ACTA ARITHMETICA
XXV (1974)

"Almost every" algebraic number-field has a large class-number

by

V. G. SPRINDŽUK (Minsk)

In 1956 the following theorem was proved by Ankeny, Brauer and Chowla [1]:

Given any positive integer $n \geqslant 2$, let s and t be any two non-negative integers such that $s+2t = n$. For every $\tau > 0$ there exist infinitely many algebraic number-fields $\boldsymbol{K}$ which have exactly s real and $2t$ imaginary conjugate fields and are such that

(1) $$h_{\boldsymbol{K}} > |D_{\boldsymbol{K}}|^{1/2-\tau}$$

holds for the class-number $h_{\boldsymbol{K}}$ and the discriminant $D_{\boldsymbol{K}}$ of $\boldsymbol{K}$.

In this note we shall prove that to satisfy this inequality for a field $\boldsymbol{K}$ is, in some sense, a standard phenomenon. This phenomenon becomes obvious if one estimates the number of the fields $\boldsymbol{K}$ with the regulators $R_{\boldsymbol{K}}$ not exceeding a large bound and compares this value with the number of such fields which satisfy the additional condition

(2) $$h_{\boldsymbol{K}} \leqslant |D_{\boldsymbol{K}}|^{\delta}$$

with any fixed δ in the interval $0 \leqslant \delta < \frac{1}{2}$.

THEOREM. *Given integers $n \geqslant 3$ and t, $0 \leqslant t \leqslant n/2$, reals $Z > 0$ and δ, $0 \leqslant \delta < \frac{1}{2}$, let $N_n(Z)$ be the number of distinct (non-isomorphic) algebraic number fields $\boldsymbol{K}$ of degree n with regulators $R_{\boldsymbol{K}} \leqslant Z$, $N_n^{(t)}(Z)$ be the number of such fields which have exactly $2t$ imaginary conjugate fields, and $N_{n,\delta}(Z)$ be the number of such fields which satisfy* (2). *Then*

(3) $$N_n(Z) < 2^{n(n-1)}3^{n-1}\exp\{2(n-1)^2c_1+(n-1)c_1^{-n+1}Z\},$$

where $c_1 = \dfrac{2}{n-2}\log\left(1+\dfrac{1}{7.5n^2\log 3n}\right)$,

(4) $$N_n^{(t)}(Z) > \exp\{c_2 Z^{1/(n-t-1)}\},$$

where $c_2 > 0$ depends only on n,

(5) $$N_{n,\delta}(Z) < c_3 Z^{(n+1)/(1-2\delta')},$$

where δ' is any number with $\delta < \delta' < \frac{1}{2}$, and c_3 depends only on n and δ'.

As $N_n(Z) \geqslant N_n^{(t)}(Z)$ for any t, we see that from (4) and (5) follows

$$N_{n,\delta}(Z) < c_4\big(\log N_n(Z)\big)^{(n-[n/2]-1)(n+1)/(1-2\delta')}.$$

For rather detailed treatment of the case $n = 2$ see [5].

Let $\boldsymbol{K}$ be any algebraic number field of degree $n \geqslant 3$ which has s real and $2t$ imaginary conjugate fields, $k = s+t-1 \geqslant 2$, $(\varepsilon_1, \ldots, \varepsilon_k)$ be a system of fundamental units of $\boldsymbol{K}$. To prove (3) it is enough to show that $\boldsymbol{K}$ has a unit ε of degree n and of the height $h(\varepsilon)$ with

$$h(\varepsilon) \leqslant 2^n \exp\{2(n-1)c_1 + c_1^{-n+1}R\}, \tag{6}$$

where $R = R_{\boldsymbol{K}}$ and c_1 is defined in the Theorem. The existence of such a unit can be easily proved by the usual application of Minkowski's theorem to the system of linear inequalities

$$\big|x_1 \log|\varepsilon_1^{\sigma}| + \ldots + x_k \log|\varepsilon_k^{\sigma}|\big| \leqslant \lambda_{\sigma}, \tag{7}$$

where σ runs through all real and $t-1$ $(t \geqslant 1)$ non-conjugate imaginary isomorphisms $\boldsymbol{K}$, all λ_σ are equal to c_1, except one which is $2^{-t+1}R$. If $(x_1, \ldots, x_k)$ is a non-trivial integral solution of (7), $\varepsilon = \varepsilon_1^{x_1} \ldots \varepsilon_k^{x_k}$ satisfies (6) and is of the degree n. The latter follows from a recent theorem by Blanksby and Montgomery [2].

