Artin's Approximation Theorem

Unit 8

Gil Cohen

November 18, 2024

Artin's Approximation Theorem

The main result we prove in this unit is the following.

Theorem 1 (The weak approximation theorem)

Let $\upsilon_1, \ldots, \upsilon_n : \mathsf{F}^\times \to \mathbb{Z}$ *be non-equivalent valuations with* $\upsilon_i(\mathsf{F}^\times) = \mathbb{Z}$ *for all* $i \in [n]$. *Let* $a_1, \ldots, a_n \in \mathsf{F}$ *and* $m_1, \ldots, m_n \in \mathbb{Z}$. *Then,*

$$\exists x \in \mathsf{F} \quad \forall i \in [n] \quad \upsilon_i(x - a_i) = m_i.$$

What is being approximated?

Recall that a large valuation corresponds to closeness, namely,

$$\upsilon_i(x - a_i) = m_i \quad \Longrightarrow \quad |x - a_i|_i = 2^{-m_i}.$$

Artin's Approximation Theorem and the CRT

Theorem 1 is a generalization of the Chinese Remainder Theorem.

E.g., say that we want $x \in \mathbb{Z}$ s.t.

$$x \equiv_{2^5} 3$$
$$x \equiv_{3^7} 10.$$

Working with p-adics, this is equivalent to

$$\upsilon_2(x-3) \geq 5$$
$$\upsilon_3(x-10) \geq 7,$$

where υ_2, υ_3 are the 2-adic and 3-adic valuations.

A lemma about discrete valuations

A valuation ring is discrete if a valuation v in the corresponding congruence class of valuations is discrete.

Lemma 2

Let $\mathcal{O}_1, \mathcal{O}_2$ be discrete valuation rings with fraction field F. *Then,*

$$\mathcal{O}_1 \subseteq \mathcal{O}_2 \quad \Longrightarrow \quad \mathcal{O}_1 = \mathcal{O}_2 \quad (\iff v_1 \sim v_2)$$

We start by proving the following claim.

Claim 3

Let $\mathcal{O}_1, \mathcal{O}_2$ be valuation rings with fraction field F. Then, TFAE:

1. $\mathcal{O}_1 \subseteq \mathcal{O}_2$
2. $\forall a \in \mathsf{F} \quad v_1(a) \geq 0 \implies v_2(a) \geq 0$
3. $\forall a \in \mathsf{F} \quad v_2(a) > 0 \implies v_1(a) > 0.$

A lemma about discrete valuations

Proof.

(1) $\iff$ (2) is straightforward.

We turn to prove (2) $\iff$ (3). By (2),

$$\forall a \in F^{\times} \quad v_1(a^{-1}) \geq 0 \implies v_2(a^{-1}) \geq 0,$$

which is equivalent to

$$\forall a \in F^{\times} \quad -v_1(a) \geq 0 \implies -v_2(a) \geq 0,$$

namely,

$$\forall a \in F^{\times} \quad v_1(a) \leq 0 \implies v_2(a) \leq 0.$$

However, the above is equivalent to

$$\forall a \in F^{\times} \quad v_2(a) > 0 \implies v_1(a) > 0.$$

This establishes (2) $\iff$ (3). □

A lemma about discrete valuations

Proof of Lemma 2.

We assume $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and wish to prove equality.

It suffices to prove that

$$v_2(a) \geq 0 \quad \Longrightarrow \quad v_1(a) \geq 0.$$

Take $b \in \mathrm{F}^\times$ s.t. $v_2(b) > 0$. Why such b exists?

Then, for every $m \geq 1$,

$$v_2(a^m b) = m v_2(a) + v_2(b) > 0.$$

Per our assumption $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and using Claim 3, we conclude that

$$v_1(a^m b) = m v_1(a) + v_1(b) > 0.$$

As the above holds for all $m \geq 1$, it must be the case that $v_1(a) \geq 0$. □

Step 1

Claim 4

Let $v_1, \ldots, v_n : \mathrm{F}^\times \to \mathbb{Z}$ be discrete non-equivalent valuations. Then, $\exists x \in \mathrm{F}$ s.t.

$$v_1(x) \geq 0,$$
$$v_i(x) < 0 \text{ for all } i > 1.$$

Proof.

