festgestellt, wie im Lemma 5 (siehe auch [1]). Wir handeln weiter wie beim Beweis Lemmas 7. Und nämlich haben wir

$$a_u = T+(M-u)n-\sigma_u = T+(M-u)n-\sigma_{u-1}+k_{M-u} < k_{M-u}.$$

Wenn die ganze Zahl r, $1 \leqslant r \leqslant M-u-1$, existiert, daß

$$a_{u+r-1} < k_{M-u} \leqslant a_{u+r}, \tag{33}$$

so nehmen wir an, daß $k'_{M-u-r} = a_{u+r}-k_{M-u}+k_{M-u-r}$. Und weiter arbeiten wir mit dem System (28) und den Gebieten

$$T_P = \prod_{v=1}^{M-u} \tau_P(t_v-\delta_v) \prod_{v=M-u+1}^{M} \mathscr{S}_P(t_v-\delta_v),$$

wo $\delta_v = k_v$, $v = 1, 2, \ldots, M-u-r-1$, $\delta_{M-u-r} = k'_{M-u-r}$, $\delta_{M-u} = k_{M-u}$, $\delta_v = 0$ für übrige $v \in V$.

Wenn (33) nicht gilt, so sind dann

$$k_v \geqslant k_{M-u} > a_{M-1} = T+n > \delta_v = (T+n)(M-u)^{-1}, \quad v = 1, 2, \ldots, M-u,$$

$$\delta_v = 0, \quad v = M-u+1, \ldots, M.$$

Das Theorem ist ganz bewiesen.

Zum Schluß des Artikels bemerken wir, daß man das Theorem auf den Ring S-adele beliebiger endlicher Körpererweiterung der rationalen Zahlen Q verallgemeinern kann.

Literaturverzeichnis

[1] V. I. Bernik, *Metric theorem on the simultaneous approximations of zero by values of polynomials with integral coefficients*, Izv. Akad. SSSR 44 (1980), pp. 24–45 (Russian) or Math. USSR Izv. 16 (1981), pp. 21–40.

[2] V. G. Sprindžuk, *Mahler's problem in metric number theory* (Russian), Minsk 1967 or Amer. Math. Soc. Transl. of math. monographs 25 (1969).

[3] — *Achievements and problems in Diophantine approximation theory*, Uspekhi Mat. Nauk 35 (4) (1980), pp. 3–68 (Russian) or Russ. Math. Surv. 35 (4) (1980), pp. 1–80.

Eingegangen am 15.10.1984 (1463)

ACTA ARITHMETICA
XLVI (1986)

Ideal class groups of cubic cyclic fields

by

Shin Nakano (Tokyo)

In this note, we apply the basic lemmas in [2] to the proof of a result on the ideal class groups of cubic cyclic fields, which gives a better estimation than Uchida [3]. We shall prove the following

Theorem. *For any given natural number n, there exist infinitely many cubic cyclic fields whose ideal class group contains a subgroup isomorphic to $(\mathbf{Z}/n\mathbf{Z})^2$.*

We fix, throughout this note, a natural number n (>1). Let $\mathscr{L}$ be the set of all prime factors of n and put $n_0 = \prod_{l \in \mathscr{L}} l$. For a number field k, denote by $k^\times$ and W_k its multiplicative group and the group of the roots of unity contained in k respectively. For a natural number ν and a prime p satisfying $p \equiv 1 \pmod{\nu}$, denote by $\left(\frac{-}{p}\right)_\nu$ the νth power residue symbol modulo p.

The basic lemmas in [2] are the following

Lemma 1. *Let K be a number field of finite degree, r be the free-rank of the unit group of K and suppose there exist $\alpha_1, \ldots, \alpha_s \in K^\times$ $(s > r)$ satisfying the following conditions:*

(i) $(\alpha_i) = \mathfrak{a}_i^n$ *for some ideal* $\mathfrak{a}_i$ *of* K $(1 \leqslant i \leqslant s)$,

(ii) $\alpha_1, \ldots, \alpha_s$ *are independent in* $K^\times/W_K K^{\times l}$ *for any* $l \in \mathscr{L}$.

Then the ideal class group of K contains a subgroup isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{s-r}$.

Lemma 2. *Let $f(X)$ be a monic irreducible polynomial in $\mathbf{Z}[X]$, θ be a root of $f(X)$, $K = \mathbf{Q}(\theta)$ and suppose there exist rational integers A_i, C_i $(1 \leqslant i \leqslant s)$ such that*

(i) $f(A_i) = \pm C_i^n$ $(1 \leqslant i \leqslant s)$,

(ii) $(f'(A_i), C_i) = 1$ $(1 \leqslant i \leqslant s)$.

