JOURNAL OF NUMBER THEORY 12, 421–436 (1980)

On the Rédei Zeta Function

JOSEPH P. S. KUNG, M. RAM MURTY, AND GIAN-CARLO ROTA*

Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Communicated by H. Zassenhaus

Received April 16, 1979

Let L be a locally finite lattice. An order function ν on L is a function defined on pairs of elements x, y (with $x \leqslant y$) in L such that $\nu(x, y) = \nu(x, z)\,\nu(z, y)$. The Rédei zeta function of L is given by $\rho(s; L) = \sum_{x \in L} \mu(\hat{0}, x)\,\nu(\hat{0}, x)^{-s}$. It generalizes the following functions: the chromatic polynomial of a graph, the characteristic polynomial of a lattice, the inverse of the Dedekind zeta function of a number field, the inverse of the Weil zeta function for a variety over a finite field, Philip Hall's ϕ-function for a group and Rédei's zeta function for an abelian group. Moreover, the paradigmatic problem in all these areas can be stated in terms of the location of the zeroes of the Rédei zeta function.

1. INTRODUCTION

Banach was fond of saying that mathematics is the study of analogies between analogies; one may optimistically draw from his aphorism that in mathematics, every apparent coincidence points to an underlying cause which awaits discovery. This paper originated from precisely one such coincidence between combinatorics and number theory.

A variety of combinatorial problems can be uniformly stated as problems concerning the location of zeroes of the characteristic polynomials of partially ordered sets. More specifically, let $\mathbf{P}$ be a finite ranked partially ordered set with a maximum $\hat{1}$ and a minimum $\hat{0}$. Let r be its rank function and μ its Möbius function. The characteristic polynomial $p(\lambda)$ of $\mathbf{P}$ is defined by

$$p(\lambda) = \sum_{x \in \mathbf{P}} \mu(\hat{0}, x)\lambda^{r(\hat{1}) - r(x)}.$$

The zeroes of this polynomial are very often combinatorially significant invariants associated with the partial ordering. For example, when $\mathbf{P}$ is the

* Supported by the National Science Foundation under Grant MCS 78-02743.

0022-314X/80/030421-16$02.00/0

lattice of contractions of a graph, the characteristic polynomial turns out to be the chromatic polynomial of the graph; its values when λ is a positive integer are the number of ways of properly coloring the vertices of the graph with λ colors.

For a long time, this reformulation of the coloring problem remained an isolated curiosity. In 1970, Crapo and Rota [1, Chap. 15] observed that this problem can be recast in geometric terms, and in so doing, they found that many other combinatorial problems fitted into the same pattern. More precisely, let S be a finite set of points in n-dimensional affine space over the finite field of order q. Let $\mathbf{L}(S)$ be the lattice of flats (or linear varieties) spanned by subsets of the points of S. For x a flat in $\mathbf{L}(S)$, let $r(x)$ be the dimension of x plus one. The value of the characteristic polynomial at q^s,

$$p(q^s) = \sum_{x \in \mathbf{L}(S)} \mu(\hat{0}, x)\, q^{s(n-r(x))},$$

has the following geometric interpretation: it is the number of s-tuples $(H_1, \ldots, H_s)$ of hyperplanes whose intersection $H_1 \cap \cdots \cap H_s$ is disjoint from S. The smallest integer s for which such a sequence can be found is called the *critical exponent* of S and is a natural generalization of the chromatic number of a graph. This observation sparked a renewed interest in the projective invariant theory of sets of points, both in its classical form (generalized to fields of arbitrary characteristic) and its combinatorial form—the theory of geometric lattices, or matroids, as they have come to be called.

It was felt, nevertheless, that not even this reformulation led to the level of generality at which the nature of the difficulty can be intuited. Later, in studying the zeta function introduced by Rédei in his attempts to understand Hajós theorem on partitions of abelian groups [7, 8], Rota [10] observed that the zeroes of Rédei's zeta function can be given a simple combinatorial interpretation. This interpretation rendered all but evident Rédei's Hauptsatz and Trägheitsatz. A detailed account of this interpretation of the zeroes of the Rédei zeta function forms the main result of this paper (Theorem 10); it includes as a special case the critical problem for affine point sets.

This interpretation in turn points towards a more general framework where the zeta functions arising in combinatorics could be studied, namely, lattices of Dirichlet type. These lattices are natural generalizations of the algebras of Dirichlet type introduced in [2]. The zeta functions of number theory can be subsumed under this formalism, and the central problems in both areas concern the location of zeroes of zeta functions of lattices of Dirichlet type.

