Number Theory Seminar

Quadratic Forms

Bonn, Winter Term 2020/21

A quadratic form over the integers is a quadratic homogeneous polynomial,

$$Q(X_1, \dots, X_d) := \sum_{i \le j} a_{ij} X_i X_j \in \mathbb{Z}[X_1, \dots, X_d].$$

The natural question is: For which $n \in \mathbb{Z}$ is $Q(x_1, \dots, x_d) = n$ solvable in $\mathbb{Z}$?

For example, a famous result of Gauss states that every $n \ge 0$ is a sum of four squares. In general, however, there is no simple answer, leading to a rich and fascinating theory.

In the seminar, we study Q by studying all its reductions Q mod N, $N \in \mathbb{N}$. In other words, we will consider Q over the p-adic integers $\mathbb{Z}_p$ for all primes p and see how its p-wise properties determine its behavior over $\mathbb{Z}$. Over $\mathbb{Q}$, the local information is completely sufficient:

Theorem (Hasse–Minkowski)**.** *The equation $Q(x_1, \dots, x_d) = n$ is solvable in $\mathbb{Q}$ if and only if it is solvable in $\mathbb{R}$ and all p-adic fields $\mathbb{Q}_p$.*

The condition (existence of solutions in $\mathbb{R}$ and all $\mathbb{Q}_p$) is clearly necessary, the converse is the so-called *local-global principle* for quadratic spaces. Looking for solutions in $\mathbb{Z}$ instead, we still obtain

Theorem. *Assume that $Q(x_1, \dots, x_d) = n$ is solvable in $\mathbb{R}$ and in all p-adic integer rings $\mathbb{Z}_p$. Then there exists a quadratic form $Q' \in \mathbb{Z}[X_1, \dots, X_n]$ in the* genus of Q *such that $Q'(x_1, \dots, x_n) = n$ is solvable in $\mathbb{Z}$.*

Q and Q' are said to be of the same genus if they are isomorphic mod N for all N. Clearly, one cannot discriminate between forms of the same genus through congruence information. For example, $X^2 + 27Y^2$ and $4X^2 + 2XY + 7Y^2$ are in the same genus, but the second form represents 7 while the first does not.

Once we group forms by genus, however, we even get a full solution count from all localizations! This result, a highlight of number theory, will be the culmination point of the seminar.

Theorem (Smith–Minkowski–Siegel 1935)**.** *Assume that Q as above is positive definite. Let $Q = Q_1, \dots, Q_k$ be representatives for the forms in the genus of Q and let $n \in \mathbb{N}$. Then*

$$\frac{1}{\sum_{i=1}^k \#\operatorname{Aut}(Q_i)} \sum_{i=1}^k \frac{\#\{x \in \mathbb{Z}^d \text{ primitive} \mid Q_i(x) = n\}}{\#\operatorname{Aut}(Q_i)} = \alpha_\infty(n) \prod_p \alpha_p(Q, n).$$

The factors on the RHS are the so-called local p-adic *representation densities*. The seminar will conclude with some applications of this formula.

Talks

The seminar follows the books *A course in Arithmetic* by J. P. Serre (Talks 1–6) and *Quadratische Formen* by M. Kneser (Talks 7–12). The p-adic numbers will be omnipresent throughout, so some prior familiarity with them will be helpful.

Talk 1: Quadratic Reciprocity

Present the material from [3, Chapter I]. The two central results are the Chevalley Theorem (§2) and the quadratic reciprocity law (§3). This settles the classification of quadratic spaces over $\mathbb{F}_p$.

Talk 2: p-adic numbers

Present the material from [3, Chapter II]. After introducing the p-adic numbers $\mathbb{Q}_p$ and their ring of integers $\mathbb{Z}_p$, prove the fundamental results on the possibility of lifting solutions (Theorem 1 and Corollaries 1–3). Also present the description of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ from §3.3.

Talk 3: Hilbert Symbol

Present the material from [3, Chapter III]. Give the definition of the Hilbert Symbol and its properties (§1.1). State the results from §1.2 and give an indication of their proof. (For time reasons, you probably have to omit some details here.) State and prove the product formula (Theorem 3).

Talk 4: Quadratic Forms

Present the material from [3, Chapter IV.1], except for Theorem 2, which is part of the next talk. The main results are the existence of an orthogonal basis (Theorem 1), the possibility to extend isometries (Theorem 3) and the cancellation result (Theorem 4).

