REPRESENTING ALGEBRAIC INTEGERS AS LINEAR COMBINATIONS OF UNITS

D. DOMBEK[1], L. HAJDU[2,3] AND A. PETHŐ[3,4]

ABSTRACT. In this paper we consider representations of algebraic integers of a number field as linear combinations of units with coefficients coming from a fixed small set, and as sums of elements having small norms in absolute value. These theorems can be viewed as results concerning a generalization of the so-called unit sum number problem, as well. Beside these, extending previous related results we give an upper bound for the length of arithmetic progressions of t-term sums of algebraic integers having small norms in absolute value.

1. INTRODUCTION

Let K be an algebraic number field with ring of integers O_K. The problem of representing elements of O_K as sums of units has a long history and a very broad literature. Instead of trying to make an account of the various results and research directions, we only refer to the excellent survey paper of Barroero, Frei and Tichy [2] and the references there. Now we mention only those results which are most important from our viewpoint.

After several partial results due to Ashrafi and Vámos [1] and others, Jarden and Narkiewicz [10] proved that for any number field K and

positive integer t, one can find an algebraic integer $\alpha \in K$ which cannot be represented as a sum of at most t units of K[1].

Observe that if K admits an integral basis consisting of units then clearly every integer of K can be represented as a sum of units. For results in this direction we refer to a paper of Pethő and Ziegler [17]. Showing that (up to certain precisely described exceptions) every number field admits a basis consisting of units with small conjugates, we prove that allowing a small, completely explicit set of (rational) coefficients every integer of K can be expressed as a linear combination of units. We would like to emphasize the interesting property that the set of coefficients allowed depends only on the degree and the regulator of K and that the latter dependence is made explicit.

Further, it is also well-known (see e.g. [2] again) that there are infinitely many number fields whose rings of integers are not generated additively by their units. In other words, in these fields one can find algebraic integers α which cannot be represented as a sum of (finitely many) units at all.

In this paper we extend this investigations to the case where one would like to represent the algebraic integers of K not as a sum of units, but as a sum of algebraic integers of small norm, i.e. using algebraic integers with $|N(\beta)| \leq m$ for some positive integer m. (For precise notions and notation see the next section.) Obviously, taking $m = 1$ we just get back the original question. First we prove that the above mentioned result of Jarden and Narkiewicz extends to this case: for any algebraic number field K and positive integers m and t one can find an algebraic integer $\alpha \in K$ which cannot be obtained as a sum of at most t integers of K of norm $\leq m$ in absolute value. Then we show that in contrast with the original case, one can give a bound m_0 depending only on the discriminant and degree of K, such that if $m \geq m_0$ then already every integer of K can be represented as a sum of integers of K with norm at most m in absolute value. Note that as it is well-known, any number field K contains only finitely many pairwise non-associated algebraic integers of given norm. Hence sums of elements of small norm can be considered as linear combinations of units with coefficients coming from a fixed finite set.

Finally, we also provide a result concerning arithmetic progressions of t-term sums of algebraic integers of small norm in a number field K. This result generalizes previous theorems of Newman (concerning

---

[1]Here and in the sequel under a unit of K we mean a unit in O_K.

arithmetic progressions of units; see [14] and [15]) and of Bérczes, Hajdu and Pethő (concerning arithmetic progressions of elements of fixed norm; cf. [3]).

The organization of the paper is as follows. In the next section we give our main results, together with the necessary notation, and also with some further details. The third section contains the proofs of Proposition 2.1 and of Theorem 2.1, which we consider the principal results of this note. The last section is dealing with the proofs of the other statements.

2. Main results

From this point on, let K be an algebraic number field of degree k, with discriminant $D(K)$ and regulator $R(K)$. Write O_K for the ring of integers of K, $N(\beta)$ for the field norm of any $\beta \in K$ and U_K for the group of units in O_K.

The unit sum number problem can be considered as a question about linear combinations of units with rational integers. We know that the resulting set is sometimes a proper subset with infinite complementer of O_K. However if we allow that the coefficients have small denominators, then the situation becomes completely different.

