ADDITIVE UNIT REPRESENTATIONS IN GLOBAL FIELDS – A SURVEY

FABRIZIO BARROERO, CHRISTOPHER FREI, AND ROBERT F. TICHY

Dedicated to Kálmán Győry, Attila Pethő, János Pintz and András Sarközy.

Abstract. We give an overview on recent results concerning additive unit representations. Furthermore the solutions of some open questions are included. The central problem is whether and how certain rings are (additively) generated by their units. This has been investigated for several types of rings related to global fields, most importantly rings of algebraic integers. We also state some open problems and conjectures which we consider to be important in this field.

1. The unit sum number

In 1954, Zelinsky [37] proved that every endomorphism of a vector space V over a division ring D is a sum of two automorphisms, except if $D = \mathbb{Z}/2\mathbb{Z}$ and $\dim V = 1$. This was motivated by investigations of Dieudonné on Galois theory of simple and semisimple rings [6] and was probably the first result about the additive unit structure of a ring.

Using the terminology of Vámos [34], we say that an element r of a ring R (with unity 1) is k*-good* if r is a sum of exactly k units of R. If every element of R has this property then we call R k*-good*. By Zelinsky's result, the endomorphism ring of a vector space with more than two elements is 2-good. Clearly, if R is k-good then it is also l-good for every integer $l > k$. Indeed, we can write any element of R as

$$r = (r - (l-k)\cdot 1) + (l-k)\cdot 1,$$

and expressing $r - (l-k)\cdot 1$ as a sum of k units gives a representation of r as a sum of l units.

Goldsmith, Pabst and Scott [17] defined the *unit sum number* $u(R)$ of a ring R to be the minimal integer k such that R is k-good, if such an integer exists. If R is not k-good for any k then we put $u(R) := \omega$ if every element of R is a sum of units, and $u(R) := \infty$ if not. We use the convention $k < \omega < \infty$ for all integers k.

Clearly, $u(R) \leq \omega$ if and only if R is generated by its units. Here are some easy examples from [17]:

- $u(\mathbb{Z}) = \omega$,
- $u(K[X]) = \infty$, for any field K,
- $u(K) = 2$, for any field K with more than 2 elements, and

2010 *Mathematics Subject Classification.* 00-02, 11R27, 16U60.

Key words and phrases. global fields, sums of units, unit sum number, additive unit representations.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.
C. Frei is supported by the Austrian Science Foundation (FWF) project S9611-N23.

- $u(\mathbb{Z}/2\mathbb{Z}) = \omega$.

Goldsmith, Pabst and Scott [17] were mainly interested in endomorphism rings of modules. For example, they proved independently from Zelinsky that the endomorphism ring of a vector space with more than two elements has unit sum number 2, though they mentioned that this result can hardly be new.

Henriksen [21] proved that the ring $M_n(R)$ of $n \times n$-matrices ($n \geq 2$) over any ring R is 3-good.

Herwig and Ziegler [22] proved that for every integer $n \geq 2$ there exists a factorial domain R such that every element of R is a sum of at most n units, but there is an element of R that is no sum of $n-1$ units.

The introductory section of [34] contains a historical overview of the subject with some references. We also mention the survey article [31] by Srivastava.

In the following sections, we are going to focus on rings of ($S-$)integers in global fields.

2. Rings of integers

The central result regarding rings of integers in number fields, or more generally, rings of S-integers in global fields ($S \neq \emptyset$ finite), is that they are not k-good for any k, thus their unit sum number is ω or ∞. This was first proved by Ashrafi and Vámos [2] for rings of integers of quadratic and complex cubic number fields, and of cyclotomic number fields generated by a primitive 2^n-th root of unity. They conjectured, however, that it holds true for the rings of integers of all algebraic number fields (finite extensions of $\mathbb{Q}$). The proof of an even stronger version of this was given by Jarden and Narkiewicz [24] for a much more general class of rings:

Theorem 1. [24, Theorem 1] *If R is a finitely generated integral domain of zero characteristic then there is no integer n such that every element of R is a sum of at most n units.*

In particular, we have $u(R) \geq \omega$, for any ring R of integers of an algebraic number field.

This theorem is an immediate consequence of the following lemma, which Jarden and Narkiewicz proved by means of Evertse and Győry's [10] bound on the number of solutions of S-unit equations combined with van der Waerden's theorem [36] on arithmetic progressions.

Lemma 2. [24, Lemma 4] *If R is a finitely generated integral domain of zero characteristic and $n \geq 1$ is an integer then there exists a constant $A_n(R)$ such that every arithmetic progression in R having more than $A_n(R)$ elements contains an element which is not a sum of n units.*

Lemma 2 is a special case of a theorem independently found by Hajdu [20]. Hajdu's result provides a bound for the length of arithmetic progressions in linear combinations of elements from a finitely generated multiplicative subgroup of a field of zero characteristic. Here the linear combinations are of fixed length and only a given finite set of coefficient-tuples is allowed. Hajdu used his result to negatively answer the following question by Pohst: Is it true that every prime can be written in the form $2^u \pm 3^v$, with non-negative integers u, v?

