References

[1] T. Agoh, *On the first case of Fermat's last theorem*, J. Reine Angew. Math. 319 (1980), 21–28.

[2] R. Fueter, *Kummers Kriterium zum letzen Theorem von Fermat*, Math. Ann. 85 (1922), 11–20.

[3] A. J. Granville, *Diophantine equations with varying exponents with special reference to Fermat's last theorem*, Ph. D. Thesis, Queen's Univ., Kingston, 1987, 207 pp.

[4] A. J. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714,591,416,091,389, Trans. Amer. Math. Soc. 306 (1988), 329–359.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II*, Jahresber. Deutsch. Math.-Verein., 1930, 204 pp. Reprinted by Physica-Verlag, Würzburg 1965.

[6] K. Inkeri, *Some extensions of criteria concerning singular integers in cyclotomic fields*, Ann. Acad. Sci. Fenn. Ser. AI, 49 (1948), 3–15.

[7] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abhandl. Königl. Akad. Wiss. Berlin, 1857, 41–74.

[8] P. Le Lidec, *Sur une forme nouvelle des congruences de Kummer–Mirimanoff*, C. R. Acad. Sci. Paris, Sér. A, 265 (1967), 89–90.

[9] — *Nouvelle forme des congruences de Kummer–Mirimanoff pour le premier cas du théorème de Fermat*, Bull. Soc. Math. France 97 (1969), 321–328.

[10] D. Mirimanoff, *L'équation indéterminée* $x^l + y^l + z^l = 0$ *et le critérium de Kummer*, J. Reine Angew. Math. 128 (1905), 45–68.

[11] P. Ribenboim, 13 *lectures on Fermat's last theorem*, Springer, New York–Heidelberg–Berlin 1979.

DEPARTMENT OF MATHEMATICS
SCIENCE UNIVERSITY OF TOKYO
Noda, Chiba 278, Japan

Received on 6.9.1988
and in revised form on 16.1.1989 (1866)

ACTA ARITHMETICA
LV (1990)

CM-fields and exponents of their ideal class groups

by

KUNIAKI HORIE (Yamaguchi) and MITSUKO HORIE (Fukuoka)

By an *algebraic number field*, we shall mean a finite algebraic extension over the rational number field $\boldsymbol{Q}$. All such fields will be supposed to lie in the complex number field $\boldsymbol{C}$. Let j denote the complex conjugation of $\boldsymbol{C}$. An algebraic number field k is called a *j-field* when k is invariant as a whole under j, i.e., $k^j = k$ and when $\sigma j = j\sigma$ on k for all isomorphisms σ of k into $\boldsymbol{C}$. Then a j-field is either a totally real algebraic number field or a CM-field, namely, a totally imaginary quadratic extension over a totally real algebraic number field.

Let l be a fixed prime number. For any algebraic number field F, let C_F denote the ideal class group of F, A_F the Sylow l-subgroup of C_F, h_F the class number of F, and s_F the order of A_F. The exponent of each finite group G will be denoted by $\exp G$. In the present paper, we shall first prove the following

THEOREM 1. *Let k be a j-field; let r, m, and n be natural numbers. Then only a finite number of CM-fields K have the following two properties:*

(i) $h_K/s_K \leqslant m$ *and* $\exp A_K \leqslant l^r$,

(ii) *there exists a sequence* $k = k_0 \subset k_1 \subset \ldots \subset k_n = K$ *of j-fields such that for each* $\nu \in \{1, 2, \ldots, n\}$, $k_\nu = k_{\nu-1}$ *or* $k_\nu/k_{\nu-1}$ *is a cyclic extension of degree l.*

Now, for each (multiplicative) abelian group $\mathfrak{M}$ on which j acts, we put

$$\mathfrak{M}^- = \{\mu \in \mathfrak{M} \mid \mu^j = \mu^{-1}\}.$$

For any j-field F, we let

$$h_F^- = h_F/h_{F^+},$$

where F^+ denotes the maximal real subfield of F; h_F^- is known to be an integer. Furthermore, as j acts on A_F in the obvious manner, we can define

$$s_F^- = |A_F^-|.$$

In the case $l > 2$, this becomes the highest power of l dividing h_F^- and we can prove the following result which is more precise than Theorem 1.

THEOREM 2. *Assume $l > 2$. Let k be a CM-field and r, m, and n natural numbers. Then only a finite number of CM-fields K have the following two properties:*

(i) $h_K^-/s_K^- \leqslant m$ *and* $\exp A_K^- \leqslant l^r$,

(ii) *there exists a sequence $k = k_0 \subset k_1 \subset \ldots \subset k_n = K$ of CM-fields such that for each $v \in \{1, \ldots, n\}$, $k_v = k_{v-1}$ or k_v/k_{v-1} is a cyclic extension of degree l.*

We shall also have

THEOREM 3. *Let k be a j-field and m a natural number. Then there exist only a finite number of CM-fields K which are abelian l-extensions over k such that $h_K/s_K \leqslant m$ and $\exp A_K \leqslant l$.*

THEOREM 4. *Assume $l > 2$. Let k be a CM-field and m a natural number. Then there exist only a finite number of CM-fields K which are abelian l-extensions over k such that $h_K^-/s_K^- \leqslant m$ and $\exp A_K^- \leqslant l$.*

Furthermore, in the last section of the paper, we shall give an explicit estimate for the conductor of an imaginary cyclic field, of degree a 2-power $\geqslant 4$, whose ideal class group has exponent 1 or 2. Here, by a cyclic field, we mean of course a finite cyclic extension over $\boldsymbol{Q}$. A finite abelian extension over $\boldsymbol{Q}$ will be called an abelian field.

Throughout the paper, the notations R_K, D_K, and $D_{K/k}$ stand respectively for the regulator of an algebraic number field K, the absolute value of the discriminant of K, and the absolute norm of the relative discriminant of K over a subfield k of K. If K/k is an abelian extension of algebraic number fields, then we write $f_{K/k}$ for the absolute norm of the conductor of K/k.

