ACTA ARITHMETICA
XLIII (1984)

Well-distributed 2-colorings of integers relative to long arithmetic progressions

by

József Beck (Budapest) and Joel Spencer (Stony Brook, N.Y.)

1. Introduction. Given any "2-coloring" $f\colon \boldsymbol{N}\to\{+1, -1\}$ of the natural numbers, and given any finite subset $A\subset \boldsymbol{N}$, let

$$\mathrm{Discr}(A) = \mathrm{Discr}(A, f) = \Big|\sum_{x\in A} f(x)\Big|$$

denote the *discrepancy* (or *irregularity*) of f relative to A.

In 1964 K. F. Roth [2] proved a remarkable result on irregularities of distribution of integer sequences relative to arithmetic progressions. His general result immediately implies the following

THEOREM A (K. F. Roth). *Given any 2-coloring $f\colon \boldsymbol{N}\to\{+1, -1\}$ of the natural numbers, and given any positive integer k, there is a (finite) arithmetic progression $P = \{a, a+d, a+2d, a+3d, \ldots\}$ of difference $d > k$ such that*

$$\mathrm{Discr}(P, f) > c_1\cdot\sqrt{d}.$$

Throughout this paper $c_1, c_2, c_3, \ldots$ denote positive absolute constants.

Our main object in this paper is to prove a partial converse to Theorem A.

THEOREM 1.1. *Let $\varepsilon > 0$ be an arbitrary small but fixed real. Then given any sufficiently large natural number $n > n_0(\varepsilon)$ there is a 2-coloring $f^*\colon \boldsymbol{N}\to\{+1, -1\}$ such that for any arithmetic progression $P = \{a, a+d, a+2d, a+3d, \ldots\}$ of difference $n^{\varepsilon}\leqslant d\leqslant n$ and of arbitrary length,*

$$\mathrm{Discr}(P, f^*) < d^{1/2+\varepsilon}.$$

Actually, we prove the following somewhat stronger result.

THEOREM 1.2. *Let n be a positive integer. Then there exists a 2-coloring $f^*\colon \boldsymbol{N}\to\{+1, -1\}$ such that for any arithmetic progression $P = \{a, a+d, a+2d, a+3d, \ldots\}$ of difference $1\leqslant d\leqslant n$ and of arbitrary length,*

$$\mathrm{Discr}(P, f^*) < c_2\cdot\sqrt{d}\cdot(\log n)^{3.5}. \tag{1}$$

Unfortunately, we cannot prove that Theorem 1.2 is valid with the RHS of (1) replaced by $d^{1/2+\varepsilon}$. As an upper bound depending only on the difference of the progression it is known the much weaker estimate $d^{(2+\varepsilon)\log d}$. That is, there is a 2-coloring g^*: $N \to \{+1, -1\}$ such that

$$\max_{a,m} \Big| \sum_{i=0}^{m} g^*(a+id) \Big| < d^{(2+\varepsilon)\log d} \tag{2}$$

simultaneously for all $d > d_0(\varepsilon)$ (see [1]).

In connection with this result the first author had the following

CONJECTURE B. *There exists a universal function $h(d)$ such that for any real $0 < \alpha \leqslant 1/2$ there is an "$(\alpha, \alpha-1)$-coloring" g_α^*: $N \to \{\alpha, \alpha-1\}$ satisfying*

$$\max_{a,m} \Big| \sum_{i=0}^{m} g_\alpha^*(a+id) \Big| < h(d)$$

simultaneously for all $1 \leqslant d < \infty$.

Observe that the particular case $\alpha = 1/2$ is settled by (2). In this paper we prove Conjecture B.

THEOREM 1.3. *Conjecture B is true with*

$$h(d) = d^{(2+\varepsilon)\log d} \quad \text{for} \quad d > d_0(\varepsilon).$$

An equivalent reformulation of Theorem 1.3 is as follows. Given an arbitrary real α, $0 < \alpha \leqslant 1/2$, there exists an infinite sequence $\mathscr{A} = \mathscr{A}(\alpha) \subset N$ of density α such that it is nearly well-distributed relative to the congruence classes in the following quantitative sense

$$\max_{j,k} \Big| \sum_{\substack{a \in \mathscr{A}: a \leqslant k \\ a \equiv j \,(\mathrm{mod}\, d)}} 1 - \alpha \cdot \sum_{\substack{a \leqslant k: \\ a \equiv j \,(\mathrm{mod}\, d)}} 1 \Big| < d^{(2+\varepsilon)\log d}$$

for all $d_0(\varepsilon) < d < \infty$.