Despite this pleasing unification, we believe that the revealing level of generality has not yet been reached with lattices of Dirichlet type. The deeper properties of zeta functions, such as functional equations, can only come from structures which are not basically finite, and on such structures, the corresponding theory of Möbius inversion would require delicate limiting processes.

Unlike most other works on zeta functions, we are not concerned in this paper with the convergence properties of Rédei zeta functions—indeed, we work throughout with *formal* Dirichlet series. Nonetheless, we believe that an adequate theory of interpolation, convergence and analytic continuation of Rédei zeta functions over the complex or p-adic fields would go very far towards the solution of many critical problems in combinatorial analysis.

2. Lattices of Dirichlet Type

Let $\mathbf{L}$ be a lattice with a unique minimal element $\hat{0}$. We denote by $\wedge$ and $\vee$ the meet and join operations in $\mathbf{L}$; moreover, if A is a finite subset of $\mathbf{L}$, then $\bar{A}$ denotes the join of all the elements in A. An *order function* ν on $\mathbf{L}$ is a function defined on pairs of elements (x, y) in $\mathbf{L}$ such that $x \leqslant y$, taking values in the positive integers and satisfying the condition

$$\text{for any triple } x \leqslant z \leqslant y, \qquad \nu(x, y) = \nu(x, z)\,\nu(z, y);$$

frequently, we abbreviate $\nu(\hat{0}, x)$ to $\nu(x)$. A lattice equipped with an order function is called a *lattice of Dirichlet type.*

Now, let E be a subset of a lattice $\mathbf{L}$ of Dirichlet type. Consider the subset $\mathbf{M}(E)$ of elements in $\mathbf{L}$ which are joins of finite subsets of E. This is a join sub-semilattice of $\mathbf{L}$. Although not a sublattice of $\mathbf{L}$, $\mathbf{M}(E)$ is a lattice when considered separately from $\mathbf{L}$ (remember that $\hat{0}$, being the join of the empty set, is in $\mathbf{M}(E)$); we call $\mathbf{M}(E)$ the *lattice spanned by E*. The subset E is called a *Rédei set* if for every element x in $\mathbf{M}(E)$ and every positive integer n, the number of elements y in $\mathbf{M}(E)$ such that $\nu(x, y) = n$ is finite. In particular, any finite set is a Rédei set.

An immediate consequence is that the lattice $\mathbf{M}(E)$ spanned by a Rédei set E is a locally finite lattice: that is, every interval $[x, y] = \{z : x \leqslant z \leqslant y\}$ is a finite set. For, suppose that $\nu(x, y) = n$. Then, as $\nu(x, z)\,\nu(z, y) = n$, $\nu(x, z)$ divides n for any z in $[x, y]$. It remains to observe that there are only a finite number of positive integers k dividing n, and for each of these divisors k, only a finite number of elements z in $\mathbf{M}(E)$ with $\nu(x, z) = k$. The same method of proof yields two other results. The first is that in defining a Rédei set, it suffices only to require that for every positive integer n, the number of elements y in $\mathbf{M}(E)$ such that $\nu(\hat{0}, y) = n$ is finite. The second is that for every integer n and every element $a \in \mathbf{L}$, the number of elements y in $\mathbf{M}(E)$ such that $\nu(a, y) = n$ is finite.

Given a Rédei set E and an element a in $\mathbf{L}$, the *Rédei zeta function of E based on a* is defined by the formula

$$\rho(s; a; E) = \sum_{A} (-1)^{|A|} \nu(a, \bar{A})^{-s},$$

where the summation ranges over all finite subsets A of E whose joins $\bar{A}$ lie above the element a. By the finiteness assumption, for a given n, there are only a finite number of subsets A whose joins $\bar{A}$ have the property that $\nu(a, \bar{A}) = n$; hence, the summation on the right is well defined as a formal Dirichlet series. The Rédei zeta function based on $\hat{0}$ is simply written $\rho(s; E)$ and is called the Rédei zeta function of E. There is no loss in generality in considering only this particular case.

The Rédei zeta function $\rho(s; E)$ is determined by the collection of Rédei zeta functions $\rho(s; A)$, where A ranges over all finite subsets of E. Indeed, it is immediate from the definition that

PROPOSITION 0.

$$\rho(s; E) = \lim_{A} \rho(s; A),$$

where the limit taken over the directed system of all finite substs of E under containment, and convergence is in the algebra of formal Dirichlet series.

3. ADDITIVE AND MULTIPLICATIVE IDENTITIES

In this section, we prsent some basic properties of the Rédei zeta function. Most of our results are generalized from Rédei's paper [7].