To prove (4) we appeal to the fields $\boldsymbol{K}$ considered by Ankeny, Brauer and Chowla [1]. In the case of $t = 0$ these fields are generated by the polynomials $f_m(x) = (x-a_1)\ldots(x-a_{n-1})(x-m)+1$, where $a_1, \ldots, a_{n-1}$ are any fixed distinct integers, $m > 0$ is an integer. Let $M > 1$ be an integer, $M/2 \leqslant m \leqslant M$, $\alpha_1, \ldots, \alpha_n$ be the roots of $f_m(x)$ arranged in such a way that

$$|\alpha_j - a_j| = \min_{1\leqslant i\leqslant n} |\alpha_i - a_j| \quad (1 \leqslant j \leqslant n-1), \qquad |\alpha_n - m| = \min_{1\leqslant i\leqslant n} |\alpha_i - m|. \tag{8}$$

It may be easily seen that

$$|\alpha_j - a_j| < c_5 M^{-1} \quad (1 \leqslant j \leqslant n-1), \qquad |\alpha_n - m| < c_5 M^{-n+1}, \tag{9}$$

where c_5 depends only on n and $a_1, \ldots, a_{n-1}$.

Let $\boldsymbol{K}_i = \boldsymbol{Q}(\alpha_i)$ $(i = 1, 2, \ldots, n)$, $\boldsymbol{Q}$ being the field of rationals. If the polynomials $f_m(x)$ and $f_{m'}(x)$ define the same field $\boldsymbol{K}$, $\alpha_1', \ldots, \alpha_n'$ are the roots of $f_{m'}(x)$ arranged like (8) and $\boldsymbol{K}_i' = \boldsymbol{Q}(\alpha_i')$ $(i = 1, 2, \ldots, n)$, the system $(\boldsymbol{K}_1', \ldots, \boldsymbol{K}_n')$ is a permutation of the system $(\boldsymbol{K}_1, \ldots, \boldsymbol{K}_n)$. Therefore not more than $n!-1$ distinct $m' \neq m$ can exist with $M/2 \leqslant m' \leqslant M$ and $f_{m'}(x)$ defining $\boldsymbol{K}$. Indeed, if $n!$ of such m' do exist, one of the two possibilities takes place: either $\boldsymbol{K}_i' = \boldsymbol{K}_i$ $(i = 1, 2, \ldots, n)$ with some m', or $\boldsymbol{K}_i' = \boldsymbol{K}_i''$ $(i = 1, 2, \ldots, n)$ with a pair of distinct m', m''. In the first case we observe that

$$\prod_{i=1}^{n} (\alpha_i - \alpha_i') \neq 0$$

is a rational integer, and then (9) gives

$$1 \leqslant \prod_{i=1}^{n} |\alpha_i - \alpha_i'| < c_6 (M^{-1})^{n-1} M,$$

which is impossible for large M. In the second case the same is true for the number

$$\prod_{i=1}^{n} (\alpha_i' - \alpha_i'').$$

Thus we see that polynomials $f_m(x)$ define not less than $(2n!)^{-1}M$ non-isomorphic fields, when m runs through the interval $M/2 \leqslant m \leqslant M$ and M is large.

It is shown in the work of [1] that the regulator of $\boldsymbol{K}$ does not exceed $c_7(\log m)^{n-1}$. Taking $M = \exp(c_8 Z)^{1/(n-1)}$, we get (4) with $t = 0$. The case of $t > 0$ takes only trivial changes.

And, finally, to prove (5) we use the theorem by Siegel–Brauer ([3], [4]), which gives $h_{\boldsymbol{K}} R_{\boldsymbol{K}} > c_9 |D_{\boldsymbol{K}}|^{1/2-\tau}$ with any $\tau > 0$. We remark that every field $\boldsymbol{K}$ of degree n contains an integer of the same degree and of the height not greater than $2^n(|D_{\boldsymbol{K}}|+1)^{1/2}$. Hence from $R_{\boldsymbol{K}} \leqslant Z$ and (2) follows $|D_{\boldsymbol{K}}| < c_{10} Z^{2/(1-2\delta-2\tau)}$, and the number of such fields is estimated by the right side of (5). This completes the proof.

References

[1] N. C. Ankeny, R. Brauer, and S. Chowla, *A note on the class numbers of algebraic number fields*, Amer. J. Math. 78 (1956), pp. 51–61.

[2] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), pp. 355–369.

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

[4] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), pp. 83–86.

[5] V. G. Sprindžuk, *The distribution of the fundamental units of real quadratic fields*, Acta Arith., this volume, pp. 405–409.

Received on 30. 5. 1973 (407)