Then the s elements $\alpha_i = \theta - A_i$ $(1 \leqslant i \leqslant s)$ satisfy the condition (i) *of Lemma* 1. *Moreover, if there exist $t \in \mathbf{Z}$ and primes $p_1, \ldots, p_s \equiv 1 \pmod{M}$, where $M = \prod_{l \in \mathscr{L}} l^{1+\operatorname{ord}_l(|W_K|)}$, so that*

(iii) $f(t)\equiv 0,\ f'(t)\not\equiv 0 \pmod{p_i}\quad (1\leqslant i\leqslant s)$,

(iv) $\left(\dfrac{t-A_j}{p_i}\right)_l = 1,\ \left(\dfrac{t-A_i}{p_i}\right)_l \neq 1\quad (1\leqslant j<i\leqslant s,\ l\in\mathscr{L})$,

then $\alpha_1,\ldots,\alpha_s$ *satisfy* (ii) *of Lemma* 1.

Remark. If K is not totally imaginary, we have $W_K=\{\pm 1\}$, consequently $M=n_0$ or $2n_0$ according to n is odd or not.

Proof of the theorem. Put $I=\{0,-1,1,-2\}$ and $n_1=n$ or $2n$, according to $n\not\equiv 2$ or $n\equiv 2 \pmod 4$. We start with the following

Lemma 3. *For each* $i\in I$ *there exist infinitely many primes* p_i *congruent to* 1 *modulo* n_1 *such that*

(1) $$\left(\frac{t-i}{p_i}\right)_l\neq 1,\quad \left(\frac{t-j}{p_i}\right)_l=1\quad (j\neq i,\ j\in I,\ l\in\mathscr{L}),$$

(2) $$\left(\frac{\dfrac{(2t+1)(t-1)(t+2)}{t(t+1)}}{p_i}\right)_n=1,$$

and

(3) $$p_i\nmid 2(t^2+t+1)$$

for some rational integer t.

Proof. Let F be the cyclotomic field of the n_1-th root of unity. We take distinct five prime ideals $\mathfrak{q}$, $\mathfrak{q}_i$ $(i\in I)$ of F prime to 6. Let $A\in\mathfrak{q}-\mathfrak{q}^2$ and $A_i\in\mathfrak{q}_i-\mathfrak{q}_i^2$ $(i\in I)$ and choose a solution $T\in F^\times$ of system

$$2T\equiv -1+A \pmod{\mathfrak{q}^2},$$
$$T\equiv i+A_i \pmod{\mathfrak{q}_i^2}\quad (i\in I)$$

of congruences. As each of $\mathfrak{q}$, $\mathfrak{q}_i$ is prime to 6, we see that for $i,\ j\in I$

$$\operatorname{ord}_{\mathfrak{q}}(2T+1)=1,\qquad \operatorname{ord}_{\mathfrak{q}}(T-j)=0,$$
$$\operatorname{ord}_{\mathfrak{q}_i}(2T+1)=0,\qquad \operatorname{ord}_{\mathfrak{q}_i}(T-j)=\delta_{ij}.$$

So the five numbers $2T+1$, $T-i$ $(i\in I)$ are independent in $F^\times/F^{\times l}$ for any $l\in\mathscr{L}$. If we put

$$E=F\left(\left(\frac{(2T+1)(T-1)(T+2)}{T(T+1)}\right)^{1/n}\right),\qquad E_i=F\left((T-i)^{1/n_0}\right)\quad (i\in I),$$

then E_i is a cyclic extension of F of degree n_0 and $E_i\cap(E\prod_{j\neq i}E_j)=F$ for each $i\in I$. Thus, by the density theorem, we can choose infinitely many prime ideals $\mathfrak{p}_i$ of F of degree 1 which do not divide $2(T^2+T+1)$ and are inert for E_i while decomposed completely in $E\prod_{j\neq i}E_j$. Put $p_i=\mathfrak{p}_i\cap \boldsymbol{Z}$ and take a rational integer t congruent to T modulo $\mathfrak{p}_i$ for all $i\in I$. Hence $p_i\equiv 1 \pmod{n_1}$ and the pair (p_i,t) satisfies (1)–(3). This completes the proof. ■