PROPOSITION 1. *Let E be a Rédei set in* $\mathbf{L}$. *Then, if a is an element in* $\mathbf{L}$ *such that there exists an element $b \in E$ such that $a \geqslant b$, then*

$$\rho(s; E \cup \{a\}) = \rho(s; E).$$

Proof. The left-hand summation can be separated into two sums,

$$\sum_{A} (-1)^{|A|} \nu(\bar{A})^{-s} + \sum_{B} (-1)^{|B|+1} \nu(\bar{B} \vee a)^{-s}, \tag{$*$}$$

where the range of summation in both cases is over all finite subsets of E. The second sum can be further separated into two sums,

$$\sum_{C} (-1)^{|C|+1} \nu(\bar{C} \vee a)^{-s} + \sum_{C} (-1)^{|C|+2} \nu(\bar{C} \vee a \vee b)^{-s},$$

where the range of summation is now over all subsets of $E\backslash\{a\}$. But, as $a \geqslant b$, $\nu(\bar{C} \vee a) = \nu(\bar{C} \vee a \vee b)$; hence, the second sum is zero and we are done.

Thus, it suffices to consider only Rédei sets which are antichains, an *antichain* being a subset for which no two elements are comparable.

Our next identity allows us to express any zeta function as a sum of zeta functions of Rédei sets E based on an element b such that every element in E covers b in $\mathbf{M}(E)$. We use the following notation: if $E \subseteq \mathbf{L}$, then $E \vee b$ is the subset $\{a \vee b\colon a \in E\}$.

PROPOSITION 2. *Suppose $a \geqslant b$. Then, for any Rédei set E*

$$\rho(s; E \cup \{a\}) = \rho(s; E \cup \{b\}) + \nu(b)^{-s} \rho(s; b; (E \vee b) \cup \{a\}).$$

Proof. We observe that

$$\rho(s; E \cup \{a\}) - \rho(s; E \cup \{b\}) = \sum_A (-1)^{|A|} [\nu(\bar{A} \vee a)^{-s} - \nu(\bar{A} \vee b)^{-s}],$$

the summation being over all finite subsets contained in E. Now,

$$\nu(\bar{A} \vee b) = \nu(b)\, \nu(b, \overline{A \vee b})$$

and, as $b \leqslant a$,

$$\nu(\bar{A} \vee a) = \nu(b)\, \nu(b, \overline{A \vee b} \vee a).$$

Thus, we can rewrite the right-hand sum as

$$\nu(b)^{-s} \sum_A (-1)^{|A|} [\nu(b, \overline{A \vee b})^{-s} - \nu(b, \overline{A \vee b} \vee a)^{-s}];$$

but this is just

$$\nu(b)^{-s} \rho(s; b; (E \vee b) \cup \{a\}).$$

As an immediate corollary, we have

COROLLARY 3. *For any Rédei set E and any element a in E,*

$$\rho(s; E) = \rho(s; E\backslash\{a\}) + \nu(a)^{-s} \rho(s; a; (E\backslash\{a\}) \vee a).$$

Another identity, whose proof is very similar to the foregoing proofs, is

PROPOSITION 4. *Let E be a Rédei set and let $a, b \in E$. Then,*

$$\rho(s; E) = \rho(s; E\backslash\{a\}) + \rho(s; E\backslash\{b\}) - \rho(s; E\backslash\{a, b\} \cup \{a \vee b\}).$$

Next, we have the following identity relating all the zeta functions of subsets of a given Rédei set.

PROPOSITION 5. *Let E be a Rédei set. Then,*

$$\sum_A \nu(\bar{A})^{-s} \rho(s; \bar{A}; (E \backslash A) \vee \bar{A}) = 1.$$

Proof. Rewrite the left-hand summation as

$$\sum_A \nu(\bar{A})^{-s} \sum_B (-1)^{|B|} \nu(\bar{A}, \bar{B} \vee \bar{A})^{-s},$$

where the inner summation ranges over all finite subsets of $E \backslash A$. This can be further simplified to

$$\sum_A \sum_B (-1)^{|B|} \nu(\overline{A \cup B})^{-s} = \sum_C \nu(\bar{C})^{-s} \sum_{D \subseteq C} (-1)^{|D|}$$

(here C ranges over all finite subsets of E)

$$= \nu(\hat{0}) = 1,$$

which is the right-hand side.