At this point let us recall that the field K is called a CM-field, if it is a totally imaginary quadratic extension of a totally real number field.

Theorem 2.1. *Suppose that either K is not a CM-field, or K is a CM-field containing a root of unity different from ± 1. Then there exists a positive integer $\ell = e^{c_1(k)R(K)}$ where $c_1(k)$ is a constant depending only on the degree of K, such that any $\alpha \in O_K$ can be obtained as a linear combination of units of K with coefficients $\{1, 1/2, 1/3, \ldots, 1/\ell\}$.*

Remark 2.1. *The condition that K is not a CM-field or K contains a non-real root of unity is necessary. Indeed, otherwise all units of K are contained in some proper subfield of K, and the statement trivially fails.*

Denote by σ_i $(i = 1, \ldots, k)$ the embeddings of K into $\mathbb{C}$ and for $\alpha \in K$ put $\overline{|\alpha|} = \max_{1 \leq i \leq k}(|\sigma_i(\alpha)|)$. Although the next statement does not fit completely in the main line of this paper, we present it among the main results because it is vital for the proof of Theorem 2.1. Moreover, we think that it is interesting also on its own.

Proposition 2.1. *Suppose that either K is not a CM-field, or K is a CM-field containing a root of unity different from ± 1. Then there exists a constant $c_2 = c_2(k)$ depending only on the degree of K, such that K has a basis consisting of units ε_i with $\overline{|\varepsilon_i|} \leq e^{c_2(k)R(K)}$, $(i = 1, \ldots, k)$.*

Now we present our results, where the summands belong to a set of integers of small norm in K. As a motivation, we mention that Newman proved that the length of arithmetic progressions consisting of units of K is at most k (see [14] and [15]). This result has been generalized by Bérczes, Hajdu and Pethő in [3] to arithmetic progressions in the set

$$\mathcal{N}_m := \{\beta \in O_K \ : \ N(\beta) = m\},$$

where $m > 0$. Now we present a result concerning a further generalization of this problem. For $m > 0$ put

$$\mathcal{N}_m^* := \{\beta \in O_K \ : \ |N(\beta)| \leq m\},$$

and write

$$t \times \mathcal{N}_m^* := \{\beta_1 + \cdots + \beta_t \ : \ \beta_i \in \mathcal{N}_m^* \ (i = 1, \ldots, t)\}$$

where t is a positive integer.

Our first theorem gives a bound for the lengths of arithmetic progressions in the sets $t \times \mathcal{N}_m^*$.

Theorem 2.2. *The length of any non-constant arithmetic progression in $t \times \mathcal{N}_m^*$ is at most $c_3(m, t, k, D(K))$, where $c_3(m, t, k, D(K))$ is an explicitly computable constant depending only on m, t, and on the degree k and discriminant $D(K)$ of K.*

Now we present results concerning the above generalization of the unit sum number problem. Slightly modifying the notation of Goldsmith, Pabst and Scott [6] we define the unit sum number $u(O_K)$ as the minimal integer t such that every element of O_K is a sum of at most t units from U_K, if such an integer exists. If it does not, we put $u(O_K) = \omega$ if every element of O_K is a sum of units, and $u(O_K) = \infty$ otherwise. We use the convention $t < \omega < \infty$ for all integers t.

As we have mentioned already, Jarden and Narkiewicz [10] proved that $u(O_K) \geq \omega$ for any number field K. Our next result yields an extension of this nice theorem. To formulate it, we define the m-norm sum number $u_m(O_K)$ as an analogue to $u(O_K)$ with the exception that instead of sums of units we consider sums of elements from $\mathcal{N}_m^*$. Clearly, $u(O_K) = u_1(O_K)$ holds.

