Annales Mathematicae Silesianae 16 (2003)

Prace Naukowe Uniwersytetu Śląskiego nr 2142, Katowice

# OPEN PROBLEMS ON THE RELATION BETWEEN ADDITIVE AND MULTIPLICATIVE STRUCTURE

JURAJ KOSTRA

**Abstract.** This paper presents open problems on the relation between additive and multiplicative structures of cyclotomic fields.

## Introduction

In the first part we consider units in cyclotomic fields. The first three problems are from papers [8], [9], [10] of Morris Newman. Let $K$ be an algebraic number field of degree $n$ over the rationals $\mathbb{Q}$. It is known that there are only finitely many units $\alpha$ of $K$ such that $\alpha + 1$ is also a unit. It was shown by Newman [7] that there cannot be more than $n$ consecutive units in $K$ and that this bound is the best possible in the sense that for every $n > 3$ there is a field $K$ of degree $n$ over $\mathbb{Q}$ containing $n$ consecutive units.

Now let $K = \mathbb{Q}(\zeta_p)$, where $\zeta_p$ is the $p$-th root of unity, $p > 3$ is a prime. In any such field there exist four consecutive units

$$\zeta_p + \zeta_p^{-1} - 1, \zeta_p + \zeta_p^{-1}, \zeta_p + \zeta_p^{-1} + 1, \zeta_p + \zeta_p^{-1} + 2.$$

Newman [9] proved the following theorem.

THEOREM A. *Let $p > 3$ be a prime. Let $R$ denote the maximum number of consecutive residues modulo $p$ and $N$ the maximum number of consecutive*

*Received: 5.11.2002. Revised: 8.01.2003.*

AMS (1991) subject classification: Primary 11R27, 11R33, 11C20.

*Key words and phrases:* Unit, normal basis, circulant matrix, cyclotomic field.

The research was supported by Grant GA ČR 201/01/0471.

*nonresidues modulo p. Then the maximum number $k_p$ of consecutive units of $\mathbb{Q}(\zeta_p)$ satisfies*

$$k_p \leqslant \max\{4, R, N\}.$$

This result implies that, for the primes $p > 3$ under 100, $k_p$ is exactly 4 for $p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 47, 73$ (and possibly for the other primes as well). Another consequence is that $k_p < 2p^{\frac{1}{2}}$.
This suggests the first problem of Newman.

PROBLEM 1. Let $k_p$ be the maximum number of consecutive units of $p$-th cyclotomic field. Is $k_p = 4$ for all primes $p > 3$?

Actually we do not know if $k_p$ is bounded by a constant, that is, if $k_p$ is independent of $p$.

In 1974 Newman asked the following question on sums of two units in $\mathbb{Q}(\zeta_p)$.

PROBLEM 2. Which rational integers are sums of two units in $p$-th cyclotomic field $\mathbb{Q}(\zeta_p)$?

It was shown independently in [10] and [6] that any number $m$ with $\gcd(m,p) \neq 1$ is not the sum of two units in $\mathbb{Q}(\zeta_p)$. In both papers the number 6 is considered. Newman [10] wrote:

"We have not managed to express 6 as the difference of two units. We do not know whether this is intrinsic to the problem or not. The integer 6 is a notorious exception in problems of this type."

In the paper [6] it is proved that for $K$ a normal tamely ramified cubic algebraic number field, the number 6 is not the sum of two units in $K$. So we can ask the following question.

PROBLEM 3. Does there exist a prime $p$ such that 6 is the sum of two units in the $p$-th cyclotomic field $\mathbb{Q}(\zeta_p)$?

In the second part we deal with integral normal bases generated by a unit, that is, with integral bases consisting of all conjugates of a unit. In 1991 in [4] it was given the following necessary condition for the existence of such a basis for tamely ramified cyclic algebraic number fields of prime degree $l$ over the rationals $\mathbb{Q}$.

