Journal of the Iranian Mathematical Society
ISSN (on-line): 2717-1612
J. Iranian Math. Soc. 1 (2020), no. 2, 163-172

COUNTING SUBRINGS OF $\mathbb{Z}^n$ OF NON-ZERO CO-RANK

S. CHIMNI, G. CHINTA AND R. TAKLOO-BIGHASH

Abstract. In this paper we study subrings of $\mathbb{Z}^{n+k}$ of co-rank k. We relate the number of such subrings R with torsion subgroup $(\mathbb{Z}^{n+k}/R)_{\text{tor}}$ of size r to the number of full rank subrings of $\mathbb{Z}^n$ of index r. We also present a number field analogue of the main result.

1. Introduction

Let $\mathbb{Z}^n$ be the set of n-tuples $(x_1, \ldots, x_n)$ of integers. This set comes with a natural addition and multiplication given by

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

and

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 \cdot y_1, \ldots, x_n \cdot y_n).$$

Under these operations $\mathbb{Z}^n$ is a ring with multiplicative identity $(1, \ldots, 1)$. A subring is defined to be a subset R of $\mathbb{Z}^n$ that is closed under both operations and contains $(1, \ldots, 1)$. As is well known the ring $\mathbb{Z}^n$ has a simple additive group structure, but when it comes to its multiplicative structure there are some very easy-to-state basic questions that we do not know how to answer. For example, let $f_n(r)$ be the number of subrings R of $\mathbb{Z}^n$ with identity of index r. Necessarily then, R is a free $\mathbb{Z}$-module of rank n. The counting function $f_n(r)$ and associated generating series $F_n(s) := \sum_{r=1}^{\infty} f_n(r) r^{-s}$ are basic objects of interest.

Communicated by Alireza Abdollahi

MSC(2020): Primary 11M41; 11R29; Secondary 11S40.

Keywords: $\mathbb{Z}^n$; subrings; Stirling numbers of the second kind; orders; number fields.

Received: 7 July 2020, Accepted: 5 November 2020.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

.

The general theory developed by Grunewald, Segal and Smith [5] shows that $F_n(s)$ can be expressed as an Euler product of rational functions of p^{-s} over all primes p, but only for $n \leq 4$ has this rational function been computed explicitly. For $n = 2$ this expression is immediate. It is originally due to Datskovksy and Wright [4] for $n = 3$ and Nakagawa [9] for $n = 4$. In fact, these authors studied the more general problem understanding the distribution of orders in cubic or quartic algebras, a particular case of which was the computation of the generating series $F_3(s)$ in [4] and $F_4(s)$ in [9]. Liu [8] proved a number of interesting theorems about $f_n(r)$, including the computation of $F_n(s) := \sum_{r=1}^{\infty} f_n(r)r^{-s}$ for $n \leq 4$ by an alternative method.

For $n > 4$ the situation is considerably more complicated. Kaplan, Marcinek, and Takloo-Bighash [7], by using the methods of p-adic integration, obtained results for the location and order of the rightmost pole of $F_5(s)$ without explicitly computing the series. They also obtained estimates for the location of the rightmost pole of $F_n(s)$ for $n > 5$. One of the reasons to study the analytic properties of the generating series $F_n(s)$ is to find asymptotic formulae for $N_n(B) = \sum_{r \leq B} f_n(r)$. The theory of p-adic integration [5] shows that $N_n(B)$ grows like a non-zero constant C_n multiplied by $B^{\alpha(n)}(\log B)^{b(n)-1}$ for $\alpha(n) \in \mathbb{Q}$ and $b(n) \in \mathbb{N}$. Combining the results of [4, 7, 9] we know the following about the behavior of $N_n(B)$:

Theorem 1.1. *If $n \leq 5$ there is a constant C_n such that*

$$N_n(B) \sim C_n B(\log B)^{\binom{n}{2}-1}$$

as $B \to \infty$. If $n \geq 6$, for any $\epsilon > 0$ we have

$$B(\log B)^{\binom{n}{2}-1} \ll N_n(B) \ll_{\epsilon} B^{\frac{n}{2}-\frac{7}{6}+\epsilon}.$$

In fact, results of Brakenhoff [3], Atanasov-Kaplan-Krakoff-Menzel [1], and [6] give better bounds for $n \geq 6$.

