Hasse-Minkowski theorem, lec 5: Sketch of proof.

0) Introduction

In Sec 4.3, we've stated the main theorem of this course whose nontrivial part is:

Theorem: If a form q with rational coefficients represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, then it represents 0 over $\mathbb{Q}$.

Baby example: $n=2$. We assume that q is diagonal, $q=[q_1,q_2]$ w. $q_1,q_2\in\mathbb{Q}^\times:=\mathbb{Q}\setminus\{0\}$. Then q represents 0 over $\mathbb{F}$ ($=\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{Q}_p$) $\Leftrightarrow d:=-\frac{q_1}{q_2}$ is a complete square in $\mathbb{F}$. This implies:

- $d>0$
- $\mathrm{ord}_p(d)$ is even, where we write ord_p for the order of d as an element of $\mathbb{Q}_p$.

We can decompose d as $\pm p_1^{\kappa_1}\dots p_e^{\kappa_e}$ ($p_1,\dots p_e$ - distinct primes, $\kappa_1,\dots\kappa_e\in\mathbb{Z}$). Then $\mathrm{ord}_p(d)=\kappa_i$ if $p=p_i$ & 0 if $p\notin\{p_1,\dots,p_e\}\Rightarrow$ all κ_i are even, so d is a complete square in $\mathbb{Q}$.

In what follows we'll discuss some ideas of proof for $n \geq 3$. A reference for what follows is Serre, "A course in Arithmetic".

2) Case $n=3$: Legendre, 1785

Here we fix $a, b \in \mathbb{Q} \setminus \{0\}$ and study the existence of nonzero $(x,y,z) \in \mathbb{Q}^3$ satisfying $z^2 = ax^2 + by^2$ (can reduce to this case by rescaling).

Proposition: Suppose $z^2 = ax^2 + by^2$ has nonzero solutions over all $\mathbb{Q}_p$ w $p > 2$ & over $\mathbb{R}$. Then it has a nonzero solution over $\mathbb{Q}$.

Proof:

Rescale to reduce to coprime integer solutions (x,y,z) to $z^2 = ax^2 + by^2$ where a, b are square-free integers. A key idea is induction on $|a| + |b|$. Assume $|a| \leq |b|$. The case $|b| = 1$ ($\Rightarrow |a| = 1$) is easy (exercise). Let $b = \pm p_1 \cdots p_k$ for primes $p_1, \ldots, p_k$, $k \geq 1$.

Lemma: Assume $z^2 = ax^2 + by^2$ has a nonzero solution in $\mathbb{Q}_{p_i}$ $\forall$ $i = 1, \ldots, k$, with $p_i > 2$. Then a is a complete square modulo b

Proof of Lemma:

If $t_i^2 \equiv a \bmod p_i \Rightarrow$ [Chinese remainder Thm] $\exists\, t \in \mathbb{Z}$ s.t $t \equiv t_i \bmod p_i \Rightarrow a \equiv t^2 \bmod b$. So, it suffices to show that a is complete square mod each $p_i =: p$. Case $p = 2$ is automatic, so assume for contradiction that a is a quadratic nonresidue mod $p > 2$. We can assume that $z^2 = ax^2 + by^2$ has a solution in $\mathbb{Z}_p^3$ where at least one of x, y, z has order 0 (else divide by p^n). But $z^2 \equiv ax^2 \bmod p \Rightarrow z, x \equiv 0 \bmod p \overset{\text{ord}_p(b)=1}{\Rightarrow} y \equiv 0 \bmod p$. Contradiction. $\square$ of Lemma.

By Lemma, $\exists\, c, b' \in \mathbb{Z} \mid c^2 - a = bb'$. Can choose $c \in \left[-\frac{|b|}{2}, \frac{|b|}{2}\right]$ Then since $|a| \leq |b|$, we get $|b'| < |b|$.

Claim: In $\mathbb{F} = \mathbb{Q}, \mathbb{Q}_p$, or $\mathbb{R}$, the set $X(\mathbb{F}) := \{z^2 - ax^2 \mid x, z \in \mathbb{F}\}$ is closed under multiplication & taking inverses (of elements $\neq 0$).