Using results by Mason [27, 28] on S-unit equations in function fields, Frei [14] proved the function field analogue of Theorem 1. It holds in zero characteristic as well as in positive characteristic.

Theorem 3. *Let R be the ring of S-integers of an algebraic function field in one variable over a perfect field, where $S \neq \emptyset$ is a finite set of places. Then, for each positive integer n, there exists an element of R that can not be written as a sum of at most n units of R. In particular, we have $u(R) \geq \omega$.*

We will later discuss criteria which show that in the number field case as well as in the function field case, both possibilities $u(R) = \omega$ and $u(R) = \infty$ occur.

3. The qualitative problem

Problem A. [24, Problem A] *Give a criterion for an algebraic extension K of the rationals to have the property that its ring of integers R has unit sum number $u(R) \leq \omega$.*

Jarden and Narkiewicz provided some easy examples of infinite extensions of $\mathbb{Q}$ with $u(R) \leq \omega$: By the Kronecker-Weber theorem, the maximal Abelian extension of $\mathbb{Q}$ has this property. Further examples are the fields of all algebraic numbers and all real algebraic numbers.

More criteria are known for algebraic number fields of small degree. Here, the only possibilities for $u(R)$ are ω and ∞, by Theorem 1. For quadratic number fields, Belcher [3], and later Ashrafi and Vámos [2], proved the following result:

Theorem 4. [3, Lemma 1][2, Theorems 7, 8] *Let $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, be a quadratic number field with ring of integers R. Then $u(R) = \omega$ if and only if*

1. $d \in \{-1, -3\}$, *or*
2. $d > 0$, $d \not\equiv 1 \mod 4$, *and $d+1$ or $d-1$ is a perfect square, or*
3. $d > 0$, $d \equiv 1 \mod 4$, *and $d+4$ or $d-4$ is a perfect square.*

A similar result for purely cubic fields was found by Tichy and Ziegler [33].

Theorem 5. [33, Theorem 2] *Let d be a cubefree integer and R the ring of integers of the purely cubic field $\mathbb{Q}(\sqrt[3]{d})$. Then $u(R) = \omega$ if and only if*

1. *d is squarefree,* $d \not\equiv \pm 1 \mod 9$, *and $d+1$ or $d-1$ is a perfect cube, or*
2. $d = 28$.

Filipin, Tichy and Ziegler used similar methods to handle purely quartic complex fields $\mathbb{Q}(\sqrt[4]{d})$. Their criterion [11, Theorem 1.1] states that $u(R) = \omega$ if and only if d is contained in one of six explicitly given sets.

As a first guess, one could hope to get information about the unit sum number of the ring of integers of a number field K by comparing the regulator and the discriminant of K. In personal communication with the authors, Martin Widmer pointed out the following sufficient criterion for the simple case of complex cubic fields:

Proposition 6. *(Widmer) If R is the ring of integers of a complex cubic number field K then $u(R) = \omega$ whenever the inequality*

$$|\Delta_K| > (e^{\frac{3}{4}R_K} + e^{-\frac{3}{4}R_K})^4 \tag{1}$$

holds. Here, Δ_K is the discriminant and R_K is the regulator of K.

Proof. Regard K as a subfield of the reals, and let $\eta > 1$ be a fundamental unit, so $R_K = \log \eta$. Since K contains no roots of unity except ± 1, the ring of integers R is generated by its units if and only if $R = \mathbb{Z}[\eta]$. By the standard embedding

$K \to \mathbb{R} \times \mathbb{C} \simeq \mathbb{R}^3$, we can regard R and $\mathbb{Z}[\eta]$ as lattices in $\mathbb{R}^3$ and compare their determinants. Let $\eta' = x + iy$ be one of the non-real conjugates of η. We get $u(R) = \omega$ if and only if

$$2^{-1}\sqrt{|\Delta_K|} = \left|\det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix}\right|.$$

Since the right-hand side of the above equality is always a multiple of the left-hand side, we have $u(R) = \omega$ if and only if

$$\sqrt{|\Delta_K|} > \left|\det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix}\right|.$$

Clearly, $\eta^{-1} = \eta'\overline{\eta'} = x^2 + y^2$, whence $|x|$, $|y| \leq \eta^{-1/2}$. With this in mind, a simple computation shows that the right-hand side of the above inequality is at most $\eta^{-3/2} + 2 + \eta^{3/2}$, so (1) implies that $u(R) = \omega$. □