As mentioned above $f_n(r)$ counts full rank $\mathbb{Z}$-submodules of $\mathbb{Z}^n$ that are of index r. A natural question to ask is whether one can quantify the distribution of subrings of $\mathbb{Z}^n$ which as $\mathbb{Z}$-submodules are not of rank n. Let us make this precise. Let $\phi_n(r)$ be the number of full-rank sublattices of $\mathbb{Z}^n$ which are closed under the multiplication of $\mathbb{Z}^n$. It is a well-known fact (e.g., Proposition 2.3 of [8]) that for each $n \geq 2, r \geq 1$ we have $f_n(r) = \phi_{n-1}(r)$. It turns out that for many purposes the function $\phi_n(r)$ is a more convenient function to work with—and in fact the theory developed in [5] deals with the function $\phi_n(r)$.

We now define an analogue of the function $\phi_n(r)$ for lattices of non-zero co-rank. For $0 \leq k \leq n$, define $\phi_{n,k}(r)$ be the number of sublattices L of $\mathbb{Z}^n$ which have the following properties:

- The lattice L is closed under multiplication;
- as a $\mathbb{Z}$-submodule, L is of co-rank k in $\mathbb{Z}^n$;
- the size of the torsion subgroup of $\mathbb{Z}^n/L$ is equal to r.

Clearly, $\phi_{n,0}(r) = \phi_n(r)$. It turns out that the function $\phi_{n,k}(r)$ and $\phi_n(r)$ have a simple relationship. The following theorem is our main result.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

Theorem 1.2. *For all n, k, r we have*

$$\phi_{n+k,k}(r) = \left\{ \begin{matrix} n+k+1 \\ n+1 \end{matrix} \right\} \cdot \phi_n(r).$$

Here, for natural numbers u, v, $\left\{ \begin{matrix} u \\ v \end{matrix} \right\}$ is the Stirling number of second kind defined as the number of partitions of a set with u elements into v non-empty subsets.

The main step in the proof of this theorem is a rigidity result (Theorem 2.4) which determines exactly what types of lattices contribute to the counting function $\phi_{n+k,k}(r)$. The rest of the proof consists of a combinatorial argument counting these lattices. For information on Stirling numbers of the second kind, see [2], especially Chapter 2, Section 3.

The rigidity result mentioned above is the statement that matrices corresponding to multiplicative sublattices will be of very special shape. The upshot of this result is that multiplicative sublattices of non-zero co-rank in $\mathbb{Z}^n$ are all obtained from full rank multiplicative sublattices in various $\mathbb{Z}^m$'s for $m < n$ in very specific ways. Let us illustrate the results we are about to prove using co-rank two multiplicative sublattices in $\mathbb{Z}^4$.

Define four maps $\mathbb{Z}^2 \to \mathbb{Z}^4$ by the following formulae:

$$f_1(x, y) = (x, y, 0, 0),$$
$$f_2(x, y) = (x, y, y, 0),$$
$$f_3(x, y) = (x, y, y, y),$$
$$f_4(x, y) = (x, x, y, y).$$

We can make more maps $\mathbb{Z}^2 \to \mathbb{Z}^4$ by considering maps of the form $\tau \circ f_j \circ \sigma$ for $\sigma \in S_2, \tau \in S_4$ — we call these maps *acceptable*. For example, the map that sends (x, y) to $(y, x, 0, x)$ is acceptable. A consequence of our rigidity result is that if L is a multiplicative sublattice of co-rank two in $\mathbb{Z}^4$, then there is a multiplicative sublattice L' of full rank in $\mathbb{Z}^2$ such that $L = f(L')$ for some acceptable map f. Furthermore, the size of the torsion subgroup of $\mathbb{Z}^4/L$ is equal to the index of L' in $\mathbb{Z}^2$. We will see that the scenario described here is completely general.

One can also consider a variation of Theorem 1.2 for number fields. Let L be a number field of degree n and fix a positive integer $k \leq n$. We are interested in understanding $\mathcal{R}_L(r; k)$ which we define to be the set of subrings R with identity of $\mathbb{Z}$-co-rank k in $\mathcal{O}_L$ such that $\#(\mathcal{O}_L/R)_{tor} = r$.

