33.1 Faltings' theorem

We have seen that in genus 0, curves have either no points or infinitely many (parameterized by $\mathbb{P}^1$). In genus 1, the Mordell-Weil theorem explains the structure when there is at least one point: it can be finite (rank 0) or infinite, but it is finitely generated in each case. The following theorem, conjectured by Mordell in 1922 and proven by Faltings in 1983, describes the situation for curves of genus larger than 1.

Theorem 33.1. *Suppose k is a number field and C/k is a curve of genus $g > 1$. Then $C(k)$ is finite.*

The original proof [1] is very technical and involved. There are two alternate proofs known: the first rests on an inequality of Vojta [2] and the second on results from p-adic Hodge theory [4].

Remark 33.2. An analogue of Falting's theorem holds in the function field setting (where k is a finite extension of $\mathbb{F}_q(x)$), but an additional assumption is needed that C is not *isotrivial*. This rules out curves that arise via base change from $\mathbb{F}_q$ for example. This analogue was proven earlier, in 1966.

33.2 Jacobian varieties

If k is a field and C/k is a smooth projective curve, then the group $\mathrm{Pic}^0_k(C)$ has the structure of a projective variety over k. Since it is also a group (and the group operations are regular maps), it is an abelian variety. This variety is called the *Jacobian* of C, and we will denote it J_C. See [5, Chapter 3] for a more detailed exposition.

We can get a better understanding of J_C by considering symmetric powers of C. If $r \in \mathbb{Z}_{\geq 1}$, write C^r for the product of r copies of C with itself.

Definition 33.3. The rth *symmetric power* $C^{(r)}$ of C is the quotient of C^r by the action of the symmetric group. Specifically, the quotient definition holds for $C^{(r)}$ as a topological space, and if U is an affine open subset of C then the functions on the affine open $U^{(r)} \subset C^{(r)}$ are defined as those functions on U^r that are fixed by all permutations.

There is a canonical identification of $C^{(r)}$ with effective divisors on C of degree r, since a formal sum is just an unordered multiset of points on C.

Proposition 33.4. *If C is a smooth projective curve then $C^{(r)}$ is a smooth variety of dimension r.*

Proof. Taking a quotient by a finite group action does not change the dimension. Smoothness follows from the fact that any symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions. For more details see [5, III.3.2]. □

If $P_0 \in C(k)$, we may define a natural map $\alpha_r : C^{(r)} \to J_C$ by

$$(P_1, \ldots, P_r) \mapsto P_1 + \cdots + P_r - rP_0.$$

Theorem 33.5. *Let g be the genus of C. For $1 \leq r \leq g$, the image of α_r is a closed subvariety W_r of J_C, and $\alpha_r : C^{(r)} \to W_r$ is birational. In particular, $C^{(g)}$ is birational to J_C.*

Proof. See [5, III.5]. □

For elliptic curves, we saw α_1 in Theorem 23.16, where it was an isomorphism and not just birational. In general, α_1 provides an embedding of C into J_C (under the assumption that C has at least one rational point!). The images arising from different choices of P_0 are related by translation on J_C.

The definition of isogeny naturally extends to abelian varieties:

Definition 33.6. If A and A' are abelian varieties, an *isogeny* from A to A' is a surjective morphism $\phi : A \to A'$ with finite kernel.

Over an algebraically closed field, if $g \leq 3$ then every principally polarized[1] abelian variety of dimension g is isogenous to the Jacobian of a genus g curve. For $g \geq 4$, the moduli space of genus g curves has smaller dimension than the moduli space of abelian varieties of dimension g, so this can no longer hold. But it is the case that any abelian variety is the quotient of a Jacobian [5, III.10.1].

33.3 Mordell-Weil for abelian varieties

The Mordell-Weil theorem holds for abelian varieties over number fields:

Theorem 33.7. *Suppose k is a number field and A/k is an abelian variety. Then $A(k)$ is a finitely generated abelian group.*

The proof has the same overall structure as for elliptic curves: prove that $A(k)/2A(k)$ is finite, and then use heights to show that $A(k)$ is finitely generated. For more details, see [3, Chapter 6].

