Prof. Dr. G. Böckle, C.V. Sriram

Proseminar in Number Theory, WS2023

Quadratic forms:
An arithmetic approach

INTRODUCTION[1]

In this proseminar, we aim to formulate and study a proof of the celebrated *Hasse principle*. This is an important occurrence of the ubuquitous principle in modern arithmetic called the *Local-Global principle*. In this introduction we will see what is the Hasse principle and briefly discuss the contents of the talks.

Let's begin by defining a *quadratic form*. Let k be a field of characteristic $\neq 2$. A quadratic form $\mathbf{f}(\underline{x})$ in $n-$variables $\underline{x} = (x_1, ..., x_n)$ is a function of the form

$$\mathbf{f}(\mathbf{x}) = \sum_{i,j} f_{ij}x_i x_j = f_{11}x_1^2 + 2f_{12}x_1x_2 + ...$$
$$\text{where } f_{ij} = f_{ji} \in k$$

A quadratic form $\mathbf{f}$ is said to be *isotropic* if $det(f_ij) \neq 0$[2] and moreover there is a non-zero solution $\underline{x} \neq 0$ for $\mathbf{f}\underline{x} = 0$.

From a historical analysis of quadratic forms it is very evident that the study of quadratic forms has mostly been the study of isotropic forms, be it the requirement to find integers satisfying $x^2 + y^2 = z^2$(to find sides of a right angled triangle) or to approximate $\sqrt{2}$ using large solutions of $x^2 - 2y^2 = \pm 1$[3]. Before doing a quantitative analysis of the solutions, it is a legitimate question to ask *whether* the quadratic form is isotropic or not. Equivalently first one needs to check if $\mathbf{f}$ has any non-trivial solutions or not.

Let's try to see what are natural obstructions to the existence of non-trivial solutions to $\mathbf{f}(\underline{x}) = 0$. Suppose for simplicity that all $f_{ij} \in \mathbb{Z}$ and we're looking for solutions $\underline{x} \in \mathbb{Z}^n$. Choose a positive integer $m \in \mathbb{N}_{>0}$. An obvious necessary condition we observe is that

$$\mathbf{f}(x_1, ..., x_n) = 0 \implies \mathbf{f}(x_1, ..., x_n) \mod m = 0$$

equivalently,

$$\forall (\bar{x}_1, ..., \bar{x}_n) \in (\mathbb{Z}/m\mathbb{Z})^n, \bar{\mathbf{f}}(\bar{x}_1, ..., \bar{x}_n) \neq 0 \mod m \implies \mathbf{f} \text{ has no non-trivial solutions}$$

Another necessary condition we require is

$$\forall \underline{x} \in \mathbb{R}^n, \mathbf{f}(\underline{x}) \neq 0 \implies \mathbf{f} \text{ has no non-trivial integer solutions}$$

For example, consider the equation $x^2 + y^2 = 6z^2$. It has no non trivial integer solution. For otherwise $z \neq 0$ and we may assume $\gcd(x, y, z) = 1$. Going $\mod 3$, we see $x^2 + y^2 = 0 \mod 3 \implies x \equiv y \equiv 0 \mod 3$
$\implies x = 3k, y = 3l$ and $3k^2 + 3l^2 = 2z^2 \implies 3|z$, a contradiction.
So one could naturally wonder whether

Question. *If a regular quadratic form* $\mathbf{f}$*, with integer coefficients, has a non-zero solution after reducing it* $\mod m$*, for all positive integer* m *and also has solutions in* $\mathbb{R}$*, does it have an integer solution?*

The answer turns out to be yes(!) and this is the Hasse principle. We will be concerned with a version of the Hasse principle which will involve the *p-adic numbers* $\mathbb{Q}_p$[4](p is a

[1] Vorbesprechung on July 18, 2023 at 11:30 a.m.(s.t.)

[2] Forms with this first condition on the non-vanishing of the determinant are called *regular*. They are also known as *non-degenerate* or *nicht ausgeartet*

[3] Exercise(!): How can one *naturally* transform this equation to a quadratic form in the above sense

[4] cf. Talk 3, Talk 4

prime number). The field $\mathbb{Q}_p$ is called a *local field* and hence one often says "$\mathbf{f}(\underline{x})$ admits a solution locally" to mean it has a solution over $\mathbb{Q}_p$. So the slogan here is

$$\mathbf{f}(\underline{x}) \text{ has a solution in } \mathbb{Q} \iff \mathbf{f}(\underline{x}) \text{ admits solutions locally(in each } \mathbb{Q}_p)$$