The analogous generalization of Theorem 1.1 remains open. We cannot prove that for any α, $0 < \alpha \leqslant 1/2$ there exists an $(\alpha, \alpha-1)$-coloring f_α^*: $N \to \{\alpha, \alpha-1\}$ such that

$$\max_{m,a} \Big| \sum_{i=0}^{m} f^*(a+id) \Big| < d^{1/2+\varepsilon} \quad \text{for all } n^\varepsilon \leqslant d \leqslant n.$$

2. Proof of Theorem 1.2. The proof is based on the following lemma.

LEMMA 2.1. *Let $\mathscr{A}_i = \{A_{i1}, A_{i2}, \ldots, A_{il_i}\}$, $1 \leqslant i \leqslant r$ be r partitions of the set $X = \{p_1, q_1, p_2, q_2, \ldots, p_t, q_t\}$. Let $\sum_{i=1}^{r} l_i = l$. Then there is a 2-coloring f: $X \to \{+1, -1\}$ such that*

$$f(p_i) + f(q_i) = 0, \quad 1 \leqslant i \leqslant t,$$

and for each A_{ij}

$$\mathrm{Discr}(A_{ij}, f) < c_3 \sqrt{i} \cdot (\sqrt{\log r \cdot \log l} \cdot \log t).$$

Lemma 2.1 $\Rightarrow$ Theorem 1.2. Let $2^{s-1} \leqslant n < 2^s$. Let $X = Z_{2^s}$, i.e. X is the set of congruence classes (mod 2^s). Let $p_i \equiv i$ (mod 2^s) and $q_i \equiv i + 2^{s-1}$ (mod 2^s), $1 \leqslant i \leqslant 2^{s-1}$. We will associate with every $1 \leqslant d \leqslant n$ some partitions of X. Let $d = 2^k \cdot$odd, and consider the following rectangular array of the congruence classes (mod 2^s):

$$M_d = \begin{bmatrix} d & 2d & 3d & \ldots & 2^{s-k}\cdot d \\ d+1 & 2d+1 & 3d+1 & \ldots & 2^{s-k}\cdot d+1 \\ d+2 & 2d+2 & 3d+2 & \ldots & 2^{s-k}\cdot d+2 \\ \vdots & & & & \\ d+2^{s-k}-1 & 2d+2^{s-k}-1 & 3d+2^{s-k}-1 & \ldots & 2^{s-k}\cdot d+2^{s-k}-1 \end{bmatrix}.$$

Let $\mathscr{B}_d^{(0)} = \{$first row of M_d, second row of $M_d, \ldots,$ last row of $M_d\}$. For each $1 \leqslant i \leqslant s-k$ we partition the rows of M_d (i.e. the elements of $\mathscr{B}_d^{(0)}$) into 2^i equal pieces, and we obtain the further partitions $\mathscr{B}_d^{(i)}$, $1 \leqslant i \leqslant s-k$ of X.

Finally, let

$$\begin{aligned} &\mathscr{A}_1 = \mathscr{B}_1^{(0)}, \quad \mathscr{A}_2 = \mathscr{B}_1^{(1)}, \quad \ldots, \quad \mathscr{A}_{s+1} = \mathscr{B}_1^{(s)}, \\ &\mathscr{A}_{s+2} = \mathscr{B}_2^{(0)}, \quad \mathscr{A}_{s+3} = \mathscr{B}_2^{(1)}, \quad \ldots, \quad \mathscr{A}_{2s+1} = \mathscr{B}_2^{(s-1)}, \\ &\mathscr{A}_{2s+2} = \mathscr{B}_3^{(0)}, \quad \mathscr{A}_{2s+3} = \mathscr{B}_3^{(1)}, \quad \ldots, \quad \mathscr{A}_{3s+2} = \mathscr{B}_3^{(s)}, \\ &\mathscr{A}_{3s+3} = \mathscr{B}_4^{(0)}, \quad \ldots \end{aligned}$$

By Lemma 2.1 there is a 2-coloring f: $Z_{2^s} \to \{+1, -1\}$ such that

$$f(y + 2^{s-1}) = -f(y) \tag{3}$$

and

$$\mathrm{Discr}(B_{d,j}, f) < c_3 \cdot \sqrt{d} \cdot (\log n)^{2.5} \tag{4}$$

for all $B_{d,j} \in \mathscr{B}_d^{(j)}$, $1 \leqslant d \leqslant n$, $0 \leqslant j \leqslant s-k$ (where $d = 2^k \cdot$odd).