We conclude this introduction with mentioning some results related to the above ones. Chowla showed in [3] the finiteness of the imaginary quadratic fields with ideal class groups of exponent 2. This finiteness theorem has been extended by Boyd–Kisilevsky [1] and also by Weinberger [12] to the imaginary quadratic fields with ideal class groups of any given exponent (partly under conjectures in number theory such as the generalized Riemann hypothesis), by the second author (née Hamamura) of the present paper to the imaginary abelian fields F with genus numbers equal to h_F (cf. [6]), and by Earnest–Körner [4] to the totally imaginary quadratic extensions, over a fixed totally real algebraic number field, having ideal class groups of exponent 2^r, where r is any given natural number. It might be quite natural to ask whether only finitely many imaginary abelian fields have ideal class groups of exponent equal to a given natural number. Recently a study of this problem has been made by Earnest [5].

Acknowledgements. It is a great pleasure to express our heartfelt gratitude to Professor K. Iwasawa who has kindly introduced us to the study in this paper. We are also grateful to Professor Y. Morita for very important comments.

1. For any algebraic number field K, we let

$$B_K = \{a \in A_K \mid a^l = 1\}$$

and if k is a subfield of K such that K/k is a cyclic extension of degree l, then we put

$$A_{K/k} = \{a \in B_K \mid a^{(\sigma-1)^{l-1}} = 1\}$$

where σ is a generator of $\mathrm{Gal}(K/k)$. Obviously $A_{K/k}$ does not depend on the choice of σ.

To prove Theorem 1, we prepare some lemmas.

LEMMA 1. *Let K/k be a cyclic extension of degree l of algebraic number fields. Then*

(i) $\mathrm{rank}\, B_K \leqslant \mathrm{rank}\, A_k + \mathrm{rank}\, A_{K/k}$,

(ii) $|B_K| \leqslant |B_k|\,|A_{K/k}| \leqslant s_k |A_{K/k}|$.

Proof. Let σ be a generator of $\mathrm{Gal}(K/k)$. Since

$$(\sigma-1)^{l-1} - (1 + \sigma + \ldots + \sigma^{l-1}) \in l\boldsymbol{Z}[\mathrm{Gal}(K/k)],$$

we see that $a^{(\sigma-1)^{l-1}} \in N_{K/k} B_K \subset B_k$ for any element a of B_K. Hence the mapping

$$a \mapsto a^{(\sigma-1)^{l-1}}, \quad a \in B_K,$$

defines a homomorphism $B_K \to B_k$, which induces an injection

$$B_K/A_{K/k} \subsetneq B_k.$$

This proves Lemma 1.

LEMMA 2. *Let K/k be the same as in Lemma 1 and let t denote the number of primes of K ramified for K/k. Then*

$$|A_{K/k}| \leqslant (s_k l^t)^{l-1}.$$

Proof. Indeed

$$|A_{K/k}| = |B_K/B_K^{(\sigma-1)^{l-1}}| = \prod_{\nu=1}^{l-1} |B_K^{(\sigma-1)^{\nu-1}}/B_K^{(\sigma-1)^{\nu}}|$$

$$\leqslant |B_K/B_K^{\sigma-1}|^{l-1} = |\{a \in B_K \mid a^{\sigma-1} = 1\}|^{l-1}$$

and the right-hand side of the above does not exceed $(s_k l^t)^{l-1}$ by the ambiguous class number formula.

LEMMA 3. *Let k, r, and n be the same as in Theorem 1. Let $k = k_0 \subset k_1 \subset \ldots \subset k_n$ be a tower of algebraic number fields such that, for each $v \in \{1, \ldots, n\}$, $k_v = k_{v-1}$ or k_v/k_{v-1} is a cyclic extension of degree l. Then*

$$\mathrm{ord}_l h_{k_n} \leqslant \Big(l^n \prod_{\nu=1}^{n} r_\nu\Big) \mathrm{ord}_l h_k + \sum_{\nu=1}^{n} l^{n-\nu}(l-1) t_\nu \prod_{i=\nu}^{n} r_i, \tag{1}$$

where

$$r_\nu = \mathrm{ord}_l(\exp A_{k_\nu}), \quad \nu \in \{1, \ldots, n\},$$

and each t_ν denotes the number of primes of k_ν ramified for $k_\nu/k_{\nu-1}$.

Proof. For the proof of this lemma by induction on n, it suffices to prove (1) with assuming that

$$\mathrm{ord}_l h_{k_{n-1}} \leqslant (l^{n-1}\prod_{\nu=1}^{n-1} r_\nu)\,\mathrm{ord}_l h_k + \sum_{\nu=1}^{n-1} l^{n-1-\nu}(l-1)\,t_\nu \prod_{i=\nu}^{n-1} r_i.$$

Since $s_{k_n} \leqslant |B_{k_n}|^{r_n}$, we have, by Lemmas 1, 2,

$$\begin{aligned}\mathrm{ord}_l h_{k_n} &\leqslant r_n(\mathrm{ord}_l |A_{k_n/k_{n-1}}| + \mathrm{ord}_l h_{k_{n-1}})\\ &\leqslant r_n((l-1)(\mathrm{ord}_l h_{k_{n-1}} + t_n) + \mathrm{ord}_l h_{k_{n-1}})\\ &= r_n l\,\mathrm{ord}_l h_{k_{n-1}} + (l-1)\,t_n r_n.\end{aligned}$$

Hence the above hypothesis implies that

$$\begin{aligned}\mathrm{ord}_l h_{k_n} &\leqslant l r_n(l^{n-1}\prod_{\nu=1}^{n-1} r_\nu)\,\mathrm{ord}_l h_k + (l-1)\Big(\sum_{\nu=1}^{n-1} l^{n-\nu} t_\nu \prod_{i=\nu}^{n} r_i + t_n r_n\Big)\\ &= (l^n \prod_{\nu=1}^{n} r_\nu)\,\mathrm{ord}_l h_k + (l-1)\sum_{\nu=1}^{n} l^{n-\nu} t_\nu \prod_{i=\nu}^{n} r_i.\end{aligned}$$

Thus the lemma is proved.