To see that condition (1) is satisfied in infinitely many cases, we consider the complex cubic fields $K_N = \mathbb{Q}(\alpha_N)$, where α_N is a root of the polynomial

$$f_N = X^3 + NX + 1, \tag{2}$$

with a positive integer N such that $4N^3 + 27$ is squarefree. By [7], infinitely many such N exist. We may assume that $\alpha_N \in \mathbb{R}$. From (2), we get

$$\frac{N^2}{N^3+1} < -\alpha_N = \frac{1}{\alpha_N^2 + N} < 1/N.$$

Since $-1/\alpha_N$ is a unit of the ring of integers of K_N, and $N < -1/\alpha_N < N + 1/N^2$, we have $R_K \leq \log(N + 1/N^2)$. The discriminant $-4N^3 - 27$ of f_N is squarefree by hypothesis, so $|\Delta_K| = 4N^3 + 27$. Now we see by a simple computation that (1) holds.

In the function field case, Frei [14] investigated quadratic extensions of rational global function fields.

Theorem 7. [14, Theorem 2] *Let K be a finite field, and F a quadratic extension field of the rational function field $K(x)$ over K. Denote the integral closure of $K[x]$ in F by R. Then the following two statements are equivalent.*

1. *$u(R) = \omega$*
2. *The function field $F|K$ has full constant field K and genus 0, and the infinite place of $K(x)$ splits into two places of $F|K$.*

This criterion can also be phrased in terms of an element generating F over $K(x)$. If, for example, K is the full constant field of F and of odd characteristic then we can write $F = K(x, y)$, where $y^2 = f(x)$ for some separable polynomial $f \in K[x] \setminus K$. Then we get $u(R) = \omega$ if and only if f is of degree 2 and its leading coefficient is a square in K ([14, Corollary 1]).

Theorem 7 holds in fact for arbitrary perfect base fields K. An alternative proof given at the end of [14] implies the following stronger version:

Theorem 8. *Let $F|K$ be an algebraic function field in one variable over a perfect field K. Let S be a set of two places of $F|K$ of degree one, and denote by R the ring of S-integers of $F|K$. Then $u(R) = \omega$ if and only if $F|K$ is rational.*

All of the rings R investigated above have in common that their unit groups are of rank at most one. Currently, there are no known nontrivial criteria for families of number fields (or function fields) whose rings of integers have unit groups of higher rank. We consider it an important direction to find such criteria.

Pethő and Ziegler investigated a modified version of Problem A, where one asks whether a ring of integers has a power basis consisting of units [39, 29]. For example, Ziegler proved the following:

Theorem 9. [39, Theorem 1] *Let $m > 1$ be an integer which is not a square. Then the order $\mathbb{Z}[\sqrt[4]{m}]$ admits a power basis consisting of units if and only if $m = a^4 \pm 1$, for some integer a.*

Since analogous results are already known for negative m [40] and for the rings $\mathbb{Z}[\sqrt[d]{m}]$, $d < 4$ [3, 33], Theorem 9 motivates the following conjecture:

Conjecture. [39, Conjecture 1] *Let $d \geq 2$ be an integer and $m \in \mathbb{Z} \setminus \{0\}$, and assume that $\sqrt[d]{m}$ is an algebraic number of degree d. Then $\mathbb{Z}[\sqrt[d]{m}]$ admits a power basis consisting of units if and only if $m = a^d \pm 1$, for some integer a.*

For rings R with $u(R) = \omega$, Ashrafi [1] investigated the stronger property that every element of R can be written as a sum of k units for all sufficiently large integers k. Ashrafi proved that this is the case if and only if R does not have $\mathbb{Z}/2\mathbb{Z}$ as a factor, and applied this result to rings of integers of quadratic and complex cubic number fields.

Let R be an order in a quadratic number field. Ziegler [38] found various results about representations of elements of R as sums of S-units in R, where S is a finite set of places containing all Archimedean places.

Another variant of Problem A asks for representations of algebraic integers as sums of distinct units. Jacobson [23] proved that in the rings of integers of the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, every element is a sum of distinct units. His conjecture that these are the only quadratic number fields with that property was proved by Śliwa [30]. Belcher [3, 4] investigated cubic and quartic number fields. A recent article by Thuswaldner and Ziegler [32] puts these results into a more general framework: they apply methods from the theory of arithmetic dynamical systems to additive unit representations.

4. The extension problem

Problem B. [24, Problem B] *Is it true that each number field has a finite extension L such that the ring of integers of L is generated by its units?*

If K is an Abelian number field, that is, $K|\mathbb{Q}$ is a Galois extension with Abelian Galois group, then we know by the Kronecker-Weber theorem that K is contained in a cyclotomic number field $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$, which is obviously generated by its units. Problem B was completely solved by Frei [13]:

Theorem 10. [13, Theorem 1] *For any number field K, there exists a number field L containing K, such that the ring of integers of L is generated by its units.*

The proof relies on finding elements of the ring of integers of K with certain properties via asymptotic counting arguments, and then using these properties to generate easily manageable quadratic extensions of K in which those elements are sums of units of the respective rings of integers. The field L is then taken as the compositum of all these quadratic extensions.