We now prove the theorem. By the above lemma, we can take distinct four primes $p_i>3$ $(i\in I)$ and a rational integer t satisfying (1)–(3). Thus, from (2), there exist a rational integer a such that

(4) $$a^n\equiv\frac{(2t+1)(t-1)(t+2)}{t(t+1)} \pmod{p_i}\quad \text{for all } i\in I.$$

Moreover a can be chosen so that

(5) $$(a,6)=1.$$

Now we consider the polynomial

$$f(X)=X^3-cX^2-(c+3)X-1,\quad \text{where}\quad c=(a^n-3)/2.$$

It is easy to see that $f(X)$ is irreducible and the discriminant is equal to $(c^2+3c+9)^2$. Thus the field defined by any root of $f(X)$ is cubic cyclic. By Lemmas 1 and 2, the existence of a field as in our theorem follows from (1) and the following properties:

(i) $f(0)=-1,\ f(-1)=1,\ f(1)=f(-2)=-a^n$.

(ii) $(f'(1),a)=(f'(-2),a)=1$.

(iii) $f(t)\equiv 0,\ f'(t)\not\equiv 0 \pmod{p_i}$ for all $i\in I$.

It is clear that (i) and (ii) are satisfied, by (5) and the definition of $f(X)$. Further we can prove the equivalence between the two congruences $f(t)\equiv 0 \pmod{p_i}$ and (4). If $t \pmod{p_i}$ is a multiple root of $f(X) \pmod{p_i}$, the discriminant $(c^2+3c+9)^2$ is divisible by p_i. The relation $a^n=2c+3$ yields

$$a^{2n}-4(c^2+3c+9)=-27,$$

thus

$$a^{2n}+27\equiv 0 \pmod{p_i}.$$

So, by (4), we have

$$\{(2t+1)(t-1)(t+2)\}^2+27\{t(t+1)\}^2\equiv 0 \pmod{p_i}.$$

This congruence contradicts (3), since the left-hand side is equal to $4(t^2+t+1)^3$. Hence we have $p_i\nmid f'(t)$.

Finally, the infiniteness follows immediately from the existence as in [1]. This completes the proof of the theorem. ■

References

[1] S. Nakano, *Class numbers of pure cubic fields*, Proc. Japan Acad. 59A (1983), pp. 263–265.

[2] – *On ideal class groups of algebraic number fields*, J. Reine Angew. Math. 358 (1985), pp. 61–75.

[3] K. Uchida, *Class numbers of cubic cyclic fields*, J. Math. Soc. Japan 26 (1974), pp. 447–453.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
GAKUSHUIN UNIVERSITY
MEJIRO, TOSHIMA-KU, TOKYO 171
JAPAN

Received on 27.12.1984
and in revised form on 6.2.1985 (1483)

ACTA ARITHMETICA
XLVI (1986)

Correction to the paper "On a kind of uniform distribution of values of multiplicative functions in residue classes", Acta Arithmetica 31 (1976), pp. 291–294

by

W. Narkiewicz (Wrocław)

1. Professor R. Warlimont kindly pointed out to me that the definition of Dirichlet-WUD (mod N) given in Section 2 of the above paper does not ensure that the Dirichlet series occurring in it have the asserted abscissas of absolute convergence. This can be repaired, without affecting the results and later applications, by restricting the definition of Dirichlet-WUD (mod N) to those multiplicative functions f which satisfy the following condition:

If $m = m(f, N)$ is the smallest integer (if it exists) such that the series $\sum p^{-1}$ (with p running over all primes for which $(f(p^m), N) = 1$) diverges, and $m \geqslant 2$, then for all $j \leqslant m-1$ the series $\sum p^{-(1/m+\varepsilon)}$ (with p running over all primes for which $(f(p^j), N) = 1$) converges for all positive ε.

2. The same error found its way also to [1], pp. 62–63, where the same amendment should be made, and the argument following the definition of Dirichlet-WUD should be disregarded.

The applications of this notion given in [1] are unaffected, since for functions considered there the additional condition stated above is anyway true, however one has to amend the definition of decent functions given on pp. 71–72 by adding to it that in the case when $a(r, j) = 0$ holds for $r = 1, 2, \ldots, n$ and all j prime to N, then the series $\sum p^{-s}$ (where p runs over all primes with $f(p^r) \equiv j \pmod{N}$) should represent a function regular in $\operatorname{Re} s > 1/(n+1)$.

Reference

[1] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Mathematics, 1087, Springer 1984.

Received on 3.4.1985 (1505)