The following lemma is a corollary of the Brauer–Siegel theorem (Theorem 2 in [2]).

LEMMA 4. *Let K range over a sequence of CM-fields such that $D_K \to \infty$ with $[K:\boldsymbol{Q}]$ bounded. Then $D_K/D_{K^+} \to \infty$ and*

$$\log h_K^- \sim \log\sqrt{D_K/D_{K^+}}, \quad \textit{i.e.,} \quad \frac{\log h_K^-}{\log\sqrt{D_K/D_{K^+}}} \to 1.$$

Proof. Let ε be any positive number $< 1/4$. By the Brauer–Siegel theorem, there exists a positive number D_ε depending only on ε such that

$$D_K^{1/2-\varepsilon} \leqslant h_{K^+} R_{K^+} \leqslant D_K^{1/2+\varepsilon}$$

if $D_{K^+} \geqslant D_\varepsilon$. Of course

$$D_K^{(1-\varepsilon)/2} \leqslant h_K R_K \leqslant D_K^{(1+\varepsilon)/2}, \quad D_K \gg 1.$$

Since $D_K/D_{K^+} = D_{K/K^+} D_{K^+} \geqslant D_{K^+}$, we have

$$\frac{R_{K^+}}{R_K}(D_K/D_{K^+})^{1/2-2\varepsilon} \leqslant h_K^- \leqslant \frac{R_{K^+}}{R_K}(D_K/D_{K^+})^{1/2+2\varepsilon} \tag{2}$$

in case $D_{K^+} \geqslant D_\varepsilon$; we have otherwise

$$\frac{D_{K^+}^{(1-\varepsilon)/2}}{h_{K^+} R_K}(D_K/D_{K^+})^{(1-\varepsilon)/2} \leqslant h_K^- \leqslant \frac{D_{K^+}^{(1+\varepsilon)/2}}{h_{K^+} R_K}(D_K/D_{K^+})^{(1+\varepsilon)/2}. \tag{3}$$

However, as is well known, $2^{[K^+:\boldsymbol{Q}]-1} R_{K^+}/R_K = 1$ or 2 and, as follows from the Hermite–Minkowski theorem, the value $h_{K^+} R_{K^+}$ is bounded if K varies, satisfying $D_{K^+} < D_\varepsilon$. Hence, by the hypothesis that $[K:\boldsymbol{Q}]$ is bounded, the above inequalities (2), (3) induce

$$\liminf_K \frac{\log h_K^-}{\log\sqrt{D_K/D_{K^+}}} \geqslant 1, \quad \limsup_K \frac{\log h_K^-}{\log\sqrt{D_K/D_{K^+}}} \leqslant 1.$$

Therefore we obtain the lemma.

Finally we add an elementary lemma.

LEMMA 5. *Let K/k be an extension with l-power degree of algebraic number fields. Then:*

(i) *h_k/s_k is a divisor of h_K/s_K,*

(ii) *$\exp A_k \leqslant [K:k]\ \exp A_K$.*

Proof. Let ι be the canonical homomorphism $C_k \to C_K$ and N the homomorphism $C_K \to C_k$ induced by the norm map for K/k, so that

$$N(\iota(c)) = c^{[K:k]}, \quad c \in C_k.$$

Since $[K:k]$ is prime to $h_k/s_k = [C_k : A_k]$, $N\circ\iota$ then defines an automorphism of C_k/A_k. Hence ι induces an injective homomorphism $C_k/A_k \to C_K/A_K$ and, in particular, the assertion (i) is proved. On the other hand,

$$a^{[K:k]\exp A_K} = N(\iota(a)^{\exp A_K}) = 1, \quad a \in A_k.$$

This proves (ii).

Proof of Theorem 1. Let K be a CM-field and assume that K has the properties (i), (ii) of the theorem. Let u be the number of distinct rational primes dividing $D_{K/k}$. For each $\nu \in \{1, \ldots, n\}$, let $r_\nu = \mathrm{ord}_l(\exp A_{k_\nu})$, let t_ν denote the number of primes of k_ν ramified for $k_\nu/k_{\nu-1}$, and let $\delta_\nu = 1$ or 0 according as the infinite primes of $k_{\nu-1}$ are ramified in k_ν or not. Since

$$t_\nu \leqslant [k_{\nu-1}:\boldsymbol{Q}](u+\delta_\nu) \leqslant l^{\nu-1}[k:\boldsymbol{Q}](u+\delta_\nu), \quad \nu \in \{1, \ldots, n\}$$

and since each r_ν is at most equal to $r+n-\nu$ by (ii) and Lemma 5, it follows from Lemma 3 that

$$\mathrm{ord}_l h_K \leqslant a_1 + a_2\delta + a_2 u,$$

with

$$\delta = \sum_{\nu=1}^{n} \delta_\nu$$

and

$$a_1 = l^n\Big(\prod_{\nu=1}^{n}(r+n-\nu)\Big)\ \mathrm{ord}_l h_k,$$

$$a_2 = (l-1)\,l^{n-1}[k:\mathbb{Q}]\sum_{\nu=1}^{n}\prod_{i=\nu}^{n}(r+n-i).$$

Note, in the above, $\delta = 0$ or 1. Therefore we see that

$$\log h_K \leqslant \log s_K + \log m \leqslant cu, \tag{4}$$

where $c = (a_1 + a_2\delta + a_2)\log l + \log m$.