Then we have the following theorem:

Theorem 1.3. *If $(n-k) \nmid n$, $\mathcal{R}_L(r; k) = \varnothing$. If $(n-k) \mid n$,*

$$\mathcal{R}_L(r; k) = \bigsqcup_K \mathcal{R}_K(r; 0)$$

where the disjoint union is over subfields K of L of degree $n-k$.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

Note that if $K/\mathbb{Q}$ is a degree $n-k$ extension, $\mathcal{R}_K(r;0)$ is the finite set of full rank orders R in K such that $\#(\mathcal{O}_K/R)=r$. We set $N_L(r;k)=\#\mathcal{R}_L(r;k)$. If $k=0$, we write $N_L(r)$ instead of $N_L(r;0)$. Then the theorem implies

$$N_L(r;k)=\sum_K N_K(r),$$

where the sum is over subfields K of L of degree $n-k$.

For example, if we let n_2 be the number of quadratic subfields of L, then for all $r\in\mathbb{N}$, there are precisely n_2 rank 2 subrings R with identity in L such that $\#(\mathcal{O}_L/R)_{tor}=r$. In particular,

$$\sum_R \frac{1}{\#(\mathcal{O}_L/R)^s_{tor}}=n_2\cdot\zeta(s),$$

where the summation is over all $\mathbb{Z}$-rank 2 subrings with identity in L.

Theorem 1.2 was discovered thanks to the Online Encyclopedia of Integer Sequences (OEIS). We computed a few values of the function $\left\{ {n \atop k} \right\}$ by hand and then a search through OEIS revealed the connection to the Stirling Numbers of the Second Kind. These numbers appear under sequence A008277 in the Encyclopedia [11].

This paper is organized as follows. In Section 2 we review basic definitions and prove the rigidity theorem. We prove the main theorem in Section 3. The last section includes the proof of Theorem 1.3.

2. Rigidity Theorem

A *lattice* is a $\mathbb{Z}$-submodule of some $\mathbb{Z}^n$. When referring to a specific $\mathbb{Z}^n$ we usually speak of a *sublattice*. We call a sublattice L of $\mathbb{Z}^n$ a *multiplicative sublattice* if for every $u,v\in L$ we have $u\cdot v\in L$. A multiplicative sublattice L is a subring if it contains the identity element $(1,\dots,1)$. We refer the reader to Liu [8] for basic properties of multiplicative lattices of full rank in $\mathbb{Z}^n$.

Let L be a lattice of rank m in $\mathbb{Z}^n$. We define the *co-rank* of L to be the integer $n-m$. The following lemma is an easy consequence of row operations.

Lemma 2.1. *Given a lattice L in $\mathbb{Z}^n$ of co-rank k there is an $(n-k)\times n$ integral matrix $M=(x_{ij})$ such that $x_{ij}=0$ whenever $j-i>k$, and with the property that the rows of M generate L.*

Note that the matrix M as in the lemma is not unique. In fact, if A is any $(n-k)\times(n-k)$ lower triangular integral matrix with determinant 1, then AM is another matrix that satisfies the conditions of the lemma.

Let M be a matrix corresponding to the lattice L of co-rank k as in Lemma 2.1. Then L is multiplicative if and only if for every two rows v,w of M, $v\cdot w\in L$.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

Proposition 2.2. *Let L be a multiplicative sublattice of $\mathbb{Z}^n$ of co-rank 1. Then L has a basis which forms the rows of a $(n-1)\times n$ matrix M such that $M_{ij}=0$ if $i<j-1$ and M has a column of zeros or two columns of M are identical.*

Proof. We prove this using induction on n. If $n=1$ then there is no sublattice of co-rank 1 so the result is vacuously true. So we consider the case $n=2$. Any multiplicative sublattice L of co-rank 1 has rank 1 and therefore is generated by a non-zero row vector of length 2,

$$M=\begin{bmatrix} x_{11} & x_{12}\end{bmatrix}.$$

As L is multiplicative, $M\cdot M$ should be a scalar multiple of M. Hence we get the following equations:

$$x_{11}^2=\lambda x_{11} \tag{2.1a}$$

$$x_{12}^2=\lambda x_{12} \tag{2.1b}$$

where $\lambda\in\mathbb{Z}$. Note that both x_{11} and x_{12} can't simultaneously be zero. If either of them are zero we get a zero column as desired and if both are non-zero we get that $x_{11}=\lambda=x_{12}$ and in that case both columns are identical.

