D3: Skolem-Mahler-Lech Theorem

Montag, 23. Juni 2025 16:39

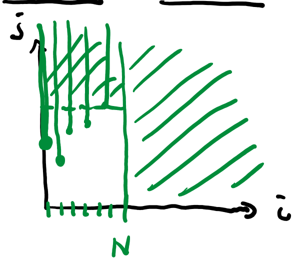
Prop 3.1 Let $(B_{i,j})_{i,j\geq 0}$ be a seq. in $\mathbb{Q}_p$.

If
- $\forall i \geq 0: \lim\limits_{j\to\infty} B_{ij} = 0$
- $\forall j \geq 0: \lim\limits_{i\to\infty} B_{ij} = 0$ uniformly in j

(i.e. $\forall \varepsilon > 0\ \exists N \geq 0\ \forall i \geq N\ \forall j \geq 0: |B_{ij}|_p < \varepsilon$)

then $\sum\limits_{i=0}^{\infty}\sum\limits_{j=0}^{\infty} B_{ij} = \sum\limits_{j=0}^{\infty}\sum\limits_{i=0}^{\infty} B_{ij}$ and both converge.

Proof: **Claim:** $\forall \varepsilon > 0\ \exists M \geq 0\ \forall i,j: \max(i,j) \geq M \Rightarrow |B_{ij}|_p < \varepsilon$



1) Pick N s.t. $\forall i \geq N\ \forall j: |B_{ij}|_p < \varepsilon$
2) For $0 \leq i \leq N-1$ pick N_i s.t. $\forall j \geq N_i: |B_{ij}|_p < \varepsilon$
3) $M := \max\{N_0, \dots, N_{N-1}, N\}$. $\square$ (Claim)

Convergence: $\sum\limits_{j=0}^{\infty} B_{ij}$, $\sum\limits_{i=0}^{\infty} B_{ij}$ converge because $\lim\limits_{j\to\infty} B_{ij} = 0$, $\lim\limits_{i\to\infty} B_{ij} = 0$.

Now $\left|\sum\limits_{j=0}^{\infty} B_{ij}\right|_p \overset{\text{ultrametric}}{\leq} \max\{|B_{ij}|_p : j \geq 0\} \leq \varepsilon\ \ \forall i \geq M$, so $\lim\limits_{i\to\infty}\sum\limits_{j=0}^{\infty} B_{ij} = 0$.

Similarly, $\lim\limits_{j\to\infty}\sum\limits_{i=0}^{\infty} B_{ij} = 0$, so double sums converge (Cor 2.2).

Equality:

$$\left|\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} B_{ij} - \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} B_{ij}\right|_p = \left|\sum_{i=0}^{M-1}\sum_{j=M}^{\infty} B_{ij} - \sum_{i=M}^{\infty}\sum_{j=0}^{\infty} B_{ij}\right|_p \overset{\text{ultrametric}}{<} \varepsilon$$

Same with $\sum\limits_{j=0}^{\infty}\sum\limits_{i=0}^{\infty} B_{ij}$, so $\sum\limits_{i=0}^{\infty}\sum\limits_{j=0}^{\infty} B_{ij} = \sum\limits_{j=0}^{\infty}\sum\limits_{i=0}^{\infty} B_{ij}$. $\square$

Thm 3.2 (Skolem-Mahler-Lech) Let K be a field, char $K = 0$.
If $(a_n)_{n\geq 0}$ is an LRS, then $\{n : a_n = 0\}$ is a union of a finite set and fin. many arithmetic progressions.

If $(a_n)_{n\geq 0}$ is an LRS, then $\{n : a_n = 0\}$ is a union of a finite set and fin. many arithmetic progressions

We only do $K=\mathbb{Q}$, general case: „specialization argument"

Prop 3.3 If $(a_n)_{n\geq 0}$ is a strict $\mathbb{Q}$-LRS, then $\{n : a_n = 0\} = F \cup (k_1 + N\mathbb{N}_0) \cup \dots \cup (k_r + N\mathbb{N}_0)$ with F finite, $N \geq 1$, $0 \leq k_1 < \dots < k_r < N$.

Thm 3.2 follows from P1.2 + P3.3.

Proof of Prop 3.3 Suppose $\forall n \geq d$: $a_n = c_1 a_{n-1} + \dots + c_d a_{n-d}$ with $c_1, \dots, c_d \in \mathbb{Q}$ and $c_d \neq 0$ (by strictness).

Without restriction $c_1, \dots, c_d \in \mathbb{Z}$: let $M \in \mathbb{N}$ be s.t. $Mc_i \in \mathbb{Z}$ $\forall i$,

$$\Rightarrow M^n a_n = (Mc_1)(M^{n-1}a_{n-1}) + (M^2 c_2)(M^{n-2} a_{n-2}) + \dots + (M^d c_d)(M^{n-d} a_{n-d}),$$

and so $(\tilde{a}_n)_{n\geq 0}$ with $\tilde{a}_n = M^n a_n \in \mathbb{Q}$ is a strict LRS with coeff's in $\mathbb{Z}$. Taking M s.t. also $Ma_i \in \mathbb{Z}$ for $0 \leq i \leq d-1$, even $M\tilde{a}_n \in \mathbb{Z}$ $\forall n \geq 0$.

Now let $a_n = u^T A^n v$ $(*)$ with

$$u = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ c_d & \cdots & & c_1 \end{pmatrix}, \quad v = \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix}, \quad \text{where } A \in \mathbb{Z}^{d\times d}$$

$(a_n)_{n\geq 0}$ strict $\Rightarrow c_d \neq 0 \Rightarrow \det A \neq 0$, $\det(A) \in \mathbb{Z}$

Fix a prime $p \neq 2$ s.t. $p \nmid \det(A)$.

$\mathbb{Z}^{d\times d} \to \mathbb{F}_p^{d\times d}$, $X \mapsto \overline{X}$ (entrywise) is a ring hom,

$\det(\overline{X}) = \overline{\det(X)}$, because $\det(X)$ is a polynomial expression in the entries.

$$\rightarrow \det(\overline{A}) \in \mathbb{F}_p^\times \Rightarrow \overline{A} \in \underbrace{GL_d(\mathbb{F}_p)}_{\text{finite group}} \Rightarrow \exists N \geq 1: \overline{A}^N = \overline{I}$$

$$\Rightarrow A^N = I + pB \text{ with } B \in \mathbb{Z}^{d\times d}$$

$\Longrightarrow A^N = I + pB$ with $B \in \mathbb{Z}^{d\times d}$

For each $0 \leq c \leq N-1$, consider $(a_{c+nN})_{n\geq 0}$

Claim: $(a_{c+nN})_{n\geq 0}$ is either identically 0 or has finitely many zeros.

$$a_{c+nN} = u^T A^{c+nN} v = u^T (A^N)^n A^c v = u^T (I+pB)^n \underbrace{A^c v}_{=:\tilde{v} \in \mathbb{Z}^d}$$

Idea: Interpolate $n \mapsto u^T(I+pB)^n v$ by a p-adic power series.

$$(I+pB)^n = \sum_{i=0}^{n} \binom{n}{i} p^i B^i = \sum_{i=0}^{\infty} \underbrace{\binom{n}{i}}_{=0 \text{ if } i>n} p^i B^i$$

$$\mathbb{Q}_p[\![x]\!] \ni f := \sum_{i=0}^{\infty} \underbrace{\binom{x}{i}}_{=\frac{x(x-1)\cdot\ldots\cdot(x-i+1)}{i!}} \underbrace{u^T B^i \tilde{v}}_{\in\mathbb{Z}} \cdot p^i = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} \underbrace{c_{ij}}_{\in\mathbb{Z},\ =0 \text{ if } j>i} \frac{p^i}{i!} x^j$$

For $x \in \mathbb{Z}_p$ $(|x|_p \leq 1)$

$$\left| c_{ij} \frac{p^i}{i!} x^j \right|_p \leq p^{-i} p^{v_p(i!)} = p^{-i + \frac{i - s_p(i)}{p-1}} \leq p^{-i \overbrace{\frac{p-2}{p-1}}^{>0}} \to 0 \text{ as } i \to \infty \quad (p \neq 2)$$

uniformly in j.

$\overset{\text{P3.1}}{\Longrightarrow}$ $f(x) = \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} c_{ij} \frac{p^i}{i!} \right) x^j$ is a convergent power series on $\mathbb{Z}_p$

interpolating a_{c+nN} $\Rightarrow$ a_{c+nN} is either identically 0

or has finitely many zeros on the compact $\mathbb{Z}_p$ $\square$

If $(a_n)_{n\geq 0}$ is strict, we can extend to $(a_n)_{n\in\mathbb{Z}}$ (uniquely),

to get a linear reccurence bi-sequence (LRBS)

Cor 3.4 If $(a_n)_{n\in\mathbb{Z}}$ is a strict $\mathbb{Q}$-LRBS, then

Cor 3.4 If $(a_n)_{n\in\mathbb{Z}}$ is a strict $\mathbb{Q}$-LRBS, then $\{n\in\mathbb{Z} : a_n = 0\} = F \cup (k_1 + N\mathbb{Z}) \cup \ldots \cup (k_r + N\mathbb{Z})$ for $N \geq 1$, $1 \leq k_1 < \ldots < k_r \leq N-1$, $F \subseteq \mathbb{Z}$ finite.

Idea: $\mathbb{Z} \subseteq \mathbb{Z}_p$, the interpolation in P3.2 works for all $n \in \mathbb{Z}$ (with minor technical changes: use $p \nmid M$ to keep $|c_{ij}|_p \leq 1$ despite $a_n \notin \mathbb{Z}$, binomial series). Or: Prop 3.3 + Exc. (1) + (2)