Next, let ε be an arbitrary positive number < 1. By (ii), Lemma 4 implies that, when D_K is sufficiently large,

$$\log h_K^- > (1-\varepsilon)\log\sqrt{D_K/D_{K^+}} \geqslant \frac{1-\varepsilon}{4}\log D_K$$

so that, by (4),

$$cu > \frac{1-\varepsilon}{4}\log D_K \tag{5}$$

and, hence, u is positive. As

$$\log D_K \geqslant \log D_{K/k} > \sum_{i=1}^{u}\log i > u\log u - u,$$

we then also obtain, from (4),

$$cu > \frac{1-\varepsilon}{4}(u\log u - u), \quad \text{i.e.,} \quad \log u < \frac{4c}{1-\varepsilon}+1.$$

This, together with (5), shows that

$$\log D_K < \frac{4ce^{1+4c/(1-\varepsilon)}}{1-\varepsilon},$$

which completes the proof of Theorem 1.

COROLLARY 1. *Let k, r, m and n be the same as in Theorem 1. Then there exist at most finitely many CM-fields L with the following properties:*

(i) $h_L/s_L \leqslant m$ *and* $\exp A_L \leqslant l^r$,

(ii) *L is a composite field of CM-fields which have the same property as K in* (ii) *of Theorem 1.*

Proof. Let $\mathscr{L}$ be the set of CM-fields L with the above properties (i), (ii); let $\mathscr{K}$ be the set of CM-fields K satisfying (ii) of Theorem 1 and contained in some field of $\mathscr{L}$.

Let us take any CM-field K in $\mathscr{K}$, so that $K \subset L$ for some L in $\mathscr{L}$. There exists a finite subset $\mathscr{S}$ of $\mathscr{K}$ containing K such that L is the composite of all fields in $\mathscr{S}$. Let $\tilde{L}$ denote the maximal unramified abelian l-extension over L and let Ω be the Galois closure of $\tilde{L}$ over k. For any CM-field K' in $\mathscr{S}$, there exists a tower of j-fields $k = k'_0 \subset k'_1 \subset \ldots \subset k'_n = K'$ with each $k'_\nu/k'_{\nu-1}$, $\nu \in \{1, \ldots, n\}$, a cyclic extension of degree dividing l. Since $\sigma^l \in \mathrm{Gal}(\Omega/k'_\nu)$ for every $\sigma \in \mathrm{Gal}(\Omega/k'_{\nu-1})$ and every $\nu \in \{1, \ldots, n\}$, each $\tau \in \mathrm{Gal}(\Omega/k)$ satisfies

$$\tau^{l^n} \in \mathrm{Gal}(\Omega/K').$$

Hence, for all $\tau \in \mathrm{Gal}(\Omega/k)$,

$$\tau^{l^n} \in \bigcap_{K' \in \mathscr{S}} \mathrm{Gal}(\Omega/K') = \mathrm{Gal}(\Omega/L)$$

and, by class field theory, the property $\exp A_L \leqslant l^r$ implies that

$$\tau^{l^{n+r}} \in \mathrm{Gal}(\Omega/\tilde{L}) \subset \mathrm{Gal}(\Omega/\tilde{K}),$$

where $\tilde{K}$ denotes the maximal unramified abelian l-extension over K. In particular,

$$\sigma^{l^{n+r}} \in \mathrm{Gal}(\Omega/\tilde{K}) \quad \text{for all } \sigma \in \mathrm{Gal}(\Omega/K).$$

This means, again by class field theory, that

$$\exp A_K \leqslant l^{n+r}. \tag{6}$$

Furthermore we obtain, from (ii) of Lemma 5,

$$h_K/s_K \leqslant h_L/s_L \leqslant m.$$

Theorem 1, together with this and (6), shows that $\mathscr{K}$ is a finite set. As every field in $\mathscr{L}$ is a composite field of CM-fields in $\mathscr{K}$, $\mathscr{L}$ is also a finite set and the corollary is proved.

Note that, in Corollary 1, an l-extension L over k has the property (ii) if $\exp \mathrm{Gal}(L/k) \leqslant l^n$ with L/k abelian. In particular, we have

COROLLARY 2. *Assume $l = 2$. Let r, m, and n be natural numbers. Then there exist only a finite number of CM-fields L which are abelian 2-extensions over $\mathbb{Q}$ such that*

$$\exp \mathrm{Gal}(L/\mathbb{Q}) \leqslant 2^n, \quad h_L/s_L \leqslant m, \quad \exp A_L \leqslant 2^r.$$

Proof of Theorem 2. Theorem 2 can be proved similarly as Theorem 1 by using Lemma 4 and the following Lemmas 6, 7, 8.

LEMMA 6. *Let $l > 2$ and let K/k be a cyclic extension with degree l of CM-fields. Then:*

(i) $\mathrm{rank}\, B_K^- \leqslant \mathrm{rank}\, A_k^- + \mathrm{rank}\, A_{K/k}^-$,

(ii) $|B_K^-| \leqslant |B_k^-|\,|A_{K/k}^-| \leqslant s_k^-\,|A_{K/k}^-|$,

(iii) $|A_{K/k}^-| \leqslant (s_k^-\, l^{t^-})^{l-1}$,

where t^- denotes the number of primes of K^+ ramified for K^+/k^+ and decomposed in K.

Proof. Noting that $\sigma j = j\sigma$ on K for all $\sigma \in \mathrm{Gal}(K/k)$, we can prove (i), (ii) by a discussion similar to that in the proof of Lemma 1. Next, as in the proof of Lemma 2, we can see easily that

$$|A_{K/k}^-| \leqslant |\{a \in B_K^-|\ a^{\sigma-1} = 1\}|^{l-1}.$$

On the other hand, by Lemma 1 of [8],

$$|\{a \in B_K^-|\ a^{\sigma-1} = 1\}| \leqslant s_k^-\, l^{t^-}.$$

Hence we obtain (iii) and the lemma is proved.

Just as Lemma 3 follows from Lemmas 1, 2, the next result follows from the above lemma.