We now consider the lattice $\mathbf{M}(E)$ as a semigroup under the binary operation of taking joins. Suppose, for the moment, that E is finite. Then, in the semigroup algebra $\mathbb{C}[\mathbf{M}(E)]$, we have the identity

$$\prod_{a \in E} (1 - a) = \sum_{A \subseteq E} (-1)^{|A|} \bar{A}.$$

Now, for a fixed s, the order function ν induces a linear functional on $\mathbb{C}[M(E)]$ in the following way: for every $x \in \mathbf{M}(E)$,

$$\nu_s(x) = \nu(x)^{-s}.$$

Applying ν_s to both sides of the identity, we obtained a weak analog of the Euler product identity,

$$\rho(s; E) = \nu_s \left(\prod_{a \in E} (1 - a) \right).$$

Unfortunately, this weak product expansion is not an actual product expansion unless ν is a *multiplicative order function relative* to E: that is, unless

$$\nu(a_1 \vee \cdots \vee a_n) = \nu(a_1) \cdots \nu(a_n)$$

for any finite subset $\{a_i\}$ of E. Note that ν need not be a homomorphism of the semigroup algebra.

PROPOSITION 6. *Let E be a (possibly infinite) Rédei set relative to which the order function ν is multiplicative. Then,*

$$\rho(s;E) = \prod_{a \in E} (1 - \nu(a)^{-s}).$$

We have already proved the proposition when E is finite; when E is infinite, we proceed by a limiting argument using Proposition 0. The details are easy and omitted.

The mystery surrounding Euler products for zeta functions accounts for the difficulties involved in both the critical problem in combinatorics [1, Chap. 15] and the theory of Artin L-series.

4. DER RÉDEISCHE HAUPTSATZ

In this section, we need some results from the theory of Möbius functions [10]. Let $\mathbf{L}$ be a finite lattice. Then, the Möbius function μ is the function defined on pairs of elements x, y in $\mathbf{L}$ as follows:

if $x \leqslant y$, then $\mu(x, y) = 0$;

if $x \leqslant y$, then μ is defined by the recursion

$$\mu(x, x) = 1,$$
$$\mu(x, y) = - \sum_{x \leqslant z < y} \mu(x, z).$$

A *cross-cut* of $\mathbf{L}$ is a subset of $\mathbf{L}$ satisfying the properties:

(a) C does not contain the minimum $\hat{0}$ or the maximum $\hat{1}$;

(b) C is an antichain;

(c) Any maximal (or saturated) chain stretched between $\hat{0}$ and $\hat{1}$ meets C.

The Möbius function $\mu(\hat{0}, \hat{1})$ can be computed from certain invariants of a cross-cut C; indeed,

$$\mu(\hat{0}, \hat{1}) = \sum_{k \geqslant 1} (-1)^k q_k, \qquad (**)$$

where q_k is the number of k-subsets of C whose join equals the maximum.

PROPOSITION 7. *Let E be a Rédei set of a lattice* $\mathbf{L}$ *of Dirichlet type. Then,*

$$\rho(s; E) = \sum_{x \in \mathbf{M}(E)} \mu(\hat{0}, x)\, v(x)^{-s},$$

where μ is the Möbius function of the lattice $\mathbf{M}(E)$ *spanned by E.*

Proof. By Proposition 1, we can delete elements from E until it is an antichain within changing its zeta function. Now, let x be in $\mathbf{M}(E)$; in the finite sublattice $[0, x]$ of $\mathbf{M}(E)$, $E \cap [0, x]$ is a cross-cut of $[0, x]$. Hence, by $(**)$,

$$\begin{aligned}
\rho(s; E) &= \sum_{A} (-1)^{|A|}\, v(\bar{A})^{-s} \\
&= \sum_{x \in \mathbf{M}(E)} \left(\sum_{\bar{A} = x} (-1)^{|A|} \right) v(x)^{-s} \\
&= \sum_{x \in \mathbf{M}(E)} \mu(\hat{0}, x)\, v(x)^{-s}.
\end{aligned}$$

This description suggests the following terminology. Suppose the lattice $\mathbf{L}$, considered as a subset of itself, is a Rédei set. Then, we define the *Rédei zeta function of the lattice* $\mathbf{L}$ by

$$\rho(s; a; \mathbf{L}) = \sum_{x \in \mathbf{L}} \mu(a, x)\, v(a, x)^{-s}.$$

If $a = \hat{0}$, we simply write $\rho(s; \mathbf{L})$. Note that $\rho(s; a; \mathbf{L})$ is usually *not* the zeta function of the Rédei set consisting of all the elements of $\mathbf{L}$.

We now generalize Rédei's main result to

THEOREM 8 (Rédei's Hauptsatz). *Suppose that* $\mathbf{L}$ *is a lattice of Dirichlet type with order function v such that* $\mathbf{L}$ *itself is a Rédei set. Let E be a Rédei set in* $\mathbf{L}$ *not containing* $\hat{0}$. *Then,*

$$\rho(s, E) = \sum_{x \in E^{\#}} v(x)^{-s}\, \rho(s; x; \mathbf{L}),$$

where

$$E^{\#} = \{x \in \mathbf{L} : x \not\geq a \ \text{ for all } a \in E\};$$

that is, $E^{\#}$ is the set of all lattice elements which do not lie above any element in E.