The proof is by induction on n. For $n = 1$ take, say, $x = 0$.

For $n = 2$, as v_1, v_2 are not equivalent, $\mathcal{O}_{v_1} \neq \mathcal{O}_{v_2}$.

Lemma 2 then implies that $\mathcal{O}_{v_1} \not\subseteq \mathcal{O}_{v_2}$. Thus we can take $x \in \mathcal{O}_{v_1} \setminus \mathcal{O}_{v_2}$.

Step 1

Proof.

Assume by induction that $\exists y \in F$ s.t. $\upsilon_1(y) \geq 0$ yet $\upsilon_i(y) < 0$ for $i = 2, \ldots, n-1$.

Using the $n = 2$ case, $\exists z \in F$ s.t. $\upsilon_1(z) \geq 0$ yet $\upsilon_n(z) < 0$.

Consider the element

$$x = y + z^m$$

for $m \geq 1$ to be chosen s.t.

$$\upsilon_i(z^m) = m\upsilon_i(z) \neq \upsilon_i(y)$$

for all $i \geq 2$ with $\upsilon_i(z) \neq 0$.

We have that

$$\upsilon_1(x) = \upsilon_1(y + z^m) \geq \min(\upsilon_1(y), m\upsilon_1(z)) \geq 0.$$

Step 1

Proof.

For $i = 2, \ldots, n-1$,

$$v_i(y + z^m) \geq \min(v_i(y), mv_i(z)).$$

Recall that $v_i(y) < 0$. If $v_i(z) = 0$ then, by the strict triangle inequality,

$$v_i(y + z^m) = \min(v_i(y), mv_i(z)) < 0.$$

If, on the other hand, $v_i(z) \neq 0$ then, by the choice of m,

$$v_i(y) \neq mv_i(z),$$

and so

$$v_i(y + z^m) = \min(v_i(y), mv_i(z)) < 0.$$

Step 1

Proof.

Lastly,

$$\upsilon_n(y + z^m) \geq \min(\upsilon_n(y), m\upsilon_n(z)).$$

As $\upsilon_n(z) < 0$, we can choose m large enough so that $m\upsilon_n(z) < v_n(y)$.

Hence, by the strict triangle inequality,

$$\upsilon_n(y + z^m) = \min(\upsilon_n(y), m\upsilon_n(z)) < 0.$$

Step 2

Claim 5

Let $\upsilon_1, \ldots, \upsilon_n : \mathsf{F}^\times \to \mathbb{Z}$ be discrete non-equivalent valuations. Then, $\exists x \in \mathsf{F}$ s.t.

$$\upsilon_1(x) > 0,$$
$$\upsilon_i(x) < 0 \text{ for all } i > 1.$$

Proof.

By Claim 4, $\exists z \in \mathsf{F}$ s.t.

$$\upsilon_1(z) \geq 0,$$
$$\upsilon_i(z) < 0 \text{ for all } i > 1.$$

Take $y \in \mathsf{F}$ with $\upsilon_1(y) > 0$, and set $x = z^m y$ for m large enough. Then,

$$\upsilon_1(x) = m\upsilon_1(z) + \upsilon_1(y) > 0$$

and for $i > 1$, taking m large enough,

$$\upsilon_i(z^m y) = m\upsilon_i(z) + v_i(y) < 0.$$

Step 3

Claim 6

Let $\upsilon_1, \ldots, \upsilon_n : \mathsf{F}^\times \to \mathbb{Z}$ be non-equivalent valuations. Then, for every $m_1, \ldots, m_n \in \mathbb{Z}$ $\exists x \in \mathsf{F}$ s.t.

$$\upsilon_1(x-1) > m_1,$$
$$\upsilon_i(x) > m_i.$$

Proof.

