SEMINAR ON LATTICES AND CODES

Introduction

A lattice Γ of rank n in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ of the form $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ where $(e_1, \ldots, e_n)$ is a basis of $\mathbb{R}^n$. An example of a lattice in $\mathbb{R}^n$ is $\mathbb{Z}^n \subset \mathbb{R}^n$. An important tool to study lattices, the so-called theta function of a lattice, comes from complex analysis. It is a holomorphic function on the complex upper half plane $\mathbb{H}$ and contains information about distributions of lattice points of fixed length. For example, if a lattice Γ is even, which means that the square of the length of x is an even integer for each $x \in \Gamma$, then the theta function can be used to count the number of lattice points of length $\sqrt{2r}$ for each positive integer r. If an even lattice has the so-called unimodularity property, then the corresponding theta function becomes a modular form, which is a holomorphic function on $\mathbb{H}$ with certain symmetry properties. The theory of modular forms is useful in the classification of lattices, for instance, it can be used to show that there is a unique even unimodular lattice of rank 8 in $\mathbb{R}^8$ up to isomorphism.

The theory of lattices interacts deeply with coding theory. Here, by definition, a code is a certain fixed set whose elements are the "codewords". Choosing this "dictionary" and its mathematical properties conveniently can enable correction of transmission errors. As such, coding theory has many applications, for example in the telephone and satellite communication. There are some surprising parallels between the theory of lattices and coding theory. For example, the notion of unimodularity in the theory of lattices is analogous to the notion of self duality in coding theory, the theta function in the theory of lattices is analogous to the so-called weight numerator in coding theory and so on.

In this seminar, we will study lattices, codes and modular forms. We will also explore connections between them including the ones mentioned above.

1. Lattices and Codes

1.1. **Introduction to lattices and codes.**

- Define lattices and discuss the notion of the fundamental parallelotope and the volume associated to lattices
- Introduce the notion of index associated to lattices Γ and Γ' such that $\Gamma \subset \Gamma'$
- Discuss the notion of dual lattices, integral lattices, even lattices and unimodular lattices
- Introduce (binary) codes and the weight of codes and discuss examples

Seminar date: 16.10.18

References: [3], Chapter 1, section 1.1, section 1.2, pages 5-7.

1.2. **Linear codes, codes to lattices.**

- Define linear codes and discuss the Hamming code as an example
- Introduce self dual and doubly even codes and discuss the extended Hamming code
- Discuss constructions of lattices from linear codes
- Prove proposition 1.3
- Discuss the lattice constructed from the extended Hamming code

Seminar date: 23.10.18

References: [3], Chapter 1, section 1.2, pages 8-10 and section 1.3.

1.3. **Root lattices.**

- Introduce roots of even lattices
- Introduce root lattices
- Discuss fundamental systems of roots
- Prove theorem 1.1
- Introduce the Coxeter-Dynkin diagram G of root lattices and study properties of G (show for example that it does not contain certain types of subgraphs etc.)

Seminar date: 30.10.18

References: [3], Chapter 1, section 1.4, pages 14-18, page 19 up to the discussion continued from page 18.

1.4. **Classification of root lattices.**

- Introduce the notion of orthogonal direct sum of lattices and discuss irreducible and reducible lattices
- Prove that every root lattice can be written as the orthogonal direct sum of the irreducible root lattices which have special Coxeter-Dynkin diagrams
- Introduce the Weyl group of root lattices
- Discuss the notion of group actions on vector spaces and show that the Weyl group of an irreducible root lattice of rank n acts irreducibly on $\mathbb{R}^n$
- Study the action of the Weyl group on the set of roots

Seminar date: 06.11.18

References: [3], Chapter 1, section 1.4, pages 19-22, page 23, Lemma 1.10.

1.5. **Irreducible root lattices and binary codes.**

- Prove proposition 1.5 (which is a statement about which irreducible root lattices can be constructed from linear binary codes.)
- Introduce the notion of the Coxeter number of root lattices
- Introduce the notion of spherical polynomials and characterize the bilinear forms which are invariant under the action of the Weyl group of irreducible root lattices
- Prove proposition 1.6

Seminar date: 13.11.18

References: [3], Chapter 1, section 1.4, pages 23-27.