LEMMA 7. *Assume $l > 2$ and let k be a CM-field. Let n be a natural number, and let $k = k_0 \subset k_1 \subset \ldots \subset k_n$ be a tower of CM-fields such that, for each $v \in \{1, \ldots, n\}$, $k_v = k_{v-1}$ or k_v/k_{v-1} is a cyclic extension of degree l. Then*

$$\mathrm{ord}_l h_{k_n}^- \leqslant (l^n \prod_{v=1}^{n} r_v^-)\,\mathrm{ord}_l h_k^- + \sum_{v=1}^{n} l^{n-v}(l-1)\,t_v^- \prod_{i=v}^{n} r_i^-,$$

where

$$r_v^- = \mathrm{ord}_l(\exp A_{k_v}^-), \qquad v \in \{1, \ldots, n\},$$

and each t_v^- denotes the number of primes of k_v^+ ramified for k_v^+/k_{v-1}^+ and decomposed in k_v.

LEMMA 8. *Let $l > 2$ and let K/k be an extension of CM-fields. Then the homomorphism $A_K^- \to A_k^-$ induced by the norm map for K/k is surjective; in particular, $\exp A_k^- \leqslant \exp A_K^-$. If, furthermore, K has an l-power degree over k, then h_k^-/s_k^- is a divisor of h_K^-/s_K^-.*

Proof. In general, let F be a CM-field, let $\tilde{F}$ denote the maximal unramified abelian l-extension over F, and put $A_F^+ = \{a \in A_F|\ a^j = a\}$. Let F' denote the intermediate field of $\tilde{F}/F$ such that $\mathrm{Gal}(\tilde{F}/F')$ is the image of A_F^+ under the Artin isomorphism φ: $A_F \to \mathrm{Gal}(\tilde{F}/F)$. Since l is odd, $A_F = A_F^- \times A_F^+$ so that φ induces an isomorphism $A_F^- \xrightarrow{\sim} \mathrm{Gal}(F'/F)$ and

$$j|F' \circ \sigma \circ j|F' = \sigma^{-1} \quad \text{for all } \sigma \in \mathrm{Gal}(F'/F).$$

Now, by class field theory, the norm map $A_K^- \to A_k^-$ defines a homomorphism

$$\lambda\colon\ \mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k), \qquad \text{with } \mathrm{Im}\,\lambda = \mathrm{Gal}(k'/k' \cap K).$$

Let σ be any element of $\mathrm{Gal}(k' \cap K/k)$ and let $j' = j|(k' \cap K)$. As K is a CM-field, we have $j'\sigma = \sigma j'$. However, by (9), $j'\sigma j' = \sigma^{-1}$. Therefore $\sigma = \sigma^{-1}$, whence $\sigma = 1$. This means that $k' \cap K = k$, namely, that λ is surjective. The first part of the lemma is thus proved. The proof of the last part is easy as that of Lemma 5.

2. For the proof of Theorem 3, we shall use the following lemmas.

LEMMA 9. *Let n be a natural number and K/k an abelian extension of algebraic number fields such that $k = k_0 \subset k_1 \subset \ldots \subset k_n = K$, with each k_v/k_{v-1}, $v \in \{1, \ldots, n\}$, a cyclic extension of degree l. Let t_v' denote, for each $v \in \{1, \ldots, n\}$, the number of finite primes of k_v ramified for k_v/k_{v-1}. Then*

$$\sum_{v=1}^{n} l^{n-v}(l-1)\,t_v' \leqslant [K:\boldsymbol{Q}]u$$

where u is the number of rational primes dividing $D_{K/k}$.

Proof. Note that each k_v/k, $v \in \{0, 1, \ldots, n\}$, is an abelian extension, and let $e_{\mathfrak{p},v}$ denote, for each prime $\mathfrak{p}$ of k, the ramification index of $\mathfrak{p}$ for k_v/k. It then follows that the number of primes of k_v above $\mathfrak{p}$ is at most equal to $[k_v:\boldsymbol{Q}]/e_{\mathfrak{p},v}$. Therefore, for each $v \in \{1, \ldots, n\}$,

$$(l-1)\,t_v' \leqslant \sum_{\mathfrak{p}} \left(\frac{e_{\mathfrak{p},v}}{e_{\mathfrak{p},v-1}} - 1\right)\frac{[k_v:\boldsymbol{Q}]}{e_{\mathfrak{p},v}} = \sum_{\mathfrak{p}} \left(\frac{1}{e_{\mathfrak{p},v-1}} - \frac{1}{e_{\mathfrak{p},v}}\right)$$

where $\mathfrak{p}$ ranges over the finite primes of k ramified in K; so that

$$\sum_{v=1}^{n} l^{n-v}(l-1)\,t_v' \leqslant l^n \sum_{\mathfrak{p}} \sum_{v=1}^{n} \left(\frac{1}{e_{\mathfrak{p},v-1}} - \frac{1}{e_{\mathfrak{p},v}}\right) \leqslant l^n \sum_{\mathfrak{p}} \left(1 - \frac{1}{e_{\mathfrak{p},n}}\right).$$

This implies the inequality of the lemma, because the number of finite primes of k ramified in K is at most equal to $[k:\boldsymbol{Q}]u$.

LEMMA 10. *For any abelian extension K/k of algebraic number fields,*

$$D_{K/k} \geqslant f_{K/k}^{[K:k]/2}.$$

Proof. Let $\mathfrak{D}$ be the relative discriminant of K/k and $\mathfrak{f}$ the conductor of K/k. It is sufficient to show that $\mathfrak{D}^2/\mathfrak{f}^{[K:k]}$ is $\mathfrak{p}$-integral for every finite prime $\mathfrak{p}$ of k. However this follows from Hasse's conductor discriminant formula (for the case $k = \boldsymbol{Q}$, see Lemma 1 of [11]; the general case can be shown quite similarly).

LEMMA 11. *Let k be a j-field, and let K range over a sequence of CM-fields such that $D_K \to \infty$ with K/k an abelian extension. Then*

$$\log h_K^- \sim \log \sqrt{D_K/D_{K^+}}.$$

Proof. By Lemma 10, the assumption implies that $[K:\boldsymbol{Q}]/\log D_K \to 0$ and consequently that the Brauer–Siegel theorem can be applied to our sequence of K. The rest of the proof is almost the same as the proof of Lemma 4 (for the case $k=\boldsymbol{Q}$, see, e.g., Theorem 1 of [7]).