By Claim 5, $\exists y \in \mathsf{F}$ s.t.

$$\upsilon_1(y) > 0,$$
$$\upsilon_i(y) < 0 \text{ for all } i > 1.$$

Then, for $m \geq 1$ to be chosen later on, we get

$$\upsilon_1(1+y^m) = 0,$$
$$\upsilon_i(1+y^m) = m\upsilon_i(y) < 0.$$

Step 3

Proof.

$$\upsilon_1(1+y^m) = 0,$$
$$\upsilon_i(1+y^m) = mv_i(y) < 0.$$

Define

$$x = \frac{1}{1+y^m}.$$

Then, for large enough m,

$$\upsilon_1(x-1) = \upsilon_1\left(-\frac{y^m}{1+y^m}\right) = m\upsilon_1(y) > m_1,$$

and for $i > 1$,

$$\upsilon_i(x) = -\upsilon_i(1+y^m) = -m\upsilon_i(y) > m_i.$$

Step 4

Claim 7

Let $\upsilon_1, \ldots, \upsilon_n : \mathrm{F}^\times \to \mathbb{Z}$ be non-equivalent discrete valuations. Let $a_1, \ldots, a_n \in \mathrm{F}$ and $m_1, \ldots, m_n \in \mathbb{Z}$. Then,

$$\exists x \in \mathrm{F} \quad \forall i \in [n] \quad \upsilon_i(x - a_i) > m_i.$$

Proof.

If $a_1 = \cdots = a_n = 0$ we can take $x = 0$. Otherwise, for $i \in [n]$, define

$$\tau_i = \min_{j \in [n]} \upsilon_i(a_j) \in \mathbb{Z}.$$

By Claim 6, $\forall j \in [n]$ $\exists x_j \in \mathrm{F}$ s.t.

$$\begin{aligned} \upsilon_j(x_j - 1) &> m_j - \tau_j \\ \upsilon_i(x_j) &> m_i - \tau_i \ \text{ for all } i \neq j. \end{aligned}$$

Step 4

Proof.

$\forall j \in [n]\ \ \exists x_j \in \mathrm{F}$ s.t.

$$\upsilon_j(x_j - 1) > m_j - \tau_j$$
$$\upsilon_i(x_j) > m_i - \tau_i \ \text{ for all } i \neq j.$$

Thus, for $i \neq j$,

$$\upsilon_i(a_j x_j) = \upsilon_i(a_j) + \upsilon_i(x_j) > \tau_i + (m_i - \tau_i) = m_i.$$

Define $x = a_1 x_1 + \cdots + a_n x_n$. Then,

$$x - a_i = (x - a_i x_i) + (a_i x_i - a_i) = \sum_{j \neq i} a_j x_j + a_i(x_i - 1).$$

Since

$$\upsilon_i(a_i(x_i - 1)) = \upsilon_i(a_i) + \upsilon_i(x_i - 1) > \tau_i + m_i - \tau_i > m_i,$$

we conclude that $\upsilon_i(x - a_i) > m_i$.

Step 5

We are now in a position to prove Theorem 1.

Proof.

By Claim 7,

$$\exists y \in \mathrm{F} \quad \forall i \in [n] \quad \upsilon_i(y - a_i) > m_i.$$

Now, for each i take $b_i \in \mathrm{F}$ s.t. $\upsilon_i(b_i) = m_i$, and apply Claim 7 again to conclude

$$\exists z \in \mathrm{F} \quad \forall i \in [n] \quad \upsilon_i(z - b_i) > m_i.$$

Define

$$x = y + z.$$

We have that

$$x - a_i = y + z - a_i = (y - a_i) + (z - b_i) + b_i,$$

and so, by the strict triangle inequality,

$$\upsilon_i(x - a_i) = \min(\upsilon_i(y - a_i), \upsilon_i(z - b_i), \upsilon_i(b_i)) = m_i.$$