Now we are ready to define the desired 2-coloring f^*: $N \to \{+1, -1\}$:

if $x \equiv y$ (mod 2^s), $0 \leqslant y < 2^s$, then let $f^*(x) = f(y)$, $x \in N$.

By (3),

$$f^*(x + 2^{s-1}) = -f^*(x),$$

thus we have

$$\sum_{i=1}^{2^{s-k}} f^*(a+id) = 0.$$

From this it follows that we can restrict ourselves to the "short" arithmetic progressions

$$P = \{a, a+d, a+2d, \ldots, a+(m-1)d\}, \quad m < 2^{s-k}.$$

Let $a \equiv j_0 \pmod{2^{s-k}}$, $0 \leqslant j_0 < 2^{s-k}$. Observe that $P \pmod{2^s}$ is a subinterval (or the union of two disjoint subintervals) of the j_0th row of M_d. Therefore, $P \pmod{2^s}$ is representable as the union of not more than $c_4 \cdot \log n$ disjoint elements of $\bigcup_{i=0}^{s-k} \mathscr{B}_d^{(i)}$. Thus, by (4)

$$\Big|\sum_{i=0}^{m-1} f^*(a+id)\Big| < c_3 \cdot \sqrt{d} \cdot (\log n)^{2.5} \cdot (c_4 \cdot \log n),$$

completing the deduction of Theorem 1.2 from Lemma 2.1. ∎

Let $L(x_1, x_2, \ldots, x_t) = a_1x_1 + a_2x_2 + \ldots + a_tx_t$ be a linear form with all $a_i \in \{+1, 0, -1\}$. We call

$$\hat{L} = \hat{L}(x_1, \ldots, x_t) = \{1 \leqslant i \leqslant t \colon a_i \neq 0\}$$

the *support* of the linear form L.

We reduce Lemma 2.1 to the following lemma on linear forms:

LEMMA 2.2. *Let $L_{i,j}(x_1, \ldots, x_t) = a_{ij}^{(1)}x_1 + \ldots + a_{ij}^{(t)}x_t$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant l_i$, be linear forms with the properties*

(α) $a_{ij}^{(u)} \in \{+1, 0, -1\}$ for all i, j and u;

(β) $\hat{L}_{i,j}$ and $\hat{L}_{i,k}$ are disjoint if $j \neq k$.

Then there exist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_t \in \{+1, -1\}$ such that

$$|L_{i,j}(\varepsilon_1, \ldots, \varepsilon_t)| < c_3 \cdot \sqrt{i} \cdot (\sqrt{\log r \cdot \log l \cdot \log t}) \tag{5}$$

for all $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant l_i$, where $l = \sum_{i=1}^{r} l_i$.

Lemma 2.2 ⇒ Lemma 2.1. Let us associate with every $A_{ij} \in \mathscr{A}_i$ the linear form $L_{i,j}(x_1, \ldots, x_t) = \sum_{u=1}^{t} a_{ij}^{(u)} x_u$, where

$$a_{ij}^{(u)} = \begin{cases} 0 & \text{if} \quad \{p_u, q_u\} \subset A_{ij}, \\ +1 & \text{if} \quad p_u \in A_{ij},\ q_u \notin A_{ij}, \\ -1 & \text{if} \quad p_u \notin A_{ij},\ q_u \in A_{ij}. \end{cases}$$

By Lemma 2.2 there exist $\varepsilon_1, \ldots, \varepsilon_t = \pm 1$ such that (5) is true. Set $f(p_u) = \varepsilon_u$ and $f(q_u) = -\varepsilon_u$, for all $1 \leqslant u \leqslant t$. Observe that f is the desired 2-coloring of X, since

$$\mathrm{Discr}(A_{ij}, f) = L_{i,j}(\varepsilon_1, \ldots, \varepsilon_t). \ ∎$$

Proof of Lemma 2.2. The proof will consist of a repeated application of the following

LEMMA 2.3. *Under the hypothesis of Lemma 2.2 there exist $\delta_1, \delta_2, \ldots, \delta_t \in \{+1, 0, -1\}$ such that*

$$|L_{i,j}(\delta_1, \ldots, \delta_t)| < c_5 \cdot \sqrt{i} \cdot (\sqrt{\log r \cdot \log l}) \text{ for all } 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant l_i, \tag{6}$$

and

$$|\{1 \leqslant i \leqslant t \colon \delta_i = 0\}| \leqslant \tfrac{9}{10} t. \tag{7}$$

We can easily prove Lemma 2.2 from Lemma 2.3. Indeed, by Lemma 2.3 there exists a function $g_1 \colon \{1, 2, \ldots, t\} \to \{+1, 0, -1\}$ such that

$$|L_{i,j}(g_1(1), g_1(2), \ldots, g_1(t))| < c_5 \cdot \sqrt{i} \cdot (\sqrt{\log r \cdot \log l})$$

and the set $Y_1 = \{1 \leqslant i \leqslant t \colon g_1(i) = 0\}$ has cardinality at most $\frac{9}{10} t$.