THEOREM B. *Let $K$ be a cyclic extension of the rationals $\mathbb{Q}$ of a prime degree $l$. Let $m = p_1 p_2 \cdots p_s$ be the square free conductor of the field $K$. Let a unit $\varepsilon$ generate integral normal basis of $K/\mathbb{Q}$. Then*

$$l^l \equiv 1 \pmod{p_i}$$

*for all* $i = 1, 2, \ldots, s$, *or*

$$l^l \equiv -1 \pmod{p_i}$$

*for all* $i = 1, 2, \ldots, s$.

For a fixed $l$, this condition implies that there exist at most a finite number of such fields. In the papers [3],[4] all fields of degrees $2, 3, 5$ and $7$ with integral normal basis were determined. In each case there are two such fields specified in the following list.

1. $K = \mathbb{Q}(\zeta_3)$ and $K \subset \mathbb{Q}(\zeta_5)$ for $l = 2$,
2. $K \subset \mathbb{Q}(\zeta_7)$ and $K \subset \mathbb{Q}(\zeta_{13})$ for $l = 3$,
3. $K = \mathbb{Q}(\zeta_{11})$ and $K \subset \mathbb{Q}(\zeta_{71})$ for $l = 5$,
4. $K = \mathbb{Q}(\zeta_{29})$ and $K \subset \mathbb{Q}(\zeta_{113})$ for $l = 7$.

In all of the above cases $Tr_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ is a unit. We note that $Tr_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ generates an integral normal basis.

PROBLEM 4. Let $K$ be a tamely ramified cyclic algebraic number field of degree $l$ over $\mathbb{Q}$ with conductor $m$. Is it possible that for $K/\mathbb{Q}$ there exists an integral normal basis generated by a unit and $Tr_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ is not a unit?

The conductors of all fields in the list above are prime numbers. So we ask the following question.

PROBLEM 5. Does there exist a tamely ramified cyclic algebraic number field of degree $l$ over $\mathbb{Q}$ with composite conductor $m$ and with integral normal basis generated by a unit over $\mathbb{Q}$?

Another observation is that in all cases considered in the list above, for given $l$, there are exactly two cyclic fields $K$ of degree $l$ over $\mathbb{Q}$ with integral normal basis generated by a unit.

PROBLEM 6. Does there exist a common upper bound for the number $t$ of fields of given degree with an integral normal basis generated by a unit? Is $t = 2$?

In the third part we discuss special circulant matrices which transform a normal basis of an order of a cyclic algebraic number field to normal bases of its suborders. In 1985 in [5] the following theorem was proved.

THEOREM C. *Let $K$ be a cyclic algebraic number field of degree $n$ over the rationals $\mathbb{Q}$. Let*

$$\mathbf{A} = circ_n(a_1, a_2, \ldots, a_n)$$

*be a regular circulant matrix over* $\mathbb{Z}$. *For* $i = 1, 2, \ldots, n$ *let* $A_i$ *be the algebraic complement of* $a_i$ *in the matrix* $\mathbb{A}$. *Assume that the following two conditions are satisfied:*

$$\sum_{i=1}^{n} a_i = \pm 1$$

*and*

$$a_i \equiv a_j \quad (mod\ \frac{|\mathbb{A}|}{(A_1, A_2, \ldots, A_n)}).$$

*Then the matrix* $\mathbb{A}$ *transforms a normal basis of any order* $B$ *of the field* $K$ *to a normal basis of an order* $C$ *of the field* $K$.

EXAMPLE. For $n = 2$ and any integers $a_1, a_2$ satisfying $a_1 + a_2 = \pm 1$ the matrix $circ_2(a_1, a_2)$ satisfies also the additional condition in the Theorem and so transforms a normal basis of any order of a quadratic field to a normal basis of an order of the field.

The circulant matrices satisfying the conditions in Theorem C have been characterized in [1], [2] as follows.

