{irr}})=\operatorname{vol}(\mathscr{F}_{0,1})\cdot 24\pi^{-4}.\tag{5.22}$$

Now the theorem follows from the argument in the proof of Theorem 2 and Proposition 2.2. q.e.d.

Proof of Theorem 4. Suppose $k_1, \ldots, k_r$ are real quadratic fields having a strictly unramified A_n-extension. It suffices to show that there exists a real quadratic field k_{r+1} which is different from k_i $(1\leqq i\leqq r)$ and has the same property. Let D_i be the discriminant of k_i and put $\tilde{U}=\left\{f\in U;\left(D(f),\prod_{i=1}^{r}D_i\right)=1\right\}$. By the same argument as in the proof of Theorem 3, we see that $\tilde{U}\cap V_{\mathbf{Z}}^{\text{irr}}$ is an infinite set. Take a binary from $f\in\tilde{U}\cap V_{\mathbf{Z}}^{\text{irr}}$ and put $k_{r+1}=\mathbf{Q}(\sqrt{D(f)})$. Then $k_{r+1}\neq k_i$ $(1\leqq i\leqq r)$ and the normal closure of K_f is a strictly unramified A_n-extension of k_{r+1}. q.e.d.

References

1. Birch, B.J., Merriman, J.R.: Finiteness theorems for binary forms with given discriminant. Proc. Lond. Math. Soc. **24**, 385–394 (1972)
2. Cassels, J.W.S.: Rational Quadratic Forms. New York London: Academic Press 1978
3. Davenport, H.: On the class number of binary cubic forms (I). J. Lond. Math. Soc. **26**, 183–192 (1951)
4. Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields II. Proc. Roy. Soc. Lond. A **322**, 405–420 (1971)
5. Lang, S.: Algebraic Number Theory. Reading Mass.: Addison-Wesley 1970
6. Lang, S.: Fundamentals of Diophantine Geometry. New York Berlin Heidelberg: Springer 1983
7. Nakagawa, J.: On the Galois group of a number field with square free discriminant. Comment. Math. Univ. Sancti Pauli **37**, 95–98 (1988)
8. Osada, H.: The Galois groups of the polynomials $X^n + aX^l + b$. J. Number Theory **25**, 230–238 (1987)
9. Shintani, T.: On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. J. Math. Soc. Japan **24**, 132–188 (1972)
10. Uchida, K.: Unramified extensions of quadratic number fields II. Tohoku Math. J. **22**, 220–224 (1970)
11. Wright, D.J.: The adelic zeta function associated with the space of binary cubic forms I: Global theory. Math. Ann. **270**, 503–534 (1985)
12. Yamamoto, Y.: On unramified Galois extensions of quadratic number fields. Osaka J. Math. **7**, 57–76 (1970)
13. Yamamura, K.: On unramified Galois extensions of real quadratic fields. Osaka J. Math. **23**, 471–478 (1986)

Oblatum 26-VI-1988 & 25-X-1988