33.4 Vojta's Inequality

Set $J_{\mathbb{R}} = J_C(k) \otimes \mathbb{R}$. By the Mordell-Weil theorem, this is a finite dimensional $\mathbb{R}$-vector space. Just as for elliptic curves, there is a canonical height function on $J_C(k)$ that induces a positive definite quadratic form on $J_{\mathbb{R}}$, which we write as $|x|$. As usual, we write $\langle x, y \rangle$ for the associated inner product:

$$\langle x, y \rangle = \frac{1}{2}(|x+y|^2 - |x|^2 - |y|^2).$$

Theorem 33.8 (Vojta's Inequality)**.** *There are constants $\kappa_1 = \kappa_1(C)$ and $\kappa_2 = \kappa_2(g)$ so that, if $z, w \in C(\overline{k})$ satisfy*

$$|z| \geq \kappa_1 \text{ and } |w| \geq \kappa_2 |z|$$

then

$$\langle z, w \rangle \leq \frac{3}{4}|z| \cdot |w|.$$

Much of Hindry and Silverman's book [2] is devoted to a proof of this theorem.

[1] A principal polarization of an abelian variety A is an isomorphism from A to its dual; the dual can be described as the space of line bundles on A.

33.5 Proof of Falting's theorem

We follow the exposition in [2, §E.1].

If $C(k)$ is empty then it is certainly finite. If not, then a choice of point gives an embedding $\alpha_1 : C(k) \hookrightarrow J_C(k)$.

Note that the kernel of the map $J(k) \to J_{\mathbb{R}}$ is the finite group $J(k)_{\mathrm{tors}}$, so it suffices to show that the image $C_{\mathbb{R}}$ of $C(k)$ in $J_{\mathbb{R}}$ is finite. We will do so by covering $J_{\mathbb{R}}$ by cones, each of which has finite intersection with $C_{\mathbb{R}}$. For $x \in J_{\mathbb{R}}$, set

$$Y_x = \{y \in J_{\mathbb{R}} : \langle x, y\rangle > \cos(\pi/12) \cdot |x| \cdot |y|\}.$$

Lemma 33.9. *The intersection $Y_x \cap C_{\mathbb{R}}$ is finite.*

Proof. Suppose not. Then there is a $z \in Y_x \cap C_{\mathbb{R}}$ with $|z| \geq \kappa_1$ since there are only finitely many $z \in J_{\mathbb{R}}$ with $|z| < \kappa_1$. Once z is fixed, we can similarly find $w \in Y_x \cap C_{\mathbb{R}}$ with $|w| \geq \kappa_2 |z|$. By Vojta's inequality we have

$$\langle z, w\rangle \leq \frac{3}{4}|z| \cdot |w|.$$

But z and w are both in the cone Y_x, so the angle between them is at most $\pi/6$, and $\cos(\pi/6) > 3/4$. □

Lemma 33.10. *There is a finite set $X \subset J_{\mathbb{R}}$ so that $J_{\mathbb{R}} - \{0\} = \bigcup_{x \in X} Y_x$.*

Proof. Let S be the unit sphere in $J_{\mathbb{R}}$. For any x, if $y \neq 0$ then $y \in Y_x \Leftrightarrow \frac{y}{|y|} \in S \cap Y_x$ since Y_x is a cone. But S is compact and all $Y_x \cap S$ are open subsets of S, so there is a finite subcover. □

Together, the lemmas imply that $C_{\mathbb{R}}$, and thus $C(k)$, is finite.

References

[1] G. Faltings. *Finiteness theorems for abelian varieties over number fields.* In *Arithmetic Geometry*, G. Cornell and J. Silverman (ed), Springer-Verlag, New York, 1986.

[2] M. Hindry and J. Silverman. *Diophantine Geometry: an Introduction.* GTM 201. Springer, New York, 2000.

[3] S. Lang. *Fundamentals of Diophantine Geometry.* Springer, New York, 1962.

[4] B. Lawrence and A. Venkatesh. *Diophantine problems and p-adic period mappings.* Inventiones mathematicae **221**, 2020.

[5] J. Milne. *Abelian Varieties.* https://www.jmilne.org/math/CourseNotes/AV.pdf.