Exercise 1* (on norms in quadratic extensions): prove this; note that if a is complete square in $\mathbb{F}\setminus\{0\} \Rightarrow X(\mathbb{F})=\mathbb{F}$

The equation $z^2-ax^2=by^2$ has a nonzero solution in $\mathbb{F}$ $\Leftrightarrow b\in X(\mathbb{F})$; $bb'\in X(\mathbb{Q})\subset X(\mathbb{F})$. So $z^2-ax^2=by^2$ has a nonzero solution in $\mathbb{F}^3 \Leftrightarrow b\in X(\mathbb{F}) \Leftrightarrow$ [Claim & $bb'\in X(\mathbb{F})$] $\Leftrightarrow$ $b'\in X(\mathbb{F}) \Leftrightarrow z^2-ax^2=b'y^2$ has a nonzero solution in $\mathbb{F}^3$.

Since $|b'|<|b|$, this gives an induction step. □

Remarks:

1) One can analyze when $z^2=ax^2+by^2$ has nonzero solutions over $\mathbb{Q}_p$ $(p>2)$ using the description of complete squares (Sec 3.2) and the Important Lemma (Sec 4.2)

Exercise 2*: $z^2=ax^2+by^2$ has a nonzero solution in $\mathbb{Q}_p^3$ if and only if one of the following holds:

- one of $a, b, -\frac{a}{b}$ is a complete square in $\mathbb{Q}_p$
- $\mathrm{ord}(a)\equiv \mathrm{ord}(b)\equiv 0 \bmod 2$

2) That one can skip $p=2$ is a special feature of $n=3$ ($x_1^2+x_2^2+x_3^2-7x_4^2$ represents 0 over $\mathbb{R}$ & all $\mathbb{Q}_p$ w. $p>2$ - exercise). We have the following result of Hilbert. Notation: write $\mathbb{Q}_\infty$ for $\mathbb{R}$. Then the number of $p \in \{\text{primes}\} \cup \{\infty\}$ s.t. $z^2=ax^2+by^2$ does not have nonzero solutions in $\mathbb{Q}_p^3$ is finite (easy) & even (non-trivial).

2) From $n \geq 4$ to $n-1$.

We want to deduce the HM theorem for n variables from that for $n-1$ variables.

Assume $q=[q_1,\dots q_n]$ w. $q_i \in \mathbb{Q}\setminus\{0\}$. By part 4 of problem 1 in the pset, for any equivalent $[q_1',\dots,q_n'] \Rightarrow q_i' \neq 0 \ \forall i$

Exercise: Let $q_1,\dots,q_n \in \mathbb{F}\setminus\{0\}$ & $m<n$. Then the following are equivalent:

1) $[q_1,\dots q_n]$ represents 0 (over $\mathbb{F}$)

2) $\exists\ a \in \mathbb{F}\setminus\{0\}$ s.t. both $[q_1,\dots q_m]$ & $[-q_{m+1},\dots,-q_n]$ represent a over $\mathbb{F}$.

Hint: if $[q_1, \ldots q_m]$ w. $q_i \neq 0$ represents 0, then it represents every element of $\mathbb{F}$.

To reduce from n to $n-1$ take $m=2$. The forms $[q_1, q_2]$ & $[-q_3, \ldots -q_n]$ represent a over $\mathbb{F} \iff [q_1, q_2, -a]$ & $[-q_3, \ldots -q_n, -a]$ represent 0 over $\mathbb{F}$, in both forms the number of variables is $< n$, so we can assume that the Minkowski theorem holds for them. Moreover, since $[q_1, \ldots q_n]$ represents 0 over $\mathbb{Q}_p$, $\exists\ a_p \in \mathbb{Q}_p \setminus \{0\} \mid [q_1, q_2, -a_p]$ & $[-q_3, \ldots, -q_n, -a_p]$ represent 0 over $\mathbb{Q}_p$ $\forall\ p \in \{\text{primes}\} \cup \{\infty\}$. It turns out that one can choose a_p to be the images of some $a \in \mathbb{Q}$ which would finish the proof. The proof that we can find such a is non-trivial (the case $n \geq 5$ is somewhat easier & more elementary as there's more flexibility while the case $n=4$ is more subtle)