Let $L_{i,j}^{(1)}$ be the "restriction" of the linear form $L_{i,j}$ to Y_1, that is, let

$$L_{i,j}^{(1)} = \sum_{k \in Y_1} a_{ij}^{(k)} x_k.$$

Applying Lemma 2.3 to the linear forms $L_{i,j}^{(1)}$ we obtain the existence of a function $g_2 \colon Y_1 \to \{+1, 0, -1\}$ such that

$$\Big|\sum_{k \in Y_1} a_{ij}^{(k)} g_2(k)\Big| < c_5 \cdot \sqrt{i} \cdot (\sqrt{\log r \cdot \log l}),$$

and the set $Y_2 = \{k \in Y_1 \colon g_2(k) = 0\}$ has cardinality at most $\frac{9}{10}|Y_1| \leqslant (\frac{9}{10})^2 \cdot t$, and so on. The procedure clearly stops within $c_6 \log t$ steps. Set $f = \sum_{i \geqslant 1} g_i$, and define $\varepsilon_i = f(i)$ for all $1 \leqslant i \leqslant t$. From the procedure above it follows that

$$|L_{i,j}(\varepsilon_1, \ldots, \varepsilon_t)| < (c_6 \cdot \log t) \cdot c_5 \cdot \sqrt{i \cdot \log r \cdot \log l},$$

which completes the deduction of Lemma 2.2 from Lemma 2.3. ∎

Finally, we prove Lemma 2.3. Let E denote the set of 2^t ±1-vectors $\vec{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_t)$, $\varepsilon_i = \pm 1$. Using the well-known asymptotic properties of binomial coefficients we get for every $L_{i,j}$

$$\big|\{\vec{\varepsilon} \in E \colon |L_{i,j}(\vec{\varepsilon})| > 2 \cdot \lambda \cdot \sqrt{|\hat{L}_{i,j}|}\}\big| = 2^{t - |\hat{L}_{i,j}|} \cdot \sum_{|k - |\hat{L}_{i,j}|/2| > 2 \cdot \sqrt{|\hat{L}_{i,j}|}} \binom{|\hat{L}_{i,j}|}{k} \leqslant 2^t \cdot e^{-\lambda^2/2}.$$

Thus, for a large enough constant c_7 the cardinality of the set

$$E_1 = \{\vec{\varepsilon} \in E \colon |L_{i,j}(\vec{\varepsilon})| < c_7 \cdot \sqrt{|\hat{L}_{i,j}| \cdot \log l} \text{ for all } 1 \leqslant i \leqslant r \text{ and } 1 \leqslant j \leqslant l_i\} \tag{8}$$

is greater than 2^{t-1}.

Define an equivalence class on E_1, placing $\vec{\varepsilon}_1$ and $\vec{\varepsilon}_2$ in the same class if for each pair (i,j), $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant l_i$

$$|L_{i,j}(\vec{\varepsilon}_1) - L_{i,j}(\vec{\varepsilon}_2)| \leqslant 2c_7 \cdot \sqrt{i \cdot \log r \cdot \log l}. \tag{9}$$

By (8) and (9), the number of equivalence classes is less than

$$W = \prod_{i=1}^{r} \prod_{j=1}^{l_i} \sqrt{\frac{|\hat{L}_{i,j}|}{i \cdot \log r}}. \tag{10}$$

We need the elementary inequality: for arbitrary positive reals $b_1, b_2, \ldots \ldots, b_n$,

$$\prod_{i=1}^{n} b_i \leqslant \exp\Big\{\sum_{i=1}^{n} b_i/e\Big\}, \quad \text{where } e = 2.718\ldots \tag{11}$$

Since $\sum_{j=1}^{l_i} |\hat{L}_{i,j}| \leqslant t$, by (10) and (11) we get

$$W \leqslant \exp\Big\{\sum_{i=1}^{r} \frac{t}{i \cdot \log r}\Big/ 2e\Big\} \leqslant e^{t/2e} < 2^{\frac{3}{10}t}.$$