THEOREM D. *Let* $G$ *be a multiplicative semigroup of circulant matrices of degree* $n$ *satisfying the assumptions of the Theorem* C. *Let* $U$ *be the multiplicative group of unimodular circulant matrices of degree* $n$. *Let* $H$ *be the semigroup of circulant matrices of the type* $circ_n(a, b, \ldots, b)$ *such that*

$$a + (n-1)b = \pm 1.$$

*Then* $G = H \cdot U$.

By the above example if a circulant matrix over rational integers transforms a normal basis of an order of a quadratic field $K$ to a normal basis of its suborder then it transforms any normal basis of any order to a normal basis of a suborder. The conjecture is that the same will hold at least for $n = 3$. We have the following open problem.

PROBLEM 7. Let $K/\mathbb{Q}$ be a cyclic extension of degree $n$. Characterize all circulant matrices of degree $n > 2$ over the rational integers $\mathbb{Z}$ which transform any normal basis of any order of $K$ to a normal basis of its suborder in $K$.

CONJECTURE. *All such matrices are characterized by theorems* C *and* D.

We do not know of any example of a circulant matrix which transforms a normal basis of an order to a normal basis of its suborder and at the same time it does not do the same for another normal basis.

PROBLEM 8. Let $K/\mathbb{Q}$ be a cyclic extension of degree $n$. Does there exist a circulant matrix $\mathbf{A}$ over $\mathbb{Z}$ with the property that there are orders $A, B, C$ in $K$ with normal bases

$$\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle, \quad \langle\beta_1, \beta_2, \ldots, \beta_n\rangle, \quad \langle\gamma_1, \gamma_2, \ldots, \gamma_n\rangle,$$

respectively, and

$$\langle\gamma_1, \gamma_2, \ldots, \gamma_n\rangle = \langle\beta_1, \beta_2, \ldots, \beta_n\rangle\mathbf{A}$$

while

$$\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle\mathbf{A}$$

is not a normal basis of any order in $K$?

## REFERENCES


[1] Z. Divišová, J. Kostra, M. Pomp, *On transformation matrix connected to normal bases in cubic field*, Acta Acad. Paed. Agrriensis, Sec. Mathematicae 27 (2002), to appear.

[2] Z. Divišová, J. Kostra, M. Pomp, *On transformation matrix connected to normal bases in orders*, Journ. of Algebra, Number Theory and Applications, to appear.

[3] A. Dvořák, D. Jedelský, J. Kostra, *The fields of degree seven over rationals with a normal basis generated by a unit*, Math. Slovaca, 49, 2 (1999), 143–153.

[4] S. Jakubec, J. Kostra, K. Nemoga, *On the existence of an integral normal basis generated by a unit in prime extensions of rational numbers*, Math. of Comput., 56, 194 (1991), 809–815.

[5] J. Kostra, *Orders with a normal basis*, Czech. Math. Journ., 35(110) (1985), 391–404.

[6] J. Kostra, *On sums of two units*, Abh. Math. Sem. Univ. Hamburg, 64 (1994), 11–14.

[7] M. Newman, *Units in arithmetic progression in an algebraic number field*, Proc. of the Amer. Math. Soc., 43, 2 (1974), 266–268.

[8] M. Newman, *Diophantine equations in cyclotomic fields*, J. reine angew. Math, 265 (1974), 84–89.

[9] M. Newman, *Consecutive units*, Proc. of the Amer. Math. Soc. 108, 2 (1990), 303–306.

[10] M. Newman, *Units differing by rationals in a cyclotomic field*, Linear and Multilinear Algebra 34, 1 (1993) 55–57.



DEPARTMENT OF APPLIED MATHEMATICS
FACULTY OF SCIENCE
UNIVERSITY OF ZILINA
J. M. HURBANA 15
01026 ZILINA
SLOVAKIA

e-mail: kostra@fpv.utc.cz