Prior to this, with an easier but conceptually similar argument, Frei [15] answered the function field version of Problem B:

Theorem 11. [15, Theorem 2] *Let $F|K$ be an algebraic function field over a perfect field K, and R the ring of S-integers of F, for some finite set $S \neq \emptyset$ of places. Then there exists a finite extension field F' of F such that the integral closure of R in F' is generated by its units.*

5. The quantitative problem

Problem C. [24, Problem C] *Let K be an algebraic number field. Obtain an asymptotic formula for the number $N_k(x)$ of positive rational integers $n \leq x$ which are sums of at most k units of the ring of integers of K.*

As Jarden and Narkiewicz noticed, Lemma 2 and Szemerédi's theorem (see [19]) imply that

$$\lim_{x\to\infty} \frac{N_k(x)}{x} = 0,$$

for any fixed k.

A similar question has been investigated by Filipin, Fuchs, Tichy, and Ziegler [11, 12, 16]. We state here the most general result [16]. Let R be the ring of S-integers of a number field K, where S is a finite set of places containing all Archimedean places. Two S-integers α, β are *associated*, if there exists a unit ε of R such that $\alpha = \beta\varepsilon$. For any $\alpha \in R$, we write

$$N(\alpha) := \prod_{\nu\in S} |\alpha|_\nu.$$

Fuchs, Tichy and Ziegler investigated the counting function $u_{K,S}(n,x)$, which denotes the number of all classes $[\alpha]$ of associated elements α of R with $N(\alpha) \leq x$ such that α can be written as a sum

$$\alpha = \sum_{i=1}^{n} \varepsilon_i,$$

where the ε_i are units of R and no subsum of $\varepsilon_1 + \cdots + \varepsilon_n$ vanishes. The proof uses ideas of Everest [8], see also Everest and Shparlinski [9].

Theorem 12. [16, Theorem 1] *Let $\varepsilon > 0$. Then*

$$u_{K,S}(n,x) = \frac{c_{n-1,s}}{n!}\left(\frac{\omega_K(\log x)^s}{\mathrm{Reg}_{K,S}}\right)^{n-1} + o((\log x)^{(n-1)s-1+\varepsilon}),$$

as $x \to \infty$. Here, ω_K is the number of roots of unity of K, $\mathrm{Reg}_{K,S}$ is the S-regulator of K, and $s = |S| - 1$. The constant $c_{n,s}$ is the volume of the polyhedron

$$\{(x_{11},\ldots,x_{ns}) \in \mathbb{R}^{ns} \mid g(x_{11},\ldots,x_{ns}) < 1\},$$

with

$$g(x_{11},\ldots,x_{ns}) = \sum_{i=1}^{s} \max\{0, x_{1i},\ldots,x_{ni}\} + \max\left\{0, -\sum_{i=1}^{s} x_{1i},\ldots,-\sum_{i=1}^{s} x_{ni}\right\}.$$

The values of the constant $c_{n,s}$ are known in special cases from [16]:

	n				
s	1	2	3	4	5
1	2	3	4	5	6
2	3	15/4	7/2	45/16	
3	10/3	7/3	55/54		
4	35/12	275/32			
5	21/10				

Furthermore, $c_{n,1} = n+1$ and $c_{1,s} = \frac{1}{s!}\binom{2s}{s}$.

In the following we calculate the constant $c_{n,s}$ for $n > 1$ and $s = 2$. This constant is the volume of the polyhedron

$$V = \{(x,y) \in \mathbb{R}^n \times \mathbb{R}^n : g(x,y) < 1\},$$

with

$$g(x,y) = \max_i \{0, x_i\} + \max_i \{0, y_i\} + \max_i \{0, -x_i - y_i\},$$

where $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$.

For any K, L, $M \in \{1, \ldots, n\}$ we consider the sets

$$V_{K,L,M} = \left\{(x,y) \in \mathbb{R}^{2n} : x_i \le x_K,\ y_i \le y_L,\ x_M + y_M \le x_i + y_i,\ g(x,y) < 1\right\}.$$

Clearly the union of these sets is V and the intersection of any two of them has volume zero. Thus

$$c_{n,2} = \sum_{K=1}^{n} \sum_{L=1}^{n} \sum_{M=1}^{n} I_{K,L,M},$$

where $I_{K,L,M}$ is the volume of $V_{K,L,M}$. For the values of $I_{K,L,M}$ we distinguish three cases:

(i) K, L, M are pairwise distinct;
(ii) exactly two of the indices K, L, M are equal;
(iii) $K = L = M$.