Our proof relies on two results relating the Möbius functions of two lattices linked by order-preserving maps. We use the following notation: μ denotes the Möbius function of $\mathbf{M}(E)$, while $\bar{\mu}$ denotes the Möbius function of $\mathbf{L}$.

Let $x \in \mathbf{L}$ and let

$$\mathbf{P}_x = \{z \in \mathbf{L}: \hat{0} \leqslant z \leqslant x\}$$

and

$$\mathbf{Q}_x = \{z \in \mathbf{M}(E): \hat{0} \leqslant z \leqslant x\}$$

These two lattices are linked by two order-preserving maps p and q, where p: $\mathbf{Q}_x \to \mathbf{P}_x$ is the inclusion map, and q: $\mathbf{P}_x \to \mathbf{Q}_x$ is defined by

$$q(y) = \bigvee \{z: z \leqslant y \text{ and } z \in \mathbf{M}(E)\}.$$

Suppose now that $x \in \mathbf{M}(E)$. Then, p and q from a Galois coconnection between $\mathbf{P}_x$ and $\mathbf{Q}_x$ such that $q(x) = x$. Using Theorem 1 in [10, p. 348], we conclude that

$$\mu(\hat{0}, x) = \sum_y \bar{\mu}(y, x),$$

the sum being over all y such that $q(y) = \hat{0}$: that is, over all y in $E^\# \cap [0, x]$ in $\mathbf{L}$. As $\mu(z, x) = 0$ if $z \notin [0, x]$, our summation may be rewritten as

$$\mu(\hat{0}, x) = \sum_{y \in E^\#} \bar{\mu}(y, x).$$

Multiplying both sides by $\nu(x)^{-s}$ and summing over all x in $\mathbf{M}(E)$, we obtain

$$\begin{aligned} \sum_{x \in \mathbf{M}(E)} \mu(0, x)\, \nu(x)^{-s} &= \sum_{x \in \mathbf{M}(E)} \sum_{y \in E^\#} \bar{\mu}(y, x)\, \nu(x)^{-s} \\ &= \sum_{y \in E^\#} \nu(y)^{-s} \sum_{x \in \mathbf{M}(E)} \bar{\mu}(y, x)\, \nu(y, x)^{-s}. \end{aligned} \tag{\dagger}$$

Now, suppose that $x \in \mathbf{L}$ but $x \notin \mathbf{M}(E)$. Then, it is no longer true that $q(x) = x$. However, q is still an order-preserving map such that the inverse image of an interval is again an interval. Moreover, the inverse image of the maximum of $\mathbf{Q}_x$ contains at least two points. Hence, by the dual version of Theorem 2 in [10, p. 348], we have

$$\sum_y \bar{\mu}(y, x) = 0,$$

the sum ranging over all $y \in \mathbf{L}$ such that $q(y) = \hat{0}$. Repeating our earlier computations, we obtain, firstly,

$$0 = \sum_{y \in E^{\#}} \bar{\mu}(y, x)$$

and secondly

$$0 = \sum_{y \in E^{\#}} \nu(y)^{-s} \sum_{x \notin \mathbf{M}(E)} \bar{\mu}(y, x)\, \nu(y, x)^{-s}.$$

Adding this to (†), we obtain

$$\rho(s, E) = \sum_{y \in E^{\#}} \nu(y)^{-s} \rho(s; y; \mathbf{L}).$$

5. Three Examples

Let K be an algebraic number field—that is, $K = \mathbb{Q}(\alpha)$ for some algebraic number α. The ring of integers $\mathcal{O}_K$ of K is the set of all numbers in K satisfying a monic polynomial with integer coefficients. The ring $\mathcal{O}_K$ is a Dedekind domain and the lattice $\mathbf{L}_K$ of its integral ideals under the order relation of *reverse* set-containment is a locally finite lattice of Dirichlet type with the order function ν

$$\nu(\mathfrak{a}, \mathfrak{b}) = N\mathfrak{a}/N\mathfrak{b},$$

where $N(\mathfrak{a})$ is the norm (over the rationals) of the ideal $\mathfrak{a}$. The norm is multiplicative in the sense of Section 4. Hence, if we take E to be the set of all prime ideals in $\mathbf{L}_K$, we have

$$\rho(s; E) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s}).$$

Thus, the Rédei zeta function is the inverse of the Dedekind zeta function of K over $\mathbb{Q}$, and

$$\rho(s; E) = \sum_{\mathfrak{a}} \mu(\mathfrak{a}) N\mathfrak{a}^{-s},$$

where $\mu(\mathfrak{a})$, the Möbius function of $\mathbf{L}_K$, is given by

$$\begin{aligned} \mu(\mathfrak{a}) &= (-1)^n && \text{if } \mathfrak{a} \text{ is the product of } n \text{ distinct prime ideals} \\ &= 0 && \text{otherwise.} \end{aligned}$$

