Hasse-Minkowski theorem, Lec 1

0) Introduction

We are interested in the study of homogeneous quadratic equations

$$(*) \quad q(x_1,\dots x_n) := \sum_{1\le i\le j\le n} q_{ij} x_i x_j = 0 \quad (q_{ij}\in\mathbb{Q})$$

and our main question is

Q: When does this equation have a <u>nonzero</u> solution in $\mathbb{Q}^n$?

Example: Consider the following equations

(1) $\sum_{i=1}^{5} x_i^2 = 0$

(2) $x_1^2 - 2x_2^2 + 3x_3^2 - 6x_4^2 = 0$

(3) $x_1^2 + x_2^3 + x_3^2 - 7x_4^2 = 0$

(4) $67x_1^2 - 2x_2^2 + 3x_3^2 - 6x_4^2 + 99x_5^2 = 0$

(1) has no nonzero solutions - even in $\mathbb{R}^5$: if at least one x_i is nonzero, the left hand side is positive.

Exercise: Show (2) & (3) have no nonzero rational solutions.

It turns out that (4) has a nonzero rational solution.

Theorem: Assume $n \geq 5$. Then the quadratic equation (*) has a nonzero rational solution if it has a nonzero real solution.

In a way, a goal of this class is to explain why this holds, although we won't fully prove this

1) Diagonalization

Our first topic is the study of homogeneous quadratic equations with coefficients in $\mathbb{R}$ or $\mathbb{Q}$. Our treatment below will apply to both these settings (unless mentioned otherwise) so we'll use $\mathbb{F}$ to denote $\mathbb{R}$ or $\mathbb{Q}$.

A common terminology: a homogeneous quadratic polynomial will be called a quadratic form. We say that a quadratic form q represents $a \in \mathbb{F}$ (over $\mathbb{F}$) if $q(x_1, \dots x_n) = a$ has a nonzero solution in $\mathbb{F}^n$ (the restriction of being nonzero is only essential if $a=0$).

1.1) Equivalence of quadratic forms

We would like to understand when two quadratic forms "behave the same."

Definition: Let $q(x_1, \dots x_n), q'(x_1, \dots x_n) \in \mathbb{F}[x_1, \dots x_n]$ be quadratic forms. We say they are equivalent if $\exists$ invertible ($\Leftrightarrow \det \neq 0$) matrix $A = (a_{ij}) \in Mat_{n\times n}(\mathbb{F})$ s.t.

$$q'(x_1, \dots x_n) = q(x_1', \dots x_n'), \text{ where } x_i' := \sum_{j=1}^{n} a_{ij} x_j,$$

in other words, if q' is obtained from q by an invertible linear change of variables. We write $q' \sim q$ in this case.

Example: $q'(x_1, x_2) = x_1^2 - x_2^2 \; (= (x_1 - x_2)(x_1 + x_2))$ & $q(x_1, x_2) = x_1 x_2$ are equivalent: set $x_1' = x_1 - x_2$, $x_2' = x_1 + x_2$ so that $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

This notion is useful b/c questions we care about such as the existence of a nonzero solution are equivalent for equivalent forms.

Exercise: Our notion of equivalence is indeed an equivalence relation in the formal sense, i.e it is:

- reflexive: $q \sim q$
- symmetric: $q \sim q' \Rightarrow q' \sim q$
- & transitive: $q \sim q', q' \sim q'' \Rightarrow q \sim q''$.

1.2) Main result

Proposition: $\forall\, q(x_1, \dots x_n) = \sum_{1 \le i \le j \le n} q_{ij} x_i x_j$ is equivalent to q' of the form $q'(x_1, \dots x_n) = \sum_{i=1}^{n} q_i x_i^2$ $(q_i \in \mathbb{F})$ (we'll say that q' is diagonal). Moreover, if q represents $a \in \mathbb{F} \setminus \{0\}$, we can find q' w. $q_1 = a$.

Proof:

Step 1: If a_{ij} $(1 \le i, j \le n)$ are as in Definition in Sec 1.1, then $q'(1, 0, \dots 0) = q(a_{11}, a_{21}, \dots, a_{n1})$. Now suppose $(a_{11}, \dots a_{n1})$ is a nonzero solution to $q(x_1, \dots x_n) = a$ w. $a \in \mathbb{F}$. We can find a_{ij} w. $j > 1$ s.t. the matrix $A = (a_{ij})$ is invertible (exercise). Then $q'(x_1, \dots x_n) = \sum_{i \le j} q'_{ij} x_i x_j$ w. $q'_{11} = q'(1, 0, \dots 0) = a$. We can replace q w. q' & assume $q_{11} = a$.

Step 2: If q does not represent any nonzero number, then $q=0$ & Proposition trivially follows. So suppose $q_{11}=a\neq 0$. Set

$$y_1 := x_1 + \sum_{j=2}^{n} \frac{q_{1j}}{2a} x_j \Rightarrow$$

$$a y_1^2 = \sum_{j=1}^{n} q_{1j} x_1 x_j + \sum_{j=2}^{n} \frac{q_{1j}^2}{4a^2} x_j^2 + \sum_{2\leq j<k\leq n} \frac{q_{1j} q_{1k}}{2a^2} x_j x_k$$

Then $q(x_1,\dots x_n) = a y_1^2 + \sum_{2\leq i\leq j\leq n} q'_{ij} x_i x_j$ for suitable q'_{ij}. The change of variables $(x_1,\dots x_n) \mapsto (y_1, x_2, \dots x_n)$ is invertible, so establishes an equivalence between q & q', where $q'(x_1,\dots x_n) = a x_1^2 + \sum_{2\leq i\leq j\leq n} q'_{ij} x_i x_j$.

Step 3: We can then apply induction on the number of variables n to find a change of variables $(x_2,\dots x_n)$ that makes $\sum_{2\leq i\leq j\leq n} q'_{ij} x_i x_j$ diagonal finishing the proof $\square$

A natural question is what happens when q represents 0. Here's an answer:

Exercise*: If q represents 0, we can find q' s.t.

$$q_1 = 0 \quad \text{or} \quad q_1 = 1,\ q_2 = -1.$$

1.3) Remark

To prove proposition we used that:

a) $\mathbb{F}$ comes with addition, subtraction & multiplication subject to the usual axioms (associativity, commutativity, etc.).

b) We also used division, more precisely that elements of the form $2a$ ($a \in \mathbb{F} \setminus \{0\}$) are invertible.

For example, Proposition will fail over $\mathbb{Z}$ (as very few elements are invertible). There's one more case of "numbers" where Proposition holds that we will need in this class: $\mathbb{F} = \mathbb{Q}_p$, p-adic numbers, that we'll introduce later.