Thus there is one equivalence class, call it E_2, with

$$|E_2| \geqslant |E_1| \cdot 2^{-\frac{3}{10}t} \geqslant 2^{\frac{7}{10}t-1}.$$

Fix $\vec{\varepsilon}_0 \in E_2$. The number of $\vec{\varepsilon} \in E$ which disagree with $\vec{\varepsilon}_0$ in at most $t/10$ places is

$$\sum_{i=0}^{t/10} \binom{t}{i} < 2\binom{t}{t/10} < 2^{\frac{7}{10}t-1}.$$

Thus there exists $\vec{\varepsilon}_1 \in E_2$ which disagrees with $\vec{\varepsilon}_0$ in at least $t/10$ places. Set

$$\vec{\varepsilon} = (\vec{\varepsilon}_0 - \vec{\varepsilon}_1)/2,$$

and Lemma 2.3 follows. ■

3. Proof of Theorem 1.3. Actually, we prove the following generalization of Theorem 1.3.

THEOREM 3.1. *Let $L_i(x_1, x_2, \ldots, x_n) = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$, $1 \leqslant i \leqslant n$, be n linear forms with all $a_{ij} \in \{0,1\}$. Let $p_1, \ldots, p_n \in [0,1]$. Then there exist $\varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}$ such that*

$$\max_{1\leqslant k\leqslant n} \Big|\sum_{1\leqslant j\leqslant k} a_{ij}(\varepsilon_j - p_j)\Big| < i^{(1/2+\delta)\log i} \quad \textit{for all } n_0(\delta) < i \leqslant n,$$

where the threshold $n_0(\delta)$ is independent of n and depends only on the positive (arbitrarily small) constant δ.

Theorem 3.1 ⇒ Theorem 1.3. Let $p_1 = p_2 = \ldots = p_n = \alpha$ and consider the linear forms $L_i = a_{i1}x_1 + \ldots + a_{in}x_n$ with the following coefficients

$$a_{\binom{d}{2}+l,j} = \begin{cases} 1 & \text{if } j \equiv l \pmod d, \\ 0 & \text{otherwise,} \end{cases}$$

where $d = 1, 2, \ldots$, $1 \leqslant l \leqslant d$ and $j = 1, 2, \ldots$

By Theorem 3.1 there exist $\varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}$ such that the sequence $\mathscr{A}(\alpha, n) = \{1 \leqslant i \leqslant n:\ \varepsilon_i = +1\}$ satisfies the property

$$\max_{1\leqslant k\leqslant n, l} \Big| \sum_{\substack{i\in\mathscr{A}(\alpha,n):\\ i\leqslant k,\, i\equiv l \pmod d}} 1 - \alpha \cdot \sum_{\substack{i\leqslant k:\\ i\equiv l \pmod d}} 1 \Big| < d^{(2+\delta)\log d} \tag{12}$$

for all $n_0(\delta) < d \leqslant \sqrt{n}$ (here $n_0(\varepsilon)$ is independent of n). Now (12) immediately yields Theorem 1.3 by a simple compactness argument as $n \to +\infty$. ■

We recall the main result of [1].

THEOREM 3.2. *Let $L_i(x_1, \ldots, x_n) = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$, $1 \leqslant i \leqslant n$, be n linear forms in n variables with all coefficients $a_{ij} \in \{0,1\}$. Then there are $\varepsilon_1, \ldots, \varepsilon_n = \pm 1$ so that*

$$\max_{1\leqslant k\leqslant n} \Big|\sum_{j=1}^{k} a_{ij}\varepsilon_j\Big| < i^{(\frac{1}{2}+\delta)\log i} \quad \textit{for all } n_0(\delta) < i \leqslant n.$$

Theorem 3.2 ⇒ Theorem 3.1. Set

$$B_i = \begin{cases} (\frac{1}{2}+\delta)\log i \\ i & \text{for } i > n_0(\delta), \\ c_8 & \text{for } i \leqslant n_0(\delta) \end{cases}$$

for convenience. Assume $p_1, \ldots, p_n$ have finite binary expansions with maximal length T. Set

$$J = \{j:\ p_j \text{ has } T\text{th digit } 1\}.$$

By Theorem 3.2 there exist $\varepsilon_j = \pm 1$, $j \in J$ so that

$$\max_{1\leqslant k\leqslant n} \Big|\sum_{j\in J: j\leqslant k} a_{ij}\varepsilon_j\Big| \leqslant B_i.$$