Theorem 2.3. *For every number field K and $m > 0$ we have $u_m(O_K) \geq \omega$, i.e. for every $m, t \in \mathbb{N}$ there exists an $\alpha \in O_K$ which cannot be obtained as the sum of at most t terms from $\mathcal{N}_m^*$.*

As it is well-known (see e.g. [2] and the references given there), for infinitely many number fields K we have $u(O_K) = \infty$. In contrast to this result, our next theorem shows that $u_m(O_K) = \omega$ is always valid

if m is "large enough" with respect to the discriminant and the degree of K. More precisely, we have the following theorem.

Theorem 2.4. *For every number field K there exists a positive integer $m_0 = m_0(D(K), k)$ depending only on the discriminant and the degree of K, such that for any $m \geq m_0$ we have $u_m(O_K) = \omega$, i.e. any $\alpha \in O_K$ can be obtained as the sum of elements from $\mathcal{N}_m^*$.*

Observe that sums of elements of $\mathcal{N}_m^*$ can be also viewed as linear combinations of units with coefficients coming from a fixed finite set (see also the proofs of Theorems 2.3 and 2.4).

3. Proofs of Proposition 2.1 and of Theorem 2.1

In the proof of Proposition 2.1 we shall need the following lemmas. The first one is due to Bugeaud and Győry [4].

Lemma 3.1. *Let K be as earlier, with unit rank s. Then K has a fundamental system of units $\varepsilon_1, \ldots, \varepsilon_s$ such that*
(i) $\displaystyle\max_{1 \leq i \leq s} \overline{|\varepsilon_i|} \leq e^{c_4(k)R(K)}$,
(ii) $\displaystyle\max_{1 \leq i \leq s, \ 1 \leq j \leq k} |\log |\sigma_j(\varepsilon_i)|| \leq c_5(k)R(K)$,
with some explicitly computable constants $c_4(k)$ and $c_5(k)$, depending only on k.

Proof. Part (i) is a simple and straightforward consequence of Lemma 1 (ii) of [4], while part (ii) follows from (i) in the standard way, using $|\sigma_1(\varepsilon_i)| \ldots |\sigma_k(\varepsilon_i)| = 1$ for $i = 1, \ldots, s$. □

The next lemma is an immediate consequence of the main theorem of Costa and Friedman [5].

Lemma 3.2. *For every positive integer k there exists a positive constant $c_6 = c_6(k)$ depending only on k, such that for every number field K of degree k and for every subfield L of K we have*

$$R(L) \leq c_6(k)R(K),$$

where $R(L)$ and $R(K)$ denote the regulators of L and K, respectively.

Proof. If $|D(K)| > 3k^k$, then the statement directly follows from the main theorem in [5].

Now assume that $|D(K)| \leq 3k^k$. Since there are only finitely many number fields of discriminant bounded by a fixed constant in absolute value (see e.g. Hasse [9], p. 619), the constant $c_6(k)$ can be effectively calculated as the maximum of the ratios $R(L)/R(K)$, where K runs through the finite list of fields of degree k with $|D(K)| \leq 3k^k$ and L runs through all proper subfields of K. □

Proof of Proposition 2.1. We prove the statement by induction on k. The statement is empty for $k = 1$, while it is obvious for $k = 2$. Let ε_0 be a root of unity and $\varepsilon_1, \ldots, \varepsilon_s$ be a fundamental system of units for K having property (i) in Lemma 3.1. If K has no proper subfield, then we have $K = \mathbb{Q}(\varepsilon_1)$, and our claim follows. So we may assume that K has proper subfields. Let L' be a proper subfield of K of maximal degree.

At first, assume that either L' is not a CM-field or it contains a root of unity different from ± 1. Note that $2\ell' \leq k$, where ℓ' is the degree of L'. We show that $\varepsilon_i \notin L'$ holds for some index $i \in \{0, 1, \ldots, s\}$. Suppose that $\varepsilon_i \in L'$ for all $i = 1, \ldots, s$. Writing s' for the unit rank of L', then $s = s'$ should be valid. Observe that $s' \leq \ell' - 1$ with equality if and only if L' is totally real, and $s \geq k/2 - 1$ with equality if and only if K is totally complex. Hence for $s = s'$ we must have $k = 2\ell'$, and it also follows that K is totally complex and L' is totally real. But K is then a CM-field, which by our assumptions implies that $\varepsilon_0 \notin L'$.