The third case is simple. Since $x_i \le x_K$, $y_i \le y_K$ implies $x_i + y_i \le x_K + y_K$ we obtain $x_i + y_i = x_K + y_K$. Thus $V_{K,K,K}$ has volume zero.

We only have to consider the remaining cases (i) and (ii). Clearly,

$$c_{n,2} = n(n-1)(n-2)I_{1,2,3} + 3n(n-1)I_{1,1,2}.$$

5.i. **Calculation of $I_{1,2,3}$.** This case can only happen if $n \ge 3$. The inequalities $x_3 + y_3 \le x_i + y_i$ give us lower bounds for x_i and y_i and we always have the upper bounds $x_i \le x_1$ and $y_i \le y_2$. Hence we have

$$x_3 + y_3 - x_i \le y_i \le y_2$$

and

$$x_i \le x_1.$$

Note that

$$g(x,y) = \max\{0, x_1\} + \max\{0, y_2\} + \max\{0, -x_3 - y_3\}.$$

We integrate with respect to the y_i's, $i \ne 2, 3$ and obtain

$$I_{1,2,3} = \int \cdots \int_{\substack{x_3+y_3-x_i \le y_i \le y_2 \\ x_i \le x_1,\ g(x,y)<1}} dxdy = \int \cdots \int_{\substack{x_3+y_3 \le x_2+y_2 \\ x_3+y_3-y_2 \le x_i \le x_1 \\ y_3 \le y_2,\ g(x,y)<1}} \prod_{j \ne 2,3} (y_2 - x_3 - y_3 + x_j) dxdy_2dy_3.$$

Next we integrate over the x_i's, $i \ne 1, 2, 3$ and obtain

$$I_{1,2,3} = \underset{\substack{x_2,x_3\leq x_1,\ y_3\leq y_2\\ x_3+y_3\leq x_2+y_2\\ g(x,y)<1}}{\int\cdots\int} \frac{1}{2^{n-3}}\left(y_2-x_3-y_3+x_1\right)^{2n-5} dx_1dx_2dx_3dy_2dy_3.$$

For the values of $g(x,y)$ we consider the following cases depending on the signs of x_1, y_2 and $-x_3-y_3$:

r	x_1	y_2	$-x_3-y_3$	$g(x,y)$
1	≥ 0	< 0	< 0	x_1
2	< 0	≥ 0	< 0	y_2
3	< 0	< 0	≥ 0	$-x_3-y_3$
4	≥ 0	≥ 0	< 0	x_1+y_2
5	≥ 0	< 0	≥ 0	$x_1-x_3-y_3$
6	< 0	≥ 0	≥ 0	$y_2-x_3-y_3$
7	≥ 0	≥ 0	≥ 0	$x_1+y_2-x_3-y_3$

According to the table we split the integral into seven parts:

$$I_{1,2,3} = \sum_{r=1}^{7} I_{1,2,3}^{(r)}.$$

One can calculate these integrals with the help of a computer algebra system. We just give the final expressions:

$$\begin{aligned} I_{1,2,3}^{(1)} = I_{1,2,3}^{(2)} = I_{1,2,3}^{(3)} &= \frac{2}{n(2n-1)(n-1)2^n}, \\ I_{1,2,3}^{(4)} = I_{1,2,3}^{(5)} = I_{1,2,3}^{(6)} &= \frac{2}{n(n-1)2^n}, \\ I_{1,2,3}^{(7)} &= \frac{2}{n2^n}. \end{aligned}$$

In conclusion we have

$$I_{1,2,3} = \frac{2(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

5.ii. **Calculation of $I_{1,1,2}$.** We proceed in the same way as in the other case. We have the same bounds

$$x_2+y_2-x_i \leq y_i \leq y_1$$

and

$$x_i \leq x_1.$$

We integrate first with respect to the y_i's and then with respect to the x_i's, $i \neq 1,2$, and obtain

$$\begin{aligned} I_{1,1,2} &= \underset{\substack{x_2+y_2-y_1\leq x_i\leq x_1\\ y_2\leq y_1,\ g(x,y)<1}}{\int\cdots\int} \prod_{j\neq 1,2}(y_1-x_2-y_2+x_j)dxdy_1dy_2 = \\ &= \underset{\substack{x_2\leq x_1,\ y_2\leq y_1\\ g(x,y)<1}}{\int\cdots\int} \frac{1}{2^{n-2}}\left(y_1-x_2-y_2+x_1\right)^{2n-4} dx_1dx_2dy_1dy_2. \end{aligned}$$