The next example is more combinatorial. Let $\mathbf{L}$ be a finite lattice satisfying the Jordan–Dedekind chain condition, and let r be its rank function. If q is a positive integer, the function ν defined by

$$\nu(x, y) = q^{r(x,y)} = q^{r(y)-r(x)}$$

is an order function of $\mathbf{L}$. The Rédei zeta function of $\mathbf{L}$ is given by

$$\rho(s; \mathbf{L}) = \sum_{x \in \mathbf{L}} \mu(\hat{0}, x)\, q^{-sr(x)}.$$

Thus, ρ is the characteristic (or Poincaré) polynomial [10, p. 343] of $\mathbf{L}$ evaluated at q^{-s}. Thus, for the Boolean algebra $\mathbf{2}^n$,

$$\rho(s; \mathbf{2}^n) = (1 - q^{-s})^n.$$

For the lattice $\mathbf{L}_p(n)$ of all subspaces of an n-dimensional vector space over a finite field of order p,

$$\begin{aligned} \rho(s; \mathbf{L}_p(n)) &= \sum_{k=0}^{n} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_k p^{k(k-1)/2}\, q^{-sk} \\ &= \prod_{k=0}^{n} (1 - p^k q^{-s}). \end{aligned}$$

Here, the p-binomial coefficient $[{n \atop k}]_p$ is defined as the number of k-dimensional subspaces of an n-dimensional vector space over a finite field of order p.

Finally, if $\mathbf{L}$ is the bond lattice of a graph G with n vertices [10, p. 361], the Rédei zeta function is

$$q^{-ns}\chi_G(q^s),$$

where χ_G is the chromatic polynomial of the graph G.

Our third example is the zeta function of an algebraic set V over a finite field K (for details, see, for example, [5]). Recall that a *divisor* of V is a formal linear combination $m = \sum m_i \mathbf{x}_i$, where m_i are positive integers and $\mathbf{x}_i$ are points in V algebraic over K. The *degree* of m is simply the sum $\sum m_i$. A divisor is a *cycle* if it satisfies the following two additional conditions: the extension fields $K(\mathbf{x}_i)$ are all the same and is an extension of degree $\sum m_i$ over K, and the set of points $\{\mathbf{x}_i\}$ is transitive under the action of the Galois group of $K(\mathbf{x}_i)$ over K. The set of cycles of K forms a lattice $\mathbf{C}(V)$ under the order relation: if $m = \sum m_i \mathbf{x}_i$ and $n = \sum n_i \mathbf{x}_i$, then

$$m \leqslant n \qquad \text{whenever} \quad m_i \leqslant n_i \text{ for all } i.$$

This lattice is of Dirichlet type with the order function

$$\nu(m, n) = q^{-s(\deg n - \deg m)}.$$

A Rédei set in $C(V)$ is the set E of all irreducible cycles (or cycles of dimension zero). As the order function ν is multiplicative for this Rédei set, we have

$$\rho(s; E) = \prod_{m \in E} (1 - q^{-s \deg m}).$$

If we set $t = q^{-s}$, the Rédei zeta function is the inverse of the Weil zeta function of the algebraic set V.

6. Lattices of Finite Abelian Groups and the Critical Problem

A lattice $\mathbf{L}$ is said to be a *lattice of (finite) abelian groups* if the following three conditions hold:

(a) the elements of $\mathbf{L}$ are finite abelian groups and are all contained in a universal abelian group (which need not be finite, however);

(b) the meet in $\mathbf{L}$ of two groups α and β is their set-theoretic intersection $\alpha \cap \beta$, while their join is the subgroup generated by α and β within the universal group;

(c) $\mathbf{L}$ has a unique minimal element and this minimum is the trivial group.