Set

$$p_j^* = \begin{cases} p_j + 2^{-T} & \text{if } \varepsilon_j = +1, \\ p_j - 2^{-T} & \text{if } \varepsilon_j = -1, \\ p_j & \text{if } j \notin J. \end{cases}$$

Then

$$\max_{1\leqslant k\leqslant n} \Big|\sum_{j\in J: j\leqslant k} a_{ij}(p_j^* - p_j)\Big| = 2^{-T} \cdot \max_{1\leqslant k\leqslant n} \Big|\sum_{j\in J: j\leqslant k} a_{ij}\varepsilon_j\Big| \leqslant 2^{-T}B_i,$$

and $p_1^*, \ldots, p_n^*$ have binary expansions with maximal length $T-1$. Applying this procedure $(T-1)$ more times we replace $p_1, \ldots, p_n$ with $\varepsilon_1, \ldots, \varepsilon_n \in \{0, 1\}$ such that

$$\max_{1\leqslant k\leqslant n}\Big|\sum_{j\leqslant k} a_{ij}(\varepsilon_j - p_j)\Big| \leqslant \sum_{h=1}^{T} 2^{-h}\cdot B_i \leqslant B_i.$$

Finally, if $p_1, \ldots, p_n \in [0, 1]$ are arbitrary the existence of $\varepsilon_1, \ldots, \varepsilon_n$ follows by a simple compactness argument. ■

References

[1] J. Beck, *Balancing families of integer sequences*, Combinatorica 1 (3) (1981), pp. 209–216.

[2] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. 9 (1964), pp. 257–260.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
Budapest, Realtanoda u. 13-15, 1053 Hungary
DEPARTMENT OF MATHEMATICS, SUNY
Stony Brook, N. Y. 11 794, U.S.A.

Received on 14. 9. 1982 (1320)

ACTA ARITHMETICA
XLIII (1984)

On the genus group of algebraic number fields

by

KIYOAKI IIMURA (Tokyo)

Introduction. Let K be a finite extension of the field $\boldsymbol{Q}$ of rational numbers. Call $C(K)$ the ideal class group of K in the narrow sense. Call $\tilde{K}$ the genus field of K, i.e., the maximal abelian extension of K which is composed of K and of an abelian extension of $\boldsymbol{Q}$ and is unramified at all the finite primes of K (cf. [1]). Call $G(K)$ the subgroup of $C(K)$ corresponding to the genus field $\tilde{K}$ in the sense of class field theory; $G(K)$ is called the principal genus of K, and the factor group $C(K)/G(K)$ is called the genus group of K. Call μ the canonical homomorphism of $C(K)$ onto $C(K)/G(K)$. Our aim of the paper is to study the image $\mu(c)$ for an element c of $C(K)$. Particularly it will be shown that if $K/\boldsymbol{Q}$ is of odd prime degree and an irreducible polynomial over $\boldsymbol{Q}$ defining K is given, then the image $\mu(H)$, where H is the subgroup of $C(K)$, generated by the classes of all the prime ideals of K ramifying fully over $\boldsymbol{Q}$, can be known by an elementary and purely rational procedure. As its immediate consequence, a generalization of Theorem 3 in [2] is obtained; this theorem states that if a purely rational condition about the rational primes ramified fully in K is satisfied, then the class number of the pure field $K = \boldsymbol{Q}(\sqrt[l]{m})$ of odd prime degree l is divisible by $l^{t+u-(l+1)/2}$, where t (resp. u) is the number of rational primes (resp. those $\equiv 1 \pmod{l}$) ramified in K.

We conclude this introduction with a remark about conventions. By a prime ideal, we will understand a finite prime ideal. Also $\boldsymbol{Z}$ will be the ring of rational integers.

1. Image $\mu(c)$. Let notations be the same as in the introduction. Call k the maximal abelian extension of $\boldsymbol{Q}$, contained in the genus field $\tilde{K}$ of K; then, by definition, $\tilde{K}$ is the compositum of k and K, and so the restriction map: $G(\tilde{K}/K)\to G(k/\boldsymbol{Q})$ is injective, where $G(L/M)$ is the Galois group of a Galois extension L/M. By means of the Artin map, the genus group $C(K)/G(K)$ is isomorphic to $G(\tilde{K}/K)$. So if we call ν the homomorphism of $C(K)$ to $G(k/\boldsymbol{Q})$ obtained by composing these two maps with μ, the study of the image $\mu(c)$ in question is reduced to that