

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

SARTHAK CHIMNI AND RAMIN TAKLOO-BIGHASH

ABSTRACT. In this paper we study subrings of \mathbb{Z}^{n+k} of co-rank k .

1. INTRODUCTION

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

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

and

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

Under these operations \mathbb{Z}^n is a ring. 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 an identity such that, as an additive subgroup, R has index r in \mathbb{Z}^n . Necessarily then, R is a free \mathbb{Z} -module of rank n . Liu [4] investigated the function $f_n(r)$ and proved a number of interesting theorems. He also found a formula for $F_n(s) := \sum_{r=1}^{\infty} f_n(r)r^{-s}$ for $n \leq 4$ expressing it as an Euler product of rational function of p^{-s} for various primes p . Using different methods Nakagawa [5] had previously studied the more general problem of understanding the distribution of orders in quartic algebras, a particular case of which was the computation of the generating series $F_4(s)$. For $n > 4$ the situation is considerably more complicated. Kaplan, Marcinek, and Takloo-Bighash [3], by using the methods of p -adic integration, obtained results for the location and order of the largest pole of $F_5(s)$ without explicitly computing the series. They also obtained estimates for the location of the largest 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 [2] 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 $b(n) \in \mathbb{N}$. The current state of knowledge about the behavior of $N_n(B)$ is the following result:

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

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

As mentioned above $f_n(r)$ counts full rank \mathbb{Z} -submodules of \mathbb{Z}^n that are of a fixed 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 sublattices of \mathbb{Z}^n which are closed under the multiplication of \mathbb{Z}^n . It's a well-known fact (e.g., Proposition 2.3 of [4]) 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 [2] 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.

Theorem 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.

This theorem is the combination of Theorem 21 and Theorem 22. The main step in the proof of this theorem is a rigidity result (Theorem 6) 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. The Stirling numbers in the statement of the theorem appear in a fairly round-about way. It would be desirable to have an explanation for the appearance of these Stirling numbers.

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 $\mathbb{Z}^2 \rightarrow \mathbb{Z}^4$ 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 $\mathbb{Z}^2 \rightarrow \mathbb{Z}^4$ 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.

Theorem 22 was discovered thanks to the Online Encyclopedia of Integer Sequences (OEIS). Originally we had only discovered Theorem 21. We computed a few values of the function $\sigma(n, k)$ 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 [6].

The second author wishes to thank the Simons Foundation for partial support of his work through a Collaboration Grant. The authors also wish to thank Nathan Kaplan and Gautam Chinta for helpful conversations.

This paper is organized as follows. In §2 we review basic definitions and prove the rigidity theorem. We present the proof of the main theorem in §3. Finally in the appendix we collect some basic results on Stirling numbers of the second kind that are used in §3.3.

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 [4] 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 3. *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 the matrix corresponding to the lattice L of co-rank k as in Lemma 3. Then L is multiplicative if and only if for every two rows v, w of M , $v \cdot w \in L$.

Proposition 4. *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:

$$x_{11}^2 = \lambda x_{11} \tag{1a}$$

$$x_{12}^2 = \lambda x_{12} \tag{1b}$$

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

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

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 $x_{k,k+1} \neq 0$. We claim that M' represents a multiplicative sublattice of \mathbb{Z}^k . Consider the dot product of the i th and j th rows R_i and R_j where $i, j < k$ but are not necessarily distinct,

$$R_i \cdot R_j = \sum_{m=1}^{m=k} \lambda_m R_m.$$

Then the equation corresponding to the last columns is $0 = \lambda_k x_{k,k+1}$. Since $x_{k,k+1} \neq 0$, $\lambda_k = 0$. So $R_i \cdot R_j$ is a linear combination of the first $k-1$ rows and therefore M' represents a multiplicative lattice. Then 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 $x_{k,j} \neq 0$. Now consider the dot product of the k th row R_k of M with itself. Then

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

So we have the following equations.

$$x_{k,k+1}^2 = \lambda_k x_{k,k+1} \quad (2a)$$

$$x_{k,j}^2 = \lambda_k x_{k,j} \quad (2b)$$

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 $(k+1)$ st columns are identical as all other entries are 0.

