Lecture 38: Hasse-Minkowski: Q.E.D.

Thm: $a_1, \dots, a_k \in \mathbb{Q}^\times$, $\varepsilon_{i,v} = \pm 1$. $\exists\, b \in \mathbb{Q}^\times$ s.t. $(a_i, b)_v = \varepsilon_{i,v}$ for all i, v if and only if

1. Almost all $\varepsilon_{i,v} = 1$.
2. $\prod_v \varepsilon_{i,v} = 1$ for each i.
3. $\exists\, x_v \in \mathbb{Q}_v^\times$ s.t. $(a_i, x_v) = \varepsilon_{i,v}$ for each i.

Hasse-Minkowski: A quadratic form q over $\mathbb{Q}$ reps 0 iff q_v reps 0 for every place v.

Proof: [Already did $n \le 3$.]

Case $n = 4$: Suppose q_v reps 0 for each v. Can take $q = ax^2 + by^2 - (cu^2 + dv^2)$ with $a, b, c, d \in \mathbb{Q}^\times$

Since q_v reps 0, there exists $x_v \in \mathbb{Q}_v^\times$ rep'd by both $f = ax^2 + by^2$ and $g = cu^2 + dv^2$.

[Reason we can take $x_v \neq 0$ is if f and g both rep 0 then they rep all of $\mathbb{Q}_v^\times$.]

By HW, this is equiv to $(x_v, -\mathrm{disc})_v = \varepsilon$, and so

$$(-ab, x_v)_v = (a, b)_v \quad \text{and} \quad (-dc, x_v)_v = (c, d)_v$$

By thm, $\exists r \in \mathbb{Q}^\times$ with $(-ab, r)_v = (a,b)_v$ and $(-cd, r)_v = (c,d)_v$ for all v.

Hence the form $ax^2 + by^2$ reps r over each $\mathbb{Q}_v \Rightarrow$ (by $n=3$ case) that ax^2+by^2 reps r over $\mathbb{Q}$.

Similarly $cu^2 + dv^2$ reps r over $\mathbb{Q}$ and hence g reps 0 over $\mathbb{Q}$, as desired.

Case $n \geq 5$: induct on n. Can write

$$g = \underbrace{a_1X_1^2 + a_2X_2^2}_{f} - \underbrace{(a_3X_3^2 + \cdots + a_nX_n^2)}_{g},$$

with $a_i \in \mathbb{Z}^\times$. If f reps b, then anything rep'd by $g' = \underbrace{bz^2 - g}_{\text{lower rank}}$ is also rep'd by g. So by induction, it suffices to show

Claim: $\exists\, b$ rep'd by f such that $g' = bz^2 - g$ reps 0 at each place v.

Let $S = \{2, \infty\} \cup \{\text{primes dividing } a_i \text{ for } i \geq 3\}$

If $v \notin S$, then g_v (and hence g'_v) reps 0

In particular, $a_3X_1^2 + a_4X_1^2 + a_5X_5^2$ repr's 0 in $\mathbb{Q}_v$ since $(-a_4/a_3, -a_5/a_3) = 1$ since these are units ↗ and $p \neq 2, \infty$.

Now as g_v repr's 0, there exist $b_v \in \mathbb{Q}_v^\times$ repr'd by both f_v and g_v. As $\mathbb{Q}$ is dense in $\prod_{v \in S} \mathbb{Q}_v$ and $(\mathbb{Q}_v^\times)^2$ is open, then (just like last time) $\exists\, b \in \mathbb{Q}^\times$ s.t. $b = b_v c_v^2$ for $v \in S$. Thus $g' = bz^2 - g$ repr's 0 since $b_v z^2 - g$ does.

This proves the claim, and thus the theorem.

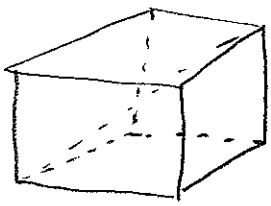
Q.E.D.

Remarks:

- Simple statement but very difficult prove, using many tools (quad. recip, Dirichlet's Thm
- Encodes many classical results

Thm (Gauss) A pos int n is the sum of 3 squares iff $n \neq 4^a(8b-1)$ with $a, b \in \mathbb{Z}$.

Proof: By HW, $x^2+y^2+z^2$ rep n over $\mathbb{Z}$ if it does so over $\mathbb{Q}$. By HM it reps n over $\mathbb{Q}$ iff it does so over each $\mathbb{Q}_v$.



For $v = \infty$ or p odd this is clearly the case, so it all comes down to $\mathbb{Q}_2$ and hence to mod 8...

Also: Every pos int is a sum of four squares and three triangular numbers $\left(= \frac{m(m+1)}{2}\right)$

Hasse-Minkowski is also key to understanding quaternion algebras (Note: can start HW now.)

Consider $\mathbb{Q} \longrightarrow \prod_{v \in V} \mathbb{Q}_v = \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3 \times \mathbb{Q}_5 \times \cdots$

$q \longmapsto (q, q, q, \ldots)$

The image of $\mathbb{Q}$ is contained in a certain natural subset of $\prod_v \mathbb{Q}_v$ called the adèles:

$$\mathbb{A}_{\mathbb{Q}} = \left\{ (x_v) \in \prod_v \mathbb{Q}_v \;\middle|\; x_v \in \mathbb{Z}_v \text{ for almost all } v \right\}$$

($\mathbb{A}_{\mathbb{Q}}$: a ring)

Topologise $\mathbb{A}_{\mathbb{Q}}$ as follows: (Not the product top.!)

Take as a basis about 0 sets of the form

$U = \prod U_v$ where $0 \in U_v$ an open subset of $\mathbb{Q}_v$

$U_v = \mathbb{Z}_v$ for almost all v.

Now the topology induced on U is the product topology; as a consequence, $\mathbb{A}_{\mathbb{Q}}$ is a locally compact topological ring

Key: $\mathbb{A}_{\mathbb{Q}} / \mathbb{Q}$ ← subgp under addition is cpt.

Compare: $\mathbb{R}/\mathbb{Z} = S^1$ or $K_{\mathbb{R}}/\mathcal{O}_K = (S^1)^n$