Talk 5: Forms over $\mathbb{Q}_p$

Present the material from [3, Chapter IV.2]. The main result is the classification of quadratic spaces over $\mathbb{Q}_p$ (Theorem 7) through their 3 invariants: dimension, discriminant and Hasse invariant. Theorem 2 from IV.1 will be needed to prove the well-definedness of the Hasse invariant.

Talk 6: Forms over $\mathbb{Q}$ — Hasse–Minkowski

Present the material from [3, Chapter IV.3]. The main results are the Hasse–Minkowski Theorem and the classification of quadratic spaces over $\mathbb{Q}$ (Theorem 9).

Talk 7: Quadratic Lattices

The reference is [2, §20]. Define quadratic forms over $\mathbb{Z}$, the discriminant and the dual lattice. State and prove the finiteness of quadratic lattices with given rank and discriminant (Propositions 20.1 and 20.2). Give some examples for the classification in low rank and discriminant as in §20.3 – §20.7 or as for binary forms in [4, p. 62] or [1, p. 29].

Talk 8: Genus and Representations

The reference is [2, §21, §22]. Define the genus of a lattice (§21) and prove the finiteness of the number of isometry classes in a genus (Proposition 21.3). Prove the fundamental result that a number is represented by a form of the genus if and only if it is represented locally at all primes (Proposition 22.1). Use this to settle the integral representability problem in examples where there is only one form in the genus, for example the cases Propositions 22.3–22.5. Some binary examples are listed in [1, Chapter 1, §2, Equation (2.28)].

Talk 9: Adelic description of the genus I

The aim of this talk is to introduce some adelic methods that go into the Smith–Siegel–Minkowski Theorem later. The reference is [2, §30–§32], but only the trivial case of $L = \{0\}$ is considered.

Introduce the ring of adeles $\mathbb{A}$ of $\mathbb{Q}$ as a topological ring. Explain how to topologize $\mathbb{A}_f$-points of varieties such as $GL_n(\mathbb{A})$ or $O(\mathbb{A} \otimes V)$. Show that there is a bijection

$$Genus(M) = O(V)\backslash O(\mathbb{A}_f \otimes V)/K_M$$

where $K_M \subseteq O(\mathbb{A}_f \otimes V)$ is the stabilizer of M. To motivate the bijection you may also recall the simpler but analogous bijections

$$GL_n(\mathbb{A}_f)/GL_n(\hat{\mathbb{Z}}) = \{\text{lattices } \Lambda \subseteq \mathbb{Q}^n\}$$

and $GL_n(\mathbb{Q})\backslash GL_n(\mathbb{A}_f)/GL_n(\hat{\mathbb{Z}}) = \{\star\}$. The latter is because the class number of $\mathbb{Q}$ is 1, showing that the definition of the genus is analogous to the definition of the class group.

Finally, assuming that M is positive definite, define the mass of a genus.

Talk 10: Adelic description of the genus II

The reference is [2, §30–§32]. Define what it means for a lattice to represent the other (Definition 30.1). Give the adelic description of the genus of a representation, introduce the notion of a Haar measure on $O(W_{\mathbb{A}})$ as in Proposition (31.11) and deduce Formula (32.2), relating the measure with representation numbers,

$$\mu(O(W)/O(W_{\mathbb{A}})) = \mu(O_{\mathbb{A}}(W,M)) \cdot \sum_k \frac{a_j(L,M_k)}{|O(M_k)|}.$$

Talk 11: The Smith–Minkowski–Siegel Theorem

The reference is [2, §32–§33]. Begin with Formula (33.2), relating the mass of a representation genus to the mass of the principal genus. Explain the normalization of the Haar measure as in Proposition (32.6) and (32.7). State the relation with representation densities (33.5) and finally the Smith–Minkowski–Siegel Theorem (33.6).

Talk 12: Applications

The reference is [2, §33 and §35]. Give some applications of the Smith–Minkowski–Siegel Theorem, as in (33.7), (33.8) and §35.

References

[1] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Vol. 34, John Wiley & Sons, 2011.

[2] M. Kneser, *Quadratische Formen*, Springer-Verlag, 2013.

[3] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, 1973.

[4] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag, 2013.