Now we assume that the result holds for $n=k$ and show that it is true for $n=k+1$ Let L be a multiplicative sublattice of $\mathbb{Z}^{k+1}$ of co-rank 1. Then L has a basis which forms the rows of a matrix $M=(x_{ij})$ such that $x_{ij}=0$ for $i<j-1$. Now M can be written as

$$M=\begin{bmatrix} M' & 0\\ v & x_{k,k+1}\end{bmatrix}.$$

Let R_i denote the i^{th} row of M. If $x_{k,k+1}=0$ then we have a column of zeros and we have nothing to prove. So from here on we assume that $x_{k,k+1}\neq 0$. Clearly M' represents a multiplicative sublattice of $\mathbb{Z}^k$. By the induction hypothesis M' has a column of zeros or a pair of identical columns.

Case 1 : M' has a column of zeros.

Suppose the j^{th} column of M' is 0. If $x_{k,j}=0$ we are done. So we assume that $x_{k,j}\neq 0$. Consider the product of the bottom row R_k of M with itself. Write

$$R_k^2=\sum_{m=1}^{k}\lambda_m R_m.$$

So we have the following equations.

$$x_{k,k+1}^2=\lambda_k x_{k,k+1} \tag{2.2a}$$

$$x_{k,j}^2=\lambda_k x_{k,j} \tag{2.2b}$$

As $x_{i,j}=0$ for $i\neq k$. Since both $x_{k,k+1}$ and $x_{k,j}$ are non-zero we have $x_{k,j}=\lambda_k=x_{k,k+1}$ which implies that the j^{th} and $(k+1)^{\text{st}}$ columns are identical as all other entries are 0.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

Case 2 : M' has a pair of identical columns.

Let the i^{th} and j^{th} columns of M' be equal. We can assume that these are non-zero columns as the first case already deals with zero columns. Therefore there is $l < k$ such that $x_{l,i} = x_{l,j} \neq 0$. Now

$$R_l \cdot R_k = \sum_{m=1}^{k} \gamma_m R_m$$

So we have

$$x_{k,i}x_{l,i} = \sum_{m=1}^{k} \gamma_m x_{m,i} \tag{2.3a}$$

$$x_{k,j}x_{l,j} = \sum_{m=1}^{k} \gamma_m x_{m,j} \tag{2.3b}$$

$$0 = \gamma_k x_{k,k+1} \tag{2.3c}$$

$\gamma_k = 0$ as $x_{k,k+1} \neq 0$. This and the fact that $x_{m,i} = x_{m,j}$ for $m < k$ gives us that each term in the summations in (3a) and (3b) are equal which implies that the sums are equal. Therefore we have that in fact $x_{k,i}x_{l,i} = x_{k,j}x_{l,j}$. Since $x_{l,i} = x_{l,j} \neq 0$ we have $x_{k,i} = x_{k,j}$. So that the i^{th} and j^{th} columns of M are identical.

□

Corollary 2.3. *Any basis of a multiplicative lattice L of co-rank 1 will form the rows of an $(n-1)\times n$ matrix M with $n-1$ distinct non-zero columns.*

Proof. The property of having a column of zeros or two identical columns is invariant under elementary row operations. This means that any matrix whose rows are the basis of a multiplicative sublattice of co-rank 1 of $\mathbb{Z}^n$ will have this property. □

Theorem 2.4 (Rigidity)**.** *Let L be a multiplicative sublattice of $\mathbb{Z}^n$ of co-rank k, then every basis of L forms the rows of a $(n-k)\times n$ matrix M with exactly $n-k$ distinct non-zero columns.*

Proof. The matrix M has column rank $n-k$. Let's say the first $n-k$ columns are linearly independent, and hence, distinct and nonzero. Let $M^{(i)}$ be the $(n-k)\times(n-k+1)$-dimensional matrix obtained by appending the i^{th} column of M to the first $n-k$ columns of M. Since the rows $M^{(i)}$ generate a multiplicative sublattice of $\mathbb{Z}^{n-k+1}$ of corank 1, the previous corollary implies that $M^{(i)}$ has exactly $n-k$ distinct nonzero columns. Hence the i^{th} column of M must be equal to one of the first $n-k$ columns or 0. Since this is true for all $i, n-k < i \leq n$, we conclude that the full matrix has exactly $n-k$ distinct nonzero columns. □

3. Proof of Theorem 1.2

We begin with a definition.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

Definition 3.1. *An injective map*

$$g : \mathbb{Z}^n \to \mathbb{Z}^{n+k}$$

of the form $g(x_1, \ldots, x_n) = (y_1, y_2, \ldots, y_{n+k})$ *with each* y_j *either equal to some* x_i *or* 0 *is called* acceptable.