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

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

So we have

$$x_{k,i} x_{l,i} = \sum_{m=1}^{m=k} \gamma_m x_{m,i} \quad (3a)$$

$$x_{k,j} x_{l,j} = \sum_{m=1}^{m=k} \gamma_m x_{m,j} \quad (3b)$$

$$0 = \gamma_k x_{k,k+1} \quad (3c)$$

$\gamma_k = 0$ 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 5. *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. \square

Theorem 6 (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. We use induction on the ordered pair (n, k) where L is a multiplicative sublattice of co-rank k in \mathbb{Z}^n . Proposition 4 takes care of the $k = 1$ case for all n . There is nothing to prove in the case that $n = 1$. That establishes the base case. Suppose the result holds for all ordered pairs (k, l) such that $k + l < n + m + 2$. Consider a sublattice L of \mathbb{Z}^{n+1} of co-rank $m + 1$. Then L has a basis which forms the rows of a matrix M such that $M_{ij} = 0$ when $i < j - m - 1$.

Case 1 : The $(n + 1)$ st column $C_{n+1} = 0$.

In this case the first n columns of M represent a multiplicative lattice L' of co-rank m in \mathbb{Z}^n . By induction hypothesis there are $n - m$ distinct non-zero columns amongst the first n columns of M . So that M also has $n - m$ distinct non-zero columns.

Case 2 : $x_{n-m, n+1} \neq 0$.

Now M can be written as

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

where M' corresponds to a multiplicative sublattice of \mathbb{Z}^n .

Lemma 7. *If the j th column of M' , $C'_j = 0$ then either the corresponding column of M is 0 or equal to the $(n + 1)$ st column of M .*

Lemma 8. *If two columns $C'_i = C'_j$ of M' are equal then the corresponding columns of M are identical.*

The proofs of Lemmas 7 and 8 are identical to the arguments in Cases 1 and 2 of Proposition 4.

Now M' corresponds to a multiplicative sublattice of co-rank $m + 1$ in \mathbb{Z}^n . By induction hypothesis M' has $n - (m + 1) = n - m - 1$ distinct non-zero columns. Lemma 8 implies that the $n - m - 1$ distinct non-zero

columns of M' correspond to $n - m - 1$ distinct non-zero columns of M . Lemma 7 says that the $(n + 1)$ st column of M is the only other distinct non-zero column. Therefore M has $n - m - 1 + 1 = (n + 1) - (m + 1)$ distinct non-zero columns. The number of distinct non-zero columns is invariant under row operations and hence we get the result. \square

3. SUBLATTICE CORRESPONDENCE

3.1. Acceptable maps. Here we look at maps

$$f : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$$

such that if we write $f(x_1, \dots, x_n) = (y_1, y_2, \dots, y_{n+k})$, then each y_j is either some x_i or 0. We call a map like this acceptable if it is injective. We call an acceptable map simple if it is of the form

$$(x_1, x_2, \dots, x_n) \mapsto (\overbrace{x_1, \dots, x_1}^{\lambda_1}, \overbrace{x_2, \dots, x_2}^{\lambda_2}, \dots, \overbrace{x_n, \dots, x_n}^{\lambda_n}, \overbrace{0, \dots, 0}^{\lambda_{n+1}})$$

with

$$1 \leq \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n.$$

For a map defined this way, we call $\underline{\lambda} = (\lambda_1, \dots, \lambda_{n+1})$ the signature of f and denote it by $\text{sign}(f)$. For a signature $\underline{\lambda}$, we define $\text{Aut}(\underline{\lambda})$ to be the group of $\tau \in S_n$ such that $\tau(\lambda_1, \dots, \lambda_n) = (\lambda_1, \dots, \lambda_n)$. In general, there are numbers $1 \leq \eta_1 < \dots < \eta_r$ and multiplicities n_1, \dots, n_r such that

$$(\lambda_1, \dots, \lambda_n) = (\overbrace{\eta_1, \dots, \eta_1}^{n_1}, \overbrace{\eta_2, \dots, \eta_2}^{n_2}, \dots, \overbrace{\eta_r, \dots, \eta_r}^{n_r}).$$

Then $\text{Aut}(\underline{\lambda}) = S_{n_1} \times S_{n_2} \times \dots \times S_{n_r}$, and

$$\# \text{Aut}(\underline{\lambda}) = n_1! n_2! \dots n_r!.$$

Here is a simple lemma:

Lemma 9. *Any acceptable map g can be written as a composite*

$$g = \sigma \circ f \circ \tau$$

with f simple, $\tau \in S_n$, and $\sigma \in S_{n+k}$.