Such a lattice is in fact a lattice of Dirichlet type, with the order function

$$\nu(\alpha, \beta) = |\beta|/|\alpha|.$$

There are two primary examples of lattices of abelian groups. Let ω be a finite abelian group; then the lattice $\mathbf{L}(\omega)$ of all its subgroups is a lattice of abelian groups. Now, let ω be an arbitrary abelian group, and $\{\alpha_i\}$ a collection of finite subgroups of ω. Then, the lattice $\mathbf{L}(\omega; \{\alpha_i\})$ consisting of all the subgroups of ω which can be generated by finite subsets of $\{\alpha_i\}$ is a lattice of abelian groups.

In this context, Theorem 8 becomes:

Proposition 9 (Rédei's Hauptsatz for abelian groups). *Let $\alpha_1, \ldots, \alpha_n$ be non-trivial subgroups of a finite abelian group ω. Then, in the lattice $\mathbf{L}(\omega)$,*

$$\rho(s; \{\alpha_i\}) = \sum_{\beta} |\beta|^{-s} \rho(s; \mathbf{L}(\omega/\beta)),$$

where the summation ranges over all subgroups β which do not contain any of the subgroups α_i, and ω/β is the quotient of ω by the subgroup β.

Over the lattice of subgroups of a finite abelian group, every Rédei zeta function can be explicitly computed. Recall that a finite abelian group ω can be decomposed into a direct sum of cyclic groups $C(p^e)$ of prime power order. If

$$\omega \cong C(p_1^{e_1}) \oplus \cdots \oplus C(p_k^{e_k}),$$

we say that it has *type* $(p_1^{e_1}, \ldots, p_k^{e_k})$. The Möbius function in $\mathbf{L}(\omega)$ depends only on the type of its arguments: indeed, for $\alpha \subseteq \beta$ in $\mathbf{L}(\omega)$, $\mu(\alpha, \beta)$ can be computed from the following facts [2]:

(a) If the quotient group β/α is an elementary abelian p-group, or more precisely, β/α is isomorphic to a direct sum of m copies of the cyclic group $C(p)$, then

$$\mu(\alpha, \beta) = (-1)^m p^{(1/2)m(m-1)};$$

(b) If β/α is any other p-group, then $\mu(\alpha, \beta) = 0$;

(c) If β/α is isomorphic to the direct sum $\gamma \oplus \delta$, where every pair of positive integers consisting of an element from type γ and an element from type δ is relatively prime, then

$$\mu(\alpha, \beta) = \mu(\hat{0}, \gamma)\, \mu(\hat{0}, \delta).$$

Using these, we obtain the following. If π is an elementary abelian group of order p^m, then

$$\begin{aligned} \rho(s; \mathbf{L}(\pi)) &= \sum_{k=0}^{m} (-1)^k \begin{bmatrix} m \\ k \end{bmatrix}_p p^{(1/2)k(k-1)-ks} \\ &= \prod_{k=0}^{m} (1 - p^{k-s}). \end{aligned}$$

If ω is any abelian group, then

$$\rho(s; \mathbf{L}(\omega)) = \prod_p \rho(s; \mathbf{L}(\pi_p)),$$

where π_p is the maximal elementary abelian p-group contained in ω. Using these results and the Hauptsatz, we can compute the zeta function of any collection of subgroups of a finite abelian group.

We come now to the main result of this paper, which is a new combinatorial interpretation of the evaluation of the zeta function at a positive integer. We restrict our account to the case of the lattice $\mathbf{L}(\omega)$, where ω is a finite abelian group. Recall that a *character* of the abelian group ω is a homomorphism of ω into the complex unit circle. Let $\alpha_1,\ldots,\alpha_k$ be a collection of subgroups of ω. Then, an n-tuple $\chi = (\chi_1,\ldots,\chi_n)$ of characters of ω *distinguishes* $\alpha_1,\ldots,\alpha_k$ if for every α_j, there exists a character χ_i such that χ_i restricted to α_j is not the trivial character.

THEOREM 10. *Let $\{\alpha_1,\ldots,\alpha_k\}$ be a collection of subgroups of the finite abelian group ω. Then, the number of n-tuples $\chi = (\chi_1,\ldots,\chi_n)$ of characters of ω distinguishing α is*

$$|\omega|^n p(n; \{\alpha_i\}).$$

Our *proof* is by Möbius inversion over the lattice $\mathbf{M}(\{\alpha_i\})$. If $\chi = (\chi_1,\ldots,\chi_n)$ is an n-tuple of characters of ω, then its *kernel* (*relative to* α) is the maximal subgroup β in $\mathbf{M}(\{\alpha_i\})$ such that χ_i restricted to β is trivial for all i; thus, β is the subgroup generated by the subcollection in α of all subgroups α_j such that χ_i restricted to α_j is trivial for all i. For each $\beta \in \mathbf{M}(\{\alpha_i\})$, let $f(\beta)$ be the number of n-tuples of characters whose kernel is exactly β, and $g(\beta)$ be the number of n-tuples whose kernel contains β. Thus,

$$g(\gamma) = \sum_{\beta \supseteq \gamma} f(\beta).$$

But, since every character χ_i which vanishes on γ defines a character of the quotient group ω/γ and conversely,

$$\begin{aligned} g(\gamma) &= \#\ n\text{-tuples of characters of } \omega/\gamma \\ &= (|\omega|/|\gamma|)^n. \end{aligned}$$