Theorem 2.4 can be formulated as follows:

Theorem 3.2. *Any multiplicative sublattice of co-rank* k *in* $\mathbb{Z}^{n+k}$ *is of the form* $g(L)$ *where* $g : \mathbb{Z}^n \to \mathbb{Z}^{n+k}$ *is an acceptable map and* L *is a multiplicative sublattice of full rank in* $\mathbb{Z}^n$.

The next observation is simple but essential for what follows. In the proof we refer to the Smith Normal Form (SNF) of the lattice L to be the diagonal matrix corresponding to the SNF of any matrix M whose rows generate L.

Lemma 3.3. *For any acceptable map* g *and any sublattice* L *in* $\mathbb{Z}^n$ *of rank* n, *we have*

$$\#(\mathbb{Z}^{n+k}/g(L))_{\text{tor}} = [\mathbb{Z}^n : L].$$

Proof. Let the Smith Normal form of the lattice L be D. Then $[\mathbb{Z}^n : L] = \text{Det(D)}$ .It follows from the definition of an acceptable map that the Smith Normal Form of $g(L)$ is

$$\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

So that $\#(\mathbb{Z}^{n+k}/g(L))_{\text{tor}} = [\mathbb{Z}^n : L]$. □

Two acceptable maps $g_1, g_2 : \mathbb{Z}^n \to \mathbb{Z}^{n+k}$ are called *equivalent* if there is a permutation $\tau \in S_n$ such that $g_1 = g_2 \circ \tau$. We next describe a complete set of representatives for this equivalence relation.

Let $g : \mathbb{Z}^n \to \mathbb{Z}^{n+k}$ be an acceptable map and $\{f_i\}$ the standard basis for $\mathbb{Z}^{n+k}$. By definition of acceptable we can write

$$g(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \left(\sum_{j \in A_i^g} f_j \right).$$

for a collection of subsets $\{A_1^g, \ldots, A_n^g\}$ of $\{1, \ldots, n+k\}$. In fact, if we define $A_0^g = \{0, \ldots, n+k\} \setminus \bigcup_{i=1}^n A_i^g$, then since each acceptable map is injective, A_i^g is non empty for each i and $\mathcal{P}^g := \{A_0^g, \ldots, A_n^g\}$ is a partition of $\{0, \ldots, n+k\}$. We will call an acceptable function g *ordered* if $\min A_i^g < \min A_j^g$ whenever $i < j$. Given an arbitrary acceptable map g there exists exactly one permutation $\tau \in S_n$ for which $g \circ \tau$ is ordered. That is,

Lemma 3.4. *The set of ordered acceptable maps is a set of representatives for the equivalence classes of acceptable maps* $\mathbb{Z}^n \to \mathbb{Z}^{n+k}$ *under the action of* S_n.

Going in the other direction, to a set partition $\mathcal{P}$ of $\{0, \ldots, n+k\}$ into $n+1$ parts, we may associate an ordered acceptable map $g_{\mathcal{P}}$ as follows. Begin by ordering $\mathcal{P} = \{A_0, A_1, ..., A_n\}$ in the

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

following way: if $i < j$ then $\min(A_i) < \min(A_j)$. In particular, $0 \in A_0$. Define

$$g_{\mathcal{P}}(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i \left(\sum_{j \in A_i} f_j \right).$$

For example $\{\{0,3,4\},\{1,5\},\{2,7,8\},\{6\}\}$ corresponds to the map from $\mathbb{Z}^3$ to $\mathbb{Z}^8$ which sends

$$(a,b,c) \mapsto (a,b,0,0,a,c,b,b),$$

i.e., 0 is in the 3 and 4 spot, 'a' in the 1 and 5 entries, 'b' in the 2, 7 and 8 entries and 'c' in the 6 th entry.