Let's briefly describe the talks. In Talk 1, we discuss the basic premise of the proseminar namely a *quadratic space* i.e. vector space V equipped with a quadratic form(equivalently a bilinear form). Next in Talk 2, isotropic spaces and isometries are defined and discussed. The next two talks, Talk 3 and Talk 4, are two parts of a discussion on p-adic numbers. Properties of the p-adic numbers sufficient to understand the rest of the proseminar would be presented here. In Talk 5 the *Norm residue symbol* is defined and its properties presented. Then we characterize the quadratic forms over $\mathbb{Q}_p$ using some arithmetic invariants in Talk 6. From Talk 7 to Talk 10 we will present a proof of the Hasse principle. Talk 7 formulates the Hasse principle and proves it for binary forms. In Talk 8 we present H. Minkowski's beautiful theory of *Geometry of numbers* and apply it in Talk 9 to show the Hasse principle for quadratic forms in 3 variables. We conclude the proseminar with the proof of a general version of the Hasse principle and also providing some quantitative measures of the solutions in Talk 10.

PRACTICALITIES

1. Prerequisites. Students are expected to have a good understanding of the topics covered in Linear algebra 1 and Linear algebra 2. Some talks require basic understanding of Analysis 1.

2. Requirements of the participants.
(a) Delivery of seminar talk. The student is expected to deliver a 90-minute talk on their chosen topic. Definitions and results must be stated clearly, and where possible illustrated with concrete examples. Ideally the student will have worked through and understood all proofs; some of these proofs should be presented, though for reasons of time others may have to be omitted. Each presentation should contain at least one example.

(b) Preparation of handout. Please create a handout for the seminar participants to accompany your presentation. This document should contain the most important definitions and results from your presentation. You are also welcome to explain details of calculations and examples there for which there is no time in the lecture.

(c) Timelines for preparation of talk and handout.

(i) Start preparing your presentation in good time (approx. 4 weeks in advance). Come two weeks before your presentation for a preliminary discussion(Appointment to be made via email with Mr. Sriram). Bring a draft of the handout to the preliminary meeting.
(ii) A template for handout is available on the seminar webpage.
(iii) Please email the completed handout to Mr. Sriram no later than Monday morning before your presentation, so that the materials can be made available to the other seminar participants in advance.

(d) Language of talk and handout. The talks must be delivered in English. The handout should also be written in English.

TALKS

Quadratic spaces (1)

We begin by defining a *quadratic space* (V, ϕ) from [Cassels, Ch.2,§1](in characteristic$\neq$ 2). *Regular quadratic spaces* and *normality* should also be discussed. Then briefly discuss *representability by quadratic forms* and *equivalence*[5] from [Cassels, Ch.1,§2]. Some examples would be appreciated here. We end this talk by stating and discussing a proof of [Cassels, Ch.2,§3,Lem.3.1].

References: [Cassels, §1.1,§2.1,§2.3]

Lecture Date:

Isotropic spaces and isometries (2)

In this lecture, we start by discussing the definition of an *isotropic space*[Cassels, Ch.2,§2] We will show in particular that every isotropic space contains an *hyperbolic plane*. Then present some results on *universal* spaces. In the second half of the talk, we discuss bijective linear map between quadratic spaces also known as *isometry*[Cassels, Ch.2,§4]. Then we study a certain class of isometries called *symmetries.* In particular, we show that any isometry $(V, \phi) \to (V, \phi)$ is a product of symmetries. We conclude the talk by proving the *Witt's lemma*.

Reference: [Cassels, §2.2 and §2.4].

Lecture Date:

p-adic numbers-I (3)

In this and the next talk, we discuss a basic concept of importance for our seminar, namely the field of *p-adic numbers* $\mathbb{Q}_p$. Motivate the talk from [Neukirch, Def'n 1.1 of Ch.II,§1]. Then the topics in [Cassels, Ch.3,§1] should be presented. In particular, this includes defining the *p-adic absolute value*$|.|_p$, constructing the field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ w.r.t. the $|.|_p$. Then some results on convergence of sequences/series in $\mathbb{Q}_p$ should be presented. Lastly talk about the *p-adic expansion* of elements of the ring of *p-adic integers* $\mathbb{Z}_p$(tying back to the beginning of the talk) (Since some participants might be seeing $\mathbb{Q}_p$ for the first time, it would be appreciated if the speaker focuses more on examples than proofs, wherever possible. For the talk [Gou, Ch.2 and Ch.3] can also be used.)

References: [Cassels, §3.1] and [Neukirch, §2.1]. One can also look at relevant parts of [Gou, CH.2 and CH. 3].