By induction, L' has a basis consisting of units $\{\eta_1, \ldots, \eta_{\ell'}\}$, with $\overline{|\eta_l|} \leq e^{c_4(\ell')R(L')}$. Take an index $i \in \{0, 1, \ldots, s\}$ with $\varepsilon_i \notin L'$. Since L' is a subfield of K of maximal degree, we have $K = L'(\varepsilon_i)$. Hence there is a basis of K of the form

$$\left\{ \eta_l \varepsilon_i^j \ : \ l \in \{1, \ldots, \ell'\}, \ j \in \{0, \ldots, k/\ell' - 1\} \right\}.$$

Since $\overline{|\varepsilon_i|} \leq e^{c_4(k)R(K)}$, and according to Lemma 3.2 we have $R(L') \leq c_6(k)R(K)$ for some positive constant $c_6(k)$, we have

$$\overline{\left|\eta_l \varepsilon_i^j\right|} \leq e^{c_7(k)R(K)} \quad (l = 1, \ldots \ell', \ j = 1, \ldots k/\ell' - 1),$$

with some constant $c_7(k)$ depending only on k, and the statement follows in this case.

Now assume that the proper subfield $L' \subset K$ of maximal degree is a CM-field with no non-real roots of unity. Let L'' be its maximal real subfield. Then the units of L'' and the units of L' coincide. If there is any non-CM proper subfield L of K containing L'', then this L is of maximal degree, and we can find an appropriate ε_i ($i = 0, 1, \ldots, s$) such that $K = L(\varepsilon_i)$ and the statement follows, just as in the previous case.

Otherwise, by $4 \deg(L'') \leq \deg(K)$ there exists an $\varepsilon_i \notin L''$ ($i = 1, \ldots, s$). Further, since now L'' is contained only in CM-subfields of K, we have $K = L''(\varepsilon_i)$. Thus we can use the same induction argument as before, since L'' is not a CM-field, and the theorem follows. $\square$

Proof of Theorem 2.1. It is clearly sufficient to show that the index of the additive group generated by the units of K inside O_K can be bounded in terms of $R(K)$ and k.

By Proposition 2.1 there exists a constant $c_2(k)$ such that we can find a basis $\varepsilon_1, \ldots, \varepsilon_k$ of K consisting of units with the property $\overline{|\varepsilon_i|} \leq e^{c_2(k)R(k)}$ $(i = 1, \ldots, k)$. Further, we also have

$$D(\varepsilon_1, \ldots, \varepsilon_k) = I^2 D(K)$$

(see e.g. [16], p. 58), where I is the index of the additive group $\mathbb{Z}[\varepsilon_1, \ldots, \varepsilon_k]$ inside the additive group of O_K, and

$$D(\varepsilon_1, \ldots, \varepsilon_k) = \begin{vmatrix} \sigma_1(\varepsilon_1) & \ldots & \sigma_1(\varepsilon_k) \\ \vdots & \ddots & \vdots \\ \sigma_k(\varepsilon_1) & \ldots & \sigma_k(\varepsilon_k) \end{vmatrix}^2.$$

Hence, as $D(K)$ is a rational integer, by part (i) of Lemma 3.1 we obtain

$$I \leq \sqrt{|D(\varepsilon_1, \ldots, \varepsilon_k)|} \leq k! \left(\max_{1 \leq i \leq k} \overline{|\varepsilon_i|} \right)^k \leq e^{c_8(k)R(K)}$$

with some constant $c_8(k)$ depending only on k. Since $\mathbb{Z}[\varepsilon_1, \ldots, \varepsilon_k]$ is a subgroup of the additive group generated by the units of K, the theorem follows. $\square$

Remark 3.1. *Note that by a result of Sprindžuk [18] there are only finitely many number fields of given degree having regulator smaller than a prescribed bound. From this one could prove an implicit variant of Theorem 2.1, without specifying the dependence upon $R(K)$.*

4. Proofs of the other theorems

In the proof of Theorem 2.2, beside Lemmas 3.1 and 3.2 we shall use the following lemmas. The first one is an immediate consequence of a result of Murty and Van Order [13].