Proof of Theorem 3. Let k' be any unramified abelian l-extension over k. Let $\mathscr{A}$ denote the set of CM-fields K which are abelian l-extensions over k', contain no proper unramified abelian extension over k, and satisfy

$$h_K/s_K \leqslant m, \quad \exp A_K \leqslant l.$$

Since there are only a finite number of unramified abelian extensions over k, it suffices to show that $\mathscr{A}$ is a finite set.

Take any field K in $\mathscr{A}$ different from k', so that $D_{K/k}>1$. Let $n=\operatorname{ord}_l[K:k']$. We can take a sequence $k'=k_0\subset k_1\subset \ldots \subset k_n=K$ of intermediate fields of K/k' such that each $k_\nu/k_{\nu-1}$, $\nu\in\{1,\ldots,n\}$, is a cyclic extension of degree l for which some prime of k_ν is ramified. By class field theory, the condition $\exp A_K\leqslant l$ then implies $\exp A_{k_\nu}\leqslant l$ for all $\nu\in\{1,\ldots,n\}$. Therefore we obtain, from Lemmas 3, 9, that

$$\operatorname{ord}_l h_K \leqslant l^n \operatorname{ord}_l h_{k'} + \sum_{\nu=1}^{n} l^{n-\nu}(l-1)t_\nu \leqslant l^n \operatorname{ord}_l h_{k'} + [K:\boldsymbol{Q}](u+1),$$

where each t_ν, $\nu\in\{1,\ldots,n\}$, denotes the number of primes of k_ν ramified for $k_\nu/k_{\nu-1}$ and u is the number of rational primes dividing $D_{K/k}$. Combining this with $\log h_K \leqslant \log m+\log s_K$, we have

$$\log h_K \leqslant \log m + l^n \log s_{k'} + (u+1)[K:\boldsymbol{Q}]\log l,$$

so that

$$\log h_K \leqslant (u+1)[K:\boldsymbol{Q}]\log(l\sqrt{ms_{k'}}). \tag{7}$$

On the other hand, it follows from Lemma 11 that

$$\log h_K \geqslant \log h_K^- \geqslant \tfrac{1}{8}\log D_K \geqslant \tfrac{1}{8}\log D_{K/k}$$

if D_K is sufficiently large. Then, by Lemma 10,

$$\log h_K \geqslant \frac{[K:k]}{16}\log f_{K/k} \geqslant \frac{[K:k]}{16}(u\log u - u).$$

This and (7) imply that

$$\log u \leqslant 32[k:\boldsymbol{Q}]\log(l\sqrt{ms_{k'}})+1,$$

$$\log f_{K/k} \leqslant 16[k:\boldsymbol{Q}](u+1)\log(l\sqrt{ms_{k'}})$$

if D_K is large enough. Consequently $f_{K/k}$ is bounded as K runs over all fields in $\mathscr{A}$, namely, $\mathscr{A}$ is a finite set.

From Theorem 3, we immediately obtain

Corollary 3. *There exist only a finite number of imaginary abelian fields, of 2-power degrees, with ideal class groups of exponents at most 2.*

Proof of Theorem 4. Let $\mathscr{A}^-$ denote the set of CM-fields K which are abelian l-extensions over k and satisfy

$$h_K^-/s_K^- \leqslant m, \quad \exp A_K^- \leqslant l.$$

Let us take any K in $\mathscr{A}^-$ with $D_{K/k}>1$, and let $n=\operatorname{ord}_l[K:k]$. By Lemma 8 and by $\exp A_K^-\leqslant l$, $\exp A_{k'}^-\leqslant l$ holds for every intermediate field k' of K/k. Therefore it follows from Lemmas 7, 9 that

$$\operatorname{ord}_l h_K^- \leqslant l^n \operatorname{ord}_l h_k^- + [K:\boldsymbol{Q}]u$$

where u is the number of rational primes dividing $D_{K/k}$. Since

$$\log h_K^- \leqslant \log s_K^- + \log m,$$

we then have

$$\log h_K^- \leqslant u[K:\boldsymbol{Q}]\log(l\sqrt{ms_k^-}).$$

On the other hand, Lemmas 10, 11 show that

$$\log h_K^- \geqslant \frac{[K:k]}{16}\log f_{K/k} \geqslant \frac{[K:k]}{16}(u\log u - u), \quad D_K \gg 1.$$

Thus, when D_K is sufficiently large,

$$\log u \leqslant 16[k:\boldsymbol{Q}]\log(l\sqrt{ms_k^-})+1,$$

$$\log f_{K/k} \leqslant 16[k:\boldsymbol{Q}]u\log(l\sqrt{ms_k^-}).$$

These imply that $\mathscr{A}^-$ is a finite set, and Theorem 4 is proved.

3. In this section, we let $l=2$ except for the final remark. For each algebraic number field M, let ζ_M denote the Dedekind zeta function of M and w_M the number of roots of unity in M. If M is an abelian field, then we let f_M denote the conductor of M: $f_M=f_{M/\boldsymbol{Q}}$. The Riemann zeta function is denoted by ζ, as usual: $\zeta(s)=\zeta_{\boldsymbol{Q}}(s)$, $s\in\boldsymbol{C}$. Let K be a CM-field and let $L(s)$, $s\in\boldsymbol{C}$, denote the Artin L-function for the non-trivial character of $\operatorname{Gal}(K/K^+)$ so that

$$\zeta_K(s)=\zeta_{K^+}(s)L(s), \quad s\in\boldsymbol{C}.$$

We denote by $\Gamma(s)$ the gamma function of $s\in\boldsymbol{C}$. By Lemma 5 of [9], the inequality

$$L(1) > c^{-1}\frac{1-\beta}{\varrho-1}D_{K^+}^{(1-\varrho)/2}\left(\frac{\pi^{\varrho/2}}{\Gamma(\varrho/2)\zeta(\varrho)}\right)^{[K^+:\boldsymbol{Q}]}$$

holds for every real number ϱ in the interval $[1+(4\log D_K)^{-1}, 2]$, where

$$c = 4\exp\left(\frac{23}{8}+\frac{1}{4\log 3}-\frac{\Gamma'(1/2)}{8\log 3\,\Gamma(1/2)}\right), \quad \beta = \max\left(\beta_0,\ 1-(4\log D_K)^{-1}\right),$$