Hence, by Möbius inversion [8, p. 344],

$$f(\gamma) = \sum_{\beta \supseteq \gamma} \mu(\gamma, \beta)(|\omega|/|\beta|)^n.$$

Setting $\gamma = 0$, the trivial subgroup, we obtain

$$|\omega|^n p(n; \{\alpha_i\}) = \#\ n\text{-tuples of characters distinguishing } \{\alpha_i\}.$$

As there are $|\omega|^n$ n-tuples of characters of ω, we also obtain

COROLLARY 11. *For every positive integer n, the number $p(n; \{\alpha_i\})$ is the probability that an n-tuple of characters of ω, chosen (with replacement) independently and at random distinguish the collection of subgroups $\{\alpha_i\}$. In particular, $p(n; \mathbf{L}(\omega))$ is the probability of choosing an n-tuple of characters distinguishing all but the trivial subgroup of ω.*

An immediate consequence is

COROLLARY 12 (Rédei's Trägheitsatz). *For every positive integer n,*

$$0 \leqslant \rho(n; \{\alpha_i\}) \leqslant 1.$$

We conclude with a simple probabilistic proof of Rédei's Hauptsatz when s equals a positive integer n. Recall that the identity in question is

$$|\omega|^n \rho(n; \{\alpha_i\}) = \sum_{\beta} |\omega/\beta|^n \rho(n; \mathbf{L}(\omega/\beta)),$$

where the sum is over all subgroups β not containing any of the subgroups α^i. The left-hand side is the number of n-tuples $\chi = (\chi_1, ..., \chi_n)$ distinguishing all the subgroups α_i. This happens precisely when the *absolute kernel* of χ, defined by

$$\text{KER}\, \chi = \bigcap_{i=1}^{n} \ker \chi_i,$$

where $\ker \chi_i$ is the ordinary kernel of χ_i considered as a homomorphism of ω into the unit circle, does not contain any of the subgroups α_i. Thus, the set of distinguishing n-tuples of characters can be partitioned into disjoint subsets according to their absolute kernels β; moreover, all the n-tuples with kernel β, by definition, distinguish all the non-trivial subgroups in ω/β. When we count the distinguishing n-tuples according to this partition, we obtain the right-hand side.

REFERENCES

1. H. H. CRAPO AND G.-C. ROTA, "Combinatorial Geometries" (preliminary ed.), MIT Press. Cambridge, Mass., 1970.
2. S. DELSARTE, Fonctions de Möbius sur les groupes abeliens finis, *Ann. of Math.* **49** (1948), 600–609.
3. P. DOUBILET, G.-C. ROTA, AND R. P. STANLEY, The idea of generating function, *in* "Proceedings, 6th Berkeley Symposium, Vol. 2, pp. 267–318, Univ. of California Press. Berkeley, 1973.
4. G. HAJÓS, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Wurfelgitter, *Math. Z.* **47** (1942), 427–467.
5. J.-R. JOLY, Équations et variétés algébriques sur un corps fini, *Enseignement Math.* **19** (1973), 1–118.
6. N. KOBLITZ, "p-adic Numbers, p-adic Analysis and Zeta-functions," Springer-Verlag. New York, 1977.
7. L. RÉDEI, Zetafunktionen in der Algebra, *Acta Math. Acad. Sci. Hungar.* **6** (1955), 5–25.
8. L. RÉDEI, Die gruppentheoretischen Zetafunktionen und der Satz von Hajós, *Acta Math. Acad. Sci. Hungar.* **6** (1955), 271–279.

9. G.-C. ROTA, On the foundations of combinatorial theory. I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368.
10. G.-C. ROTA, "Théorie combinatoire des invariant classiques," Seminar notes by J. Désarménien, IRMA, Strasbourg, 1977.
11. L. SOLOMON, Zeta functions and integral representation theory, *Advances in Math.* **26** (1977), 306–326.
12. L. SOLOMON, Partially ordered set with colors, *in* "Relations between Combinatorics and Other Parts of Mathematics" (D. K. Ray-Chaudhuri, Ed.), pp. 309–330, Amer. Math. Soc., Providence, R.I., 1979.