1.6. **The highest root and Weyl vector.**

- Introduce the notion of positive and negative roots associated to irreducible root lattices and use this notion to introduce a partial ordering on the set of roots
- Discuss the existence of the highest root of irreducible root lattices
- Define the Weyl vector
- Discuss interactions of the Coxeter number with the highest root
- Introduce the notion of the extended Coxeter-Dynkin diagram
- Discuss how the Coxeter number can be used to compute the length of the Weyl vector

Seminar date: 20.11.18

References: [3], Chapter 1, section 1.5

2. Theta functions, modular forms and weight enumerators

2.1. **Theta function of a lattice and the modular group.**

- Introduce the theta function of a lattice, explain how it can be used to count the number of lattice points lying on spheres
- Show that the theta function of a lattice is holomorphic on the upper complex half plane
- Introduce the modular group $\mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ and discuss the action of the modular group on the upper complex half plane
- Prove theorem 2.2 (This theorem discusses the fundamental domain of the action of the modular group.)

Seminar date: 27.11.18

References: [3], Chapter 2, sections 2.1, section 2.2 pages 34-36, section 2.4, lemma 2.2.

Additional references: [1], Chapter 1, sections 1.1-1.2, pages 3-7.

Note: This talk uses various notions from complex analysis.

2.2. **Introduction to modular form.**

- Define modular forms
- Discuss the Poisson summation formula including proof
- Show that the theta function of an even unimodular lattice is a modular form

Seminar date: 04.12.18

References: [3], Chapter 2, section 2.1, theorem 2.1, section 2.2, pages 36-37 (discussion of the definition of modular forms), sections 2.3-2.4.

2.3. **Important examples of modular forms.**

- Discuss the Eisenstein series in detail
- Introduce the normalized Eisenstein series
- Introduce cusp forms

Seminar date: 11.12.18

References:: [3], Chapter 2, section 2.5.

Additional references: [1], Chapter 2, section 2.1, pages 13-14, section 2.4, pages 20-22.

Note: This talk uses a lot of complex analysis.

2.4. **The algebra of modular forms.**

- Show that the space of modular forms of weight k is a finite dimensional vector space
- Show that the space of all modular forms yield a graded algebra and prove that it is isomorphic to $\mathbb{C}[E_4, E_6]$

Seminar date: 18.12.18

References: [3], Chapter 2, section 2.6.

Additional references: [1], Chapter 1, section 1.3, chapter 2, section 2.1.

Note: This talk uses complex analysis.

2.5. **The weight enumerator of a code.**

- Introduce the weight enumerator of codes and discuss examples
- Investigate the weight enumerator of self-dual doubly even codes using the theta function
- Introduce the notion of t-design, prove proposition 2.9 and theorem 2.6

Seminar date: 08.01.19

References: [3], Chapter 2, section 2.7, and section 2.8, up to the proof of theorem 2.6.

Note: This talk is challenging.

2.6. **The extended Golay code, the MacWilliams Identity and the Gleason's theorem.**

- Briefly outline the construction of the extended Golay code and introduce the Leech lattice
- Discuss the MacWilliams Identity and prove the Gleason's theorem

Seminar date: 15.01.18

Reference: [3], Chapter 2, section 2.8, pages 58-61, section 2.9, pages 62-65.

Additional references: [2], Chapter 7, theorem 6.

Note: This talk is challenging.

3. Even Unimodular Lattices

3.1. **Theta function with spherical coefficients.**

- Discuss spherical polynomials and state theorem 3.1
- Briefly recap the Fourier transform and give examples
- Discuss modified theta functions
- Study the action of $\mathrm{SL}_2(\mathbb{Z})$ on the modified theta functions

Seminar date: 22.01.19

Reference: [3], Chapter 3, section 3.1, pages 77-83.

3.2. **Root systems in even unimodular lattices and a classification result.**

- Introduce the notion of level of lattices and introduce various subgroups $\mathrm{SL}(2,\mathbb{Z})$ of finite index
- Discuss the reciprocity law for Gaussian sums
- Study the action of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ on theta functions with spherical coefficients and prove theorem 3.2
- Discuss applications of theorem 3.2 to root systems of even unimodular lattices

Seminar date: 29.01.19

References: [3], Chapter 3, section 3.1, pages 84-87, and section 3.2.

3.3. **Overlattices, codes and classification theorems.**

- Discuss the notion of overlattices
- Discuss classification questions for lattices which contain a given lattice as the root sublattice
- Discuss analogous statements for doubly even codes
- Lattice-code correspondence for doubly even codes and even lattices containing a root lattice of type nA_1
- Briefly discuss the Niemeier's theorem on the classification of even unimodular lattices of rank 24

Seminar date: 05.02.19

References: [3], Chapter 3, section 3.3, and section 3.4, page 94.

References

[1] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of modular forms*. Springer-Verlag, Berlin, 2008.

[2] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999.

[3] Wolfgang Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, third edition, 2013.