Lemma 4.1. *Let K be an algebraic number field of degree k and $m > 1$ be an integer. Then there are at most $c_9(k, D(K))m$ pairwise non-associated elements $\alpha \in O_K$ with $|N(\alpha)| \leq m$, where $c_9(k, D(K))$ is an explicitly computable constant depending only on k and $D(K)$.*

Proof. In view of part (ii) of Lemma 3.1 and a result of Landau [11] implying that $|D(K)| \geq c_6(k)R(K)$ where $c_6(k)$ is a constant depending only on k, the statement is a simple corollary of Theorem 5 of [13]. $\square$

To formulate our second lemma we need some further notation. If K is an algebraic number field, write K^* for the multiplicative group of the nonzero elements of K and let Γ be a multiplicative subgroup of K^* of finite rank $r > 0$. Let t be a positive integer and let $\mathcal{A} \subset K^t$ be a finite nonempty set with n elements. Put

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^t a_i x_i \ : \ (a_1, \ldots, a_t) \in \mathcal{A}, (x_1, \ldots, x_t) \in \Gamma^t \right\}.$$

The next result is Theorem 1.1 of Hajdu and Luca in [8]. For the first (non-explicit) result of this type see also [7]. Further, note that Jarden and Narkiewicz [10] proved a similar (but also not explicit) result, concerning the special case where the coefficients a_i can take the values $-1, 0, 1$ only.

Lemma 4.2. *The length of any non-constant arithmetic progression in $H_t(\Gamma, \mathcal{A})$ is bounded by a constant $L = L(n, t, r)$ with*

$$L(n, t, r) < \exp \left((8(n + t + r))^{8(n+t+r)^4} \right).$$

Proof of Theorem 2.2. Let s be the unit rank of K. Note that $s \leq k-1$. It is well-known by the famous result of Dirichlet that the group of units in O_K is of the form

$$U_K = \{ \eta_0^{j_0} \eta_1^{j_1} \cdots \eta_s^{j_s} \ : \ j_i \in \mathbb{Z} \ (i = 0, 1, \ldots, s) \},$$

where $\eta_1, \ldots, \eta_s$ is a system of fundamental units of K and η_0 is a root of unity in K. Denote by $M(m)$ a full set of pairwise non-associated algebraic integers in K with norm bounded by m in absolute value. Then Lemma 4.1 implies $|M(m)| \leq c_9(k, D(K))m$. Putting all this together, we see that

$$t \times \mathcal{N}_m^* = H_t(\Gamma, \mathcal{A}),$$

where $\Gamma = U_K$ is of rank $r = s + 1 \leq k$ and

(1) $\mathcal{A} = \{ (\gamma_1, \ldots, \gamma_t) \ : \ \gamma_i \in M(m) \ (i = 1, \ldots, t) \}$

has cardinality $n \leq (c_9(k, D(K))m)^t$. Hence by Lemma 4.2 the theorem follows. $\square$

Proof of Theorem 2.3. We follow a similar path as in the proof of Theorem 2.2. Since $\mathcal{N}_m^* = H_1(\Gamma, \mathcal{A})$ with $\Gamma = U_K$ and $\mathcal{A}$ as in (1) above, we can easily see that the set of numbers being the sum of at most t elements of $\mathcal{N}_m^*$ coincides with the set $H_t(U_K, M(m))$.