Lecture Date:

p-adic numbers- II (4)

In this talk we focus on the ring of p-adic integers $\mathbb{Z}_p$. Begin by presenting the *Strong approximation theorem*[Cassels, Lem.3.1,Ch.3], after recalling the statement of the *Chinese remainder theorem*(as a consequence also state the *Weak approximation theorem*,

[5] *Kongruent bilinear formen*

without proof). Then discuss the Hensel's lemma [Cassels, Ch.3, Lemma 4.1] and its application(for instance [Cassels, Ch.3, Lemma 1.6]). Finally, present on how to view the ring $\mathbb{Z}_p$ as a *projective limit*, and depending on the time prove/state [Neukirch, Ch.2, Prop. 1.4].

References: [Cassels, §3.1 and §3.4], [Gou, §3.4] and [Neukirch, §2.1].

Lecture Date:

The Norm residue symbol (5)

We introduce a symbol known as *norm residue symbol*, denoted $\left(\frac{a,b}{p}\right)$, which provides us with a reasonable way to deal with ternary quadratic forms [6]. Begin the talk by briefly discussing the notion of *quadratic residues* from [Serre, §3.1,§3.2 and §3.3], by providing basic definitions/properties and stating(without proof) the quadratic reciprocity law(hopefully with examples). Then describe the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ [Cassels, Ch.3, Cor.1.6]. Later discuss [Cassels, Ch.3, Lem.2.1] (multiplication table of $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ need not be gone through). Conclude the talk by proving the *product formula for the norm residue symbol.*

References: [Cassels, §3.2-§3.3]. For presentation on quadratic residues and reciprocity law see [Serre, §3.1,§3.2 and §3.3].

Lecture Date:

Quadratic forms over $\mathbb{Q}_p$ (6)

The main focus of this talk would be a characterization of the quadratic forms over $\mathbb{Q}_p$(including $\mathbb{R}$), involving some arithmetic invariants. Here the contents from [Cassels, Ch.4,§1-§2] should be presented(the last Lemma 2.8 can be excluded from the talk).

References: [Cassels, §4.1-4.2]

Lecture Date:

Strong-Weak Hasse principle (7)

In this talk, we formulate the *Strong Hasse principle*, which is one of the central results of this proseminar[7]. Begin the talk by stating the [Cassels, Ch.6,Thm.1.1] and obtaining some immediate corollaries from the theorem, such as *Meyer's theorem* and others. Also state the *Weak Hasse principle* and prove it [Cassels, §2]. Illustrate some examples to demonstrate the importance of the two principles discussed(here the [Cassels, Example 1 and 2] can be used). Conclude the talk by proving strong Hasse principle for binary quadratic forms [Cassels, §3].

References: [Cassels, §6.1,6.2,6.3].

Lecture Date:

[6] but also being a technique of importance in its own right

[7] Also known as the *Hasse-Minkowski principle*

Geometry of numbers: a digression (8)

Here we learn a technique which being novel in its own right, will be used in the next talk to prove the Hasse principle for the ternary quadratic forms. The contents to be presented in this talk are [Cassels, Ch.5, §1-2], in particular *Minkowski's Linear Forms Theorem* [Cassels, Thm.2.4]. Conclude the talk, as an application, with a proof of the fact that every positive integer can be represented as the sum of four perfect squares, the so called *Four Square Theorem*[Cassels, Example 2].

References: [Cassels, §5.1-2, Example 2]. An alternate reference of the same theory is [Neukirch, Ch.1,§4].

Lecture Date:

Ternary quadratic forms (9)

In this talk, we prove the Strong Hasse principle for Ternary Quadratic forms. After making some standard reductions, prove the result of *Legendre* [Cassels, Ch.6,§4, Thm.4.1], which uses tools from previous talk. Discuss the size of the solutions and conclude the talk by proving [Cassels, §4, Cor.2], which says that if a ternary form is isotropic over $\mathbb{Q}_p$ for all *but* one prime p_0, then it is isotropic over $\mathbb{Q}$.

References: [Cassels, §6.4]

Lecture Date:

Strong Hasse principle - General case (10)

In this talk we conclude the discussion of Hasse principle, by discussing a proof for quadratic forms with four or higher variables. The contents of [Cassels, Ch.6,§5-6] should be presented here. Conclude the talk by a discussion on the size of solutions [Cassels, §8].

References:: [Cassels, §6.5,§6.6,§6.8].

Lecture Date:

References

[Cassels] Rational quadratic forms. Academic press, London

[Serre] A course in arithmetic. Springer

[Neukirch] Algebraic number theory. Springer

[Gou] Gouvea, F.: p-adic Numbers: An Introduction. Springer University text, ISBN 978-3-662-22278-2 (eBook) .

[Kat] Katok, S.: p-adic Analysis Compared with Real. AMS Student Mathematical Library 37 (2007).

[Rud] Rudin, Walter: Principles of Mathematical Analysis.