It is clear that the maps $g \mapsto \mathcal{P}^g$ and $\mathcal{P} \mapsto g_P$ are inverse to one another and provide a bijection between ordered acceptable maps $\mathbb{Z}^n \to \mathbb{Z}^{n+k}$ and set partitions of $\{0, \dots, n+k\}$ into $n+1$ parts. This and the definition of Stirling numbers of the second kind lead to the next corollary:

Corollary 3.5. *The number of equivalence classes of acceptable maps $\mathbb{Z}^n \to \mathbb{Z}^{n+k}$ is equal to $\left\{ {n+k+1 \atop n+1} \right\}$.*

The final step in the proof of Theorem 1.2 is a refinement of Theorem 3.2.

Proposition 3.6. *Any multiplicative sublattice of co-rank k in $\mathbb{Z}^{n+k}$ is of the form $g(L)$ where $g : \mathbb{Z}^n \to \mathbb{Z}^{n+k}$ is an ordered acceptable map and L is a multiplicative sublattice of full rank in $\mathbb{Z}^n$. Moreover, such g and L are uniquely determined.*

Proof. A consequence of Theorem 2.4 is that any multiplicative sublattice L' of co-rank k in $\mathbb{Z}^{n+k}$ will correspond to some partition $\mathcal{P}$ of $\{0,1,...n+k\}$ into $n+1$ parts. This partition is obtained by the same method that associated a partition to an acceptable map. The partition $\mathcal{P}$ corresponds to a unique ordered acceptable map $f_{\mathcal{P}}$. The lattice L' is clearly in the range of $f_{\mathcal{P}}$ so ${f_{\mathcal{P}}}^{-1}(L')$ is the unique lattice L in $\mathbb{Z}^n$ which maps to L' under $f_{\mathcal{P}}$. □

Proof of Theorem 1.2. Combine Proposition 3.6 with Corollary 3.5. □

4. Proof of Theorem 1.3

Recall the notation from the introduction. Let L be a number field of degree n and we fix a positive integer $k \leq n$. We define $\mathcal{R}_L(r;k)$ to be the set of subrings R with identity of $\mathbb{Z}$-co-rank k in $\mathcal{O}_L$ such that $\#(\mathcal{O}_L/R)_{tor} = r$.

Suppose $\mathcal{R}_L(r;k) \neq \varnothing$, and let $R \in \mathcal{R}_L(r;k)$. Let $K = \mathbb{Q}(R)$ be the subfield of L generated by R. By [10, Section 2.1, Theorem 1], $R \subset \mathcal{O}_K$.

Lemma 4.1. *We have $[K : \mathbb{Q}] = n - k$.*

Proof. Let $\alpha_1, \dots, \alpha_{n-k}$ be a $\mathbb{Z}$-basis of R. It is easy to see that $\alpha_1, \dots, \alpha_{n-k}$ are $\mathbb{Q}$-linearly independent. We will show that K is equal to $\mathbb{Q}$-subspace of L spanned by $\alpha_1, \dots, \alpha_{n-k}$, denote this latter vector space by $\mathbb{Q}R$. It is clear that $\mathbb{Q}R$ is closed under addition and multiplication. We

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

just need to show that it is closed under inversion. Let $z \in \mathbb{Q}R$. Then there is an integer m such that $x = mz \in R$. It is sufficient to show that $x^{-1} \in \mathbb{Q}R$. Since x is algebraic over $\mathbb{Q}$, there are rational numbers $c_0, \dots, c_l$ such that $x^{-1} = c_0 + c_1 x + \cdots + c_l x^l$, but this latter expression is in $\mathbb{Q}R$ because $1, x, \dots, x^l \in R$. □

As a result, since $\mathbb{Q} \subset K \subset L$, $(n-k) \mid n$. In particular, if $(n-k) \nmid n$, then $\mathcal{R}_L(r;k) = \varnothing$. This means that R is a $\mathbb{Z}$-module of full rank in $\mathcal{O}_K$, and by the classification theorem of finitely generated modules over a PID, $\mathcal{O}_K/R$ is finite. Our next goal is to prove that $\#(\mathcal{O}_L/R)_{tor} = \#(\mathcal{O}_K/R)$. We need a lemma:

Lemma 4.2. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of S-modules, with S some commutative ring with identity. Assume $C_{tor} = 0$. Then $A_{tor} \simeq B_{tor}$.*