We define $\text{sign}(g) = \text{sign}(f)$.

3.2. Images of sublattices under acceptable maps. In this subsection we study the behavior of general lattices in \mathbb{Z}^n under acceptable maps $\mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$.

The group S_n acts on \mathbb{Z}^n by permuting the coordinates. For any sublattice L of \mathbb{Z}^n , let $[L]$ denote the orbit of L under the action of S_n and let $\text{Aut}(L)$ denote the stabilizer, i.e., $\text{Aut}(L) = \{\sigma \in S_n \mid \sigma(L) = L\}$. Then clearly,

$$|[L]| = \frac{n!}{|\text{Aut}(L)|}. \quad (4)$$

Now observe that if $L \sim L'$ then

$$\bigcup_g g(L) = \bigcup_g g(L')$$

where the union is over all acceptable maps $g : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$. This follows from the fact that if $L' = \tau(L)$ for some $\tau \in S_n$, then $\sigma(f(\alpha(L))) = \sigma f(\alpha(\tau^{-1}(L')))$.

Lemma 10. *Let f be a simple map of signature $\underline{\lambda}$. Then f induces an injective homomorphism $\bar{f} : S_n \rightarrow \text{Hom}(f(\mathbb{Z}^n), \bar{f}(\mathbb{Z}^n))$ where $\alpha \rightarrow \alpha_f = f \circ \alpha \circ f^{-1}$. Furthermore, $\alpha_f \in S_{n+k}$ if and only if $\alpha \in \text{Aut}(\underline{\lambda})$.*

Lemma 11. *For lattices L, L' , if $\sigma(f(\tau(L))) = \sigma'(f'(\tau'(L')))$ with f, f' simple, then*

- $f = f'$;
- $\sigma'^{-1} \circ \sigma \in S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}} \times \bar{f}(\text{Aut}(\underline{\lambda}))$;
- $L \sim L'$.

Proof. Let $\sigma'^{-1} \circ \sigma = \gamma$. Then we have that $\gamma(f(\tau(L))) = f'(\tau'(L'))$. If the signature of f' is $\underline{\lambda}'$ then this is a partition of the coordinates of $f'(\tau'(L'))$, thus also a partition of the coordinates of $\gamma(f(\tau(L)))$. Since a permutation doesn't alter the partition, this implies that $\text{sign}(f) = \text{sign}(f')$, therefore $f = f'$. So we have that $\gamma(f(\tau(L))) = f(\tau'(L'))$. Let $\text{sign}(f) = \underline{\lambda}$. Note that γ preserves f i.e the first λ_1 coordinates of both sides are equal, the next λ_2 coordinates are equal and so on. This forces γ to be either be a composition of permutations of groups of λ_j coordinates and permutations that swap two groups of coordinates λ_i, λ_j where $\lambda_i = \lambda_j$. That is γ is in the subgroup of S_{n+k} generated by $S_{\lambda_1}, S_{\lambda_2}, \dots, S_{\lambda_n}$ and $\bar{f}(\text{Aut}(\underline{\lambda}))$. Note that these subgroups are pairwise disjoint and that they commute with each other. So we have that $\gamma \in S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}} \times \bar{f}(\text{Aut}(\underline{\lambda}))$. In fact we can write $\gamma = \gamma_1 \circ \gamma_2$ where $\gamma_1 \in \bar{f}(\text{Aut}(\underline{\lambda}))$ and $\gamma_2 \in S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}}$. Observe that γ_2 preserves $f(\tau(L))$ so that $\gamma(f(\tau(L))) = \gamma_1(f(\tau(L)))$. But $\gamma_1 = \alpha_f$ for some $\alpha \in \text{Aut}(\underline{\lambda})$ so that $f(\alpha(L)) = \gamma(f(\tau(L))) = f(\tau'(L'))$. The function f is injective so that $\tau'^{-1}(\alpha(L)) = L'$. \square