Proceeding as in the previous section we again split the integral into seven parts $I_{1,1,2}^{(r)}$, $r = 1,\ldots,7$, and obtain:

$$\begin{aligned} I^{(1)}_{1,1,2} = I^{(2)}_{1,1,2} = I^{(3)}_{1,1,2} &= \frac{1}{n(2n-1)(n-1)2^n}, \\ I^{(4)}_{1,1,2} = I^{(5)}_{1,1,2} = I^{(6)}_{1,1,2} &= \frac{1}{n(n-1)2^n}, \\ I^{(7)}_{1,1,2} &= \frac{1}{n2^n}. \end{aligned}$$

Hence

$$I_{1,1,2} = \frac{(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

Conclusion. *The value of $c_{n,2}$ is*

$$\frac{(n+1)(2n+1)}{2^n}.$$

Remark. *The computation of $c_{n,s}$ for $s > 2$ seems to be more difficult and might be considered later.*

6. Matrix rings

6.1. **Matrix rings over arbitrary rings.** Let R be any ring with 1. We say that two elements $a, b \in R$ are equivalent ($a \sim b$) if there exist two units $u, v \in R^\times$ such that $b = uav$. Vámos [34, Lemma 1] already noticed the following simple fact.

Lemma 13. *Let R be a ring and $a, b \in R$. If $a \sim b$ then, for all $k \geq 1$, a is k-good if and only if b is k-good.*

We consider the ring $M_n(R)$ of $n \times n$ matrices, with $n \geq 2$, over an arbitrary ring R with 1. As usual $GL_n(R)$ denotes the group of units of $M_n(R)$.

For $a \in R$ the matrix $E_n(a, i, j)$, $i, j \in \{1, \ldots, n\}$, $i \neq j$, is the $n \times n$ matrix with 1 entries on the main diagonal, a as the entry at position (i, j) and 0 elsewhere. We call this kind of matrices *elementary matrices* and denote by $E_n(R)$ the subgroup of $GL_n(R)$ generated by elementary matrices, permutation matrices and $-I$, where I is the identity matrix of $M_n(R)$.

Let us consider a more specific kind of k-goodness introduced by Vámos [34].

Definition. *A square matrix of size n over R is strongly k-good if it can be written as a sum of k elements of $E_n(R)$. The ring $M_n(R)$ is strongly k-good if every element is strongly k-good.*

The following lemma is Lemma 1 from [21] and Lemma 5 from [34].

Lemma 14. *Let R be a ring and $n \geq 2$. Then any diagonal matrix in $M_n(R)$ is strongly 2-good.*

A ring R is called an *elementary divisor ring* (see [25]) if every matrix in $M_n(R)$, $n \geq 2$, can be diagonalized. Lemma 14 implies that, in this case, $M_n(R)$ is 2-good. In particular, if any matrix in $M_n(R)$ can be diagonalized using only matrices in $E_n(R)$ then $M_n(R)$ is strongly 2-good.

The following two remarks can be deduced without much effort from the proof of Lemma 14 that is given in [34].

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then the representation of a matrix in $M_n(R)$ as a sum of two units is never unique.*

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then every element of $M_n(R)$ has a representation as a sum of two distinct units.*

As we have already mentioned, Henriksen [21] proved that $M_n(R)$, where R is any ring, is 3-good. Henriksen's result was generalized by Vámos [34] to arbitrary dimension:

Theorem 15. [34, Theorem 11] *Let R be a ring and let F be a free R-module of rank α, where $\alpha \geq 2$ is a cardinal number. Then the ring of endomorphisms E of F is 3-good.*

If α is finite and R is 2-good or an elementary divisor ring then E is 2-good. If R is any one of the rings $\mathbb{Z}[X]$, $K[X,Y]$, $K\langle X,Y\rangle$, where K is a field, then $u(E) = 3$. Here $K\langle X,Y\rangle$ is the free associative algebra generated by X, Y over K.

To prove that a matrix ring over a certain ring has unit sum number 3, Vámos used the following proposition.

Proposition 16. [34, Proposition 10] *Let R be a ring, $n \geq 2$ an integer and let $L = Ra_1 + \cdots + Ra_n$ be the left ideal generated by the elements $a_1, \ldots, a_n \in R$. Let A be the $n \times n$ matrix whose entries are all zero except for the first column which is $(a_1, \ldots, a_n)^T$. Suppose that*

1. L cannot be generated by fewer than n elements, and
2. zero is the only 2-good element in L.

Then A is not 2-good.

We now apply Lemma 14 to a special case. Let R be a ring and suppose there exists a function

$$f : R \setminus \{0\} \to \mathbb{Z}_{\geq 0},$$

with the following property: for every $a, b \in R$, $b \neq 0$, there exist $q_1, q_2, r_1, r_2 \in R$ such that

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{where} \quad r_1 = 0 \text{ or } f(r_1) < f(b), \\ a &= b q_2 + r_2, \quad \text{where} \quad r_2 = 0 \text{ or } f(r_2) < f(b). \end{aligned}$$

Then we say that R has *left and right Euclidean division.*

The next theorem is a generalization of the well known fact that every square matrix over a Euclidean domain is diagonalizable. The proof strictly follows the line of the one in the commutative case (see Section 3.5 of [18]), hence it is omitted.