Now suppose that for fixed m, t we can write any $\alpha \in O_K$ as the sum of at most t elements from $\mathcal{N}_m^*$. Then because O_K is a ring, we can construct an arithmetic progression in $H_t(\Gamma, \mathcal{A})$ of arbitrary length and this contradicts Lemma 4.2. $\square$

Remark 4.1. *Note that based upon the main result of* [10] *a similar, alternative proof of Theorem 2.3 could also be given.*

Proof of Theorem 2.4. Any ring of integers O_K possesses an integral basis $\alpha_1, \ldots, \alpha_k$, i.e. $O_K = \alpha_1 \mathbb{Z} + \ldots + \alpha_k \mathbb{Z}$. By a result Mahler [12] (Corollary on p. 436), there exists an integral basis satisfying $|N(\alpha_i)| \leq (k^{k/2}\sqrt{D(K)})^k$ $(i = 1, \ldots, k)$. If we choose $m_0 = m_0(D(K), k) = (k^{k/2}\sqrt{D(K)})^k$, then for any $m \geq m_0$, the integral basis of O_K belongs to the set $\mathcal{N}_m^*$ and the statement follows. $\square$

5. Acknowledgement

The authors are grateful to the referee for his helpful comments.

References

[1] N. Ashrafi, P. Vámos, *On the unit sum number of some rings*, Q. J. Math. **56** (2005), 1–12.

[2] F. Barroero, C. Frei, R. F. Tichy, *Additive unit representations in rings over global fields - a survey*, Publ. Math. Debrecen **79** (2011), 291–307.

[3] A. Bérczes, L. Hajdu, A. Pethő, *Arithmetic progressions in the solution sets of norm form equations*, Rocky Mountain Math. J. **40** (2010), 383–396.

[4] Y. Bugeaud, K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. **74** (1996), 67–80.

[5] A. Costa, E. Friedman, *Ratios of regulators in totally real extensions of number fields*, J. Number Theory **37** (1991), 288–297.

[6] B. Goldsmith, S. Pabst, A. Scott, *Unit sum numbers of rings and modules*, Q. J. Math. **49** (1998), 331–344.

[7] L. Hajdu, *Arithmetic progressions in linear combinations of S-units*, Period. Math. Hungar. **54** (2007), 175–181.

[8] L. Hajdu, F. Luca, *On the length of arithmetic progressions in linear combinations of S-units*, Archiv der Math. **94** (2010), 357–363.

[9] H. Hasse, *Number theory*. Translated from the third (1969) German edition. Edited and with a preface by Horst Günter Zimmer. Classics in Mathematics. Springer-Verlag, Berlin (2002).

[10] M. Jarden, W. Narkiewicz, *On sums of units*, Monatsh. Math. **150** (2007), 327–332.

[11] E. Landau, *Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen*, Nachr. Akad. Wiss. Göttingen (1918), 79–97.

[12] K. Mahler, *Inequalities for ideal bases in algebraic number fields*, J. Austral. Math. Soc. **4** (1964), 425–448.

[13] M. R. Murty, J. Van Order, *Counting integral ideals in a number field*, Expo. Math. **25** (2007), 53–66.

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

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

[16] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers.* Polska Akademia Nauk., Instytut Matematyczny, Monografie matematyczne **57** (1974).
[17] A. Pethő, V. Ziegler, *On biquadratic fields that admit unit power integral basis,* Acta Math. Hungar. **133** (2011), 221-241.
[18] V. G. Sprindžuk, *"Almost every" algebraic number-field has a large class-number,* Acta Arith. **25** (1973/74), 411-413.

D. Dombek, Department of Mathematics FNSPE, Czech Technical University in Prague, Trojanova 13, 120 00 Praha 2, Czech Republic
E-mail address: dombedan@fjfi.cvut.cz

L. Hajdu, University of Debrecen, Institute of Mathematics, H-4010 Debrecen, P.O. Box 12., Hungary
E-mail address: hajdul@science.unideb.hu

A. Pethő, University of Debrecen, Department of Computer Science, H-4010 Debrecen, P.O. Box 12., Hungary
E-mail address: Petho.Attila@inf.unideb.hu