Lemma 12. *For any sublattice of full rank L in \mathbb{Z}^n , and $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$ simple of signature λ , we have*

$$\text{Aut}(f(\tau(L))) = S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}} \times \bar{f}((\text{Aut}(\tau(L)) \cap \text{Aut}(\underline{\lambda}))).$$

Proof. Suppose $\sigma(f(\tau(L))) = f(\tau(L))$ then we have from Lemma 11 that $\sigma \in S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}} \times \bar{f}(\text{Aut}(\underline{\lambda}))$. We can write $\sigma = \sigma_1 \circ \sigma_2$ where $\sigma_1 \in \text{Aut}(\underline{\lambda})$ and $\sigma_2 \in S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}}$. Clearly $\sigma_2 \in \text{Aut}(f(\tau(L)))$ so that we have $\sigma(f(\tau(L))) = \sigma_1(f(\tau(L))) = f(\tau(L))$. Now $\sigma_1 = \alpha_f$ where $\alpha \in \text{Aut}(\underline{\lambda})$ so that $\sigma_1(f(\tau(L))) = f(\alpha(\tau(L))) = f(\tau(L))$. f is injective so that $\alpha(\tau(L)) = \tau(L)$ and therefore $\alpha \in \text{Aut}(L) \cap \text{Aut}(\underline{\lambda})$. \square

Corollary 13. $|[f(\tau(L))]| = \frac{1}{|\text{Aut}(\underline{\lambda}) \cap \text{Aut}(L)|} \binom{n+k}{\lambda_1, \lambda_2, \dots, \lambda_{n+1}}$.

Proof. This is immediate from Lemma 12 and Equation (4). \square

Corollary 14. *Let g, g' be acceptable maps and L, L' be full rank sublattices of \mathbb{Z}^n then if $[g(L)] = [g'(L)]$ then $[L] = [L']$.*

Corollary 15. $\bigcup_{g \text{ acceptable}} g([L]) = \bigcup_{g \text{ acceptable}} [g(L)]$.

Lemma 16. *Suppose $\tau(L) \neq \tau'(L)$, then $[f(\tau(L))] = [f(\tau'(L))]$ if and only if $\tau' \circ \tau^{-1} \in (\text{Aut}(\underline{\lambda}))$.*

Proof. If $\alpha = \tau' \circ \tau^{-1} \in \text{Aut}(\underline{\lambda})$ then $\alpha_f \in S_{n+k}$ and $\alpha_f(f(\tau(L))) = f(\tau'(L))$. Conversely suppose $\sigma(f(\tau(L))) = f(\tau'(L))$. Now observe that $(\tau' \circ \tau^{-1})_f(f(\tau(L))) = f(\tau'(L))$. So that $\sigma^{-1} \circ \tau' \circ \tau^{-1} \in \text{Aut}(f(\tau(L)))$. Since $\text{Aut}(f(\tau(L))) = S_{\lambda_1} \times \cdots \times S_{\lambda_{n+1}} \times \bar{f}((\text{Aut}(\tau(L)) \cap \text{Aut}(\underline{\lambda}))) \subset S_{n+k}$, we have that $(\tau' \circ \tau^{-1})_f \in S_{n+k}$ and by Lemma 10 we have that $\tau' \circ \tau^{-1} \in \text{Aut}(\underline{\lambda})$. \square

Corollary 17. *There are $\frac{n!}{|\text{Aut}(L)|} \cdot \frac{|\text{Aut}(\underline{\lambda}) \cap \text{Aut}(L)|}{|\text{Aut}(\underline{\lambda})|}$ orbits corresponding to a fixed simple map f .*

Proposition 18. *If L is a full rank sublattice of \mathbb{Z}^n , we have*

$$\left| \bigcup_{g \text{ acceptable}} g([L]) \right| = \sum_{\underline{\lambda} \text{ signature}} \frac{1}{\#\text{Aut}(\underline{\lambda})} \binom{n+k}{\lambda_1, \lambda_2, \dots, \lambda_{n+1}}.$$

Proof. This follows from Corollary 13 and Corollary 17. \square

3.3. Multiplicative sublattices. Everything we said in the last subsection applies to multiplicative sublattices. In fact, if L is a multiplicative sublattice in \mathbb{Z}^n and $\tau \in S_n$, $\tau(L)$ is a multiplicative sublattice in \mathbb{Z}^n of the same rank as L . Also, if $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$ is an acceptable map, then $f(L)$ is a multiplicative sublattice in \mathbb{Z}^{n+k} whenever L is a multiplicative sublattice in \mathbb{Z}^n .