Proof. Let $f : A \to B$ and $g : B \to C$ be the relevant maps. Clearly, since f injective, f injects A_{tor} into B_{tor}. We need to show f maps A_{tor} onto B_{tor}. Let $x \in B_{tor}$. Then $g(x) \in C_{tor} = \{0\}$. So $x \in \ker g = \mathrm{im} f$. Hence there is $y \in A$ such that $x = f(y)$. Since $x \in B_{tor}$, there is a non-zero $s \in S$ such that $sx = 0$. Consequently, $0 = sx = sf(y) = f(sy)$. Since f is injective and $f(sy) = 0$, we conclude that $sy = 0$ and as a result $y \in A_{tor}$. □

We apply this lemma in the following fashion: We have an exact sequence

$$0 \to \mathcal{O}_K/R \to \mathcal{O}_L/R \to \mathcal{O}_L/\mathcal{O}_K \to 0.$$

We claim $(\mathcal{O}_L/\mathcal{O}_K)_{tor}$ considered as a $\mathbb{Z}$-module is trivial. Let $z \in \mathcal{O}_L$ represent a torsion element in $(\mathcal{O}_L/\mathcal{O}_K)_{tor}$. This means there is a non-zero $m \in \mathbb{Z}$ such that $mz \in \mathcal{O}_K$. This means $z \in K$, but $z \in \mathcal{O}_L$, so $z \in K \cap \mathcal{O}_L = \mathcal{O}_K$. The lemma implies

$$\#(\mathcal{O}_L/R)_{tor} = \#(\mathcal{O}_K/R)_{tor} = \#(\mathcal{O}_K/R).$$

The theorem is now immediate.

Acknowledgments

The second named author is partially supported by NSF DMS 1601289. The third author wishes to thank the Simons Foundation for partial support of his work through a Collaboration Grant. The authors wish to thank Nathan Kaplan for helpful conversations and Samit Dasgupta for a crucial comment that was used in Section 4. We also wish to thank the referee for a careful reading of the manuscript and making numerous comments that led various improvements of the paper and also for suggesting that we consider the case of number fields.

References

[1] S. Atanasov, N. Kaplan, B. Krakoff and J. Menzel, Counting finite index subrings of $\mathbb{Z}^n$, arXive-printsarXiv: 1609.06433.

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020

[2] K. P. Bogart, Introductory Combinatorics Third edition, Harcourt/Academic Press, San Diego, CA, 2000. xx+654 pp. ISBN: 0-12-110830-9.

[3] J. F. Brakenhoff, Counting problems for number rings, Doctoral thesis, Leiden University, 2009.

[4] B. Datskovsky and D. J. Wright, The adelic zeta function associated to the space of binary cubic forms. II. Local theory, *J. Reine Angew. Math.* **367** (1986) 27–75.

[5] F. J. Grunewald, D. Segal and G. C. Smith, Subgroups of finite index in nilpotent groups, *Invent. Math.* **93** (1988), no. 1, 185–223.

[6] K. Isham, Lower bounds for the number of subrings in $\mathbb{Z}^n$, arXive-printsarXiv:2010.09123.

[7] N. Kaplan, J. Marcinek, and R. Takloo-Bighash, Distribution of orders in number fields, *Res. Math. Sci.* 2 (2015), Art. 6, 57 pp.

[8] R. I. Liu, Counting subrings of $\mathbb{Z}^n$ of index k , *J. Combin. Theory Ser. A* **114** (2007), no. 2, 278–299.

[9] J. Nakagawa, Orders of a quartic field, *Mem. Amer. Math. Soc.* **122** (1996), no. 583, viii+75 pp.

[10] P. Samuel, Algebraic Theory of Numbers, Houghton Mifflin Co., Boston, Mass. 1970.

[11] Stirling Numbers of the Second Kind, the Online Encyclopedia of Integer Sequences, available at https://oeis.org/A008277

Sarthak Chimni

Department of Mathematics, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 S Morgan St (M/C 249), Chicago, IL 60607.

Email: schimn2@uic.edu

Gautam Chinta

Department of Mathematics, The City College of New York, New York, NY 10031.

Email: gchinta@ccny.cuny.edu

Ramin Takloo-Bighash

Department of Mathematics, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 S Morgan St (M/C 249), Chicago, IL 60607.

Email: rtakloo@uic.edu

DOI: https://dx.doi.org/10.30504/jims.2020.238412.1020