Theorem 17. *Let R be a ring with left and right Euclidean division and $n \geq 2$. For every $A \in M_n(R)$ there exist two matrices $U, V \in E_n(R)$ such that*

$$UAV = D,$$

where D is a diagonal matrix.

Corollary. *Let R be a ring with left and right Euclidean division and $n \geq 2$. Then $M_n(R)$ is strongly 2-good.*

We apply the previous result to the special case of quaternions. Consider the quaternion algebra

$$Q = \left\{ a + bi + cj + dk \mid a,\, b,\, c,\, d \in \mathbb{Q},\, i^2 = -1,\, j^2 = -1,\, k = ij = -ji \right\}.$$

Definition. *The ring of Hurwitz quaternions is defined as the set*

$$H = \left\{ a + bi + cj + dk \in Q \quad s.\ t. \quad a, b, c, d \in \mathbb{Z} \quad or \quad a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

For basic properties about Hurwitz quaternions see [5, Chapter 5].

In Q the ring of Hurwitz quaternions plays a similar role as maximal orders in number fields.

The units of H are the 24 elements ± 1, $\pm i$, $\pm j$, $\pm k$ and $(\pm 1 \pm i \pm j \pm k)/2$, so $u(H) = \omega$.

It is well known that H has left and right Euclidean division. Therefore, we get the following corollary.

Corollary. *For $n \geq 2$, $M_n(H)$ is strongly 2-good.*

6.2. **Matrix rings over Dedekind domains.** Let R be a ring and A an $r \times c$ matrix. The *type* of A is the pair (r, c) and the *size* of A is $\max(r, c)$. Let A_1 and A_2 be matrices of type (r_1, c_1) and (r_2, c_2), respectively. The *block diagonal sum* of A_1 and A_2 is the block diagonal matrix

$$diag(A_1, A_2) = \left[\begin{array}{cc} A_1 & 0 \\ 0 & A_2 \end{array} \right],$$

of type $(r_1 + r_2, c_1 + c_2)$. A matrix of positive size is *indecomposable* if it is not equivalent to the block diagonal sum of two matrices of positive size.

In 1972 Levy [26] proved that, for a Dedekind domain R, the class number, when it is finite, is an upper bound to the number of rows and columns in every indecomposable matrix over R. Vámos and Wiegand [35] generalized Levy's result to Prüfer domains (under some technical conditions) and applied it to the unit sum problem.

Theorem 18. *(see* [35, Theorem 4.7]*) Let R be a Dedekind domain with finite class number c. For every $n \geq 2c$, $M_n(R)$ is 2-good.*

Unfortunately we do not know a criterion. The only sufficient condition we know for a matrix not to be 2-good is given by Proposition 16. For rings R of algebraic integers this proposition is of limited use. Since ideals in Dedekind domains need at most 2 generators, condition (1) can be fulfilled only for $n = 2$. Concerning condition (2) it is not hard to see that, if the unit group is infinite, there is a nonzero sum of two units in every nonzero ideal in a ring of algebraic integers. Therefore we can apply Proposition 16 only to the non-PID complex quadratic case.

Corollary. [35, Example 4.11] *Let R be the ring of integers of $\mathbb{Q}(\sqrt{-d})$, where $d > 0$ is squarefree and R has class number $c > 1$. Then $u(M_2(R)) = 3$ and $u(M_n(R)) = 2$ for every integer $n \geq 2c$.*

Question A. [35, Example 4.11] *With the hypotheses of the previous corollary, what is the value of $u(M_n(R))$ for $3 \leq n < 2c$?*

Question B. [35, Question 4.12] *If R is any ring of algebraic integers with class number c, what is the value of $u(M_n(R))$ for $2 \leq n < 2c$?*

References

[1] N. Ashrafi. A finer classification of the unit sum number of the ring of integers of quadratic fields and complex cubic fields. *Proc. Indian Acad. Sci. Math. Sci.*, 119(3):267–274, 2009.

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

[3] P. Belcher. Integers expressible as sums of distinct units. *Bull. Lond. Math. Soc.*, 6:66–68, 1974.

[4] P. Belcher. A test for integers being sums of distinct units applied to cubic fields. *J. Lond. Math. Soc. (2)*, 12(2):141–148, 1975/76.

[5] J. H. Conway and D. A. Smith. *On quaternions and octonions: their geometry, arithmetic and symmetry.* A K Peters, Natick, Massachusetts, 2003.