Theorem 6 can be formulated as follows:

Theorem 19. *Any multiplicative sublattice of co-rank k in \mathbb{Z}^{n+k} is of the form $g(L)$ where $g : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n+k}$ is an acceptable map and L is a multiplicative sublattice of full rank in \mathbb{Z}^n .*

The next observation is the following simple but absolutely important fact:

Lemma 20. *For any acceptable map f and any sublattice L in \mathbb{Z}^n of rank n , we have*

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

So let's define three quantities:

$$\phi_{n+k,k}(r) = \#\{L \text{ mult. sub-lat. in } \mathbb{Z}^{n+k} \mid L \text{ co-rank } k, \#(\mathbb{Z}^{n+k}/L)_{\text{tor}} = r\};$$

$$\phi_n(r) = \#\{L \text{ mult. sub-lat. in } \mathbb{Z}^n \mid [\mathbb{Z}^n : L] = r\};$$

$$\sigma(n, k) = \sum_{\underline{\lambda} \text{ signature}} \frac{1}{\#\text{Aut}(\underline{\lambda})} \binom{n+k}{\lambda_1, \lambda_2, \dots, \lambda_{n+1}}.$$

What we have said above gives the following theorem:

Theorem 21. *For all n, k, r we have*

$$\phi_{n+k, k}(r) = \sigma(n, k) \cdot \phi_n(r).$$

Proof. This is a direct consequence of Lemma 20, Proposition 18, and Theorem 19. \square

We now express $\sigma(n, k)$ in terms of Stirling numbers of the second kind.

Theorem 22. *We have*

$$\sigma(n, k) = \left\{ \begin{matrix} n+k+1 \\ n+1 \end{matrix} \right\},$$

where the quantity on the right hand side is the Stirling number of the second kind.

Proof. Write

$$\binom{n+k}{\lambda_1, \lambda_2, \dots, \lambda_{n+1}} = \binom{n+k}{\lambda_{n+1}} \cdot \binom{n+k-\lambda_{n+1}}{\lambda_1, \lambda_2, \dots, \lambda_n}.$$

This means

$$\begin{aligned} \sigma(n, k) &= \sum_{\lambda_{n+1}=0}^k \binom{n+k}{\lambda_{n+1}} \sum_{\substack{1 \leq \lambda_1 \leq \dots \leq \lambda_n \\ \sum_i \lambda_i = n+k-\lambda_{n+1}}} \frac{1}{\#\text{Aut}(\underline{\lambda})} \binom{n+k-\lambda_{n+1}}{\lambda_1, \lambda_2, \dots, \lambda_n} \\ &= \sum_{j=n}^{n+k} \binom{n+k}{j} \sum_{\substack{1 \leq \lambda_1 \leq \dots \leq \lambda_n \\ \sum_i \lambda_i = j}} \frac{1}{\#\text{Aut}(\underline{\lambda})} \binom{j}{\lambda_1, \lambda_2, \dots, \lambda_n}. \end{aligned}$$

By Lemma 23,

$$\left\{ \begin{matrix} n+k+1 \\ n+1 \end{matrix} \right\} = \sum_{j=n}^{n+k} \binom{n+k}{j} \left\{ \begin{matrix} j \\ n \end{matrix} \right\}.$$

Consequently, in order to prove our theorem it suffices to prove that for $j \geq n$

$$\sum_{\substack{1 \leq \lambda_1 \leq \dots \leq \lambda_n \\ \sum_i \lambda_i = j}} \frac{1}{\#\text{Aut}(\underline{\lambda})} \binom{j}{\lambda_1, \lambda_2, \dots, \lambda_n} = \left\{ \begin{matrix} j \\ n \end{matrix} \right\}.$$