β_0 being the maximal real number such that $L(\beta_0)=0$. Note that $\beta_0<1$ whence $\beta<1$. On the other hand, it is well known that

$$L(1) = \frac{2\pi^{[K^+:\mathbf{Q}]} R_K h_K D_{K^+}^{1/2}}{w_K R_{K^+} h_{K^+} D_K^{1/2}} \leqslant \frac{(2\pi)^{[K^+:\mathbf{Q}]} h_K^-}{(D_{K^+} D_{K/K^+})^{1/2}}.$$

Therefore

$$(8) \qquad h_K^- \geqslant L(1)(D_{K^+} D_{K/K^+})^{1/2}(2\pi)^{-[K^+:\mathbf{Q}]} > \frac{1-\beta}{(\varrho-1)c} D_{K^+}^{\frac{1}{2}-\varrho/2} D_{K/K^+}^{1/2}\left(2\pi^{1-\varrho/2}\,\Gamma\left(\frac{\varrho}{2}\right)\zeta(\varrho)\right)^{-[K^+:\mathbf{Q}]},$$

for any $\varrho\in[1-(4\log D_K)^{-1}, 2]$.

Now, we assume K to be an imaginary cyclic field of degree a 2-power $\geqslant 4$ such that $\exp C_K \leqslant 2$. It then follows from Lemmas 3, 8 of [9] that $L(s)$ has no zero for $s\in[1-(4\log D_K)^{-1}, 1)$, whence $\beta = 1-(4\log D_K)^{-1}$. Assume further $D_K \geqslant e^c$. Putting $\varrho = 1+(4c)^{-1}$ in (8), we have

$$\log h_K^- > (\log D_K)^{-1} D_K^{1/4-1/(16c)} b^{-[K^+:\mathbf{Q}]},$$

where

$$b = 2\pi^{1/2-1/(8c)}\,\Gamma\left(\frac{1}{2}+\frac{1}{8c}\right)\zeta\left(1+\frac{1}{4c}\right).$$

Let ε be any positive number less than $1/4-1/(16c)$, D the positive number $>e$ such that $\varepsilon = \log\log D/\log D$, and u the number of rational primes ramified in K. In the case $D_K \geqslant D$, it follows from the above and Lemma 10 that

$$h_K^- > D_K^{1/4-1/(16c)-\varepsilon} b^{-[K^+:\mathbf{Q}]} \geqslant (f_K^{1/4-1/(16c)-\varepsilon} b^{-1})^{[K^+:\mathbf{Q}]}.$$

Since $\log f_K \geqslant u\log u - u$, this together with (7) shows that if $D_K \geqslant \max(e^c, D)$, then

$$(9) \qquad (u+1)\log 4 > \left(\frac{1}{4}-\frac{1}{16c}-\varepsilon\right)\log f_K - \log b \geqslant \left(\frac{1}{4}-\frac{1}{16c}-\varepsilon\right)(u\log u - u) - \log b.$$

Take the maximal natural number u^* satisfying

$$(u^*+1)\log 4 \geqslant \left(\frac{1}{4}-\frac{1}{16c}-\varepsilon\right)(u^*\log u^* - u^*) - \log b.$$

We put

$$0 = (4^{u^*+1} b)^{1/(1/4-1/(16c)-\varepsilon)},$$

so that, by (9),

$$f_K < 0 \quad \text{if } D_K \geqslant \max(e^c, D).$$

Finally let $\varepsilon = \log(8536)/8536$, i.e., $D = e^{8536}$. Then simple calculations show that

$$u^* = 758, \quad 0 < e^{4269}.$$

Since $c<112$, we have proved the following result.

PROPOSITION 1. *For any imaginary cyclic field K of degree a 2-power $\geqslant 4$,*

$$f_K < e^{4269} \quad \text{if } \exp C_K \leqslant 2.$$

Assume next that K is an imaginary quadratic field, and let $L(s)$, $s\in\mathbf{C}$, denote (as before) the Dirichlet L-function for the quadratic Dirichlet character with conductor $-D_K$. Weinberger [12] has shown that if $L(s)$ has no zero for $s\in[1-(4\log D_K)^{-1}, 1)$, then $\exp C_K \leqslant 2$ implies $D_K \leqslant 5460$.

Using a similar method as in [12], we can also show

PROPOSITION 2. *Let K be an imaginary biquadratic field and assume that the Artin L-function $L(s)$, $s\in\mathbf{C}$, for the non-trivial character of $\mathrm{Gal}(K/K^+)$ has no zero in the interval $[1-(4\log D_K)^{-1}, 1)$. Then*

$$f_K \leqslant e^{71.91} \quad \text{if } \exp C_K \leqslant 2.$$

Proof. Let k and k' be the imaginary quadratic subfields of K; $kk' = K$. We suppose $\exp C_K \leqslant 2$, so that

$$\exp C_k \mid 4, \quad \exp C_{k'} \mid 4.$$

Replacing k by k' if necessary, we may further suppose $\exp C_{k'} \mid \exp C_k$.

Now, in the case $\exp C_k \leqslant 2$, [12] shows that $f_k \leqslant 5460$, $f_{k'} \leqslant 5460$, and hence $f_K \leqslant f_k f_{k'} < e^{71.91}$.

