MA 254 notes: Diophantine Geometry

(Distilled from [Hindry-Silverman])

Dan Abramovich

Brown University

January 27, 2016

Goals

- The Mordell-Weil Theorem
- Roth's Theorem
- Maybe Siegel's Theorem
- Faltings's theorem

We follow the outline of Hindry-Silverman Part E, page 369, but skipping part A:

- Part B, 1-5 and maybe 7,
- Part C, 1-2
- Part D, 1-7 and maybe 9,
- Part E.

Theorem (Mordell-Weil)

Let k be a number field and A/k an abelian variety. Then the group of rational points $A(k)$ is a finitely generated abelian group.

Theorem (Roth)

Let $\alpha \in \bar{\mathbb{Q}}$ and $\epsilon > 0$. There are only finitely many rationals p/q with $\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^{2+\epsilon}}$.

Theorem (Siegel)

Let k be a number field and S a finite set of primes. Let $\mathcal{C}$ be a model over $\mathcal{O}_{k,S}$ of a smooth affine curve C/k of genus > 0. Then the set of integral points $\mathcal{C}(\mathcal{O}_{k,S})$ is finite.

Theorem (Faltings)

Let k be a number field C/k a smooth curve of genus > 1. Then the set of rational points $C(k)$ is finite.

Absolute values

Definition (Absolute value)

An absolute value on a filed k is a function $|\cdot|\colon k \to [0,\infty)$ such that

- $|x| = 0 \Leftrightarrow x = 0$
- $|x||y| = |xy|$
- $|x+y| \leq |x| + |y|$.

It is nonarchimedean if

- $|x+y| \leq \max\{|x|,|y|\}$.

Some absolute values on $k = \mathbb{Q}$ are $|x|_\infty = \max\{x,-x\}$, and $|x|_p = p^{-ord_p(x)}$. The set of these is denoted $M_\mathbb{Q}$. By Ostrovsky's theorem these represent all up to topological equivalence.

Standard absolute values

- An absolute value on a number field k is standard if it restricts to an element of $M_{\mathbb{Q}}$.
- We denote these by M_k. We write $v(x) = -\log |x|_v$, with $v(0) = \infty$ (this way v is a valuation).
- The archimedean ones are denoted M_k^∞, and the other alernatively $M_k^0, M_k^{fin}, M_k^{na}, M_k^{<\infty}$.
- For k'/k finite and $v \in M_k$, $w \in M_{k'}$ we say $w|v$ if $w|_k = v$.
- We have $\prod_{v\in M_{\mathbb{Q}}} |x|_v = 1$, equivalently $\sum_{v\in M_{\mathbb{Q}}} v(x) = 0$ for all nonzero $x \in \mathbb{Q}$. We want to generalize this to M_k.

Product formula

We use the following:

Proposition (Degree formula)

$\sum_{w|v}[k'_w : k_v] = [k' : k]$

Working over $\mathbb{Q}$ it is natural to define the local degree $n_v = [k_v : \mathbb{Q}_v]$ for v im M_k, and the normalized absolute value $\|x\|_v = |x|_v^{n_v}$. It is normalized for norms rather than restrictions: for $v_0 \in M_{\mathbb{Q}}$ we have $\prod_{v|v_0} \|x\|_v = |N_{k/\mathbb{Q}}(x)|_{v_0}$ (Lang).

Proposition (Product formula)

Let k be a number field and $x \in k^*$. Then $\prod_{v\in M_k} \|x\|_v = 1$.

Proof.

$\prod_v \|x\|_v \quad = \quad \prod_{v_0} \prod_{v|v_0} \|x\|_v \quad = \quad \prod_{v_0} |N_{k/\mathbb{Q}}(x)|_{v_0} = 1.$ ♠

valuations, embeddings and multiplicities

- Archimedean valuations correspond to real embeddings $\sigma : k \to \mathbb{R}$ and conjugate-pairs of complex embeddings $\sigma, \bar{\sigma} : k \to \mathbb{C}$.
- Nonarchimedean valuations correspond to prime ideals in the ring of integers, denoted R_k or $\mathcal{O}_k$.
- For each prime $\mathfrak{p}$ with uniformizer $\pi_\mathfrak{p}$ one defines the order by setting $\mathrm{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$, equivalently for each $x \in k^*$ we have that the fracrional ideal $x\mathcal{O}_k = \prod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}$.
- If $\mathfrak{p}|p$ denote the ramification index over $\mathbb{Q}$ by $e_\mathfrak{p} := \mathrm{ord}_\mathfrak{p}(p)$.
- Then writing $|x|_\mathfrak{p} = p^{-\mathrm{ord}_\mathfrak{p}(x)/e_\mathfrak{p}}$ (normalized so that $|p|_\mathfrak{p} = |p|_p$) we have the absolute value associated to $\mathfrak{p}$, with valuation denoted $v_\mathfrak{p}$,
- so $\|x\|_\mathfrak{p} = \left(N_{k/\mathbb{Q}}\mathfrak{p}\right)^{-\mathrm{ord}_\mathfrak{p}(x)}$ and $v_\mathfrak{p}(x) = -\log|x|_\mathfrak{p}$.

Rings of integers and S-integers

- We have the ring of integers
  $R_k = \mathcal{O}_k = \{x \in k \mid v(x) \geq 0 \ \ \forall v \in M_k^0\}$.
- More generally, for a finite set of absolute values $S \supset M_k^\infty$ we define the ring of S-integers
  $R_S = \mathcal{O}_{k,S} := \{x \in k \mid v(x) \geq 0 \ \ \forall v \in M_k, v \notin S\}$.
  This generalizes: $R_k = R_{M_k^\infty}$.