We now proceed to prove this identity. Suppose there are a_1 1's, a_2 2's, ..., and a_m m 's among the λ_i 's. Then $\# \text{Aut}(\underline{\lambda}) = a_1!a_2!\dots a_m!$. This means

$$\frac{1}{\# \text{Aut}(\underline{\lambda})} \binom{j}{\lambda_1, \lambda_2, \dots, \lambda_n} = \frac{j!}{(1!)^{a_1}(2!)^{a_2} \dots (m!)^{a_m} a_1!a_2!\dots a_m!}.$$

The numbers a_1, \dots, a_m will have to satisfy

$$\begin{cases} a_1 + 2a_2 + \dots + ma_m = j \\ a_1 + a_2 + \dots + a_m = n. \end{cases}$$

The result now follows from Corollary 25 in the Appendix. \square

4. APPENDIX: STIRLING NUMBERS OF THE SECOND KIND

In this appendix we collect some facts about Stirling numbers of the second kind which are used in §3.3. Recall that for natural numbers n, k , the Stirling number of the second kind $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is defined to be the number of equivalence relations on a set with n elements with k equivalence classes. Alternatively, $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is equal to the number partitions of a set with n elements to k un-ordered non-empty subsets. Bogart [1], especially Ch. 3, has a lot of good information on Stirling numbers.

Lemma 23. *For any n, k we have*

$$\left\{ \begin{smallmatrix} n+1 \\ k+1 \end{smallmatrix} \right\} = \sum_{j=k}^n \binom{n}{j} \left\{ \begin{smallmatrix} j \\ k \end{smallmatrix} \right\}.$$

Proof. Theorem 3.2, Ch. 2 of Bogart [1]. \square

Lemma 24. *The number of partitions of a set with j elements into a_1 classes of size 1, a_2 classes of size 2, up to a_m classes of size m is equal to*

$$\frac{j!}{(1!)^{a_1}(2!)^{a_2} \dots (m!)^{a_m} a_1!a_2!\dots a_m!}.$$

provided that $\sum_i ia_i = j$.

Proof. Theorem 1.6, Ch. 2 of Bogart [1]. \square

For $j \geq n$ let $S(j, n)$ be the set of sequences (a_1, \dots, a_m) of non-negative numbers of some length m such that

$$\begin{cases} a_1 + 2a_2 + \dots + ma_m = j \\ a_1 + a_2 + \dots + a_m = n. \end{cases}$$

Corollary 25. *For $j \geq n$ we have*

$$\sum_{(a_1, \dots, a_m) \in S(j, n)} \frac{j!}{(1!)^{a_1}(2!)^{a_2} \dots (m!)^{a_m} a_1!a_2!\dots a_m!} = \left\{ \begin{smallmatrix} j \\ n \end{smallmatrix} \right\}.$$

REFERENCES

- [1] Bogart, Kenneth P. Introductory combinatorics. Third edition. Harcourt/Academic Press, San Diego, CA, 2000. xx+654 pp.
- [2] Grunewald, F. J.; Segal, D.; Smith, G. C. Subgroups of finite index in nilpotent groups. *Invent. Math.* 93 (1988), no. 1, 185–223.
- [3] Kaplan, Nathan; Marcinek, Jake; Takloo-Bighash, Ramin. Distribution of orders in number fields. *Res. Math. Sci.* 2 (2015), Art. 6, 57 pp.
- [4] Liu, Ricky Ini. Counting subrings of \mathbb{Z}^n of index k . *J. Combin. Theory Ser. A* 114 (2007), no. 2, 278–299.
- [5] Nakagawa, Jin. Orders of a quartic field. *Mem. Amer. Math. Soc.* 122 (1996), no. 583, viii+75 pp.
- [6] Stirling Numbers of the Second Kind, the Online Encyclopedia of Integer Sequences, available at <https://oeis.org/A008277>

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S MORGAN ST (M/C 249), CHICAGO, IL 60607

E-mail address: sarthakchimni@gmail.com

E-mail address: rtakloo@uic.edu