Let us next consider the case $\exp C_k = 4$. It is then obvious that $f_k > 8$, i.e., $\log f_k > 2$. It also follows that $h_k \leqslant 4^{v-1}$ where v denotes the number of rational primes ramified in k. However, putting $\varepsilon = 1/\log f_k$ in Lemma 9 of [10], we obtain, from our hypothesis,

$$\frac{2\pi h_k}{w_k\sqrt{f_k}} = L(1) > \frac{0.655}{e\log f_k}.$$

Therefore

$$4^{v-1} \geqslant h_k > \frac{0.655\sqrt{f_k}}{\pi e\log f_k}.$$

Here, if $v \geqslant 23$, then $f_k/2$ is at least equal to the product of 83^{v-22} and all prime numbers $\leqslant 79$, whence the right-hand side of the above exceeds 4^{v-1}. This contradiction implies $v \leqslant 22$, so that we have $f_k \leqslant e^{71.91}$. On the other hand,

since $\exp C_K \leqslant 2$, K is unramified over k. In particular, $f_K = f_k$ and therefore the proposition is completely proved.

Remark. By means of Theorem 2 of [9], we can obtain for each $v \in \{1, 2, 3, 4\}$, an upper bound of D_K for the CM-fields K which have the properties of Theorem v but are not contained in any biquadratic field. However the estimates are complicated; so we omit the details here.

References

[1] D. W. Boyd and H. Kisilevsky, *On the exponent of the ideal class group of complex quadratic fields*, Proc. Amer. Math. Soc. 31 (1971), 433–436.

[2] R. Brauer, *On the zeta-functions of algebraic number fields*, Amer. J. Math. 69 (1947), 243–250.

[3] S. Chowla, *An extension of Heilbronn's class-number theorem*, Quart. J. Math. Oxford 2, 5 (1934), 304–307.

[4] A. G. Earnest and O. H. Körner, *On ideal class group of 2-power exponent*, Proc. Amer. Math. Soc. 86 (1982), 196–198.

[5] A. G. Earnest, *Exponents of class groups of imaginary abelian number fields*, Bull. Austral. Math. Soc. 35 (1987), 231–245.

[6] M. Hamamura, *On absolute class fields of certain algebraic number fields*, Nat. Sci. Rep. Ochanomizu Univ. 32 (1981), 23–34.

[7] K. Horie, *On the index of the Stickelberger ideal and the cyclotomic regulator*, J. Number Theory 20 (1985), 238–253.

[8] Y. Kida, *l-extensions of CM-fields and cyclotomic invariants*, ibid. 12 (1980), 519–528.

[9] H. M. Stark, *Some effective cases of Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.

[10] T. Tatuzawa, *On a theorem of Siegel*, Japanese J. Math. 21 (1951), 163–178.

[11] K. Uchida, *Class numbers of imaginary abelian number fields II*, Tôhoku Math. J. 23 (1972), 487–499.

[12] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. 22 (1973), 117–124.

DEPARTMENT OF MATHEMATICS
YAMAGUCHI UNIVERSITY
Yoshida, Yamaguchi 753
Japan

DEPARTMENT OF MATHEMATICS
KYUSHU UNIVERSITY
Hakozaki, Fukuoka 812
Japan

Received on 27.9.1988 (1872)

ACTA ARITHMETICA
LV (1990)

Darstellung total positiver ganzer algebraischer Zahlen als Summe N-freier Zahlen

von

ROTRAUT LAUN (Marburg)*

1. Einleitung. Evelyn und Linfoot untersuchten in einer Reihe von Arbeiten [2]–[6] das asymptotische Verhalten der Anzahl $A_m(v)$ der Darstellungen einer natürlichen Zahl v als Summe von m N-freien Zahlen für $v \to \infty$. Eine natürliche Zahl heißt N-frei, falls sie nicht durch die N-te Potenz einer Primzahl teilbar ist. Barham und Estermann [1] verbesserten die von ihnen erzielte Asymptotik für $m \geqslant 4$. Mit Hilfe der Hardy–Littlewoodschen Methode erhielten sie

$$A_m(v) = \frac{v^{m-1}}{(m-1)!\,\zeta^m(N)} \cdot S(v) + O(v^{m-2+1/N} \log^{\alpha} v) \quad (m \geqslant 4) \tag{1.1}$$

mit

$$S(v) := \prod_{p^N \nmid v} \left(1 + \frac{(-1)^{m+1}}{(p^N-1)^m}\right) \prod_{p^N \mid v} \left(1 + \frac{(-1)^m}{(p^N-1)^{m-1}}\right)$$

und

$$\alpha := \begin{cases} 3, & \text{falls } N = 2,\ m = 4, \\ 2, & \text{sonst.} \end{cases} \tag{1.2}$$

In [7] verallgemeinerten Evelyn und Linfoot die Fragestellung, indem sie für $v \to \infty$ das asymptotische Verhalten der Anzahl $A_m(v; b, a)$ der Darstellungen einer natürlichen Zahl v als Summe von m N-freien Zahlen untersuchten, welche in einer festen Restklasse $b \pmod a$ liegen. Man setzt voraus, daß (a, b) N-frei ist und daß $v \equiv mb \pmod a$ ist, da andernfalls $A_m(v; b, a) = 0$ ist. Mirsky [12] verbesserte ihre Asymptotik für $m \geqslant 3$.

Setzt man $a = \prod_{j=1}^{\infty} p_j^{\beta_j}$, so erhielt er mit elementaren Methoden

$$A_m(v; b, a) = S(v; b, a)\left(\left(\frac{v}{a}\right)^{m-1} \frac{1}{(m-1)!} + O(v^{m-2+\frac{m}{(m-1)N+1}+\varepsilon})\right) \quad (m \geqslant 3) \tag{1.3}$$

* Diese Arbeit ist eine gekürzte Fassung meiner Dissertation. Herrn Prof. Dr. W. Schaal, der diese Arbeit anregte, bin ich für seine vielfältige Unterstützung und Betreuung aufrichtig dankbar. Auch Herrn Prof. Dr. J. Hinz danke ich für viele anregende Gespräche.