[6] J. Dieudonné. La théorie de Galois des anneux simples et semi-simples. *Comment. Math. Helv.*, 21:154–184, 1948.

[7] P. Erdös. Arithmetical properties of polynomials. *J. London Math. Soc.*, 28:416–425, 1953.

[8] G. R. Everest. Counting the values taken by sums of S-units. *J. Number Theory*, 35(3):269–286, 1990.

[9] G. R. Everest and I. E. Shparlinski. Counting the values taken by algebraic exponential polynomials. *Proc. Amer. Math. Soc.*, 127(3):665–675, 1999.

[10] J.-H. Evertse and K. Győry. On the numbers of solutions of weighted unit equations. *Compositio Math.*, 66(3):329–354, 1988.

[11] A. Filipin, R. F. Tichy, and V. Ziegler. The additive unit structure of pure quartic complex fields. *Funct. Approx. Comment. Math.*, 39(1):113–131, 2008.

[12] A. Filipin, R. F. Tichy, and V. Ziegler. On the quantitative unit sum number problem—an application of the subspace theorem. *Acta Arith.*, 133(4):297–308, 2008.

[13] C. Frei. On rings of integers generated by their units. *submitted*.

[14] C. Frei. Sums of units in function fields. *Monatsh. Math., DOI: 10.1007/s00605-010-0219-7.*

[15] C. Frei. Sums of units in function fields II - The extension problem. *to appear in Acta Arith.*

[16] C. Fuchs, R. F. Tichy, and V. Ziegler. On quantitative aspects of the unit sum number problem. *Arch. Math.*, 93:259–268, 2009.

[17] B. Goldsmith, S. Pabst, and A. Scott. Unit sum numbers of rings and modules. *Q. J. Math.*, 49(195):331–344, 1998.

[18] F. M. Goodman. *Algebra: abstract and concrete.* SemiSimple Press, Iowa City, IA, 1998.

[19] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

[20] L. Hajdu. Arithmetic progressions in linear combinations of S-units. *Period. Math. Hung.*, 54(2):175–181, 2007.

[21] M. Henriksen. Two classes of rings generated by their units. *J. Algebra*, 31:182–193, 1974.

[22] B. Herwig and M. Ziegler. A remark on sums of units. *Arch. Math. (Basel)*, 79(6):430–431, 2002.

[23] B. Jacobson. Sums of distinct divisors and sums of distinct units. *Proc. Am. Math. Soc.*, 15:179–183, 1964.

[24] M. Jarden and W. Narkiewicz. On sums of units. *Monatsh. Math.*, 150(4):327–332, 2007.

[25] I. Kaplansky. Elementary divisors and modules. *Trans. Amer. Math. Soc.*, 66:464–491, 1949.

[26] L. S. Levy. Almost diagonal matrices over Dedekind domains. *Math. Z.*, 124:89–99, 1972.

[27] R. C. Mason. Norm form equations. I. *J. Number Theory*, 22(2):190–207, 1986.

[28] R. C. Mason. Norm form equations. III. Positive characteristic. *Math. Proc. Camb. Philos. Soc.*, 99(3):409–423, 1986.

[29] A. Pethő and V. Ziegler. On biquadratic fields that admit unit power integral basis,. *submitted*.

[30] J. Śliwa. Sums of distinct units. *Bull. Acad. Pol. Sci.*, 22:11–13, 1974.

[31] A. K. Srivastava. A survey of rings generated by units. *Ann. Fac. Sci. Toulouse Math. (6)*, 19, 2010.

[32] J. Thuswaldner and V. Ziegler. On linear combinations of units with bounded coefficients. *preprint*.

[33] R. F. Tichy and V. Ziegler. Units generating the ring of integers of complex cubic fields. *Colloq. Math.*, 109(1):71–83, 2007.

[34] P. Vámos. 2-good rings. *Q. J. Math.*, 56(3):417–430, 2005.

[35] P. Vámos and S. Wiegand. Block diagonalization and 2-unit sums of matrices over Prüfer domains. *to appear in Trans. Amer. Math. Soc.*

[36] B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk (2)*, 15:212–216, 1927.

[37] D. Zelinsky. Every linear transformation is a sum of nonsingular ones. *Proc. Am. Math. Soc.*, 5:627–630, 1954.

[38] V. Ziegler. The additive S-unit structure of quadratic fields. *to appear in Int. J. Number Theory.*

[39] V. Ziegler. On unit power integral bases of $\mathbb{Z}[\sqrt[4]{m}]$. *to appear in Period. Math. Hung.*

[40] V. Ziegler. The additive unit structure of complex biquadratic fields. *Glas. Mat.*, 43(63)(2):293–307, 2008.

E-mail address: `barroero@math.tugraz.at`

E-mail address: `frei@math.tugraz.at`

E-mail address: `tichy@tugraz.at`

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria