PMATH 945: ARITHMETIC DYNAMICS

HEESUNG YANG

1. September 15

Definition 1.1. The ring of p-adic integers: $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(a_1, a_2, \dots) : a_i \in \mathbb{Z}/p^i\mathbb{Z}, a_{i+1} \equiv a_i \pmod{p^i} \text{ for all } i\}$

Remark 1. Note that $\mathbb{Z}_p$ is a abelian group with the operations $(a_1, a_2, \dots) \oplus (b_1, b_2, \dots) = (a_1 + b_1, a_2 + b_2, \dots)$ and $(a_1, a_2, \dots) \otimes (b_1, b_2, \dots) = (a_1 b_1, a_2 b_2, \dots)$.

Proposition 1.2. *$\mathbb{Z}_p$ is an integral domain and we have an embedding $\psi : \mathbb{Z} \to \mathbb{Z}_p$ (a ring homomorphism) such that the image of ψ is dense.*

Proof. Suppose that we have a product that vanishes, i.e., there exist $(a_1, a_2, \dots)(b_1, b_2, \dots) = 0$ in $\mathbb{Z}_p$. Then this means that $a_i b_i \equiv 0 \pmod{p^i}$ for all i. Suppose that neither $(a_1, a_2, \dots)$ nor $(b_1, b_2, \dots)$ is zero. Then there exist i such that $a_i \not\equiv 0 \pmod{p^i}$ and j such that $b_j \not\equiv 0 \pmod{p^j}$. Thus we have $a_{i+j} b_{i+j} \not\equiv 0 \pmod{p^{i+j}}$ (by the projective limit definition of $\mathbb{Z}_p$, we know that $p^i \nmid a_{i+j}$ and $p^j \nmid b_{i+j}$), so this will give a contradiction and so we get the desired result.

To construct ψ, notice that for all $j \geq 1$, we have $\psi_j : \mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$. We define

$$\psi(n) = (\psi_1(n), \psi_2(n), \dots) = (n + p\mathbb{Z}, n + p^2\mathbb{Z}, n + p^3\mathbb{Z}, \dots).$$

This is injective since the kernel of ψ is $\{(0, 0, 0, \dots)\}$.

For the "dense" part of the proposition, start with $(a_1 + p\mathbb{Z}, a_2 + p^2\mathbb{Z}, \dots) \in \mathbb{Z}_p$ with $a_1, a_2, \dots \in \mathbb{Z}$. Let $n_i = a_i$ for all i. Then notice that

$$\begin{aligned}(a_1 + p\mathbb{Z}, a_2 + p^2\mathbb{Z}, \dots) - \psi(n_k) &= (a_i + p^i\mathbb{Z})_i - (a_k + p^i\mathbb{Z})_i \\ &= (0 + p\mathbb{Z}, 0 + p^2\mathbb{Z}, \dots, 0 + p^k\mathbb{Z}, a_{k+1} - a_k + p^{k+1}\mathbb{Z}, \dots)\end{aligned}$$

So $|(a_i + p^i\mathbb{Z})_i - \psi(n_k)|_p \leq p^{-k} \to 0$ as $k \to \infty$. Therefore $\{\psi(n_k)\}_{k=0}^{\infty}$ isa a Cauchy sequence whose limit is $(a_i + p^i\mathbb{Z})_i$. Thus $\psi(\mathbb{Z})$ is dense in $\mathbb{Z}_p$. Henceforth we shall identify $\mathbb{Z}$ with its image in $\mathbb{Z}_p$. □

Remark 2. In this assignment, you will show that $\mathbb{Z}_p$ is *a local ring*, with the maximal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$.

Remark 3. If we invert p, we have $\mathbb{Z}_p[\frac{1}{p}] =: \mathbb{Q}_p$, the field of fractions of $\mathbb{Z}_p$ (also known as *the field of p-adic numbers*). In $\mathbb{Q}_p$, every element is of the form $\frac{a}{p^k}$, where $k \geq 0, a \in \mathbb{Z}_p$. Note that the representation of each element is not unique, since one can find $a, a' \in \mathbb{Z}_p$ so that $p^k a' = p^j a$ for some $j, k \in \mathbb{Z}$. But we can still put the p-adic norm, defined on the p-adic numbers as follows:

$$|x|_p = \left|\frac{a}{p^k}\right|_p = \frac{|a|_p}{p^{-k}} = p^k |a|_p.$$

Date: 2 September 2016.

Remark 4. Every $x \in \mathbb{Q}_P$ can be written *uniquely* as

$$x = p^a u, \text{ where } u \in \mathbb{Z}_p, |u|_p = 1, a \in \mathbb{Z}.$$

Then $|x|_p = p^{-k}$ for some k. Thus, $|p^{-k}x|_p = 1$, or $x = p^k(p^{-k}x) = p^k a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Proposition 1.3. *Let K be a finitely-generated field extension of $\mathbb{Q}$. Then there exists infinitely many primes p for which we can embed $K \hookrightarrow \mathbb{Q}_p$. Moreover, if $S \subseteq K \setminus \{0\}$ then we have infinitely many p for which $S \hookrightarrow \mathbb{Z}_p \setminus p\mathbb{Z}_p$.*

Example 1.4. We claim that $\mathbb{Q}(i) \not\hookrightarrow \mathbb{Q}_3$. In fact, $\mathbb{Q}(i) \not\hookrightarrow \mathbb{Q}_p$ for all $p \equiv 3 \pmod 4$. To get started, let's suppose we have an embedding, i.e.,

$$i \mapsto 3^k a, \text{ where } k \in \mathbb{Z}, a \in \mathbb{Z}_3 \setminus 3\mathbb{Z}_f = \mathbb{Z}_3^*.$$

Thus we have $i^2 = -1 \mapsto 3^{2k}a^2$, so $1 = |-1|_3 = |3^{2k}a^2|_3 = |3^{2k}|_3|a^2|_3 = 3^{-2k}$. Hence $k = 0$. So $i \mapsto a \in \mathbb{Z}_3 \setminus 3\mathbb{Z}_3$, where $a = (a_1 + 3\mathbb{Z}, a_2 + 9\mathbb{Z}, \dots)$ with $a_{i+1} \equiv a_i \pmod{a^i}$. So $-1 = (a_1^2 + 3\mathbb{Z}, a_2^2 + 9\mathbb{Z}, a_3^2 + 27\mathbb{Z}, \dots)$, but this is impossible as $a_1^2 \not\equiv -1 \pmod 3$ for any $a_1 \in \mathbb{Z}$, a contradiction.

However, $\mathbb{Q}(i) \hookrightarrow \mathbb{Q}_5$. Notice that $2^2 \equiv -1 \pmod 5$. Thus one can find $x_2, x_3, x_4, \dots$ such that

$$i \mapsto (2 + 5\mathbb{Z}, x_2 + 25\mathbb{Z}, x_3 + 125\mathbb{Z}, \dots)$$

with $x_2 = 2 + 5k$ for some k and $x_2^2 \equiv -1 \pmod{25}$. We see that $4 + 20k + 25k^2 \equiv 4 + 20k \equiv -1 \pmod{25}$, so $k = 1$.

2. September 17

Lemma 2.1 (Hensel's Lemma). *Let p be a prime and let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial, and suppose that there exists $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod p$ (that is, $f(a) \in p\mathbb{Z}_p$, or $|f(a)|_p < 1$), and that $f'(a) \not\equiv 0 \pmod p$. Then there exists $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $b \equiv a \pmod p$.*

Example 2.2. Recall that $\mathbb{Q}(i) \hookrightarrow \mathbb{Q}_5$ and that $i \mapsto (2 + 5\mathbb{Z}, x_2 + 25\mathbb{Z}, \dots) \in \mathbb{Z}_5$, and let $f(x) = x^2 + 1$. Since $f(2) \equiv 0 \pmod 5$ and $f'(2) \not\equiv 0 \pmod 5$, we can apply Hensel to find $b \in \mathbb{Z}_5$ such that $f(b) = 0, b^2 + 1 = 0$, namely with $i \mapsto b$.

Proof. **Strategy:** For each $k \geq 1$, we will produce a number $n_k \in \mathbb{Z}$ such that $f(n_k) \equiv 0 \pmod{p^k}$ (by induction with $n_1 = a$ as the base case). Then we will use the fact that $\mathbb{Z}_p$ is compact and $\{n_k\}_k \subset \mathbb{Z}_p$ is Cauchy and it will converge to some $b \in \mathbb{Z}_p$.

Suppose we have $n_1(= a), n_2, n_3, \dots, n_k \in \mathbb{Z}$ such that $p^i \mid f(n_i)$ for all $1 \leq i \leq k$, with $n_{i+1} \equiv n_i \pmod{p^i}$ for all i. We now show how to construct n_{k+1}. We want $n_{k+1} \equiv n_k \pmod{p^k}$ and $p^{k+1} \mid f(n_{k+1})$. We need to find some $x \in \mathbb{Z}$ such that $p^{k+1} \mid f(n_k + p^k x)$. Apply Taylor's theorem:

$$f(a + x) = f(a) + f'(a)x + \frac{f''(a)}{2!}x^2 + \cdots + \frac{f^{(d)}(a)}{d!}x^d,$$

if f is a polynomial of degree d. Hence

$$\begin{aligned} f(n_k + p^k x) &= f(n_k) + p^k x f'(n_k) + p^{2k}x^2\frac{f^{(2)}(n_k)}{2!} + \cdots + \frac{f^{(d)}(n_k)}{d!}p^{dk}x^d \\ &\equiv f(n_k) + f'(n_k)p^k x \pmod{p^{k+1}}. \end{aligned}$$

Thus, it suffices to find x such that $f(n_k) + p^k x f'(n_k) \equiv 0 \pmod{p^{k+1}}$. By our inductive hypothesis, we have $f(n_k) = p^k y$ for $y \in \mathbb{Z}_p$. Hence $p^k y + p^k x f'(n_k) \equiv 0 \pmod{p^{k+1}}$, which holds if and only if $y + xf'(n_k) \equiv 0 \pmod{p}$. Since $n_k \equiv n_q = 1 \pmod{p}$, and $f'(n_k) \equiv f'(a) \neq 0 \pmod{p}$, it follows that $x \equiv -[f'(a)]^{-1} y \in \mathbb{Z}_p \pmod{p}$. Thus there exist $(x_0, x_1, \dots)$ such that $-[f'(a)]^{-1}y = (x_0 + p\mathbb{Z}, x_1 + p^2\mathbb{Z}, \dots)$. Then the choice $n_{k+1} = n_k + p^k x$ works for the next step, and notice that $|n_{k+1} - n_k|_p \leq p^{-k}$, since $p^k \mid (n_{k+1} - n_k)$, and $|n_a - n_b| \leq p^{-\min(a,b)}$, so $\{n_k\}$ is Cauchy and letting $b := \lim\limits_{k\to\infty} n_k \in \mathbb{Z}_p$, then $f(b) = \lim\limits_{k\to\infty} f(n_k) = 0$, as required. □

We need two facts to get an embedding:

(1) If $f(x_1, \dots, x_d) \in \mathbb{C}[x_1, \dots, x_d]$ is a non-zero polynomial, then there exists $(a_1, a_2, \dots, a_d) \in \mathbb{Z}^d$ such that $f(a_1, \dots, a_d) \neq 0$.

Proof (sketch). If $d = 1$, then the claim is immediate: $f(x_1)$ has only finitely many roots, so pick a_1 non-root. Now suppose this is true for $< d$ variables. Write $f(x_1, \dots, x_d) = Q_r(x_1, \dots, x_{d-1})x_d^r + Q_{r-1}(x_1, x_2, \dots, x_{d-1})x_d^{r-1} + \cdots + Q_0(x_1, \dots, x_{d-1})$. By assumption, some $Q_i \neq 0$ so there exists $(a_1, \dots, a_d) \in \mathbb{Z}^{d-1}$ so that $Q_i(a_1, \dots, a_{d-1}) \neq 0$. Then

$$f(a_1, a_2, \dots, a_{d-1}, x_d) = Q_i(a_1, \dots, a_{d-1})x_d^i + \sum_{\substack{j=0 \\ j\neq i}}^{r} Q_j(a_1, \dots, a_{d-1})x_d^j \neq 0.$$

Thus by the case, there exists $a_d \in \mathbb{Z}$ satisfying the condition. □

(2) If $f(x) \in \mathbb{Z}[x]$ is non-constant the there are infinitely many primes p such that $f(x)$ has a root mod p.

Proof. Suppose otherwise. Then there is just a finite set of primes, say $\{p_1, \dots, p_k\}$ for which $f(x)$ has a root mod p. Then if $n \in \mathbb{Z}$, we have $f(n) = \pm \prod_{i=1}^{k} p_i^{j_i}$. So let $f(0) = \pm \prod_{i=1}^{k} p_i^{e_i}$, and $N = \prod_{i=1}^{k} p_i^{e_i+1}$. Then for $m \in \mathbb{Z}$, we have $f(Nm) = f(0 + Nm) = f(0) + Nmf'(0) + (Nm)^2 \frac{f''(0)}{2!} + \cdots + (Nm)^d \frac{f^{(d)}(0)}{d!} \equiv f(0) \pmod{N}$. In particular, notice that $p_i^{e_i} \parallel f(Nm)$ for all $1 \leq i \leq k$. So $f(Nm) = \pm \prod_{i=1}^{k} p_i^{e_i}$ for all $m \in \mathbb{Z}$. Hence $f(x)^2 - \prod_{i=1}^{k} p_i^{2e_i} = 0$ for all $x = N, 2N, 3N, \dots$. But since f is non-constant, it follows that f^2 cannot be constant, which is a contradiction. □

2.1. **Strategy for the embedding.** Let K be a finitely-generated extension over $\mathbb{Q}$, i.e., $K = \mathbb{Q}(\theta_1, \dots, \theta_m) \hookrightarrow \mathbb{Q}_p$. Order $\theta_1, \dots, \theta_m$ so that the first r elements are algebraically independent over $\mathbb{Q}$, where $0 \leq r \leq m$. Let $L := \mathbb{Q}(\theta_1, \dots, \theta_r)$ and $K = L(\alpha)$ where α is algebraic over L.

3. September 19

Theorem 3.1. *IF K is a finitely-generated field extension of $\mathbb{Q}$ (i.e., $K = \mathbb{Q}(a_1, a_2, \ldots, a_s)$), then there exists an infinite set of primes p such that $\psi : K \hookrightarrow \mathbb{Q}_p$. Moreover, if $S \setminus K \setminus \{0\}$ is finite, then we can find infinitely many p for which $\psi(S) \setminus \mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.*

Proof. Step 1: Write $K = \mathbb{Q}(t_1, t_2, \ldots, t_s)[\theta]$ where $t_1, t_2, \ldots, t_s$ are algebraically independent over $\mathbb{Q}$ (i.e., $\{t_1, t_2, \ldots, t_s\}$ is a transcendence basis) and θ is algebraic over $\mathbb{Q}(t_1, t_2, \ldots, t_s)$. Note that this is possible by the primitive element theorem. Notice that θ has a minimal polynomial in $\mathbb{Q}(t_1, t_2, \ldots, t_s)[x]$. Namely, the minimal polynomial is

$$\sum_{i=0}^{m} f_i(t_1, t_2, \ldots, t_s)x^i =: F(t_1, t_2, \ldots, t_s; x) = F(x).$$

By clearing denominators, we may assume that each $f_i(t_1, t_2, \ldots, t_s) \in \mathbb{Z}[t_1, t_2, \ldots, t_s]$.

Suppose that $S = \{\alpha_1, \ldots, \alpha_r\} \in K^*$. Then

$$\alpha_i = \sum_{j=0}^{n-1} \psi_{ij}(t_1, t_2, \ldots, t_s)\theta^j.$$

Now pick $D(t_1, t_2, \ldots t_s) \in \mathbb{Z}[t_1, t_2, \ldots t_s] \setminus \{0\}$ such that $D(t_1, \ldots, t_s)\psi_{ij}(t_1, \ldots, t_s) \in \mathbb{Z}[t_1, \ldots, t_s]$ for all i, j. Notice that $F(x), F'(x) \in \mathbb{Q}(t_1, \ldots, t_s)[x]$, and that they have gcd 1 – since F is minimal, F is irreducible also. Hence one can find $a(x), b(x) \in \mathbb{Q}(t_1, \ldots, t_s)[x]$ such that $a(x)F(x) + b(x)F'(x) = 1$. Thus there exists $H(t_1, \ldots, t_s) \in \mathbb{Z}[t_1, \ldots, t_s] \setminus \{0\}$ such that $H(t_1, \ldots, t_s)a(x), H(t_1, \ldots, t_s)b(x) \in \mathbb{Z}[t_1, tdots, t_s][x]$. Thus $(Ha)F + (Hb)F' = H$.

Step 2: Consider the polynomial $HD \in \mathbb{Z}[t_1, \ldots, t_s] \setminus \{0\}$. One can find $(a_1, a_2, \dot{;} sa_s) \in \mathbb{Z}^s$ such that $HD \neq 0$ (see Fact (1) in the September 17 lecture).

Step 3: Notice that

$$F(x) = F(t_1, t_2, \ldots, t_s; x) = \sum_{i=0}^{m} f_i(t_1, \ldots, t_s)x^i.$$

Consider

$$\tilde{F}(x) = F(a_1, \ldots, a_s; x) = \sum_{i=0}^{m} f_i(a_1, \ldots, a_s)x^i \in \mathbb{Z}[x].$$

Then $\tilde{F}(x)$ is non-constant, since $f_m(a_1, \ldots, a_s) \neq 0$.

Step 4: By Fact (2) in the September 17 lecture, there exist infinitely many primes p such that $\tilde{F}(x) \equiv 0 \pmod{p}$. Now pick any prime p satisfying the following properties:

(i) $\tilde{F}(x)$ has a root mod p

(ii) $p > |f_m(a_1, \ldots, a_s)H(a_1, \ldots, a_s)D(a_1, \ldots, a_s)|$.

Step 5: We shall show that ψ embeds $K \hookrightarrow \mathbb{Q}_p$ and $S \hookrightarrow \mathbb{Z}_p$. Observe that $\mathbb{Q}(t_1, \ldots, t_s) \hookrightarrow \mathbb{Q}_p$ since $\mathbb{Q}_p$ has an uncountable transcendence degree, i.e., there exist $e_1, \ldots, e_s \in \mathbb{Q}_p$ such that $\{e_1, \ldots, e_s\}$ algebraically independent over $\mathbb{Q}$.

Now since $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, there exists $N > 0$ such that $p^N e_{,1}, \ldots, p^N e_s \in \mathbb{Z}_p$ (which are again algebraically independent over $\mathbb{Q}$). Thus, without loss of generality assume $e_1, \ldots, e_s \in \mathbb{Z}_p$. Embed $\mathbb{Q}(t_1, \ldots, t_s) \hookrightarrow \mathbb{Q}_p$ by using the following map: $t_i \mapsto a_i + pe_i$.

Step 6: We will find an element in $\mathbb{Z}_p$ corresponding to θ. Let

$$\widehat{F}(a_1 + pe_1, \ldots, a_s + pe_s; x) = \sum_{i=0}^{m} f_i((a_j + pe_j)_{j=1}^{s})x^i \in \mathbb{Z}_p[x].$$

We claim two things;

(1) $\widehat{F}(x)$ has an integer root α mod p.

(2) $\widehat{F}'(\alpha) \not\equiv 0 \pmod{p}$.

Hensel's lemma gives $\widehat{\theta} \in \mathbb{Z}_p$ so that $\widehat{\theta} \equiv \alpha \pmod{p}$ and $\widehat{F}(\widehat{\theta}) = 0$. Then we can embed $K \hookrightarrow \mathbb{Q}_p$ via the map $t_i \mapsto a_i + pe_i$ and $\theta \mapsto \widehat{\theta}$. Note that

$$K \cong \mathbb{Q}(t_1, \ldots t_s)[x]/(F(x)) \cong \mathbb{Q}(a_1 + pe_i, \ldots, a_s + pe_s)[x]/(\widehat{F}(x)).$$

Step 7: We've now embedded $K \hookrightarrow \mathbb{Q}_p$. By assumption, $D(t_1, t_2, \ldots, t_s)\alpha_i \in \mathbb{Z}[t_1, \ldots, t_s; \theta]$ for all i, so $D(a_1+pe_1, \ldots, a_s+pe_s)\psi(\alpha_i) \in \mathbb{Z}_p$ for all i. We claim also that $D(a_1+pe_1, \ldots, a_s+pe_s) \in \mathbb{Z}_p^*$. Recall that the units of $\mathbb{Z}_p$ are non-zero mod p. Thus $D(a_1 + pe_1, \ldots, a_s + pe_s) \equiv D(a_1, \ldots, a_s) \not\equiv 0 \pmod{p}$. Thus $p > |D(a_1, \ldots, a_s)||H(a_1, \ldots, a_s)||f_m(a_1, \ldots a_s)|$. So $D(a_1 + pe_1, \ldots, a_s + pe_s)\psi(\alpha_i) \in \mathbb{Z}_p$. Thus $\psi(\alpha_i) \in \mathbb{Z}_p$ for all $1 \leq i \leq s$. So if we use the set $S = \{\alpha_1, \ldots, \alpha_s, \alpha_1^{-1}, \ldots, \alpha_s^{-1}\}$, we have $\psi(\alpha_i), \psi(\alpha_i^{-1}) \in \mathbb{Z}_p$, then $\psi(\alpha_i)\psi(\alpha_i^{-1}) = 1$. Thus $\psi(\alpha_i) \in \mathbb{Z}_p^*$ for all i, as required. □

We now prove Claims (1) and (2) from Step 6.

Proof of Claim (1). We have

$$\begin{aligned} \widehat{F}(x) &= \sum_{i=0}^{m} f_i(a_1 + pe_1, \ldots, a_s + pe_s)x^i \\ &\equiv \sum_{i=0}^{m} f_i(a_1, \ldots, a_s)x^i = \tilde{F}(x) \pmod{p}. \end{aligned}$$

So by our choice of p, one can find $\alpha \in \mathbb{Z}$ so that $\tilde{F}(\alpha) \equiv 0 \pmod{p}$. □

Proof of Claim (2). Since $H(t_1, t_2, \ldots, t_s) \in (F(x), F'(x))_{\mathbb{Z}[t_1, \ldots, t_s; x]}$ so if we plug in $t_i = \alpha_i$ and $x = \alpha$, we have $H(a_1, \ldots, a_s) \in (\tilde{F}(\alpha), \tilde{F}'(\alpha)) \in p\mathbb{Z}$. But since $p > |H(a_1, \ldots, a_s)|$ this is impossible. □

4. September 22

Last time, we proved that there are infinitely many primes p with $K \hookrightarrow \mathbb{Q}_p$ and $S \hookrightarrow \mathbb{Z}_p^*$ where K is a finitely-generated field extension of $\mathbb{Q}$ and $S \subseteq K \setminus \{0\}$ and $|S| < \infty$. Note that this gives the SML theorem. Recall that if $f : \mathbb{N}_0 \to K$ satisfies a linear occurrence over K. Then one can find $c_{ij}, \alpha_1, \ldots, \alpha_m \in \overline{K}$ such that

$$f(n) = \sum_{i=0}^{e} \sum_{j=1}^{n} c_{ij} n^i \alpha_j^n$$

for all sufficiently large n.

Let $K_0 \subseteq \overline{K}$ be the subfield of $\overline{K}$ generated by the c_{ij}'s and the α_j's. That is,

$$\begin{tikzcd} K_0 = \mathbb{Q}(c_{ij}, \alpha_1, \ldots, \alpha_m) \arrow[d, dash, "f.g."] \\ \mathbb{Q} \end{tikzcd}$$

and

$$S := \{c_{ij}, \alpha_j : 0 \leq i \leq e, 1 \leq j \leq n\} \in K_0^*.$$

By Lech's embedding theorem, there exists some prime $p > 2$ such that:

- $K_0 \hookrightarrow \mathbb{Q}_p$
- $S \hookrightarrow \mathbb{Z}_p^*$.

Without loss of generality, assume that $K = \mathbb{Q}_p$, $c_{ij}, \alpha_j \in \mathbb{Z}_p^*$.

Main trick behind Skolem's method was

$$f(n) = \sum c_{ij} n^i \alpha_j^n.$$

Imagine we have

$$f(n) = c_1 n^2 + c_2 n e^n + c_3 c^{-n} + c_4 \to F(z) = c_1 z^2 + c_2 z e^z + c_3 e^{i\pi/2z} + c_4$$

such that $F(n) = f(n)$ for all $n \geq 0$.

4.1. Infinite series in $\mathbb{Q}_p$.

Proposition 4.1. *$\sum a_n$ is convergent if and only if $|a_n|_p \to 0$ as $n \to \infty$.*

Definition 4.2. Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$. We say that $f(z)$ is *p-adic analytic* on $\mathbb{Z}_p$ if there exist $a_0, a_1, \cdots \in \mathbb{Q}_p$ with $|a_i|_p \to 0$ as $i \to \infty$ such that

$$f(z) = \sum_{i=0}^{\infty} a_i z^i$$

for all $z \in \mathbb{Z}_p$. We say that $f(z) = a_n z^n$ is *p-adic analytic on an open subset $U \subseteq \mathbb{Z}_p$* if $f(z)$ converges for all $z \in U$.

Example 4.3. The function

$$\exp_p(z) = \sum \frac{z^n}{n!}$$

is *not* p-adic analytic on $\mathbb{Z}_p$, since $|(n!)^{-1}|_p \to \infty$. But it *is* analytic on

$$B(0, p^{-\frac{1}{p-1}}) = \{z \in \mathbb{Z}_p : |z|_p < p^{-\frac{1}{p-1}}\}.$$

Let $a \in \mathbb{Z} \setminus \{0\}$. Let's write $v_p(a)$ be the unique nonnegative integer k such that $p^k \parallel a$. Then we have $|a|_p = p^{-v_p(a)}$. Since

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \le \sum_{i=0}^{\infty} \frac{n}{p^i} \le \frac{n}{p-1}.$$

Let s be an integer such that $p^s \le n < p^{s+1}$. Then

$$\begin{aligned} \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \ge \sum_{i=1}^{s} \left(\frac{n}{p^i} - 1 \right) &= \frac{n}{p-1} - \frac{p}{p^{s+1}} \cdot \frac{n}{p-1} - s \\ &\ge \frac{n}{p-1} - \frac{p}{p-1} - \log_p n. \end{aligned}$$

If $|z|_p < p^{-1/(p-1)}$, then $|z|_p = p^{-1/(p-1)-\varepsilon}$. So

$$\begin{aligned} \left| \frac{z^n}{n!} \right|_p &= \left(p^{-1/(p-1)-\varepsilon}\right)^n \cdot p^{-v_p(n)} \\ &\le p^{-n/(p-1)-n\varepsilon} \cdot p^{-n/(p-1)+p/(p-1)+\log_p n} = p^{-n\varepsilon+p/(p-1)+\log_p n} \to 0. \end{aligned}$$

Remark 5. If $p > 2$, then

$$\exp_p(pz) = \sum_{n=0}^{\infty} \frac{p^n z^n}{n!}$$

is p-adic analytic on $\mathbb{Z}_p$, since if $z \in \mathbb{Z}_p$ then $pz \in p\mathbb{Z}_p \subseteq B(0, p^{-1/(p-1)})$, and since $p > 4$ we have $|z'|_p \le 1/p$ for all $z' \in p\mathbb{Z}_p$.

Example 4.4. Consider the function

$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots .$$

This function is analytic on $B(0,1)$ but not on $\mathbb{Z}_p$, since $|\frac{1}{n}|_p \not\to 0$. Start with $|z|_p = p^{-\varepsilon}$ for some $\varepsilon > 0$. Then we have $|z^n/n|_p = \frac{p^{-\varepsilon n}}{|n|_p} \to 0$.

Remark 6. For all $p > 2$,

(1) $\exp_p \circ \log_p(1+pz)$ is p-adic analytic on $\mathbb{Z}_p$ and is equal to $1 + pz$ for all $z \in \mathbb{Z}_p$.

Proof. Let $h(z) = \exp_p(\log_p(1+pz))$. Then we have $h'(z) = \exp_p'(\log_p(1+pz))\frac{p}{1+pz} = h(z)\frac{p}{1+pz}$ for all $z \in \mathbb{Z}_p$. Let $g(z) = 1 + pz$. Then $g'(z) = g(z)\frac{p}{1+pz}$ for all $z \in \mathbb{Z}_p$. Thus $(h/g)' = 0$. Hence $h(z) = cg(z)$ for some $c \in \mathbb{Z}_p$. □

(2) For $n \in \mathbb{N}_0, z \in \mathbb{Z}_p$, we have $n \log_p(1+pz) = \log_p(1+pz)^n$.

Remark 7. If $\alpha \in \mathbb{Z}_p, \alpha \equiv 1 \pmod{p}$ and $p > 2$, then there exists a p-adic analytic map $h : \mathbb{Z}_p \to \mathbb{Z}_p$ so that $h(n) = \alpha^n$ for all $n \in \mathbb{N}_0$.

Proof. Write $\alpha = 1 + p\theta$ with $\theta \in \mathbb{Z}_p$. Let $\beta = \log_p(1+p\theta) \in p\mathbb{Z}_p$. Let $h(z) = \exp_p(\beta z)$, which is analytic on $\mathbb{Z}_p$, since $\beta z \in p\mathbb{Z}_p$ for all z. Now

$$\begin{aligned} h(n) = \exp_p(\beta n) &= \exp_p(n \log_p(1+p\theta)) \\ &= \exp_p(\log_p(1+p\theta)^n) \\ &= (1+p\theta)^n = \alpha^n. \end{aligned}$$

Suppose that

$$f(n) = \sum_{i,j} c_{ij} n^i \alpha_j^n,$$

where $c_{ij}, \alpha_j \in \mathbb{Z}_p^*$ (note that $p \nmid \alpha_j$). Then there exist $\alpha_j \in \mathbb{Z}$ such that $\alpha_j \equiv a_j \pmod{p}$, so $\alpha_j^{p-1} \equiv 1 \pmod{p}$ (by Fermat's little theorem). For $r = 0, 1, \ldots, p-1$, let

$$f_r(n) = f((p-1)n + r) = \sum_{i,j} c_{ij}((p-1)n + r)^i (\alpha_j^{p-1})^n \cdot \alpha_j^r.$$

Then if we let $H_r(z) = \sum_{i,j} c_{ij}((p-1)z + r)^i \alpha_j^r \exp(z \log_p(\alpha_j^{p-1}))$, then $H_r(z)$ is p-adic analytic in $\mathbb{Z}_p$. □

5. September 24: Skolem-Mahler-Lech and Dirksen's proof on the characteristic p case

Theorem 5.1 (Skolem-Mahler-Lech theorem)**.** *Let K be a field of characteristic 0 and suppose that $f : \mathbb{N}_0 \to K$ satisfies a linear recurrence on K. Then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a finite union of arithmetic progression $\{cn + d : n \geq 0\}, c \geq 1, d \geq 0$ along with a finite set.*

Proof. Step 1 (Skolem). Let $\alpha_1, \ldots, \alpha_m \in \overline{K}$ and $c_{ij} \in \overline{K}$. Write

$$f(n) = \sum_{i,j} c_{ij} n^i \alpha_j^n$$

for all sufficiently large n. Without loss of generality, suppose $f(n) = \sum c_{ij} n^i \alpha_j^n$ for all $n \geq 0$.

Step 2 (Lech). Let $K_0 = \mathbb{Q}(c_{ij}, \alpha_j)/\mathbb{Q}$. Then $K_0 \hookrightarrow \mathbb{Q}_p$ where $p > 2$, and the maps satisfies $\{c_{ij}, \alpha_j\} \setminus \{0\} \hookrightarrow \mathbb{Z}_p^*$. In particular, we may assume that the α_j's are nonzero and so $\alpha_j \equiv a \pmod{p}$ for $p \nmid a, a \in \mathbb{Z}$. By Fermat's little theorem, we have $\alpha_j^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$.

Step 3. We showd that if $\gamma \equiv 1 \pmod{p}$, i.e., $\gamma = 1 + p\beta$ for some β, then there exists a p-adic analytic function $h_\gamma(z)$ such that $h(\gamma(n) = \gamma^n$ for all $n \geq n_0$. Then $h_\gamma(z) = \exp_p(z \log_p(1 + p\beta)$, and $\log_p(1 + p\beta) = p\beta - (p\beta)^2/2 + (p\beta)^3)/3 + \cdots = p\theta$ for some $\theta \in \mathbb{Z}_p$. Hence $h_\gamma(z) = \exp_p(p\theta z)$. Thus there exists $h_1, \ldots, h_m$ p-adic analytic such that $h_j(n) = \left(\alpha_j^{p-1}\right)^n$ for all $n \geq 0$.

Step 4. For $r \in \{0, 1, \ldots, p-2\}$, let

$$\begin{aligned} f_r(n) := f((p-1)n + r) &= \sum_{i,j} c_{ij}((p-1)n + r)^i \alpha_j^{(p-1)n + r} \\ &= \sum_{i,j} c_{ij} \alpha_j^r ((p-1)n + r)^i (\alpha_j^{p-1})^n. \end{aligned}$$

Note that $c_{ij}\alpha_j^r \in \mathbb{Z}_p$.

Let $F_r(z) := \sum_{i,j} c_{ij} \alpha_j^r ((p-1)z + r)^i h_j(z)$ and $F_r(n) = f_r(n)$ for all $n \geq 0$. Then $F_r(z)$ is p-adic analytic. Now we need to use Strassman's theorem:

Theorem 5.2 (Strassman)**.** *Let $f(z) = \sum a_n z^n$ be p-adic analytic in $\mathbb{Z}_p$. Then if $f(z)$ has infinitely many zeroes in $\mathbb{Z}_p$ then $f(z) \equiv 0$.*

Step 5. Since $F_r(z)$ is p-adic analytic, then by Theorem 5.2, either:

(1) $\{n : F_r(n) = f_r(n) = 0\}$ is finite OR

(2) $F_r(z) \equiv 0 \Rightarrow F_r(n) = f_r(n) = 0$ for all $n \geq 0$.

So either $\{n : f((p-1)n + r) = 0\}$ is all of $\mathbb{N}_0$ or it is finite. Thus, we have

$$\{n \in \mathbb{N}_0 : f(n) = 0\} = \left(\bigcup_{i=0}^{p-2}((p-1)\mathbb{N}_0 + i)\right) \sqcup \left(\bigcup_{i=0}^{p-2}\{n : F_i(n) = 0\}\right).$$

Thus, the first set of the RHS is the finite union of arithmetic progressions while the second one is finite, as required. □

Recall that we proved last time:

Claim. For a prime p and $z \in \mathbb{C}$,

(1) $\exp_p(\log_p(1+pz)) = 1 + pz$

(2) $n \log_p(1+pz) = \log_p(1+pz)^n$ for all $n \in \mathbb{N}$.

Lemma 5.3. *Let $f(z) = \sum a_n z^n$ be p-adic analytic on $\mathbb{Z}_p$. Suppose that $f(z) \neq 0$. Let N be the unique non-negative integer such that:*

- *$|a_N|_p > |a_n| > p$ for all $n > N$*
- *$|a_N|_p \geq |a_i|_p$ for all $i \leq N$.*

Then $f(z)$ has at most N zeroes in $\mathbb{Z}_p$.

Proof. Let's divide $f(z)$ by a_N:

$$\frac{f(z)}{a_N} = \sum_{n=0}^{\infty} \frac{a_n}{a_N} z^n = \sum_{n=0}^{\infty} b_n z^n =: g(z).$$

Then $b_N = 1$. If $n > N$ and $|b_n|_p < 1$ then $b_n \in p\mathbb{Z}_p$; and if $i \leq N$ and $|b_i|_p \leq 1 = |b_N|_p$ then $b_i \in \mathbb{Z}_p$. So

$$g(z) \equiv b_0 + b_1 z + \cdots + b_{N-1} z^{N-1} + z^N (=: Q(z)) \pmod{p},$$

as $b_n \equiv 0 \pmod{p}$ for all $n > N$. So we will factor $g(z) = Q(z)h(z)$, where Q is a monic polynomial of degree N and $h(z)$ has no zeroes in $\mathbb{Z}_p$.

Claim. For each $j \geq 1$, there exist polynomials $Q_j(z), h_j(z)$ such that

(1) $Q_j(z)$ is monic of degree N, and $h_j(z) \equiv 1 \pmod{p}$.

(2) $g(z) \equiv Q_j(z)h_j(z) \pmod{p^j}$.

(3) For all $j \geq 2$, we have

$$Q_j(z) \equiv Q_{j-1}(z) \pmod{p^{j-1}}$$
$$h_j(z) \equiv h_{j-1}(z) \pmod{p^{j-1}}.$$

Proof of Claim. We prove via induction on j. If $j = 1$, then the verification of the first two claims is straightforward while the third claim is vacuously true.

Now suppose that the claim hold for $j < m$ for $m \geq 2$. We have $Q_{m-1}(z)$ and $h_{m-1}(z)$ such that $g(z) \equiv Q_{m-1}(z)h_{m-1}(z) \pmod{p^{m-1}}$. Thus there exists a polynomial $H(z)$ such that $\sum b_i z^i = g(z) \equiv Q_{m-1}(z)h_{m-1}(z) - p^{m-1}H(z) \pmod{p^n}$ with $|b_i|_p \to 0$. To get the claim at step N , we need to find polynomials $R(z)$ and $T(z)$ satisfying:

(1') $Q_m(z) = Q_{m-1}(z) + p^{m-1}R(z), h_m(z) = h_{m-1}(z) + p^{m-1}T(z)$ (property 3)

(2') Need $\deg R(z) < N$ (property 1)

(3') $g(z) \equiv Q_m(z)h_m(z) = (Q_{m-1}(z) + p^{m-1}R(z))(h_{m-1}(z) + p^{m-1}T(z)) \pmod{p^m}$ (property 2)

Look at (3'):

$$\begin{aligned}g(z) &\equiv (Q_{m-1}(z)+p^{m-1}R(z))(h_{m-1}(z)+p^{m-1}T(z)) \pmod{p^m}\\ &\equiv Q_{m-1}(z)h_{m-1}(z)+p^{m-1}Q_{m-1}(z)T(z)+p^{m-1}R(z)h_{m-1}(z)\\ &+p^{2m-2}R(z)T(z) \pmod{p^m}\\ &\equiv g(z)+p^{m-1}H(z)+p^{m-1}Q_{m-1}(z)T(z)+p^{m-1}R(z)h_{m-1}(z) \pmod{p^m}.\end{aligned}$$

Therefore, it follows that

$$\begin{aligned}0 &\equiv p^{m-1}H(z)+p^{m-1}Q_{m-1}(z)T(z)+p^{m-1}R(z)h_{m-1}(z) \pmod{p^m}\\ -H(z) &\equiv Q_{m-1}(z)T(z)+R(z)h_{m-1}(z) \pmod{p}\\ -H(z) &\equiv Q_{m-1}(z)T(z)+P(z) \pmod{p}\\ -H(z) &\equiv Q_1(z)T(z)+R(z) \pmod{p}.\end{aligned}$$

So there exists $T(z), R(z)$ with the desired properties. □

Let $G(z)=\sum b_n z^n$. Then one can find N so that $|b_N|=1$, $|b_n|_p<1$ for all $n>N$ and $b_i \in \mathbb{Z}$ for al $i \leq N$. We showed that for each $j \geq 1$, there exist polynomials $P_j(z), h_j(z)$ such that

(1) $G(z) \equiv P_j(z)h_j(z)$
(2) $P_j(z)$ is monic of degree N, $h_j(z) \equiv 1 \pmod{p}$.
(3) $P_j(z) \equiv P_{j-1}(z) \pmod{p^{j-1}}, h_{j-1}(z) \pmod{p^{j-1}}$.

Let $P(z)=\lim\limits_{j\to\infty} P_j(z)$ and $h(z)=\lim\limits_{j\to\infty} h_j(z)$, and we have $G=Ph$, which holds for mod p^j for all $j \geq 1$. Notice now that $G(z)=0 \Leftrightarrow P(z)=0$ or $h(z)=0$. Notice that $h(z)$ never vanishes on $\mathbb{Z}_p$: since $h(z) \equiv 1 \pmod{p}$, each h_j is $h(z)=h_0+h_1z+h_2z^2+\cdots \equiv 1+0z+0z^2+\cdots \pmod{p}$, and $h_0 \equiv 1 \pmod{p}, h_i \equiv 0 \pmod{p}$ for all $i>0$. Thus $h(a) \neq 0$, whereas $P(z)$ has at most N zeroes. The proof is complete. □

6. September 26: Positive characteristic case

We saw that S-M-L is false when $\mathrm{char}(K)>0$, e.g. $K=\mathbb{F}_p(t)$ with $f(n)=(1+t)^n-t^n-1$. $f(n)$ satisfies a linear recurrence relation over K, but we have $f(n)=0 \Leftrightarrow n \in \{1,p,p^2,p^3,\dots\}$. Derksin's version says that in the positive characteristic case, the zero sets are finite union of arithmetic progressions, finite sets, and *p-normal sets.* The proof involves using a finite-state machine.

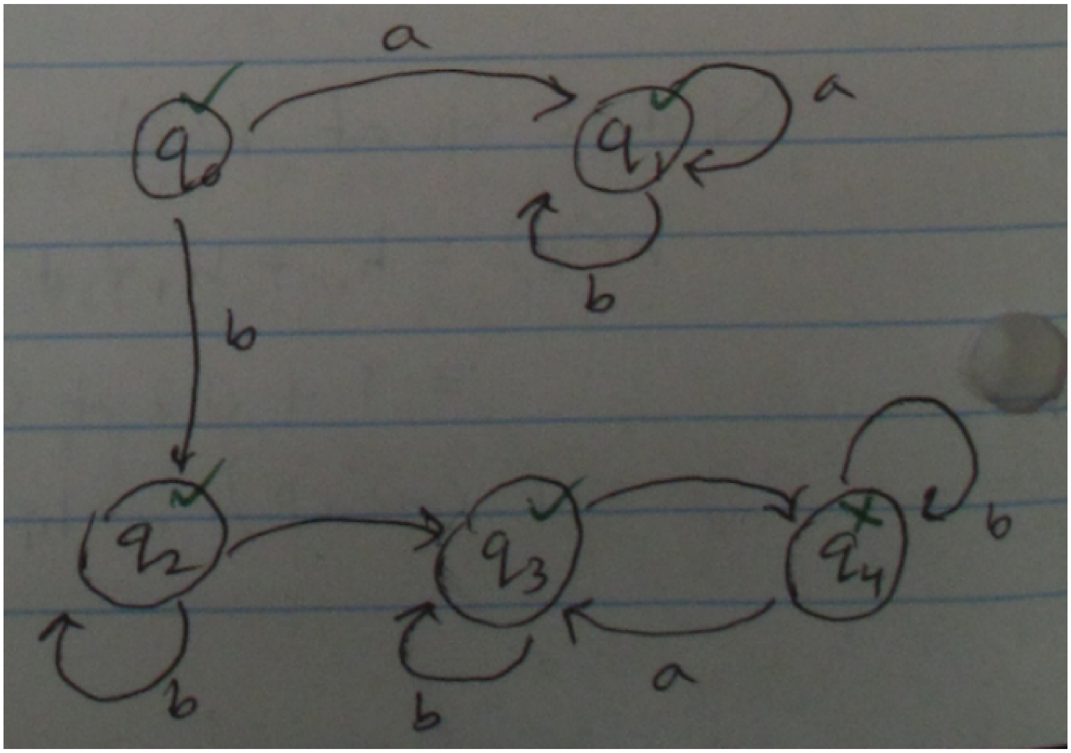
Definition 6.1. A (deterministic) *finite-state automaton* is a five-tuple

$$\Gamma=(\Sigma,Q,q_0,\delta,F),$$

where:

- Σ is *a finite non-empty set of symbols* (input alphabet)
- Q is *a finite non-empty set of states*
- $q_0 \in Q$ denotes *the initial state*
- δ is *a transition function* $\delta: Q\times\Sigma\to Q$
- $F \subseteq Q$, possibly empty, is called *the final (or accepting) states.*

Example 6.2. Let $\Sigma=\{a,b\}, Q=\{q_0,q_1,q_2,q_3,q_4\}$. Then the directed graph looks like

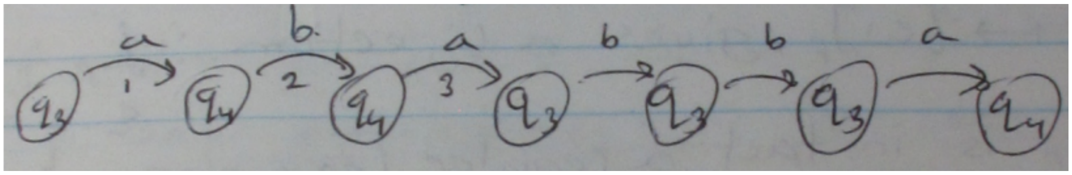


So we have $\delta(q_3, a) = q_4$, $\delta(q_2, b) = q_2$, and so forth, and $F = \{q_0, q_1, q_2, q_3\}$.

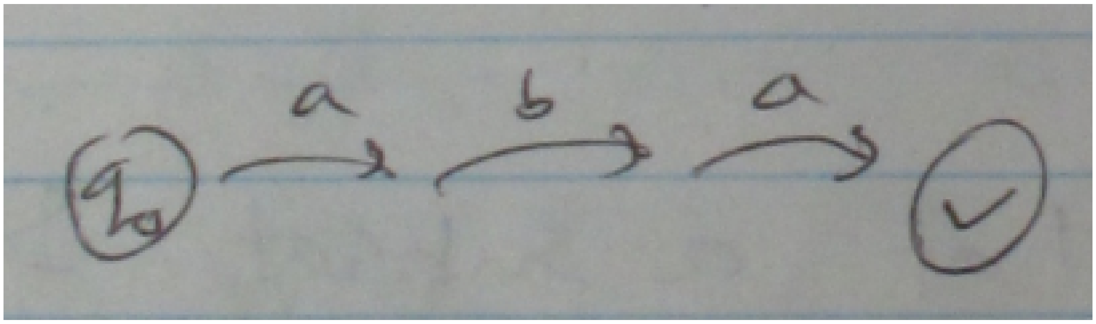
Remark 8. Let Σ^* be the free monoid on Σ (i.e., it is the collection of finite length strings on Σ). For example, if $\Sigma = \{a, b\}$, then $\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, \dots\}$. Notice we can extend the transition function δ to a map

$$\delta : Q \times \Sigma^* \to Q.$$

So, for instance, $\delta(q_3, abbaba) = q_4$.



Notice that to a *deterministic finite-state automaton (DFA)*, we can associate a subset $\mathcal{L} \subseteq \Sigma^* = \{w \in \Sigma^* : \delta(q_0, w) \in F\}$ which is all words $w \in \Sigma^*$ such that $f(q_0, w) \in F$. In our example, $\mathcal{L} = \Sigma^* a \cup \{b\}^* \cup \{\text{word with an odd number of } a \text{ concatenated with } b\}$. ($\{b\}^* =$ monoid generated by b)

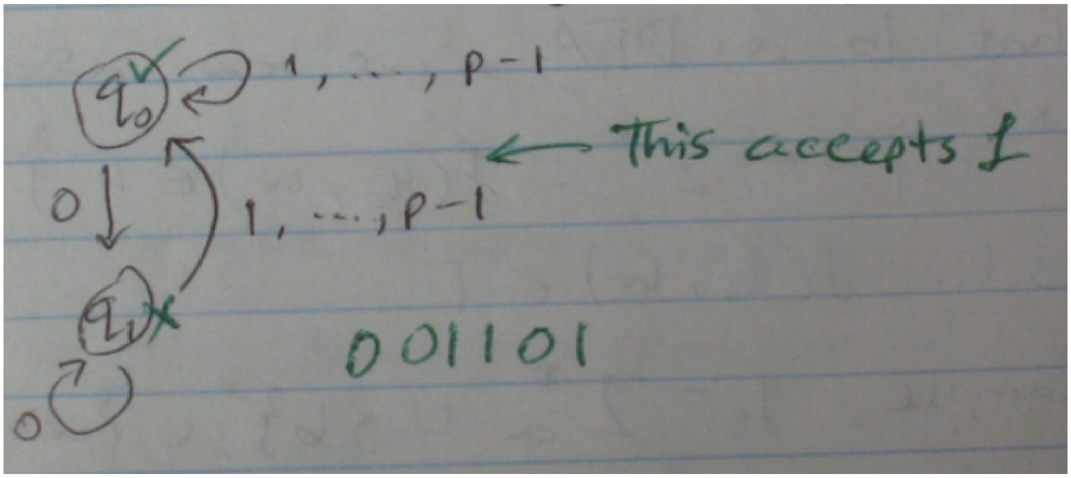


Definition 6.3. A language $\mathcal{L} \subseteq \Sigma^*$ produced from a finite-state automaton is called a *regular language (or rational language).*

Remark 9. If $\mathcal{L}_n = \{w \in \mathcal{L} : (\text{length of } w) = n\}$, then $f(n) = |\mathcal{L}_n|$ satisfies a linear recurrence.

Let $p \in \mathbb{N}, p \geq 2$ (think of p as a prime). Henceforth we shall work with the alphabet $\Sigma = \{0, 1, \dots, p-1\}$. Notice to $w \in \Sigma^*, w = i_s i_{s-1} \cdots i_0$ we can associate a non-negative integer $[w]_p := i_0 + i_1 p + \cdots + i_s p^s$, and $[\varepsilon]_p = 0$.

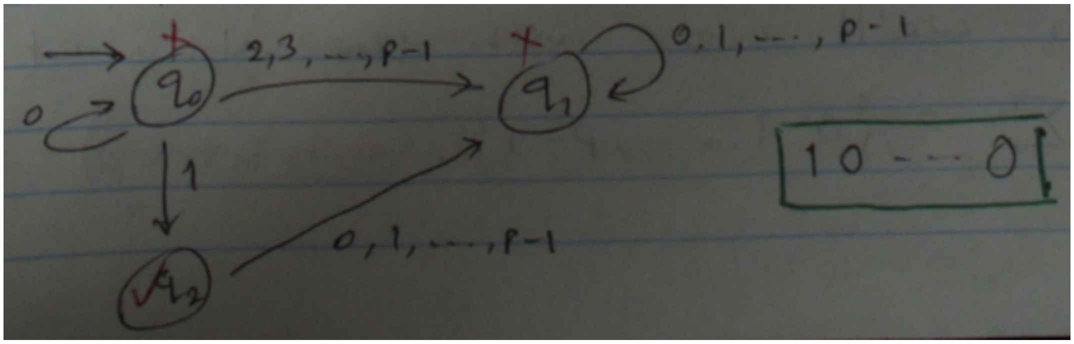
If $p = 2$, then $[1101]_2 = 1 + 0 \cdot 2 + 1 \cdot 4 + 1 \cdot 8 = 13 \in \mathcal{L}_2$ while $[001101]_2 = 13 \notin \mathcal{L}_2$. We shall let $\mathcal{L}_p \subseteq \Sigma$ be the words that do not begin with 0. Then $w \mapsto [w]_p$ gives a bijection between $\mathcal{L}_p$ and $\mathbb{N}_0$ (and note that $[\varepsilon] \mapsto 0$). In fact, $\mathcal{L}_p$ is a regular language.



7. September 29

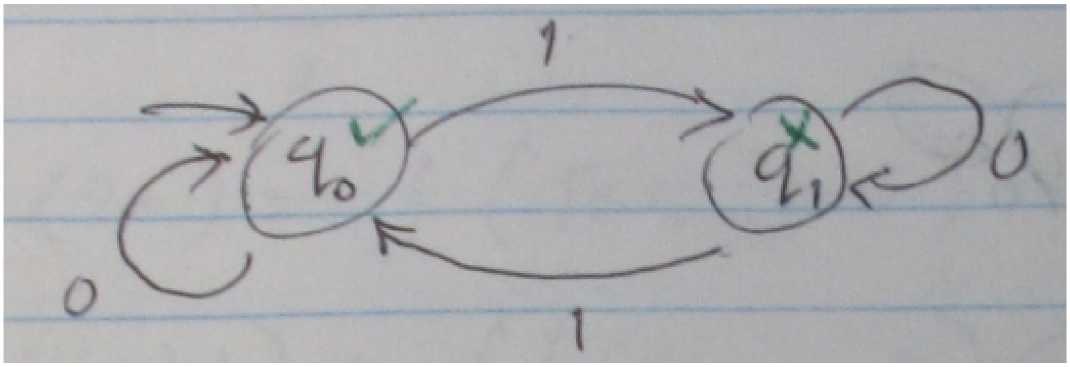
Definition 7.1. Let $p \geq 2$. We say that a subset $S \subseteq \mathbb{N}_0$ is *p-automatic* if there exists a deterministic finite-state automaton Γ with input alphabet $\Sigma = \{0, 1, \dots, p-1\}$ such that $S = \{[w]_p : w \in \mathcal{L}_p \text{ and } w \text{ is accepted by } \Gamma, \text{ i.e. } \mathcal{L}(q_0, w) \in F\}$.

Example 7.2. Show that $S = \{1, p, p^2, \dots\}$ is p-automatic. Consider the following finite-state automaton:



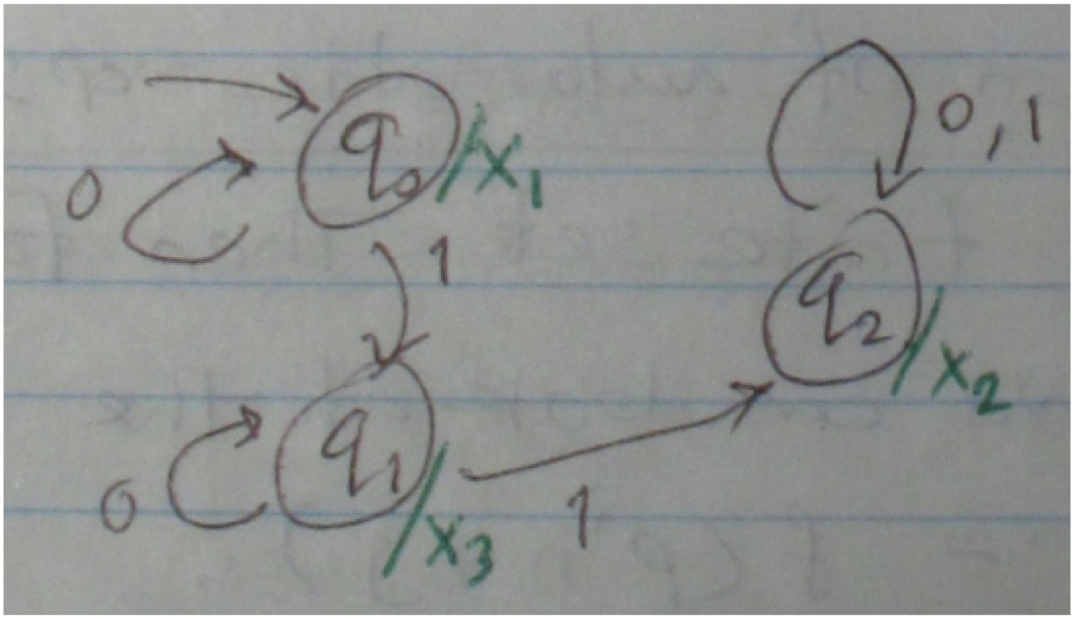
A word w is accepted if and only if $w = 10 \cdot 0$; that is, $[w]_p = p^j$.

Example 7.3. The Thue-Morse set $\{j \in \mathbb{N}_0 : \text{ binary expansion of } j \text{ has an even number of 1s}\}$. Let $\Sigma = \{0, 1\}$. Then $S = \{0, 3, 5, 6, 9, \dots\}$. This set is 2-automatic since the following DFA accepts the elements in the Thue-Morse set:

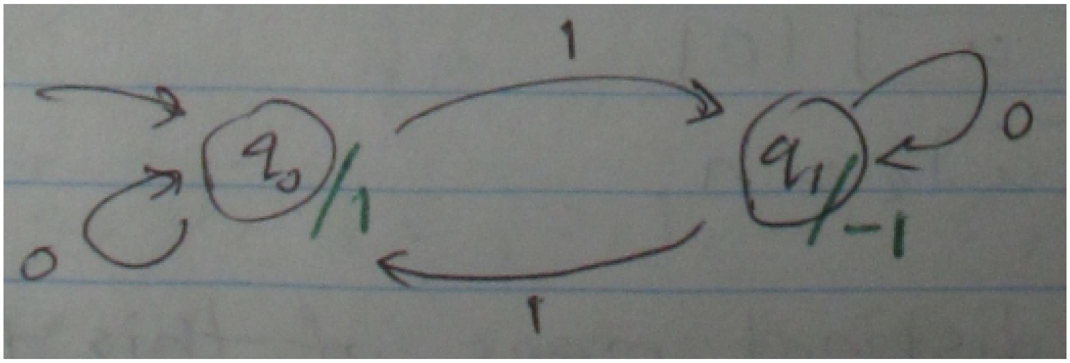


Definition 7.4. Let $f : \mathbb{N} \to \Delta$ where Δ is some finite set. We say that f is a *p-automatic map (or sequence)* if there exists a DFA $\Gamma = (\{0, 1, \ldots, p-1\}, Q, q_0, \delta, F)$ and a map $g : Q \to \Delta$ such that $f(n) = g(\delta(q_0, w_n))$ where w_n is the unique element of 1_p such that $[w_k]_p = n$, i.e., w_n is the base-p expansion of n.

Example 7.5. Let $p = 2$ and $\Delta = \{x_1, \ldots, x_5\}$. We have $g(q_0) = x_1, g(q_1) = x_3, g(q_2) = x_4$.



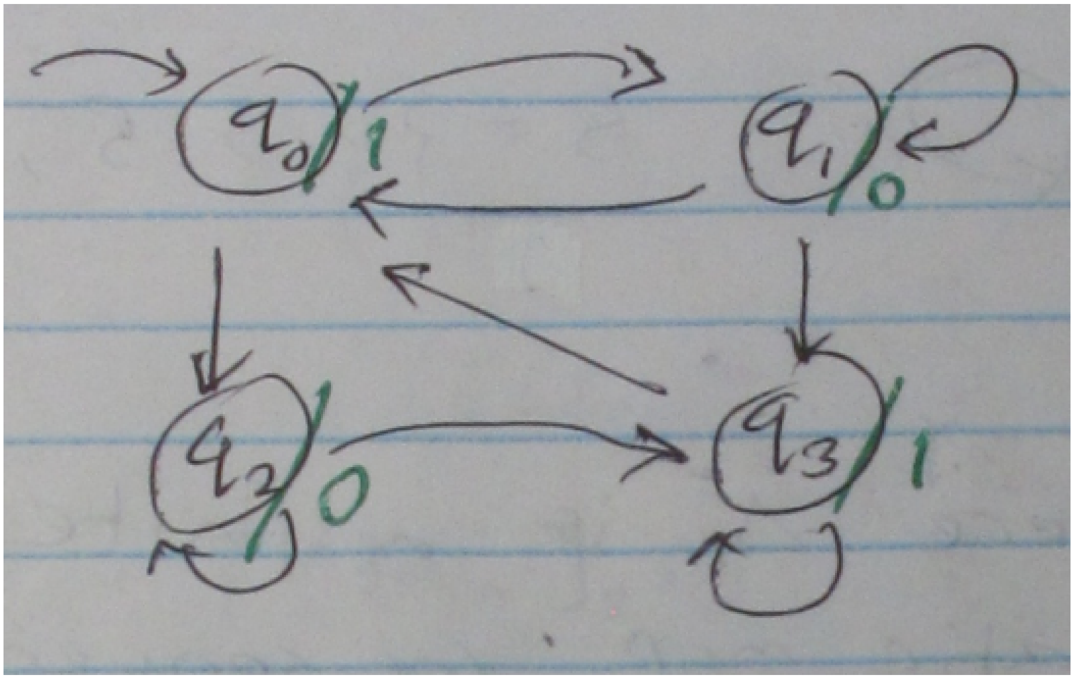
Example 7.6. The Thue-Morse sequence $f : \mathbb{N} \to \{-1, 1\}$. Then $f(13) = f([1101]_2) \mapsto q_1$, so output is -1.



Example 7.7. If $S \subseteq \mathbb{N}_0$ is p-automatic, then

$$\chi_S(n) = \begin{cases} 1 & (n \in S) \\ 0 & (n \notin S) \end{cases}$$

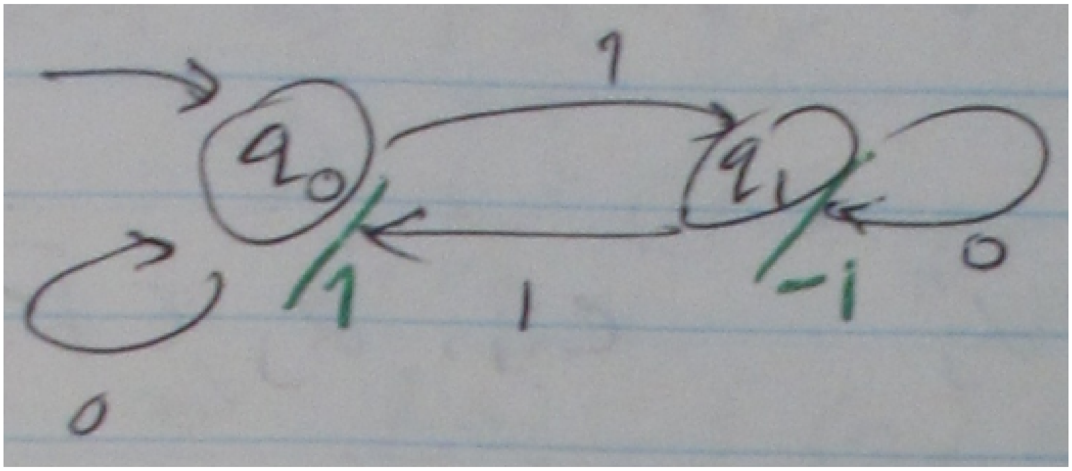
is a p-automatic map.



Theorem 7.8 (Derksen's First Theorem)**.** *Let K be a field of characteristic $p > 0$ and suppose that $f : \mathbb{N}_0 \to K$ satisfies a linear occurrence over K. Then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a p-automatic set.*

Remark 10 (Eilenberg's characterization of automatic maps)*.* Let $f : \mathbb{N}_0 \to \Delta$ and Δ a finite sets. THen for each $i \geq 0$ and $j \in \{0, 1, \ldots, p^i - 1\}$, we can look at the map (subsequence) $f_{i,j}(n)$ such that $f_{i,j}(n) = f(p^i n + j)$. We call the set of *distinct* maps of this form the *p-kernel of $f(n)$*.

Example 7.9. Let $f(n)$ be the Thue-Morse sequence ($p = 2$).



$$
\begin{aligned}
f(2n) &= f([w_n]_2 0) = f(n) \\
f(2n+1) &= f([w_n]_2 1) = -f(n) \\
f(4n) &= f([w_n]_2 00) = f(n) \\
f(2^i n + j) &= f(n) f(j) \in \{\pm 1\}.
\end{aligned}
$$

Thus the 2-kernel has size 2.

Example 7.10. Let $f(n)$ be a characteristic function of the set of perfect squares, i.e.,

$$
f(n) = \begin{cases} 1 & \text{if } n \text{ is a perfect square} \\ 0 & \text{if } n \text{ is not.} \end{cases}
$$

Then we have

$$
\begin{aligned}
f(n) &= 1,1,0,0,1,0,0,0,0,1,\dots \\
f(2n) &= 1,0,0,0,1,\dots \\
f(4n+1) &= 1,0,1,\dots \\
f(8n+1) &= 1,1,0,\dots,
\end{aligned}
$$

and all the sequences are distinct.

Example 7.11. Let $f : \mathbb{N}_0 \to \{0,1\}$ be the indicator function of p-powers ,i.e.,

$$
f(n) = \begin{cases} 1 & \text{if } n = p^j, j \geq 0 \\ 0 & \text{otherwise} \end{cases}.
$$

If $i \geq 0, j \in \{0,1,\dots,p^i - 1\}$, then

$$
f(p^i n + j) = \begin{cases} 0 & (j \neq 0,1) \\ \chi_{\{0\}}(n) & (j = 1) \\ f(n) & (j = 0) \end{cases}.
$$

Definition 7.12. A linear recurrence is called *simple* if

$$
f(n) = \sum_j c_j \alpha_j^n
$$

for sufficiently large n (i.e., there are no higher powers of n appearing).

Remark 11 (Reductions in Derksen's proof). Recall that if $f : \mathbb{N}_0 \to K$ satisfies a linear recurrence over K, then $f(n) = c_{ij} n^i \alpha_j^n$ where $c_{ij}, \alpha_j \in \overline{K}$ for all sufficiently large n. If

$\operatorname{char} K = p > 0$, then for $r \in \{0, 1, 2, \ldots, p-1\}$,

$$\begin{aligned} f(pn+r) &= \sum_{i,j} (pn+r)^i \alpha_j^{pn+r} \\ &= \sum_{i,j} c_{ij} r^i \alpha_j^r (\alpha_j^p)^n \\ &= \sum_j \left(\sum_i c_{ij} r^i \alpha_j^r \right) (\alpha_j^p)^n \\ &= \sum_j \lambda_j \alpha_j^{pn}, \end{aligned}$$

as $\sum c_{ij} r^i \alpha_j^r$ is a constant in $\overline{K}$.

Reduction I: Without loss of generality we may assume that $f(n)$ is simple. The reason is as follows. Let $h_r(n) = f(pn+r)$ for $r = 0, 1, \ldots, p-1$. Then each h_r is simple and if $S_r = \{n \in \mathbb{N}_0 : h_r(n) = 0\}$ then $\bigcup_{r=0}^{p-1} \{pn + r \in \mathbb{N}_0 : f(pn+r) = 0\} = \{n \in \mathbb{N}_0 : f(n) = 0\} = \bigcup_{r=0}^{p-1} (pS_r + r)$. If we know Derksen's first theorem for simple linear recurrences, then each S_r is p-automatic because each $h_r(n)$ is simple. From Assignment #2, we will prove that $pS_r + r$, $\bigcup_{r=0}^{p-1} (pS_r + r)$, and $\{n : f(n) = 0\}$ is p-automatic.

Remark 12 (Quick aside from Remark 11). Let K be a field of characteristic $p > 0$. Then let $K^{\langle p \rangle} := \{x^p : x \in K\}$. If $x, y \in K^{\langle p \rangle}$, then there exists $a, b \in K$ such that $x = a^p, y = b^p$. Thus $x + y = a^p + b^p = (a+b)^p$ and $xy = a^p b^p = (ab)^p$, and if $x \neq 0$ then $x = (a^{-1})^p$. So $K^{\langle p \rangle} \subseteq K$ is a subfield. If $K^{\langle p \rangle} = K$ then we say that K is a *perfect field*. For instance, any finite field is perfect, and any algebraic closure of a function field over the finite fields is perfect. For any $\alpha \in K$, the equation $x^p - \alpha = 0$ has a root in K since K is algebraically closed. Thus $\alpha = u^p$ for some $u \in K$.)

8. October 01

Recall that Derksen's main goal in his Invent. Math. 2007 paper was to show the following: if K is a field of characteristic $p > 0$ and $f : \mathbb{N}_0 \to K$ satisfies a linear recurrence over K, then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ isa p-automatic set. We showed in the last lecture that we can reduce to a simple linear recurrence, i.e., $f(n) = b_1 \lambda_1^n + \cdots + b_m \lambda^m$ for all $n \geq 0, \beta_i \in \overline{K}$.

LeT $K_0 = \mathbb{F}_p(\beta_1, \ldots, \beta_m, \lambda_1, \ldots, \lambda_m) \subseteq K$. Recall that

$$K_0^{\langle p \rangle} := \{x^p : x \in K_0\},$$

which is a subfield if K_0. In the assignment you show that $[K_0 : K_0^{\langle p \rangle}] < \infty$.

Example 8.1. If $K_0 = \mathbb{F}_p(t)$ then ${K_0}^{\langle p \rangle} = \mathbb{F}_p(t^p)$. If $a(t)/b(t) \in K_0$, then $a(t)^p/b(t)^p = a(t^p)/b(t^p)$. So K_0 has a ${K_0}^{\langle p \rangle}$ basis given by $\{1, t, t^2, \ldots, t^{p-1}\}$.

If $a(t)/b(t) \in K_0$, then

$$\frac{a(t)b(t)^{p-1}}{b(t)^p} = \frac{c(t)}{b(t^p)} = \sum_{r=0}^{p-1} t^r \frac{c_r(t^p)}{b(t^p)},$$

where

$$\begin{aligned} c(t) &= \sum_{i=0}^{m} c_i t^i = \sum_{r=0}^{p-1} \sum_{i \equiv r \pmod p} c_i t^i \\ &= \sum_{r=0}^{p-1} \sum_{j} c_{pj+r} t^{pj+r} \\ &= \sum_{r=0}^{p-1} t^r \left(\sum_{i} c_{pj+r} t^j \right)^p . \end{aligned}$$

So let $c_r(t) := (\sum c_{pg+r} t_j)^p$.

If $[K_0 : K_0{}^{\langle p \rangle}] < \infty$ and we let $e_1, \ldots, e_s$ be a basis for K_0 as a $K_0{}^{\langle p \rangle}$-vector spaces, then if $a \in K_0$ we have a unique decomposition. Write

$$a = \sum_{i=1}^{s} \alpha_i e_i = \sum_{i=1}^{s} \gamma_i^p e_i$$

where each $\gamma_i \in K$ is unique and satisfies $\gamma_i^p = \alpha_i$. To see why they are unique, let γ_i be some solution to the equation $x^p - \alpha_i = x^p - \gamma_i^p = (x - \gamma_i)^p$. Thus $x^p = \gamma_i \Leftrightarrow x = \gamma_i$.

We then have projection maps $\pi_1, \ldots, \pi_s : K \to K$ satisfying

$$a = \sum_{i=1}^{s} \pi_i(a)^p e_i$$

i.e. $\pi_j(a) = \gamma_j$.

Example 8.2. If $K_0 = \mathbb{F}_3(t)$ and $K_0^{\langle 3 \rangle} = \mathbb{F}_3(t^3)$, and let $\{e_1, e_2, e_3\} = \{1, t, t^2\}$. What are π_1, π_2, π_3 of $(1+t^2)^{-1}$? First, start by writing

$$\begin{aligned} \frac{1}{1+t^2} &= \frac{(1+t^2)^2}{1+t^6} = \frac{1+2t^2+t^4}{1+t^6} \\ &= \frac{1}{1+t^6} \cdot 1 + \frac{t^3}{1+t^6} \cdot t + \frac{2}{1+t^6} \cdot t^2. \end{aligned}$$

Thus, we have $\pi_1((1+t^2)^{-1}) = (1+t^2)^{-1}, \pi_2((1+t^2)^{-1}) = t(1+t^2)^{-1}, \pi_3((1+t^2)^{-1}) = 2(1+t^2)^{-1}$.

Remark 13. Two remarks:

(1) The π are not linear, but we do have $\pi(c^p \alpha + \beta) = c\pi_i(\alpha) + \pi_i(\beta)$ for all $\alpha, \beta, c \in K$. Note that we can write $\alpha = \gamma_1^p e_1 + \cdots + \gamma_s^p e_s, \beta = \delta_1^p e_1 + \cdots + \delta_s^p e^s$, so $c^p \alpha + \beta = (c^p \gamma_1^p + \delta_1^p) e_1 + \cdots + (c^p \gamma_s^p + \delta_s^p) e_s = \sum (c\gamma_i + \delta_i)^p e_i$. So the claim follows.

(2) $\alpha \in K = 0 \Leftrightarrow \pi_1(\alpha) = \cdots = \pi_s(\alpha) = 0$. How will this help? Recall that

$$f(n) = \sum_{i=1}^{m} \beta_i \lambda_i^n.$$

What is $f(pn+j)$ then?

$$f(pn+j) = \sum_{i=1}^{m} \beta_i \lambda_i^{pn+j} = (\beta_1 \lambda_1^j)(\lambda_1^p)^n + \cdots + (\beta_m \lambda_m^j)(\lambda_m^p)^n.$$

So

$$\pi_k(f(pn+j)) = \pi_k(\beta_1 \lambda_1^j)\lambda_1^n + \cdots + \pi_k(\beta_n \lambda_n^j)\lambda_m^n.$$

Lemma 8.3 (Derksen's technical lemma)**.** *Let K_0 be a finitely-generated extension on $\mathbb{F}_p$. Suppose also that $V \subseteq K_0$ is a finite-dimensional $\mathbb{F}_p$-vector space of K_0. Then there exists a finite-dimensional $\mathbb{F}_p$-vector space $V \subseteq W \subseteq K_0$ such that $\pi_k(VW) \subseteq W$ for all k, where VW is the $\mathbb{F}_p$-vector space of products spanned by vw where $v \in V, w \in W$.*

We apply Lemma 8.3 as follows. Take $V = \mathbb{F}_p$-span of all $\{\beta_i \lambda_i^j : i = 1, \ldots, m, 0 \leq j \leq p-1\}$. Apply Lemma 8.3 to see that there exists $W \supseteq V$ such that $\pi_k(VW) \subset W$ for all k.

Let $\mathscr{S} = W^m = W \times W \times \cdots \times W$. Note that $\mathscr{S}$ is a *finite* set because $\mathbb{F}_p$ is finite and W is finite-dimensional over $\mathbb{F}_p$.

For each $w = (w_1, \ldots, w_m) \in \mathscr{S}$, let $f_w(n) = w_1\lambda_1^n + \cdots + w_m \lambda_m^n$. Notice $b = (\beta_1, \beta_2, \ldots, \beta_m \in \mathscr{S}$ and $f(n) = \beta_1 \lambda_1^n + \cdots + \beta_m \lambda_m^n = f_b(n)$. THen it follows

$$\begin{aligned}\pi_k(f_w(pn+j)) &= \pi_k(w_1 \lambda_1^j \lambda_1^{pn} + \cdots + w_m \lambda_m^j \lambda_m^{pn}) \\ &= \pi_k(w_1\lambda_1^j)\lambda_1^n + \cdots + \pi_k(w_m \lambda_m^j)\lambda_m^n.\end{aligned}$$

So by Dersken's lemma there exists $w' = (w_1', w_2', \ldots, w_m') \in \mathscr{S}$ so that $\pi_k(f_w(pn+j)) = f_{w'}(n)$. For each $(w_1, \ldots, w_m) \in \mathscr{S}$, define

$$\chi_w(n) = \begin{cases} 1 & (\text{if } f_w(n) = 0) \\ 0 & (\text{if } f_w(n) \neq 0) \end{cases},$$

i.e., a characteristic sequence of the zero set of $f_w(n)$.

In particular, $\chi_b(n)$ is equal to the char sequence of the zero set of f. Let $\mathscr{T}$ be the collection of all finite products of functions of the form $\chi_w(n)$. In fact, since $\chi^2 = \chi$, we don't need repeats, meaning $\mathscr{T}$ is a finite set.

Claim. If $g(n) \in \mathscr{T}$, then $g(pn+j) \in \mathscr{T}$ for $j = 0, 1, \ldots, p-1$.

Proof (sketch). We will show first how this gives us the result. By induction, if $g(p^i n + j) \in \mathscr{T}$ for $i \geq 0, 0 \leq j \leq p^i$. Thus $g(p^2 n + j_1 p + j_2) = g(p(pn + j_1) + j_2) = h(pn + j_1) \in \mathscr{T}$ for some $h \in \mathscr{T}$. □

Corollary 8.4. *If $g(n) \in \mathscr{T}$, then the p-kernel of g is finite.*

Proof. Note that the p-kernel of g in contained in $\mathscr{T}$ and $|\mathscr{T}| < \infty$. $g(n)$ is a p-automatic map. But $\chi_b(n) \in \mathscr{T}$, so $\chi_b(n)$ is p-automatic. The zero set thus is a p-automatic set. □

9. October 3

Remark 14. Suppose that $\mathscr{T}$ is in a finite collection of maps $h : \mathbb{N}_0 \to \Delta$ such that for each $j \in \{0, 1, \ldots, p-1\}$ and for each $g(n) \in \mathscr{T}$ we have $g(pn+j) \in \mathscr{T}$. Thus each $g(n) \in \mathscr{T}$ is p-automatic. To prove this, it suffices to show that for all $g(n) \in \mathscr{T}$, all $i \geq 1$ and all $j \in \{0, 1, 2, \ldots, p^i - 1\}$ and $g(p^i n + j) \in \mathscr{T}$, the p-kernel of g is finite. We prove this by induction on n.

The case is immediate if $i = 1$ (base case). Now suppose that it is true for $i < d$. Then if $a \in \{0, 1, 2, \dots, p^d - 1\}$, we ant to show that $g(p^d n + a) \in \mathscr{T}$ and $g \in \mathscr{T}$. Write $a = p^{d-1}b + j$ with $j \in \{0, 1, \dots, p^{d-1} - 1\}$ and $b \in \{0, 1, \dots, p - 1\}$. Thus $g(p^d n + a) = g(p^d n + p^{d-1} b + j) = g(p^{d-1}(pn + b) + j)$. By inductive hypothesis, $g(p^{d-1}m + j) = h(m)$ for some $h \in \mathscr{T}$. So $g(p^{d-1}(pn + b) + j) = h(pn + b) \in \mathscr{T}$ by assumption.

Remark 15 (Overview of Derksen's proof). Without loss of generality, let $f(n) = \beta_1 \lambda_1^n + \cdots + \beta_m \lambda_m^n$ for all $n \geq 0$. Let $K_0 = \mathbb{F}_p(\beta_1, \dots, \beta_m, \lambda_1, \dots, \lambda_m) \subseteq \overline{K}$ with $[K_0 : K_0{}^{\langle p \rangle}] = s < \infty$ and $K_0 = K_0{}^{\langle p \rangle} e_1 \oplus \cdots \oplus K_0{}^{\langle p \rangle} e_s$ where $e_1, \dots, e_s \in K_0$.

These give "projections" $\pi_i : K_i \to K_0$ such that $\alpha \in K_0 \mapsto \sum_{i=1}^{s} \pi_i(a)^p c_i$. Let $V = \operatorname{span}_{\mathbb{F}_p}\{\lambda_i \beta_i \lambda_i^j : i = 1, 2, \dots, m, j = 0, 1, \dots, p-1\}$. Derksen proved that there exists W so that $V \subseteq W \subseteq K$ such that $\dim_{\mathbb{F}_p} W < \infty$ and $\pi_k(VW) \subseteq W$ for all k¿

Let $\mathscr{S} = \{f_w(n) : w \in W^m\}$ where $f_w(n) = w_1 \lambda_1^n + \cdots + w_m \lambda_m^n$. Since $V \subseteq W$, note that $f(n) = f_b(n) \in \mathscr{S}$. THen we let $\mathscr{T}$ be all finite products of

$$\chi_w(n) = \begin{cases} 1 & \text{if } f_w(n) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Claim. If $g \in \mathscr{T}$, then $g(pn + j) \in \mathscr{T}$ for $j = 0, 1, \dots, p-1$.

Corollary 9.1. *If $g \in \mathscr{T}$ then $g(n)$ is p-automatic. Then if $\chi_b(n)$ is a character sequence f zero sets of $f(n)$, then χ_b is p-automatic. Therefore, $\{n : f(n) = 0\}$ is p-automatic.*

Proof of the above claim. If $w \in W^m$, then, for $k = 1, 2, \dots, s$ there exists $(w_{1,k}, w_{2,k}, \dots, w_{n,k}) \in W^m$ such that

$$\begin{aligned} \pi_k(w_1 \lambda_1^{pn+j} + \cdots + w_m \lambda_m^{pn+j}) &= \pi_k(w_1 \lambda_1^j)\lambda_1^n + \cdots + \pi_k(w_m \lambda_m^j)\lambda_m^n \\ &= w_{1,k}\lambda_1^n + \cdots + w_{m,k}\lambda_m^n. \end{aligned}$$

Then

$$\begin{aligned} \chi_w(pn + j) = 1 &\Leftrightarrow f_w(pn + j) = 0 \Leftrightarrow w_1 \lambda_1^{pn+j} + \cdots + w_m \lambda_m^{pn+j} = 0 \\ &\Leftrightarrow \pi_k(w_1 \lambda_1^{pn+j} + \cdots + w_m \lambda_m^{pn+j}) = 0 \text{ for } k = 1, 2, \dots, s \\ &\Leftrightarrow w_{1,k}\lambda_1^n + \cdots + w_{m,k}\lambda_m^n = 0 \text{ for } k = 1, 2, \dots, s \\ &\Leftrightarrow \chi_w(n) = 1 \text{ for } k = 1, 2, \dots, s \\ &\Leftrightarrow \prod_{i=1}^{s} \chi_w(n) = 1. \end{aligned}$$

Thus $\chi_w(pn + j) = \prod_{k=1}^{s} \chi_w(n) \in \mathscr{T}$. The rest follows from the general finite products. □

Example 9.2 (for Lemma 8.3). Let $K = \mathbb{F}_2(t)$ and $K^{\langle p \rangle} = \mathbb{F}_2(t^2)$. Let $e_1 = 1, e_2 = t$. If $V = \operatorname{span}\{1, t^{-1}\}$, then $\pi_1(t^{-1}) = \pi_1(t/t^2) = \pi(t)/t = 0$ while $\pi_2(1/t) = \pi_2(t)/t = 1/t$. Let $W = \operatorname{span}_{\mathbb{F}_2}\{1, t^{-1}, t^{-2}, \dots, t^{-2m}, t, t^2, \dots, t^{2m}\}$. What is WV? $WV = \operatorname{span}_{\mathbb{F}_2}\{t^{-2m-1}, \dots, t^{2m}\}$. If $j = 2l$, then $\pi_1(t^{2l} = t^l(\pi_1(1)) = t^p$ and $\pi_2(t^{2l}) = t^l \pi_2(1) = 0$. If $j = 2l + 1$, then $\pi_1(t^j) = \pi_1(t^{2l+1}) = t^l \pi_1(t) = 0$ while $\pi_2(t^j) = \pi_2((t^l)^2 t) = t^l \pi_2(t) = t^l$. Thus $\pi_1(WV), \pi_2(WV) \subseteq \{t^{-n}, \dots, t^m\} \subseteq W$.

Proof of Lemma 8.3. Let $\{t_1, \dots, t_r\} \subseteq K$ be a basis for V. We extend this to a generating set $\{t_1, t_2, \dots, t_m\} \in K$ for K as an extension of $\mathbb{F}_p$. For $k = 1, \dots, s$, we have

$$\pi_k(t_i) = \frac{P_{i,k}(t_1, \dots, t_m)}{Q(t_1, \dots, t_m)}.$$

for some polynomials $P_{i,k}$ and Q with $Q \neq 0$.

Let $D = \max(\deg P_{i,k}, \deg Q)$. Let

$$W = \operatorname{span}_{\mathbb{F}_p} \left\{ \left(\frac{t_1^{i_1} \cdots t_m^{i_m}}{Q^j} \right) : 0 \leq j \leq p, i_1 + \cdots + i_m < 6D, i_1, \dots, i_m \geq 0. \right\}$$

We want to show that $\pi_k(Wt_1) \subseteq W$. So it is sufficient to show that $\pi(\frac{t_1^{i_1} \dots t_m^{i_m}}{Q_j} \cdot t_i) \in W$ where $i_1 + i_2 + \cdots + i_m \leq 6D$ and $j \leq p$. □

10. October 6

Lemma 10.1 (Derksen's technical lemma). *Let $V \subseteq K$ where V is a finite-dimensional $\mathbb{F}_p$-vector space and K a finitely-generated field extension over $\mathbb{F}_p$, $\pi_1, \dots, \pi_s : K \to K$ the projection maps. Let $\{e_1, \dots, e_s\}$ be a basis for $K/K^{\langle p \rangle}$ and write $a = \sum_{i=1}^{s} \pi_i(a)^p e_i$. Then there exists a finite-dimensional $\mathbb{F}_p$-vector space W such that $V \subseteq W \subseteq K$ and $\pi(WV) \subseteq W$ for all i.*

Proof. Let $V = \operatorname{span}_{\mathbb{F}_p}\{x_1, \dots, x_r\}$. Extend this to a generating set for K, i.e., extend so that $\{x_1, x_2, \dots, x_r, x_{r+1}, \dots, x_m\}$. For $k = 1, \dots, s$ and $0 \leq i_1, \dots, i_m \leq p - 1$. we have $\pi_k(x_1^{i_1} \cdots x_m^{i_m}) = P_{i_1, i_2, \dots, i_m; k}(x_1, \dots x_m)/Q(x_1, \dots, x_n)$. Let $D = \max(\deg P_{i_1, \dots, i_m; k}, Q)$. Let

$$W = \operatorname{span}_{\mathbb{F}_p} \left\{ \frac{x_1^{j_1} \dots x_m^{j_m}}{Q_l} : 0 \leq l \leq p, j_1 + j_2 + \cdots + j_n \leq 6D \right\}.$$

So it remains to show $\pi_i(WV) \subseteq W$ for all i. It suffices to show, by $\mathbb{F}_p$-linearity, that

$$\pi_i \left(\frac{x_1^{j_1} \cdots x_m^{j_m}}{Q^l} \cdot x_s \right) \in W,$$

where $j_1 + \cdots + j_m \leq 6D$ and $0 \leq l \leq p, 1 \leq s \leq m$. We have

$$\pi_i \left(\frac{x_1^{j_1} \cdots x_m^{j_m}}{Q^l} \cdot x_s \right) = \pi_i \left(\frac{x_1^{j_1} \cdots x_m^{j_m} Q^{p-l}}{Q^p} \cdot x_s \right) = \frac{1}{Q} \pi_i \left(x_1^{j_1} \cdots x_m^{j_m} Q^{p-l} x_s \right),$$

so $x_1^{j_1} \cdots x_m^{j_m} Q^{p-1} x_s$ has degree at most $6D + D(p - l) + 1 \leq 6D + pD + D = (7 + p)D$. Thus $x_1^{j_1} \cdots x_m^{j_m} Q^{p-l} x_s$ is an $\mathbb{F}_p$-linear combination of monomials of the form $x_1^{l_1} \cdots x_m^{l_m}$ with $l_1 + \cdots + l_m \leq (7 + p)D$. Notice that $\pi_i(x_1^{l_1} \cdots x_m^{l_m} = \pi(x_1^{p\lfloor \frac{l_1}{p} \rfloor} \cdots x_m^{p\lfloor \frac{l_m}{p} \rfloor} x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m})$ with

$0 \le \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \le p-1$. Hence

$$\begin{aligned}\pi(x_1^{p\lfloor\frac{l_1}{p}\rfloor} \cdots x_m^{p\lfloor\frac{l_m}{p}\rfloor} x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}) &= x_1^{\lfloor\frac{l_1}{p}\rfloor} \cdots x_m^{\lfloor\frac{l_m}{p}\rfloor} \pi_i(x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}) \\ &= x_1^{\lfloor\frac{l_1}{p}\rfloor} \cdots x_m^{\lfloor\frac{l_m}{p}\rfloor} \frac{P_{\varepsilon_1,\ldots,\varepsilon_m;i}(x)}{Q(x)} \\ &= \frac{(\text{some polynomial of total degree} \le D + \frac{(7+p)D}{p})}{Q}.\end{aligned}$$

Since $p \ge 2$, $D + \frac{7+p}{p}D \le 2D + 3.5D < 6D$. So $\pi_i(x_1^{j_1} \cdots x_m^{j_m} Q^{p-l} x_s) = \frac{\text{poly of deg} \le 6D}{Q}$, and

$$\begin{aligned}\pi_i\left(\frac{x_1^{j_1} \cdots x_m^{j_m}}{Q^l} x_s\right) &= \frac{1}{Q}\pi_i(x_1^{j_1} \cdots x_m^{j_m} Q^{p-l} x_s) \\ &\subseteq \frac{\text{polynomials of total degree} \le 6D}{Q^2} \subseteq W.\end{aligned}$$

□

10.1. **Derksen's refinement.**

Definition 10.2. We will call a set S a *p-Derksen set* if there exist a prime $p \ge 2$ and $m \ge 0$ and words $w_0, w_1, \ldots, w_m, t_1, \ldots, t_n \in \{0, 1, \ldots, p-1\}$ such that $S = \{[w_0 t_1^{i_1} w_1 t_2^{i_2} \cdots w_{m-1} t_m^{i_m} w_m]_p : i_1, \ldots, i_m \ge 0\}$.

Example 10.3. $\{1, p, p^2, \ldots\} = \{[10^i]_p : i \ge 0\}$, let $m = 1, w_0 = 1, t_1 = 0, w_1 = \varepsilon$.

A subset $S \subseteq \mathbb{N}_0$ is p-normal if S is a finite union of p-Derksen sets.

Theorem 10.4 (Skolem-Mahler-Lech for positive characteristic)**.** *Let K be a field of characteristic $p > 0$ and let $f : \mathbb{N}_0 \to K$ satisfy a linear recurrence over K. Then $\{n \in \mathbb{N}_0 : f_(n) = 0\}$ is a finite union of arithmetic progressions along with a p-normal set.*

Let $\Gamma = (\Sigma, Q, q_0, \delta, F)$ be a DFA. Given two states $q, q' \in Q$, we say that q' is *reachable* from q if there exists $w \in \Sigma^*$ such that $f(q, w) = q'$. We say that $q \sim q'$ ("equivalent") if q' is reachable from q and q is reachable from q'.

Given $q \in Q$, we will let $[q]$ denote the equivalence class of q. We say $[q] \preceq [q']$ if q' is reachable from q.

Lemma 10.5 (Derksen's second lemma)**.** *If Γ is an automaton that accepts the zero set of $f(n)$, then there exists at most one cycle in each equivalence class.*

We need the following claim to prove Derksen's second lemma:

Claim. If $\Sigma = \{0, 1, \ldots, p-1\}$ and suppose that $\Gamma = (\Sigma, Q, q, \delta, F)$ is a DFA that accepts a a subset $S \subseteq \mathbb{N}_0 \cong \{1, 2, \ldots, p-1\} \cdot \{0, 1, \ldots, p-1\}^* \cup \{\varepsilon\}$. Suppose also that each equivalence class in Γ has at most one cycle in it, and all the terminal classes get rejected. Then S is p-normal.

11. October 8

Definition 11.1. Recall that *p-normal sets* are finite unions of sets of the form

$$\{[w_0 t_1^{i_1} w_1 t_2^{i_2} \cdots w_{m-1} t_m^{i_m} w_m]_p : i_1, i_2, \ldots, i_m \geq 0\},$$

and $w_0, \ldots, w_m, t_0, \ldots, t_m \in \{0, 1, \ldots, p-1\}^*$.

Let $\Gamma = (\Sigma, Q, q_0, \delta, F)$ be a DFA. We put an equivalence class $\sim$ on Q: $q \sim q'$ if and only if $[q] \preceq [q']$.

Definition 11.2. We call a DFA a *saguaro* if

(1) there exists a *unique* cycle in all non-maximal equivalence classes with respect to $\preceq$;
(2) all the states in every maximal class are rejecting.

Example 11.3. Let $p = 2$. (Enter the relevant diagram)

Claim. If we have a saguaro then the language $\mathcal{L} \subseteq \Sigma^*$ accepted by it is a finite union of sets of the form

$$\{w_0 t_1^{i_1} w_1 t_{i_2}^{2} \ldots w_{m-1} t_m^{i_m} : i_1, \ldots, i_m \geq 0\}, \tag{1}$$

where $m \geq 0, w_0, w_1, \ldots, w_m, t_1, t_2, \ldots, t_m \in \Sigma^*$. In particular, if $\Sigma = \{0, 1, 2, \ldots, p-1\}$ then we get a p-normal set.

Let $q \preceq q'$ in Q and let $\mathcal{L}_{q,q'} \subseteq \Sigma^*$ be all paths from q to q'. Then we claim that $\mathcal{L}_{q,q'}$ is a finite union of sets of the form (1). Notice that this finishes the proof because $\mathcal{L} = \bigcup_{q \in F} \mathcal{L}_{q_0,q}$.

Proof of the main claim. We prove the main claim by induction on d, where d is the largest non-negative integer such that there exists a chain $[q] = [p_0] \prec [p_1] \prec \cdots \prec [p_d] = [q']$. Base case: $d = 0$. Note that q, q' are in the same class, so there exists a unique cycle t based at q'. Thus $t \in \Sigma^*$, and there exists a shortest path $w_0 \in \Sigma^*$ such that $q \to q'$. Then $\mathcal{L}_{q,q'} = \{wt^i : i \geq 0\}$.

Now suppose that this holds whenever $d < k$ and consider the case when all maximal chains from q to q' have length $\leq k$ and there exists at least one with length k. So there exists a unique cycle based at q or $[q] = q$ and there are no cycles in $[q]$. Also there exist a finite number of minimal paths from $[q]$ to $[u]$ ($[u]$ an immediate successor of $[q]$) with $[q] \prec [u]$ (Note that there cannot exist $[v]$ so that $[q] \prec [v] \prec [u]$ therefore.). So if $w^{(1)}, w^{(2)}, \ldots, w^{(r)}$ are these minimal paths then every path from q to q' starts out as $t^i u_i w^{(i)}$, where u_i is a minimal path from p to the starting vertex of $w^{(i)}$.

Let $p^{(1)}, \ldots, p^{(r)}$ be the terminal vertices of $w^{(i)}$. Then $[q] \prec [p^{(i)}]$. In particular, all maximal chains from $p^{(i)}$ to p' have length $< k$. So

$$\mathcal{L}_{q,q'} = \sum_{i=1}^{r} \{t^j u_i w^{(i)}\} \cdot \mathcal{L}_{p^{(i)},q'},$$

and by the inductive hypothesis, we know that $\mathcal{L}_{p^{(i)},q'}$ is a finite union of things of form (1) – observe that $\{t^i a\} \cdot \{w_1 s_1^j w_2\} = \{t^i (a w_1) s_1^j w_2\}$, which is of the form (1). □

12. October 10

Definition 12.1. A simple linear recurrence

$$f(n) = \sum_{i=1}^{m} c_i \lambda_i^n \quad (c_i \neq 0)$$

is called *degenerate* if there exist $i \neq j$ and $a \geq 1$ such that $\lambda_i^a = \lambda_j^a$ (i.e., λ_i/λ_j is a root of unity). If not degenerate, then we say that $f(n)$ is *non-degenerate.*

Proposition 12.2. *If $f(n)$ is a simple linear recurrence then if $\{n \in \mathbb{N}_0 : f(n) = 0\}$ contains an infinite arithmetic progression then $f(n)$ is degenerate.*

Proof. Suppose that $f(an+r) = 0$ for all $n, a \geq 1$. Start with $0 = f(an+r) = (c_1\lambda_1^2)(\lambda_1^a)^n + \cdots + (c_m\lambda_m^r)(\lambda_m^a)^n =: y_1\beta_1^n + \cdots + y_m\beta_m^n$. So we have

$$y_1\beta_1^n + \cdots + y_m\beta_m^n = 0, \tag{2}$$

for all n and $y_1, \ldots, y_m$ all non-zero.

Claim. If (2) holds for all n, then there exist i, j such that $i \neq j$ and $\beta_i = \beta_j$.

For the above claim, use the Vandermonde matrix:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_n \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{n-1} & \beta_2^{n-1} & \cdots & \beta_m^{n-1} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix} = 0.$$

Since the determinant of the Vandermonde matrix must be zero, the claim follows. □

Theorem 12.3 (Derksen)**.** *Let $f : \mathbb{N}_0 \to K$, where $\operatorname{char} K = 0$, be a simple non-degenerate linear recurrence ($f(n) = \beta_1\lambda_1^n + \cdots + \beta_m\lambda_m^n$). Then $\{n : f(n) = 0\}$ is p-normal.*

Proof. So we have $f(n) = \beta_1\lambda_1^n + \cdots + \beta_m\lambda_m^n, \beta_1, \ldots, \beta_n$ all non-zero, λ_i all non-zero and λ_i/λ_j is not a root of unity for all $i \neq j$.

Step 1. Recall that we found a finite-dimensional $\mathbb{F}_p$-vector space W, such that $\mathscr{S} = \{f_w(n) := w_1\lambda_1^n + \cdots + w_m\lambda_m^n\}$ has the property that $\mathscr{T}$:= all finite products of

$$\chi_w(n) = \begin{cases} 1 & (f_w(n) = 0) \\ 0 & \text{otherwise} \end{cases}$$

is finite and if $h(n) \in \mathscr{T}$ and $0 \leq j \geq p-1$, then $h(pn+j) \in \mathscr{T}$.

Step 2. (Compare #2 on Assignment 2)

We make an automaton $\Gamma = (\Sigma, Q, q_0, \delta, F)$, and take $\Sigma = \{0, 1, \ldots, p-1\}, Q = \mathscr{T}, q_0 = \chi_{\beta_1,\ldots,\beta_m}(n)$ and $F = \{h \in \mathscr{T} : h(0) = 1\}$. If $h_1, h_2 \in \mathscr{T}$ and $h_1(pn+j) = h_2(n)$ then we draw a labelled edge from h_1 to h_2 with label j. Then Γ accepts exactly the $n \in \mathbb{N}_0$ for which $f(n) = 0 (\Leftrightarrow \chi_{\beta_1,\ldots,\beta_m}(n) = 1)$.

More generally, if we change q_0 to some other $g \in \mathscr{T}$, then Γ will accept the n for which $g(n) = 1$.

Step 3. Show that these exists at most one cycle in all non-maximal classes. Suppose otherwise. Then there exists $h \in \mathscr{T}$ in this class that has two cycles based on h. Call the cycles t_1 and t_2. Let $a = \text{length}(t_1), b = \text{length}(t_2)$ and let $u_1 = t_1^b, u_2 = t_2^a$. So length(u_1) = length$(u_2) = ab$, where u_1, u_2 are two paths from h to h of the same length but distinct paths. We will show that how this gives a contradiction.

First, $h \in \mathscr{T}$. So $h(n) = \chi_{w_1^{(1)},\ldots w_m^{(1)}}(n) \cdots \chi_{w_1^{(r)},\ldots,w_m^{(r)}}(n)$. Thus $h(n)$ is the characteristic sequence of the intersection of the zero sets of

$$w_1^{(i)}\lambda_1^m + \cdots + w_n^{(i)}\lambda_m^n \quad (\text{all } w_j^{(i)}\lambda_j^n \text{ nondegenerate})$$

for $i = 1, \ldots, r$. To get a contradiction, we shall suppose that we have a state $h \in \mathscr{T}$ with two paths u_1, u_2 of the same length from $h \to h$, and that h is the characteristic sequence of the intersection of zero sets of simple non-degenerate linear recurrences all of length $\leq d$ (d being the smallest number with respect to this property). So $h(n) = \chi_S(n)$ where S is an intersection of zero sets of $h_i(n) = c_{i1}\gamma_{i1}^n + \cdots + c_{id}\gamma_{id}^n$ $(1 \leq i \leq r), \gamma_{ij} \in \{\lambda_1, \ldots, \lambda_m\}$.

Let s be the length of u_1 (hence the length of u_2 also). Let $j_1 = [u_1]_p < p^s$ and $j_2 = [u_2]_p < p^s$. (Example: if $u_1 = 031, u_2 = 151$ and $p > 5$, then $[u_1]_p = 3p + 1 < p^3$ and $[u_2]_p = 1 + 5p + p^2 < p^3$.) So we have

$$h(n) = h(p^s n + j_1) = h(p^s n + j_2) \quad (\forall n \geq 0)$$

Thus $h(n) = 1$ if and only if

$$c_{i1}\gamma_{i1}^n + \cdots + c_{id}\gamma_{id}^n = 0$$

for all $1 \leq i \leq r$, which is also equivalent to saying

$$c_{i1}\gamma_{i1}^{p^s n + j_k} + \cdots + c_{id}\gamma_{id}^{p^s n + j_k} = 0,$$

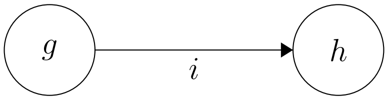
where $1 \leq i \leq r, k = 1, 2$. [lecture stopped] □

13. October 15

Recall that our goal is to prove the following theorem:

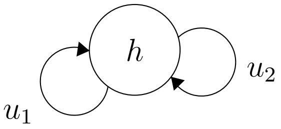
Theorem 13.1. *If $f(n) = \beta_1\lambda_1^n + \cdots + \beta_m\lambda_m^n$ is a simple non-degenerate linear recurrence over K with* char$(K) = p > 0$ *then (by Derksen) $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is p-normal, which is a finite union of $\{c_0 + c_1 p^{s_1 j_1} + \cdots + c_m p^{s_1 j_1 + \cdots + s_m j_m} : j_1, \ldots, j_m \geq 0\}$.*

Let $\Gamma = (\Sigma, Q, q_0, \delta, F)$ be an automaton. Let Q be the functions in τ, i.e., products of characteristic functions of zero sets of $w_1\lambda_1^n + \cdots + w_m\lambda_m^n, (w_1, w_2, \ldots, w_m) \in W^m$. Let, for $g, h \in \tau$,



where $g(pn + i) = h(n)$. Define $F = \{g \in \tau : g(0) = 1\}$, and $q_0 = \chi_S$, where S is the zero set of f.

If $h \in \tau$ is not in a maximal equivalence class, then we cannot have



Once we get this, we are done. To see why, start with the fact that we get ≤ 1 cycle in each non-maximal class, and we claim the states in mammal classes cannot accept

$\Rightarrow$ Γ is a saguaro

$\Rightarrow$ γ accepts a p-normal set (because Γ accepts the zero set of f)

$\Rightarrow$ the zero set of f is p-normal.

As for what happens in a maximal class, Derksen showed that if $h \neq \chi_\phi$ then we get at most 1 cycle. In the proof, we argued that if there exist at least two cycles based at h and $h \neq \chi_\phi$, then let $w_1 = u_1^{l(u_2)}$ and $w_2 = u_2^{l(u_1)}$. Let $s = l(w_1) = l(w_2)$, and $j_1 = [w_1]_p, j_2 = [w_2]_p < p^s$. Then $h(p^s n + j_1) = h(p^s n + j_2) = h(n)$. Now by assumption, let $h \neq \chi_\phi$. So $h(n)$ is the characteristic sequence of an intersection of zero sets of non-degnerate linear recurrences $h(n) = \chi_S(n)$, where

$$S = \bigcap_{i=1}^{r} \{n : w_1^{(i)} \lambda_1^n + \cdots + w_m^{(i)} \lambda_m^n = 0\}.$$

Remark 16. If $\lambda_1, \ldots, \lambda_d \in K \setminus \{0\}$, then λ_i / λ_j is not a root of unity for $i \neq j$. Then if $(a_1, \ldots, a_d) \in K^d$ and $(b_1, \ldots, b_d) \in K^d$ are linearly independent over K, then $\{n : a_1\lambda_1^n + \cdots + a_d \lambda_d^n = 0 \& b_1 \lambda_1^n + \cdots + b_d \lambda_d^n = 0\}$, which is the intersection of zero sets of simple linear recurrences of length $< d$.

Proof. Without loss of generality, suppose $a_1 b_2 - a_2 b_1 \neq 0$. Start off with

$$a_1 \lambda_1^n + \cdots + a_d \lambda_d^n = 0 \tag{3}$$

$$b_1 \lambda_1^n + \cdots + b_d \lambda_d^n = 0. \tag{4}$$

Then we have

$$(b_1 a_2 - a_1 b_2)\lambda_2^n + \cdots + (b_1 a_d - a_1 b_d)\lambda_d^n = 0 \tag{5}$$

$$(b_2 a_1 - a_2 b_1)\lambda_1^n + \cdots + (b_2 a_d - a_2 b_d)\lambda_d^n = 0. \tag{6}$$

(Note $(5) = b_1(3) - a_1(4), (6) = b_2(3) - a_1(4))$. Then both (3) and (4) $= 0$ iff (5) and (6)$= 0$ because $a_1 b_2 - b_1 a_2 \neq 0$.

So if $h(n)$ is the hcaracteristirc sequence of the intersection of zero sets of

$$g_i(n) = \sum_{j=1}^{d} c_{ij} \gamma_{ij}^n, 1 \leq i \leq r$$

So $h(p^s n + j_1) = h(p^s n + j_2) = 0 \Leftrightarrow h(n) = 1 \Leftrightarrow g_1(n) = \cdots = g_r(n) = 0$, and this is equivalent to saying $g_1(p^s n + j_1) = \cdots = g_r(p^s n + j_1) = g_2(p^s n + j_2) = \cdots = g_r(p^s n + j_2) = 0$.

Then for $g_1(n)$, which is of length $\leq d$ and non-denegrate,

$$g_1(p^s n + j_1) = \sum_{j=1}^{d} c_{ij} \gamma_{ij}^{j_1} \left(\gamma_{ij}^{p^s}\right)^n,$$

and

$$g_1(p^s n + j_2) = \sum_{j=1}^{d} c_{ij} \gamma_{ij}^{j_2} (\gamma_{ij}^{p^s})^n.$$

Define $c_{ij} \lambda_{ij}^{j_1} = a_j, c_{ij} \gamma_{ij}^{j_2} = b_j$. Then for

$$c_1 \gamma_1^{j_1} (\gamma_1^{p^s})^n + \cdots + (c_d \gamma_d^{j_1})(\gamma_1^{p^s})^n$$

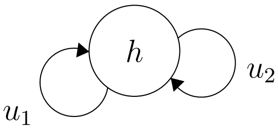
$$c_1 \gamma_1^{j_2} (\gamma_2^{p^s})^n + \cdots + (c_d \gamma_d^{j_2})(\gamma_2^{p^s})^n,$$

Suppose without loss of generality that $c_1, c_2 \neq 0$:

$$(c_1\gamma_1^{j_1})(c_2\gamma_2^{j_2}) - (c_2\gamma_2^{j_1})(c_1\gamma_1^{j_2}) = c_1c_2\gamma_1^{j_1}\gamma_2^{j_1}(\gamma_2^{j_2-j_1} - \gamma_1^{j_2-j_1}). \tag{7}$$

So the intersection of zero sets of $g_1(p^s n + j_1), \ldots, g_r(p^s n + j_1), g_1(p^s n + j_2), \ldots, g_r(p^s n + j_2)$ is an intersection of zero sets of simple non-degenerate linear recurrence of length $< d$. Thus the result follows by induction. □

Corollary 13.2. *If $h \neq \chi_\theta$, it is impossible to get*



.

Thus we get Derksen's theorem.

Corollary 13.3 (Derksen)**.** *Let $f : \mathbb{N}_0 \to K$ satisfy a linear recurrence over K, with* $\mathrm{char}(K) = p > 0$*. Then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a finite union of arithmetic progressions along with a p-normal set.*

Proof. Step 1. Let

$$f(n) = \sum_{i,j} c_{ij} n^i \alpha_j^n \text{ for all sufficiently large } n.$$

Without loss of generality, we may assume that

$$f(n) = \sum_{i,j} c_{ij} n^i \alpha_j^n \text{ for all } n \geq 0.$$

Step 2. For $r = 0, 1, \ldots, p-1$, let

$$f_i(n) = f(pn + r) = \sum_{i,j} c_{ij} r^i \alpha_j^r (\alpha_j^p)^n.$$

If S_r is the zero set of f_r then the zero set of f is the union of $pS_r + r$. Therefore it's enough to consider simple linear recurrences.

Step 3. If $f(n)$ is simple and non-generate we are done. Otherwise, consider all $i \neq j$ such that there exists $a_{ij} > 0$ with $\lambda_i^{a_{ij}} = \lambda_j^{a_{ij}}$, where $f(n) = \sum\limits_{i=1}^{m} c_i \lambda_i^n$. Then let $A = \mathrm{lcm}(a_{ij})$. For $t \in \{0, 1, \ldots, A-1\}$, let $f_t(n) := f(An + t)$, which is non-degenerate or identically zero. To see why, suppose $\lambda_1^{a_{12}} = \lambda_2^{a_{12}}$, so $A = a_{12}$ So we have

$$\begin{aligned}\sum_{i=1}^{m} c_i \lambda_i^{An+t} &= \sum_{i=1}^{m} (c_i\lambda_i^t)(\lambda_i^A)^n \\ &= (c_1\lambda_1^t + c_2\lambda_2^t)(\lambda_1^A)^n + (c_3\lambda_3^t)(\lambda_3^A)^n + \cdots + c_m(\lambda_m^A)^n.\end{aligned}$$

So either $f(n) \equiv 0 \Leftrightarrow f(An + t) \equiv 0$. Thus $\{n : f_t(n) = 0\}$ is p-normal. So

$$f(n) = \sum_{t=0}^{A_1} (A \cdot (\text{zero set of } f_t(n)) + t).$$

Note that each one is either p-normal of an arithmetic progression. □

14. October 17

Definition 14.1. We define $\pi_s(x)$ to be the *counting function*, i.e.,

$$\pi_s(x) := \#\{n \in \mathbb{N}_0 \cap S : n \leq x\}.$$

Definition 14.2. We call $\bar{f}(S)$ the *upper density of* S and $\underline{f}(S)$ the *lower density of* S where:

$$\bar{\delta}(S) = \limsup_{x\to\infty} \frac{\pi_S(x)}{x}$$
$$\underline{\delta}(S) = \liminf_{x\to\infty} \frac{\pi_S(x)}{x}.$$

Moreover, if

$$\bar{\delta}(S) = \underline{\delta}(S) = \lim_{x\to\infty} \frac{\pi_S(x)}{x},$$

then we call this the *density of* S.

Example 14.3. If $S = \{1, 4, 9, 16, ...\}$ then $\pi_S(x) \sim \sqrt{x}$, so $\delta(S) = 0$.

Example 14.4. If $S = \{1, p, p^2, \dots\}$, then $\pi_S(x) \sim \log_p(x)$. Thus $\delta(S) = 0$. In fact, if S is p-normal, then we have $\delta(S) = 0$.

Example 14.5. Let $S = \{n \in \mathbb{N}_0 : \text{binary expansion of } n \text{ has an even number of 1's}\}$. Then $\pi_S(x) \sim x/2$, and $\pi_S(2^n - 1) = 2^{n-1}$. Thus $\delta(S) = 1/2$.

Example 14.6. However, it is entirely possible to have

$$\bar{\delta}(S) = 1$$
$$\underline{\delta}(S) = 0.$$

Consider the following indicator function:

$$\chi_S(n) = \begin{cases} 1 & \text{if there exists } j \text{ such that } (2j)! \leq n < (2j+1)! \\ 0 & \text{if there exists } j \text{ such that } (2j+1)! \leq n < (2j+2)!. \end{cases}$$

Since $\pi_S((2j+1)!) \geq (2j+1)! - (2j)!$, we have

$$\frac{\pi_S((2j+1)!)}{(2j+1)!} \geq 1 - \frac{1}{2^{j+1}} \to 1.$$

On the other hand, note

$$\pi_S((2j)!) \leq 1 + (2j-1)! - 1 = (2j-1)!,$$

so

$$\frac{\pi_S((2j)!)}{(2j)!} \leq \frac{1}{2j-1} \to 0.$$

Conjecture (Erdős-Turan (1936))**.** *If $S \subset \mathbb{N}$ and $\bar{f}(S) > 0$, then if $k \in \mathbb{N}$ there exist $a, b \in \mathbb{N}_0$ with $a \geq 1$ such that $b, b+a, b+2a, \dots, b+(k-1)a \in S$ (k-term arithmetic progression).*

Theorem 14.7 (Roth (1953))**.** *Erdős-Turan is true for $k = 3$.*

Theorem 14.8 (Szemerédi (1975))**.** *Erdős-Turan is true.*

Furstenberg (1977) and Gowers (2001) gave proofs independently.

Theorem 14.9 (Bézivin (1987))**.** *Let K be a field and let $f : \mathbb{N}_0 \to K$ satisfy a linear recurrence over K. Then if $S := \{n \in \mathbb{N}_0 : f(n) = 0\}$ and has $\bar{\delta}(S) > 0$, then S contains an infinitely many arithmetic progression.*

Proof of Bézivin's result. Start with the fact that

$$f(n) = \sum_{i=1}^{j} p_i(n)\lambda_i^n$$

for all sufficiently large n. Suppose that $p_i(n)$ are polynomials in n such that $p_i(x) \in K[x]$, and $\lambda_i \in \overline{K}$. Let D_j denote the degree of $p_j(x)$. The main claim is as follows:

Claim. If $f(n) = \sum\limits_{i=1}^{d} p_i(n)\lambda_i^n$ is zero on an arithmetic progression of length $\geq D_1 + D_2 + \cdots + D_d + d + 1$, then it is zero on the whole infinite arithmetic progression.

Proof of the main claim. We prove by induction on $M := D_1 + D_2 + \cdots + D_d + d$. If $M = 1$, it is trivial. Now assume this is true whenever $M < k$, and consider the case when $M = k$. By assumption, there exist b and $a \geq 1$ so that $f(b) = f(b+a) = \cdots = f(b+ka) = 0$. Now we need to show that $f(b+na) = 0$ for all $n \geq 0$. Let

$$\begin{aligned} f(b+an) &= \sum_{i=1}^{d} p_i(b+an)\lambda_i^{b+an} \\ &= \sum_{i=1}^{d} \underbrace{[p_i(b+an)\lambda_i^b]}_{=:q_i(n)} \underbrace{(\lambda_i^a)^n}_{=:\beta_i}. \end{aligned}$$

Then we have $q_1(n)\beta_1^n + \cdots + q_d(n)\beta_d^n = 0$ for $n = 0, 1, \ldots, k$. Define

$$q_1(n)\beta_1^n + \cdots + q_d(n)\beta_d^n = 0 \quad (n = 0, \ldots, k) \tag{8}$$

$$q_1(n+1)\beta_1^{n+1} + \cdots + q_d(n+1)\beta_d^{n+1} = 0 \quad (n = 0, \ldots, k-1). \tag{9}$$

Now compute (8) $\times\ \beta_1 -$ (9):

$$[[q_1(n) - q_1(n+1)]\beta_1]\beta_1^n + [q_2(n)\beta_1 - q_2(n+1)\beta_2]\beta_2^n + \cdots + [q_d(n)\beta_1 - q_d(n+1)\beta_d]\beta_d^n = 0$$

for $n = 0, \ldots, k-1$. Let

$$D_i' = \deg(q_i(n)\beta_1 - q_i(n+1)\beta_i).$$

Then $D_i' \leq D_i$, and let $d' =$ length of equation, $d' \leq d$. If $D_1 = 0$ then d goes down (no first term) and $d' < d$. In other words,

$$D_1' + \cdots + D_d' + d' < D_1 + \cdots + D_d + d.$$

It vanishes on an arithmetic progression of length $k \geq D_1' + D_2' + \cdots + D_d' + d + 1$. So by inductive hypothesis it vanishes on the entire progression. □

At this we are really done. Note that we just showed that $q_1(n)\beta_1^n + \cdots + q_d(n)\beta_d^n = 0$ for all $n \geq 0$. If not, there exists smallest m so that $q_1(m+1)\beta_1^{m+1} + \cdots + q_d(m+1)\beta_d^{m+1} \neq 0$. By minimality $q_1(m)\beta_1^m + \cdots + q_d(m) + \beta_d^m = 0$. We just showed that $\beta_1(q_1(m)\beta_1^m + \cdots + q_d(m) + \beta_d^m) - (q_1(m+1)\beta_1^{m+1} + \cdots + q_d(m+1)\beta_d^{m+1}) = 0$. Thus $q_1(m+1)\beta_1^{m+1} + \cdots + q_d(m+1)\beta_d^{m+1} = 0$, but this is a contradiction. □

Definition 14.10. A map $f : \mathbb{N}_0 \to \mathbb{C}$ is called a *holonomic (or p-recursive) sequence* if there exists $d \geq 1$ and polynomials $P_0(x), \ldots, P_d(x) \in \mathbb{C}[x]$ not all zero such that

$$P_0(n)f(n) + P_1(n)f(n-1) + P_d(n)f(n-d) = 0,$$

for sufficiently large n.

15. October 20

If we let

$$F(x) = \sum_{n \geq 0} f(n)x^n \in \mathbb{C}[[x]],$$

then we have

Theorem 15.1. *$f : \mathbb{N}_0 \to \mathbb{C}$ is holonomic (or p-resursive) if and only if $F(x)$ satisfies a differential equation of the form*

$$\sum_{j=0}^{e} q_j(x)F^{(j)}(x) = P(x), \tag{10}$$

where $q_0, q_1, \ldots, q_e, P \in \mathbb{C}[x]$.

For instance, if $aF + bF' = P$, then $aF' + a'F + b'F' + bF'' = P'$. Then we have $(aF + bF') - P' - (aF' + a'F + b'F' + bF'')P = 0$.

Rubel (1972) asked whether SML holds for $f : \mathbb{N}_0 \to \mathbb{C}$, where f is holonomic. Bézivin (1981) proved a weaker variant for $F(x) = \sum f(n)x^n$ satisfying (10) with $q_0 q_e \neq 0$, and q_0, q_e not zero at $x = 0$. Methfessel (2000) removed the restrictions on q_0, q_e.

Theorem 15.2. *Let $F(x) = \sum f(n)x^n$ satisfying* (10)*. Then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a finite union of arithmetic progressions along with a set of S of density zero, i.e., $\delta(S) = 0$.*

Around 1994, Dénid began looking at a "dynamical" version of SML.

Theorem 15.3 (Multidimensional Skolem-Mahler-Lech)**.** *Let $\operatorname{char} K = 0$, and $T : K^n \to K^n$ a linear transformation. Suppose also that $v \in K^n, W = \{x : w^T x = 0\} \subset K^n$. If $[T] = A$, Then $\{n \in \mathbb{N}_0 : T^n(v) \in W\} = \{n \in \mathbb{N}_0 : A^n v \in W\} = \{n \in \mathbb{N}_0 : w^T A^n v = 0\}$ is a finite union of arithmetic progressions along with a finite set.*

Dénis asked more generally whether this was true for $\phi : X \to X$, where $X = K^n$ is a quasi-projective variety and $\phi : X \to X$ is a morphism from K^n to K^n such that $(\alpha_1, \ldots, \alpha_n) \to (P_1(\alpha_1, \ldots, \alpha_n), \ldots, P_n(\alpha_1 \ldots, \alpha_n))$. If $Y \subseteq X$ is Zariski-closed (Y subspace of K^n) and $x \in X$, then:

Question 1. Is it true that $\{n \in \mathbb{N}_0 : \phi^n(x) \in Y\}$ is a finite union of arithmetic progressions along with a finite set? Assume $\operatorname{char} K = 0$.

Question 2. If $\operatorname{char} K$ need not be zero, can we get the result when we replace finite set by a set of zero density?

Dénid proved Question 1 for $X = \mathbb{P}^n$ and $\phi \in \operatorname{Aut}(\mathbb{P}^n)$.

Proof of Theorem 15.1. ($\Rightarrow$) There exist $d, P_0, \dot{;}sP_d \in \mathbb{C}[x]$ not all zero so that

$$P_0(n)f(n) + \cdots + P_d(n)f(n-d) = 0$$

for sufficiently large n. So one can write

$$\sum_{i=0}^{R}\sum_{j=0}^{d} c_{ij}n^i f(n-j) = 0$$

for all sufficiently large n. Notice that we can also write this as

$$\sum_{i,j} b_{ij}(n-j)^{(i)} f(n-j)$$

for some constants b_{ij} where $X^{(i)} = X(X-1)\cdots(X-i+1)$ and $X^{(0)} = 1$. (See Example following this proof for an example.)

Given

$$G(x) = \sum_{n\geq 0} g(n)x^n,$$

we will write $[x^N]G(x) = g(N)$. Then what is $[x^n]x^{i+j}F^{(j)}(x)$? For sufficiently large n:

$$\begin{aligned}
j = 0 &: [x^n]x^iF(x) = [x^{n-i}]F(x) = f(n-1)\\
j = 1 &: [x^n]x^{i+1}F'(x) = [x^{n-i}]xF'(x) = (n-i)f(n-i)\\
&\quad F'(x) = \sum_j jf(j)x^{j-1}\\
&\quad xF'(x) = \sum_j jf(j)x^j.\\
j = 2 &: [x^n]x^{i+2}F\text{"}(x) = (n-i)(n-i-1)f(n-i)
\end{aligned}$$

So we have

$$\sum b_{ij}(n-j)^{(i)}f(n-j) = \sum b_{ij}[x^i]x^{i+j}F^{(i)}(x) = 0.$$

So

$$[x^n]\left(\sum_{i,j} b_{ij}X^{i+j}F^{(i)}(x)\right) = 0,$$

for all sufficiently large n. So

$$\sum_{i,j} b_{ij}x^{i+j}F^{(i)}(x) = P(x)$$

for some polynomial P. Grouping the terms gives

$$\sum_i q_i(x)F^{(i)}(x) = P(x),$$

where $q_i(x) = \sum\limits_j b_{ij}x^{i+j}$.

($\Leftarrow$) This process follows easily, since the argument done in ($\Rightarrow$) is reversible. □

Example 15.4. Let $n^2 f(n) + (2n-3)f(n-1) = 0$ for all sufficiently large n. Then one can rewrite the given relation of the form

$$(n^{(2)} + n^{(1)})f(n) + 2((n-1)^{(1)} + (n-1)^{(0)})f(n-1) - 3(n-1)^{(0)}f(n-1) = 0,$$

so we have

$$n^{(2)}f(n) + n^{(1)}f(n) + 2(n-1)^{(1)}f(n-1) - (n-1)^{(0)}f(n-1) = 0.$$

Definition 15.5. A topological space X is *Noetherian* if it satisfies the descending chain condition on closed subsets, i.e., if $C_1 \supseteq C_2 \supseteq \cdots C_f \supseteq \ldots$ with C_i closed there exists n so that $C_n = C_{n+1} = C_{n+2} = \cdots$.

Let X be a Noetherian topological space, $\phi : X \to X$ continuous, and Y a closed subset of X, and $x \in X$. We will show that $\{n \in \mathbb{N}_0 : \phi^n(x) \in Y\}$ is a finite union of arithmetic progression along with a set of S with $f(S) = 0$, from which we can answer affirmative to Dénis' second question and prove the Bézivin-Methfessel result.

Remark 17. If X is a Noetherian topological space and $\mathcal{S}$ is a non-empty collection of closed subsets of X, then $\mathcal{S}$ has a minimal element, with respect to $\supseteq$. Take $C_1 \in \mathcal{S}$. If C_1 is minimal, then we are done. Otherwise, there exists $C_2 \in \mathcal{S}$ so that $C_2 \subsetneq C_1$. If C_2 is minimal, we are done. Otherwise, search for C_3 so that $C_3 \subsetneq C_2$. Since X is Noetherian, we cannot have an infinite chain. Thus there exists n such that C_n is minimal.

16. October 22

Theorem 16.1. *Let X be a Noetherian topological space, and let $f : X \to X$ be continuous. Let $Y \subseteq X$ be closed and let $x \in X$. Then $\{n \in \mathbb{N}_0 : f^n(x) \in Y\}$ is a finite union of arithmetic progressions along with a set S of density zero.*

Lemma 16.2 (Combinatorial lemma)**.** *Let $S \subseteq \mathbb{N}_0$ be a subset with $\overline{\delta}(S) > 0$. Then there exists $a \in \mathbb{N}$ with $a \geq 1$ such that*

$$T := \{i \in \mathbb{N}_0 : i, i+a \in S\}$$

has $\overline{\delta}(T) > 0$.

Proof. Let $S \subseteq \mathbb{N}_0$ have positive upper density. We shall show that we can take $a \in \left\lceil \frac{3}{\overline{\delta}(S)} \right\rceil$. Choose $N := \left\lceil \frac{3}{\overline{\delta}(S)} \right\rceil$. Let $S_0 := \{i \geq 0 : |\{iN, \ldots, (i+1)N-1\} \cap S| \leq 1\}$ and $S_1 := \{i \geq 0 : |\{iN, \ldots, (i+1)N-1\} \cap S| \geq 2\}$. Then $S_0 \cup S_1 = \mathbb{N}_0$. Then let's estimate:

$$\begin{aligned}\pi_S(mN-1) = \#\{i \leq nN-1 : i \in S\} &= \sum_{j=0}^{m-1} |\{jN, jN+1, \ldots, (j+1)N-1\} \cap S| \\ &= \sum_{\substack{j=0 \\ j \in S_0}}^{m-1} |\{jN, \ldots, (j+1)N-1\} \cap S| + \sum_{\substack{j=0 \\ j \in S_1}}^{m-1} |\{jN, \ldots, (j+1)N-1\} \cap S| \\ &\leq \pi_{S_0}(m-1) + N\pi_{S_1}(m-1).\end{aligned}$$

So we have $\pi_S(mN-1) \leq \pi_{S_0}(m-1) + N\pi_{S_1}(m-1)$. We claim that the upper density of S_1 must be positive. If not, then the upper density of S_1 will be zero. Since

$$\frac{\pi_S(mN-1)}{mN-1} \leq \frac{\pi_{S_0}(m-1)}{mN-1} + \frac{N\pi_{S_1}(m-1)}{mN-1} \leq \frac{m}{mN-1} + \frac{N\pi_{S_1}(m-1)}{mN-1},$$

and $\frac{N\pi_{S_1}(m-1)}{mN-1} \to 0$ as $m \to \infty$ (since $\pi_{S-1}(m-1) = o(m)$ and $mN-1$ grows faster than the numerator), it follows that for any sufficiently large m, we have

$$\frac{\pi_S(mN-1)}{mN-1} \leq \frac{2}{N} < \frac{3}{4}\overline{\delta}(S),$$

due to our choice of N. By assumption, there exists $\{x_n\} \in \mathbb{N}$ so that, as $x_n \to \infty$, we have

$$\frac{\pi_S(x_n)}{x_n} \to \overline{\delta}(S).$$

Note that for $x \in \mathbb{N}$, there exists a unique j so that $jN-1 < x \leq (j+1)N-1$. So $\pi_S(jN-1) \leq \pi_S(x) \leq \pi_S((j+1)N-1)$, and we also have

$$\frac{\pi_S(jN-1)}{(j+1)N-1} \leq \frac{\pi_S(x)}{x} \leq \frac{\pi_S((j+1)N-1}{jN-1}.$$

Thus

$$\frac{\pi_S(x)}{x} \leq \frac{\pi_S((j+1)N-1)}{(j+1)N-1} \cdot \frac{(j+1)N-1}{jN-1} < \frac{3}{4}\overline{\delta}(S) \cdot \frac{12}{11} < \overline{\delta}(S),$$

or

$$\limsup_{x\to\infty} \frac{\pi_S(x)}{x} = \overline{\delta}(S) \leq \frac{36}{44}\overline{\delta}(S),$$

but this is a contradiction, since $\overline{\delta}(S) > 0$. Hence $\overline{\delta}(S_1) > 0$, as required. S ofor each $i \in \mathbb{N}_0$, there exist $y, z \in \{iN, \ldots, (i+1)N-1\} \cap S, y < z$ and $1 \leq z - y < N$. For $a \in \{1, 2, \ldots, N-1\}$, let

$$T_a = \{i \in S_1 : \text{ there exists } y, y+a = z \in \{iN, \ldots, (i+1)N-1\} \cap S\}.$$

Then we have $S_1 = T_1 \cup T_2 \cup \cdots \cup T_{N-1}$. Notice that

$$0 < \overline{\delta}(S_1) \leq \sum_{j=1}^{N-1} \overline{\delta}(T_j).$$

So there exists $a \in \{1, 2, \ldots, N-1\}$ so that $\overline{\delta}(T_a) > 0$. Let $T = \{j \in \mathbb{N}_0 : j, j+a \in S\}$. Then we claim that $\overline{\delta}(T) > 0$. Notice that $\pi_T(mN-1) \geq \pi_{T_a}(m-1)$. To see why, we begin by noting that $i \in T_a$ implies that there exists $y \in \{iN-1, \ldots, (i+1)N-1\} \cap T$; therefore, it follows

$$\frac{\pi_T(mN-1)}{mN-1} \geq \frac{\pi_T(m-1)}{mN-1} \geq \frac{\pi_{T_a}(m-1)}{m-1} \cdot \frac{1}{2N}$$

for all sufficiently large m, hence $\overline{\delta}(T) \geq \frac{1}{2N}\overline{\delta}(T_a) > 0$, as required. □

Proposition 16.3. *Let X be a Noetherian topological space, $f : X \to X$ continuous, $Y \subseteq X$ closed, $x \in X$. Then if $S := \{n \in \mathbb{N}_0 : f^n(x) \in Y\}$ has positive upper density, then S contains an infinite arithmetic progression $a\mathbb{N} + b$.*

Proof. Suppose not, and let $\mathcal{S}$ be the collection of closed subsets $Z \subseteq X$ for which there exist a continuous map $g_Z : X \to X$ and a point x_z such that $\{n \in \mathbb{N}_0 : g^n(x) \in Z\}$ has a positive upper density but does not contain an arithmetic progression. By assumption, $\mathcal{S} \neq \emptyset$. So there exist a minimal element $Z_0 \in \mathcal{S}$ and $g : X \to X$ and $x \in X$ such that $\{n : g^n(x) \in \mathbb{Z}_0\} =: S_0$ has positive upper density but does not contain an arithmetic progression. Then $\overline{\delta}(S_0) > 0$. By the combinatorial lemma, there exists $a \geq 1$ so that

$$T_0 := \{i \in \mathbb{N}_0 : i, i + a \in S_0\}$$

has positive upper density. Thus, $i \in \mathcal{T}_0 \Leftrightarrow i, i + a \in S_0 \Leftrightarrow g^i(x), g^{i+a}(x) \in Z_0 \Leftrightarrow g^i(x), g^a(g^i(x)) \in Z_0$. Let $Y_0 := \{z \in Z_0 : g^a(z) \in Z_0\}$. Then Y_0 is closed since both $g^{-a}(Z_0)$ and Z_0 are closed, and $Y_0 = g^{-a}(Z_0) \cap Z_0$. Two possible cases:

<u>Case I:</u> $Y_0 \subsetneq Z_0$

Notice that $g^i(x) \in Y_0 \Leftrightarrow i \in T_0$, and $\overline{\delta}(T_0) > 0$. By minimality of Z_0, $Y_0 \notin \mathcal{S}$. So T_0 contains an arithmetic progression but $T_0 \subseteq S_0$.

<u>Case II</u>: $Y_0 = Z_0$

Note that $Y_0 = Z_0 \Leftrightarrow g^{-a}(Z_0) \supseteq Z_0 \Leftrightarrow g^a(Z_0) \subseteq Z_0$. This implies that S_0 contains an infinite arithmetic progression: note that if $i \in S_0$ then $i + a \in S_0$. □

Theorem 16.4. *If X is a Noetherian topological space, $Y \subseteq X$ closed, $f : X \to X$ continuous and $x \in X$, then $\{n \in \mathbb{N}_0 : f^n(x) \in Y\}$ is a finite union of arithmetic progression along with a set of zero density.*

Proof. Suppose otherwise. Let $\mathcal{S}$ be the collection of closed subsets $Z \subseteq X$ for which $g = g_Z : X \to X, x = x_z \in X$ such that the conclusion doesn't hold. By assumption, $S \neq \emptyset$. Let $Z_0 \in \mathcal{S}$ be minimal and let $g : X \to X$ continuous and $x \in X$ be such that

$$S_0 := \{n \in \mathbb{N}_0 : g^n(x) \in Z_0\}$$

is not a finite union of arithmetic progressions along with a set of density zero. If $\overline{\delta}(S_0) = 0$, then we are done. So we may assume that $\overline{\delta}(S_0) > 0$. So by the proposition, there exist $a \geq 1, b \geq 0$ such that $S_0 \supseteq a\mathbb{N} + b$. Thus we have $g^{an+b}(x) \in Z_0$ for all $n \geq 0$. Now let

$$Y_0 = \overline{\{g^b(x), g^{b+a}(x), \ldots, \}} \subseteq Z_0.$$

Consider $i \in \{0, 1, \ldots, a-1\}$, and suppose $b \in \{0, 1, \ldots, a-1\}$. Consider $\{n : g^{an+i}(x) \in Z_0\}$. When $i = b$, then this is all of $\mathbb{N}_0$ and in fact we are always in $Y_0 \subseteq Z_0$. In general, if $i \neq b$, then $g^{an+i}(x) \in Z_0$. We also know that $g^{an+a+b}(x) \in Z$, where $a + b > i, a + b - i = k, 1 \leq k \leq 2a - 1$. So if $g^{an+i}(x) \in Z$ then $g^{an+i}(x) \in Z$ and $g^{an+i+k}(x) \in Z$. Thus $g^{an+i}(x) \in Z \cap g^{-k}(Z)$. Two cases:

<u>Case I:</u> $Z \cap g^{-k}(Z) = Z$

In this case, we have $g^k(Z) \subseteq Z$, so $g^i(x) \in Z$ hence $g^{i+k}(x) \in Z$. Thus $\{n : g^n(x) \in Z\}$ is a finite union of arithmetic progressions.

<u>Case II:</u> $Y_0 = Z_0 \cap g^{-k}(Z_0) \subsetneq Z_0$

Y_0 is closed, so $Y_0 \notin \mathcal{S}$ by minimality of Z_0. So $\{n : g^{an+i}(x) \in Z_0\} = \{n : g^{an+i}(x) \in Y_0\}$. By minimality of Z_0, $\{m : g^m(x) \in Y_0\}$ is a finite union of arithmetic progressions along with a set of density zero. So for $i \in \{0, \ldots, a-1\}$, the set of $\{n : g^{an+i}(X) \in Z_0\}$ is a finite union of arithmetic progressions along with a set of density 0. Thus

$$\{n : g^n(x) \in Z_0\} = \bigcup_{i=0}^{a-1} \{n \in \mathbb{N}_0 : g^{an+i}(x) \in Z_0\}.$$

Since a finite union of a finite union of arithmetic progressions is a finite union of arithmetic progressions and is a finite union of sets of density 0 is density 0, we get a contradiction. □

17. October 27: Beginning of Phase IV – algebraic geometry?

Note: Proof of the combinatorial lemma done on 27 October is written under the last lecture's section. See the proof of Lemma 16.2.

Definition 17.1. Let K be a field, and $\overline{K}$ the algebraic closure of K. Write

$$\begin{aligned} \mathbb{A}^n &= \{(x_1, \dots, x_n) : x_1, \dots, x_n \in \overline{K}\} \\ \mathbb{P}^n &= (\mathbb{A}^{n+1} \setminus \{(0, 0, \dots, 0)\}) / \sim . \end{aligned}$$

Denote $[x_0, \dots, x_n]$ the equivalence class of $(x_0, \dots, x_n) \in \mathbb{P}^n$. Then $V \subseteq \mathbb{A}^n$ is called an *affine subvariety of* $\mathbb{A}^n$ if there exists $S \subseteq \overline{K}[x_1, \dots, x_n]$ such that $V = \{(a_1, \dots, a_n) \in \mathbb{A}^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in S\}$.

Example 17.2. If $n = 2$, and $V = x\text{-axis} \cap y\text{-axis}$ is an affine subvariety, since $f(x, y) = 0$ for all points in V.

If $T \subseteq \mathbb{A}^n$, then we can associate an ideal $\mathcal{I}(T) \subseteq \overline{K}[x_1, \dots, x_n]$, where

$$\mathcal{I}(T) := \{f \in \overline{K}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in T\}.$$

Similarly, given an ideal $J \subseteq \overline{K}[x_1, \dots, x_n]$ we can associate an affine subvariety $Z(J) \subseteq \mathbb{A}^n$, where

$$Z(J) = \{(a_1, \dots, a_n) \in \mathbb{A}^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in J\}.$$

Note that there is a bijection between $Z(J)$ and J, i.e., between

$\mathbb{A}^n$	$\overline{K}[x_1, \dots, x_n]$
Y (subvarieties)	$\mathcal{I}(Y)$ (radical ideals)
$Z(J)$	J

there is a inclusion-reversing bijection $Y_1 \subseteq Y_2 \Leftrightarrow \mathcal{I}(Y_1) \supseteq \mathcal{I}(Y_2)$.

Definition 17.3. The *Zariski topology on* $\mathbb{A}^n$ is the topology in which the affine subvarieties are the closed subsets. If Y_1, Y_2 are affine subvarieties such that $Y_1 = Z(J_1), Y_2 = Z(J_2), Y_1 \cup Y_2 = Z(J_1 J_2), Y_\alpha = Z(J_\alpha) \Rightarrow \bigcap Y_\alpha = Z(\sum J_\alpha)$.

18. October 29

Definition 18.1. A *projective subvariety* $V \subseteq \mathbb{P}^n$ is a subset given by the set of points $[x_0 : x_1 : \dots : x_n] \in \mathbb{P}^n$ that vanish on some set $\mathcal{S} \subseteq k[x_0, x_1, \dots, x_n]$ consisting of homogeneous polynomials.

Remark 18. Note that we need the polynomials to be homogeneous so that the solutions are well-defined. For instance, the solution to $x_0^2 - x_1$ is $[a^2 : a] = [a : 1]$, but $[1 : 1] = [2 : 2]$, and $[2 : 2]$ is not a solution.

Definition 18.2. *Zariski topology on* $\mathbb{P}^n$ is given by the topology where the closed subsets are precisely the projective subvarieties of $\mathbb{P}^n$.

We have

$$\mathbb{P}^n = \bigcup_{i=0}^{n} \mathbb{A}_i^n,$$

where

$$\mathbb{A}_i^n := \{[x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n : x_i \neq 0\},$$

and that $\mathbb{P}^n \setminus V(x_i = 0) = \mathbb{A}_i^n \cong \mathbb{A}^n$ via the map $[x_0 : x_1 : \cdots : x_n] \mapsto (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i) \in \mathbb{A}^n$. Also, $\mathbb{A}_i^n$ is open in $\mathbb{P}^n$.

Definition 18.3. A *quasi-projective variety* is an open subset $U \subseteq V \subseteq \mathbb{P}^n$ of a projective subvariety V of $\mathbb{P}^n$ for some n. A quasi-projective variety X is called *irreducible* if X cannot be written as $X = X_1 \cup X_2$ with $X_1, X_2 \subsetneq X$ closed.

Thus, U gets a topology from the topology on $\mathbb{P}^n$ and we call this the Zariski topology on U.

Definition 18.4. If X is an irreducible quasi-projective variety, and we have $f(x) = [a_0 : a_1 : \cdots : a_n]$, we say that a map $f : X \to \mathbb{A}^1$ is *regular* at $x \in X$ if for any $X \subseteq Y \subseteq \mathbb{P}^n$ with X open and Y closed, there exists $P, Q \in \overline{K}[x_0, x_1, \ldots, x_n]$ homogeneous polynomials of the same degree such that $Q(a_0, a_1, \cdots, a_n) \neq 0$ and there exists an open neighbourhood $x \in U \subseteq X$ such that $Q|_U \neq 0$ and $f = P/Q$ on U. In particular, $f = P/Q$ on U and so it holds on an open *dense* set of X. Note that if $Y = X \setminus U$, then $X = \overline{U} \cup Y$. Since Y is proper, we have $\overline{U} = X$.

If f is regular at all $x \in X$, then we say f is *regular*.

Definition 18.5. Let $\mathcal{O}_X$ denote the collection of regular functions on X. Then $\mathcal{O}_X$ is a ring. WHen X is affine, we call $\mathcal{O}_X$ the *(affine) coordinate ring of* X.

Example 18.6. Suppose $K = \overline{K} = \mathbb{C}$. Clearly $\mathbb{A}^1 \subseteq \mathbb{P}^1$. $f : \mathbb{A}^1 \to \mathbb{A}^1$ is regular at $[1 : a]$ if

$$f([1 : y]) = \frac{P[1 : y]}{Q[1 : y]},$$

with P, Q homogeneous of same degree and $Q([1 : a]) \neq 0$. In other words, for all $a = [1 : a] \in \mathbb{A}^1$, there is some rational function $\phi_a(t) \in \mathbb{C}(t)$. Then $f(x) = \phi_a(x)$ for x in an open neighbourhood of U_a. Notice properly closed sets in $\mathbb{A}^1$ are finite. So if $a, b \in \mathbb{A}^1$ and $\phi_a(x) = \phi_b(x)$ on $U_a \cap U_b$, then $\phi_a \equiv \phi_b$. So we have $f \equiv \phi$. But $f(x)$ is regular, so it can have no pole. Thus, $f(x) = P(x)$ for some polynomial P. It follows that $\mathcal{O}_{\mathbb{A}^1} \cong \mathbb{C}[x]$. Similarly, we get that $\mathcal{O}_{\mathbb{A}^2} \cong \mathbb{C}[x, y]$ and $\mathcal{O}_{\mathbb{P}^1} = \mathbb{C}$.

Definition 18.7. If X is an irreducible quasi-projective variety and $Y \subseteq X$ closed, then we define the *local ring of* X *along* Y $\mathcal{O}_{X,Y}$ such that $\mathcal{O}_{X,Y}$ is the collection of paris (U, f) where $U \subset X$ open and $U \cap Y \neq \emptyset$ and $f \in \mathcal{O}_U$ with $f : U \to \mathbb{A}^1$ regular modulo the equivalence $(U, f) \sim (V, g)$ if $f \equiv g$ on $U \cap V$. Addition and multiplication are defined as follows:

$$[(U, f)] \cdot [(V, g)] = [(U \cap V, fg)]$$
$$[(U, f)] + [(V, g)] = [(U \cap V, f + g)].$$

Remark 19. Note that $\mathcal{O}_{X,Y}$ is a local ring, i.e., it has a unique maximal ideal. Write $[(U, f)]$ for the class of (U, f). Then

$$\mathfrak{m}_{X,Y} := \{[(U, f)] : f \equiv 0 \text{ on } U \cap Y\}$$

is the unique maximal ideal of $\mathcal{O}_{X,Y}$. To see why, start with $[(U,f)] \notin \mathfrak{m}_{X,Y}$. Thus $f \not\equiv 0$ on $U \cap Y$. Let $V = \{x \in U : f(x) \neq 0\} \subseteq U$ open. Then $\frac{1}{f}$ is regular on V, and

$$\left[\left(V, \frac{1}{f}\right)\right] \cdot [(U,f)] = \left[\left(V \cap U, f \cdot \frac{1}{f}\right)\right] = [(V,1)].$$

Thus $\mathcal{O}_{X,Y} \setminus \mathfrak{m}_{X,Y} = \mathcal{O}^*_{X,Y}$.

Remark 20. If $Y = \{x\}$, then $\mathcal{O}_{X,Y} = \mathcal{O}_{X,x}$ is a local ring at x. If $Y = X$, then we have $\mathfrak{m}_{X,X} = (0)$ so $\mathcal{O}_{X,X}$ is a field. This prompts us to introduce the following definition.

Definition 18.8. We call $\mathcal{O}_{X,X}$ the *field of rational functions* on X. We denote $\mathcal{O}_{X,X}$ by $\overline{K}(X)$.

19. Happy Halloween!

Definition 19.1. Let X, Y be quasi-projective irreducible varieties and $X \subseteq \mathbb{P}^n, Y \subseteq \mathbb{P}^m$, and $f : X \to Y$ with $x \in X$ and $f(x) \in Y$. We say that f is *regular* at x if $f(x) \in \mathbb{P}^m = \bigcup\limits_{i=0}^{m} \mathbb{A}^m_i$, then there exists i so that $f(x) \in \mathbb{A}^m_i$.

Remark 21. So regularity at $x \in X$ means that there exists $x \in U \subseteq X$ an open neighbourhood of x such that $f(U) \subseteq \mathbb{A}^m_i$. So $f|_U : U \to \mathbb{A}^m_i$. We just want that each projection

$$\begin{tikzcd} f|_U : U \arrow[r] \arrow[dr, dashed] & \mathbb{A}^m \arrow[d, "\pi_j"] \\ & \mathbb{A}^1 \end{tikzcd}$$

(where $j = 1, 2, \ldots, m$).

Definition 19.2. $f : X \to Y$ is called a *morphism* if it is regular at all $x \in X$. f is called an *isomorphism* if there exists a morphism $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y, g \circ f = \mathrm{id}_X$. If $Y = X$, then we call f an *endomorphism*, and if $f : X \to X$ is an isomorphism then f is an *automorphism*.

Remark 22. The collection of automorphisms of X is a group under composition. It is denoted by $\mathrm{Aut}(X)$.

Example 19.3. $\mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}}) = \mathrm{PGL}_{n+1}(\mathbb{C}) = \mathrm{GL}_{n+1}(\mathbb{C})/Z$

Example 19.4. $\mathrm{Aut}(\mathbb{A}^2_{\mathbb{C}})$ has two automorphisms: linear and triangular

$$(x,y) \mapsto (\alpha x + \beta y + c_1, \gamma x + \delta y + c_2) \quad (\alpha\delta - \beta\gamma \neq 0) \text{ (linear)}$$
$$(x,y) \mapsto (x, y + p(x)) \quad (p(x) \text{ polynomial; triangular})$$

Definition 19.5. A map $\phi : X \dashrightarrow Y$ is *rational* if there exists an open subset $U \subseteq X$ so that $\phi|_U : U \to Y$ is a morphism. However, ϕ need not be defined for all $x \in X$.

Remark 23. If $f : X \dashrightarrow Y$ is rational and the image of f is dense (dominant), then f induces a map

$$f^* : \overline{K}(Y) = \mathcal{O}_{Y,Y} \to \overline{K}(X) = \mathcal{O}_{X,X}$$

such that $f^*(\phi) = \phi \circ f$. Thus, if $f : X \to Y$ is a morphism and $f(x) = y$ then

$$f^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}.$$

Counterexample. Let $X = Y = \mathbb{A}^1$, and $f : \mathbb{A}^1 \to \mathbb{A}^1$ b $x \mapsto p(x)$. Note that we have $\mathcal{O}_{\mathbb{A}^1} \cong \mathbb{C}[x]$, and that closed sets of $\mathbb{A}^1$ is the union of finite sets of points and $\mathbb{A}^1$. Then

$$f(x) = \begin{cases} x & (x \notin \{0,1\}) \\ 1 & (x = 0) \\ 0 & (x = 1) \end{cases}$$

is continuous but $f(x)$ is not a polynomial in x.

Corollary 19.6 (Dénis' conjecture)**.** *Let X be an irreducible quasi-projective variety, and let $\phi : X \to X$ be an endomorphism, let $x \in X$ and let $Y \subseteq X$ be closed. Then $\{n \in \mathbb{N}_0 : \phi^n(x) \in Y\}$ is a finite union of arithmetic progressions along with a set of density zero.*

Proof. Since X is Noetherian (why?), ϕ continuous and Y is closed, it follows from Theorem 16.1. □

Corollary 19.7 (Bézivin-Methfessel theorem)**.** *Let $F(x) := \sum f(n)x^n \in \mathbb{C}[[x]]$ and suppose that $F(x)$ satisfies a non-trivial differential equation of the form*

$$\sum_{i=0}^{m} p_i(x)F^{(i)}(x) = Q(x),$$

where $P_i, Q \in \mathbb{C}[x]$. Then $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a finite union of arithmetic progressions along with a set of density zero.

Proof. Note that there exists $r \geq 1$ and polynomials $h_0(x), \ldots, h_r(x)$ such that

$$h_0(n)f(n) + h_1(n)f(n-1) + \cdots + h_r(n)f(n-r) = 0$$

for all sufficiently large n with $h_0(x) \not\equiv 0$. So for all sufficiently large n, we have $h_0(n) \neq 0$, hence

$$f(n) = \phi_1(n)f(n-1) + \cdots + \phi_r(n)f(n-r),$$

where

$$\phi_i(x) := -\frac{h_i(x)}{h_0(x)}.$$

Consider the map

$\varphi := ((f(n-1), f(n-2) \ldots, f(n-r), n) \in \mathbb{A}^{r+1}_{\mathbb{C}} \mapsto (f(n), f(n-1), \ldots, f(n-r+1), n+1)$

Consider

$$\varphi : \mathbb{A}^{r+1} \dashrightarrow \mathbb{A}^{r+1},$$

with

$$(t_1, \ldots, t_r, x) \mapsto (\phi_1(x)t_1 + \cdots + \phi_r(x)t_r, t_1, \ldots, t_{r-1}, x+1).$$

Then φ is regular at all points where $h_0(x) \neq 0$ (i.e., in an open set $\mathbb{A}^r \times (A^1 \setminus V(h_0) = 0) =: U$).

Let

$$V = \{(t_1, t_2, \ldots, t_r, x) \in \mathbb{A}^{r+1} : \phi^n(t_1, t_2, \ldots, t_r, x) \in U \;\forall n \geq 0\}.$$

Then $V \subseteq \mathbb{A}^{r+1}$ is a Noetherian topological space with the subspace topology. Notice also that $\varphi(V) \subseteq V$ is continuous. Note also that There exists n_0 so that $\alpha = (f(n_0 - 1), \ldots, f(n_0 - r), n_0) \in V$. Then

$$\varphi^n(\alpha) = \varphi^n(f(n_0-1), \ldots, f(n_0-r), n_0) = (f(n_0+n-1), \ldots, f(n_0+n-r), n_0+r),$$

and that $\varphi^n(\alpha) \in Y \Leftrightarrow f(n_0+n-1) = 0$. By the theorem for Noetherian topological spaces, $\{n \in \mathbb{N}_0 : \varphi^n(\alpha) \in Y\} = \{n \in \mathbb{N}_0 : f(n + n_0 - 1) = 0\}$ is a finite union of arithmetic progressions along with a set of density zero. Hence $\{n \in \mathbb{N}_0 : f(n) = 0\}$ is a finite union of arithmetic progressions along with a set of density zero. □

20. November 3: Beginning of Phase IV

20.1. p-adic functions.

Remark 24. When doing p-adic analysis, it is often better to use $\binom{z}{0}, \binom{z}{1}, \binom{z}{2}, \dots, \binom{z}{n}, \cdots$ as a basis for polynomials. Mahler was the first one to notice this. This basis is useful in proving the following lemma.

Lemma 20.1 (Pólya-Szego lemma)**.** *Let*

$$f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Q}[x],$$

and suffuse that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Then $d!a_i \in \mathbb{Z}$ for all i.

Proof. We use $\{\binom{x}{0}, \dots, \binom{x}{d}\}$ as a $\mathbb{Q}$-basis for the polynomials in $\mathbb{Q}[x]$ of degree $\leq d$. Then there exist $b_0, \dots, b_d \in \mathbb{Q}$ such that $f(x) = \sum\limits_{i=0}^{d} b_i \binom{x}{i}$.

Claim. If $f(n) \in \mathbb{Z}$ for all n, then $b_i \in \mathbb{Z}$ for all i.

Proof of Claim. Notice that

$$\begin{aligned} f(0) &= b_0 \in \mathbb{Z} \\ f(1) &= b_0 + b_1 \in \mathbb{Z} \\ f(2) &= b_0 + 2b_1 + b_2 \in \mathbb{Z} \Rightarrow b_2 \in \mathbb{Z} \\ &\vdots \end{aligned}$$

By induction, we have $b_i \in \mathbb{Z}$ for all $i = 0, 1, \dots, d$. □

Observe that

$$f(x) = b_0 + b_1 \binom{x}{1} + \cdots + b_d \binom{x}{d},$$

and that $i!\binom{x}{i} \in \mathbb{Z}[x]$. So

$$d!f(x) = \sum_{i=0}^{d} b_i d! \binom{x}{i} \in \mathbb{Z}[x],$$

so the result follows. □

20.2. Mahler series.

Definition 20.2. We say that a series

$$f(z) = \sum_{i=0}^{\infty} a_i \binom{z}{i}$$

with $a_i \in \mathbb{Q}_p$ and $|a_i|_p \to 0$ as $i \to \infty$ is a *Mahler series.*

Remark 25. Mahler series always converges on $\mathbb{Z}_p$ and is continuous. To see why, consider the following claim:

Claim. If $z \in \mathbb{Z}_p$ and $i \geq 0$, then $\binom{z}{i} \in \mathbb{Z}_p$.

Proof. Consider the map $g : \mathbb{Z}_p \to \mathbb{Q}_p$ defined as $g(z) := \binom{z}{i}$. Notice that if $n \in \mathbb{Z}$, then $g(n) = \frac{n(n-1)\cdots(n-i+1)}{i!} \in \mathbb{Z}$. Thus $g|_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}_p$. Since g is continuous, $g^{-1}(\mathbb{Z}_p)$ is closed, as $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is closed. And it contains $\mathbb{Z}$, which is dense in $\mathbb{Z}_p$. It follows that $g^{-1}(\mathbb{Z}_p) = \mathbb{Z}_p)$ and so $g : \mathbb{Z}_p \to \mathbb{Z}_p$. Observe then if

$$f(z) = \sum_{i=0}^{\infty} a_i \binom{z}{i}, |a_i|_p \to 0$$

and we define

$$f_n(z) := \sum_{i=0}^{n} a_i \binom{z}{i},$$

which is continuous, then for $z \in \mathbb{Z}_p$, we have

$$|f(z) - f_n(z)| = \left| \sum_{i=n+1}^{\infty} a_i \binom{z}{i} \right| \leq \max_{i>n} |a_i|_p \to 0$$

as $n \to \infty$. So $f(z)$ is continuous since $f_n \to f$ uniformly, and each f_n is continuous. □

Strikingly, the converse holds also:

Theorem 20.3 (Mahler). *If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous, then there exist $a_i \in \mathbb{Q}_p$ with $i \geq 0$ with $|a_i|_p \to 0$ such that*

$$f(z) = \sum_{i=0}^{\infty} a_i \binom{z}{i}.$$

Definition 20.4. Let $\mathscr{C}_p$ be all the continuous maps $f : \mathbb{Z}_p \to \mathbb{Q}_p$. Then the *forward difference operator* on continuous functions $\Delta : \mathscr{C}_p \to \mathscr{C}_p$ is defined as $\Delta(f(z)) = f(z+1) - f(z)$.

Suppose that

$$f(z) = \sum_{i=0}^{\infty} a_i \binom{z}{i}$$

is a Mahler series. What is $\Delta f(z)$? $\Delta(f(z)) = f(z+1) - f(z) = 0 + a_1\binom{z}{0} + a_2\binom{z}{1} + \cdots$. In particular,

$$\Delta^N f(z) = a_N + a_{N+1}\binom{z}{1} + a_{N+2}\binom{z}{2} + \cdots.$$

Thus, we observe that $\Delta^n f(z)|_{z=0} = a_n$. It will be useful to have another expression for $\Delta^j f(z)$:

$$\begin{aligned}
\Delta^0 f(z) &= f(z)\\
\Delta^1 f(z) &= f(z+1) - f(z)\\
\Delta^2 f(z) &= f(z+2) - 2f(z+1) + f(z)\\
&\vdots\\
\Delta^j f(z) &= \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} f(z+i)\\
&\vdots
\end{aligned}$$

Lemma 20.5. *If $k \geq d$, then*

$$\Delta^k z^d = \begin{cases} d! & \text{if } k = d \\ 0 & \text{if } k > d \end{cases}.$$

Proof (sketch). We prove by induction. If $d = 1$, then $\Delta z = 1 = 1!$ and $\Delta^2 z = 1 - 1 = 0$. If true for $d < m$, then

$$\begin{aligned}
\Delta^m z^m &= \Delta^{m-1}(\Delta z^m) = \Delta^{m-1}((z+1)^m - z^m) = \Delta^{m-1}(mz^{m-1} + \text{lower degree terms})\\
&= m\Delta^{m-1} z^{m-1} + \underbrace{\Delta^{m-1}(\text{polynomial of degree} \leq m-2)}_{=0} = m!.
\end{aligned}$$

□

The following is one application of forward differential operators:

Theorem 20.6 (Fermat's little theorem)**.** *For any $a \in \mathbb{N}_0$, $a^p \equiv a \pmod{p}$ for all primes p.*

Proof (Euler). If $a = 0$, then the claim is immediate. If the identity holds for $a = 0, 1, \ldots, m$, then

$$\begin{aligned}
(m+1)^p = m^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} m^{p-i}\right) + 1 &\equiv m^p + 1 \pmod{p}\\
&\equiv m + 1 \pmod{p},
\end{aligned}$$

by the inductive hypothesis. □

Theorem 20.7 (Wilson's theorem)**.** *p is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$.*

Proof (Euler). Notice that

$$(p-1)! = \Delta^{p-1} z^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} (z+i)^{p-1},$$

which is constant for all $z \in \mathbb{Z}$. In particular, this holds when $z = 0$:

$$\begin{aligned}
(p-1)! &= \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} i^{p-1} \\
&= \sum_{i=1}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} i^{p-1} \\
&\equiv \sum_{i=1}^{p-1} (-1)^{p-1-i} \pmod{p} \text{ (By Fermat's little theorem)} \\
&\equiv \underbrace{\sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^{p-1-i}}_{(1-1)^{p-1}} - \binom{p-1}{0} (-1)^{p-1} \pmod{p} \\
&\equiv -\binom{p-1}{0} (-1)^{p-1} \equiv -1 \pmod{p},
\end{aligned}$$

as required. □

21. November 5

Let

$$f(z) = \sum_{n=0}^{\infty} a_n \binom{z}{n},$$

with $a_n \in \mathbb{Q}_p$, $|a_n|_p \to 0$. Then $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous.

Theorem 21.1. *If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous then there exists $a_n \in \mathbb{Q}_p$ with $|a_n|_p \to 0$ such that $f(z) = \sum\limits_{n} a_n \binom{z}{n}$ for all $z \in \mathbb{Z}_p$.*

Lemma 21.2 ("Modulo"[1] lemma)**.** *Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be continuous. Then*

$$|(\Delta^n(f))(0)|_p = \left| \sum_{j=0}^{n} \binom{n}{j} f(j) (-1)^{n-j} \right|_p \to 0 \text{ as } n \to \infty.$$

Proof of Theorem 21.1 ("modulo"/assuming the lemma). Let $a_n = \Delta^n(f)(0)$ and let

$$g(z) = \sum_{i=0}^{\infty} a_i \binom{z}{i}.$$

[1] Professor Bell couldn't think of any other way to express ”assuming the lemma” so he used modulo instead, which is arguably awkward. We settled with "assuming the lemma" or "modulo the proof of the lemma", but this whole incident was amusing enough to warrant a mention here!

Then the above series is a Mahler series because $|a_i|_p \to 0$ as $i \to \infty$. Then

$$\Delta^n(g(z)) = \sum_{i=0}^{\infty} a_{i+n}\binom{z}{i}.$$

Thus $\Delta^n(g)(0) = a_n = \Delta^n(f)(0)$.

Claim. $g(j) = f(j)$ for all $j \in \mathbb{N}_0$.

Proof of Claim. $g(0) = a_0 = \Delta^0(f)(0) = f(0)$. Thus the claim holds for $j = 0$. Assume now that $g(j) = f(j)$ for all $0 \le j \le n-1$. Then

$$\sum_{j=0}^{n}\binom{n}{j}g(j)(-1)^{n-j} = \Delta^n(g)(0) = \Delta^n(f)(0) = \sum_{j=0}^{n}\binom{n}{j}f(j)(-1)^{n-j}.$$

By inductive hypothesis,

$$\begin{aligned}\sum_{j=0}^{n}\binom{n}{j}f(j)(-1)^{n-j} &= \sum_{j=0}^{n-1}\binom{n}{j}g(j)(-1)^{n-j}\binom{n}{n}f(n)\\ &= \sum_{j=0}^{n}\binom{n}{j}g(j)(-1)^{n-j} + f(n) - g(n).\end{aligned}$$

Therefore $f(n) = g(n)$, as required. □

By assumption, $f, g : \mathbb{Z}_p \to \mathbb{Q}_p$ are continuous. Let $h := f - g$ is continuous and is zero on all $\mathbb{N}_0$, so it is zero on $\overline{\mathbb{N}_0} = \mathbb{Z}_p$. Thus $h \equiv 0$ so $f = g$, as desired. □

Proof of the "modulo" lemma (Lemma 21.2). Since $\mathbb{Z}_p$ is compact and f continuous, there exists a maximum, say, $M := \max\limits_{z\in\mathbb{Z}_p}|f(z)|$.

Claim. For all $d \ge 0$, there exists $N_d \in \mathbb{N}$ such that

$$|\Delta^n f(z)| \le \frac{M}{p^d} \text{ for all } z \in \mathbb{Z}_p$$

whenever $n \ge N_d$.

Proof of the claim. . If $d = 0$, take $N_0 = 0$, since

$$\begin{aligned}|\Delta^n f(z)|_p &= \left|\sum_{j=0}^{n}\binom{n}{j}(-1)^{n-j}f(z+j)\right|\\ &\le \max_{0\le j\le n}\underbrace{\left|\binom{n}{j}\right|_p}_{\in\mathbb{Z},\le 1}\underbrace{|f(z+j)|_p}_{\le M} \le M.\end{aligned}$$

Just for fun, let's take a look at the $d = 1$ case. We need a right $N_1 \in \mathbb{N}$ so that $|\Delta^n f(z)|_p \le M/p$ for all $n \ge N_1, z \in \mathbb{Z}_p$. Since f is continuous, we have that, for $m \ge 1$, such that

$|f(z+p^m)-f(z)|_p < Mp^{-1}$ for all $z \in \mathbb{Z}_p$. This is uniformly continuous, since any continuous function over a compact space is necessarily uniformly continuous. Let

$$\begin{aligned} g(z) = \Delta^{p^n} f(z) &= \sum_{j=0}^{p^m} \binom{p^m}{j} (-1)^{p^m-j} f(z+j) \\ &= f(z+p^m) + (-1)^{p^m} f(z) + \sum_{j=1}^{p^m-1} \binom{p^m}{j} (-1)^{p^m-j} f(z+j). \end{aligned}$$

So

$$\begin{aligned} |g(z)|_p &\leq \max\left(|f(z+p^m)+(-1)^{p^m} f(z)|_p, \left\{ \left| \binom{p^m}{j} \right|_p |f(z+j)|_p : j = 1, 2, \ldots, p^m - 1 \right\} \right) \\ &\leq \max\left\{ \frac{M}{p}, \ldots, \frac{M}{p} \right\} = \frac{M}{p}. \end{aligned}$$

By the argument we did in the $d = 0$ case, we have

$$|\Delta^n(g(z))|_p = |\Delta^{n+p^m}(f(z))|_p \leq \frac{M}{p}$$

for all $n \geq 0, z \in \mathbb{Z}_p$ So we can take $N_1 = p^m$ for $d = 1$.

Now, in general, if we have produced an N_d for some d, we may let $h(z) = \Delta^{N_d} f(z)$. Then $|h(z)|_p \leq M/p^d$ for all $z \in \mathbb{Z}_p$. So now we can do $d = 1$ case on $h(z)$: we know there exists $N_1' \in \mathbb{N}$ such that

$$|\Delta^n h(z)|_p \leq \frac{M/p^d}{p} = \frac{M}{p^{d+1}}$$

for all $z \in \mathbb{Z}_p, N \geq N_1'$. But $\Delta^n h = \Delta^{n+N_d} f$, so

$$|\Delta^n f(z)|_p < \frac{M}{p^{d+1}} \text{ for all } n \geq N_d + N_1' =: N_{d+1}.$$

The result follows by induction. □

Now that we proved the claim, the lemma follows also. □

Remark 26. Quick aside remark on Ruzsa's conjecture:

Conjecture (Ruzsa's conjecture). *Let $f : \mathbb{Z} \to \mathbb{Z}$ have the property that for every prime p and every $n \in \mathbb{Z}$, we have $f(n+p) \equiv f(n) \pmod{p}$. Suppose also that there exists $\alpha \in (0, 1)$ such that*

$$|f(n)| < \exp(\alpha|n|)$$

for all sufficiently large n. Then $f(n)$ is a polynomial in n.

Ruzsa proved this for all $|f(n)| < C(e-1)^{|n|}$ for all sufficiently large n. This proof uses the forward differential operator. First, observe that if $n \geq p$ then $p \mid \Delta^n f(0)$, since

$$\Delta^p f(n) = \sum_{j=0}^{p} \binom{p}{j} (-1)^{p-j} f(n+p) \equiv f(n+p) - f(n) \equiv 0 \pmod{p}.$$

So for all $m \geq p$, $\Delta^m f(n) \equiv 0 \pmod{p}$. If $n \geq p$, then $p \mid \Delta^n f(0)$, and in particular,

$$\prod_{p \leq n} p \mid \Delta^n f(0)$$

for all $n \geq 2$. But

$$\begin{aligned} |\Delta^n f(0)| &= \left| \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} f(j) \right| \\ &\leq \sum_{j=0}^{n} \binom{n}{j} |f(j)| \leq \sum_{j=0}^{n} \binom{n}{j} C(e-1)^{(1-\varepsilon)j} \\ &\leq C(1+(e-1)^{1-\varepsilon})^n < e^{\left(1-\frac{\varepsilon}{2}\right)^n} \end{aligned}$$

for all sufficiently large n. Since

$$\log\left(\prod_{p \leq n} p\right) \sim n \text{ as } n \to \infty$$

(the prime number theorem), and since $\log(|\Delta^n f(0)|+1) < (1-\frac{\varepsilon}{2})n$ for all sufficiently large n, it follows (think about it!) $\Delta^n f(0) = 0$ for all sufficiently large n. Therefore (think about it no. 2!), $f(n)$ is a polynomial.

The following result by Umberto Zannier is the best result so far:

Theorem 21.3 (Zannier). *Ruzsa's conjecture holds for all* $|f(n)| < 2.117^{|n|}$ *for all sufficiently large* $|n|$.

22. November 7

Recall that we proved the following last class:

- Every continuous $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is a Mahler series.
- Not every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is analytic.

We would like a criterion that tells us when a Mahler series is analytic.

Proposition 22.1. *Suppose that*

$$F(z) = \sum_{n \geq 0} a_n \binom{z}{n}$$

satisfies $|\frac{a_n}{n!}|_p \to 0$ *as* $n \to \infty$. *Then* $F(z)$ *is* p*-adic analytic.*

Proof. Let

$$\begin{aligned} F_n(z) &= \sum_{j=0}^{n} a_j \binom{z}{j} = \sum_{j=0}^{n} c_{j,n} z_j \quad (c_{j,n}) \in \mathbb{Q}_p) \\ &= c_{j,n} z^j \qquad \text{where } c_{j,n} = 0 \text{ for all } j > n. \end{aligned}$$

So we have

$$F_{n+1}(z) - F_n(z) = a_{n+1} \binom{z}{n+1} = \frac{a_{n+1}}{(n+1)!} \underbrace{(z(z-1)(z-2)\cdots(z-n))}_{\in \mathbb{Z}[z]}.$$

Observe also that $|\frac{a_{n+1}}{(n+1)!}|_p \to 0$. This is also equal to

$$\sum_{j=0}^{\infty} c_{j,n+1} z^j - \sum_{j=0}^{\infty} c_{j,n} z^j = \sum_{j=0}^{\infty} (c_{j,n+1} - c_{j,n}) z^j$$

$$\Rightarrow |c_{j,n+1} - c_{j,n}| \leq \left|\frac{a_{n+1}}{(n+1)!}\right|_p \text{ for all } n, j$$

Since

$$\left|\frac{a_{n+1}}{(n+1)!}\right|_p \to 0,$$

we have that for fixed j, $\{c_{j,n}\}_{n\geq 0}$ is a Cauchy sequence. By completeness, one can find $b_j \in \mathbb{Q}_p$ such that $c_{j,n} \to b_j$ as $n \to \infty$. Also, given $\varepsilon > 0$, there exists N such that $|c_{j,n} - b_j|_p < \varepsilon$ for all $n \geq N, j \geq 0$.

Let $G(z) := \sum b_j z^j$. Two claims, which will finish the proof of this proposition:

Claim. $G(z)$ is p-adic analytic, i.e., $|b_j|_p \to 0$. Moreover, $G(z) = F(z)$.

Proof of the claim. For the first claim, we start with arbitrary $\varepsilon > 0$. Then there exists $N = N(\varepsilon)$ such that

$$|c_{j,n} - b_j| < \frac{\varepsilon}{2} \text{ for all } n \geq N, \jmath \geq 0.$$

In particular, if $j > N$, we take $n = N$ so that

$$|c_{j,N} - b_j|_p < \frac{\varepsilon}{2} \Rightarrow |b_j|_p < \frac{\varepsilon}{2} \text{ for all } j > N.$$

Thus $|b_j|_p \to 0$, as required.

As for the second part, since $F(z)$ is continuous and $|a_n|_p \to 0$, we know that $F_n(z) \to F(z)$ uniformly on $\mathbb{Z}_p$. Also,

$$G(z) - F_n(z) = \sum_{j=0}^{\infty} (b_j - c_{j,n}) z^j,$$

and $c_{j,n} \to b_j$ uniformly, so $F_n(z) \to G(z)$ uniformly. Thus $G \equiv F$, as desired. □

Thus, the claim follows. □

Remark 27 (On Poonen's interpolation theorem). Consider the map $f : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ and $\alpha := (\alpha_1(0), \ldots, \alpha_d(0)) \in \mathbb{Z}_p^d$ such that $f^n(\alpha) = (\alpha_1(n), \ldots, \alpha_d(n)) \in \mathbb{Z}_p^d$. Then Poonen's interpolation theorem states that under certain conditions (to be clarified later) there exist $g_1, g_2, \ldots, g_d : \mathbb{Z}_p \to \mathbb{Z}_p$ all of which are p-adic analytic such that $\alpha_i(n) = g_i(n)$ for all $n \in \mathbb{N}_0$.

Definition 22.2. Let p be prime. We define the *Tate algebra*

$$\mathbb{Z}_p\langle x_1, x_2, \ldots, x_d\rangle \subseteq \mathbb{Z}_p[[x_1, x_2, \ldots, x_d]]$$

as the set of convergent power series on $\mathbb{Z}_p^d$, i.e.,

$$\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle = \left\{ \sum_{i_1,\ldots,i_d \geq 0} c_{i_1,\ldots,i_d} x_1^{i_1} \cdots x_d^{i_d} : c_{i_1,\ldots,i_d} \in \mathbb{Z}_p \ \forall i_1, \ldots, i_d, \ |c_{i_1,\ldots,i_d}|_p \to 0 \text{ as } \sum_{i=1}^{d} c_i \to \infty \right\}$$

Theorem 22.3 (Poonen's interpolation theorem (2013))**.** *Let $p \geq 3$. If $f_1, \dots, f_d \in \mathbb{Z}_p\langle x_1, \dots, x_d\rangle$ satisfy*

$$f_i(x_1, \dots, x_d) \equiv x_i \pmod{p},$$

or equivalently,

$$f_i(x_1, \dots, x_d) = \sum c_{j_1,\dots,j_d} x_1^{j_1} \dots x_d^{j_d}$$

where

$$c_{j_1,\dots,j_d} \in \begin{cases} p\mathbb{Z}_p & (j_1, \dots, j_{i-1}, j_i, j_{i_1}, \dots, j_d) \neq (0, \dots, 0, 1, 0, \dots, 0) \\ 1 + p\mathbb{Z}_p & \textit{otherwise} \end{cases}.$$

Then we can make a map $F : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ defined by $(\alpha_1, \dots, \alpha_d) \mapsto (f_1(\alpha_1, \dots, \alpha_d), \dots, f_d(\alpha_1, \dots, \alpha_d))$. If $(\beta_1, \dots, \beta_d) \in \mathbb{Z}_p^d$, thenthere exists p-adic analytic maps $g_1, g_2, \dots, g_d$ such that

$$(g_1(n), \dots, g_n(d)) = F^n(\beta_1, \dots, \beta_d).$$

Proof. Let $R = Z_p\langle x_1, \dots, x_d\rangle$. We shall construct a map $\Delta : R^d \to R^d$ by $\Delta(h_1, \dots, h_d) = (h_1 \circ F, \dots, h_d \circ F) - (h_1, h_2, \dots, h_d)$.

Claim. $\Delta : R^d \to (pR)^d$.

Proof. Note that

$$\begin{aligned} \Delta(h_1, \dots, h_l) &= (h_1(f_1, \dots, f_d), \dots, h_d(f_1, \dots, f_d)) - (h_1, \dots, h_d) \\ &= (h_1(x_1 + pg_1, \cdots, x_d + pg_d), \dots, h_d(x_1 + pg_1, \dots, x_d + pg_d)) \\ &\qquad - (h_1(x_1, \dots x_d), \dots, h_d(x_1, \dots, x_d)). \end{aligned} \tag{11}$$

Since $h_i(x_1 + pg_1, \dots, x_d + pg_d) - h_i(x_1, \dots, x_d) \equiv 0 \pmod{p}$ for all i, we have (11) $\equiv 0$ (mod $(pR)^d$).

In general, we see that $\Delta^m : R^d \to (p^m R)^d$, since we can pull out powers of p as we continuously apply Δ. □

Poonen's trick goes as follows: let

$$\begin{aligned} G(z) &:= \sum_{j=0}^{\infty} \Delta^j \underbrace{(x_1, \dots, x_d)}_{\in (p^j R)^d} \binom{z}{j} \\ &= \sum_{j=0}^{\infty} (\theta_{1j}(x_1, \dots, x_d), \dots, \theta_{dj}(x_1, \dots, x_d)) \binom{z}{j}, \end{aligned}$$

where $(\theta_{1j}, \dots, \theta_{dj}) = \Delta^j(x_1, \dots, x_d) \in (p^j R)^d$. Note that G depends on $x_1, \dots, x_d$ and z. So we will write $G(z) = G(x_1, \dots, x_d; z)$. And let $(\beta_1, \dots, \beta_d) \in \mathbb{Z}_p^d$, and consider

$$G(\beta_1, \dots, \beta_d; z) = \sum_{j=0}^{\infty} \underbrace{(\theta_{1j}(\beta_1, \dots, \beta_d), \dots, \theta_{dj}(\beta_1, \dots, \beta_d))}_{\in (p^j \mathbb{Z}_p)^d} \binom{z}{j}.$$

Now define

$$g_i(z) := \sum_{j=0}^{\infty} \theta_{ij}(\beta_1, \dots, \beta_d) \binom{z}{j}.$$

Then $(g_1(z), \dots, g_d(z)) = G(\beta_1, \dots, \beta_d; z)$. We remain to prove these claims (proving them next class):

- $g_i(z)$'s are p-adic analytic
- $(g_1(n), \dots, g_d(n)) = F^n(\beta_1, \dots, \beta_d)$ for all $n \geq 0$.

To be continued next Monday... □

23. November 10

Starting from where we left off:

Claim. We are done once we prove the following two claims:

- $g_i(z)$'s are p-adic analytic
- $(g_1(n), \dots, g_d(n)) = F^n(\beta_1, \dots, \beta_d)$ for all $n \geq 0$.

Proof. Recall that

$$g_i(z) = \sum_{n=0}^{\infty} \theta_{in} \binom{z}{n}$$

and by our criterion, it is enough to show that

$$\left| \frac{\theta_{in}}{n!} \right|_p \to 0$$

as $n \to \infty$. Note that $\theta_{in} \in p^n \mathbb{Z}_p$, so $|\theta_{in}|_p \leq p^{-n}$. Since

$$|n!|_p = p^{-\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \cdots} = p^{-\frac{n}{p-1} + O(\log_p n)},$$

it follows that

$$\left| \frac{\theta_{in}}{n!} \right|_p = p^{-n + \frac{n}{p-1} + O(\log_p n)} \to 0$$

as $n \to \infty$ (and note that we assume $p \geq 3$).

So this proves the first claim. For the second one, since we have

$$G(x_1, x_2, \dots, x_d; z) = \sum_{j=0}^{\infty} \Delta^j (x_1, \dots, x_d) \binom{z}{j},$$

so when $z = n$,

$$G(x_1, x_2, \dots, x_d; n) = \sum_{j=0}^{n} \Delta^j (x_1, \dots, x_d) \binom{n}{j}.$$

Let $I : R^d \to R^d$ be the identity operator. Then we have

$$\begin{aligned} G(x_1, x_2, \dots, x_d; n) &= \sum_{j=0}^{n} \Delta^j (x_1, \dots, x_d) \binom{n}{j} \\ &= (I + \Delta)^n (x_1, \dots, x_d). \end{aligned}$$

Since $\Delta(h_1, \dots, h_d) = (h_1 \circ F, \dots, h_d \circ F) - (h_1, h_2, \dots, h_d)$, we have $(I + \Delta(h_1, \dots, h_d) = (h_1 \circ F, \dots, h_d \circ F)$. Therefore, by induction,

$$(I + \Delta)^n (x_1, \dots, x_d)|_{(x_1, \dots, x_d) = (\beta_1, \dots, \beta_d)} = (x_1 \circ F^n, \dots, x_d \circ F^n)(\beta_1, \dots, \beta_d) = F^n(\beta_1, \dots, \beta_d),$$

as required. □

We claim that this gives SML. To see why, let's start with $f : \mathbb{N}_0 \to K$ (assume $\operatorname{char} K = 0$). This satisfies a linear recurrence over K. Then we know there exist $w, v \in K^d, A \in \mathrm{M}_d(K)$ such that $f(n) = w^T A^n v$ for all sufficiently large n. However, what is not as well-known is the fact that we can assume that A is invertible.

Why we can assume A to be invertible (sketch). Suppose $n \geq 0$ and $v_n = A^n v \in K^d$. Let $W_n = \operatorname{span}_K\{v_n, v_{n+1}, \ldots\}$. Since $K^d \supset W_1 \supset W_2 \supset \cdots$, so there exists m so that $W := W_m = W_{m+1} = \cdots$ by the Noetherian property.

Remark 28. First, we have $A(W) \subseteq W$, and $A|_W : W \to W$ is surjective. In particular, $A|_W$ is invertible.

Suppose $x := v_m \in W$ and $B := A|_W$. Then $B^n x = A^n v_m = v_{m+n} \in W$. Now $w^T A^n v = w^T v_n = f(n)$ for all sufficiently large n. Consider $g : W \to K$ such that $g(y) = w^T y$. Then there exists $z \in W$ such that $w^T A^n v_m = z^T B^n x$. Let $u^T = z^T B^{-m}$, which is well-defined since B is invertible. Then $u^T B^n x = z^T B^{-m} B^n x = z^T B^{n-m} x = f(n)$ for all sufficiently large n, as required. □

Now we are ready to apply Poonen's interpolation theorem (Theorem 22.3) to prove SML.

Proof of SML with PIT. Let $f : \mathbb{N}_0 \to K$ satisfy a linear recurrence over K. Then there exists $d \geq 1$ so that $w, v \in K^d, A \in \mathrm{GL}_d(K)$ such that $f(n) = w^T A^n v$ for all sufficientl ylarge n. Write

$$w = \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}, v = \begin{bmatrix} c_1 \\ \vdots \\ c_d \end{bmatrix},$$

with $\Delta := \det(A) \in K$.

Step 1. Let $K_0 := \mathbb{Q}(b_1, \ldots, b_d, c_1, \ldots, c_d, a_{ij})$, a finitely-generated extension of $\mathbb{Q}$. By Lech's embedding theorem, there exists $p \geq 3$ such that $K_0 \hookrightarrow \mathbb{Q}_p$ such that $b_1, \ldots, b_d, c_1, \ldots, c_d, a_{ij}, \Delta, \Delta^{-1}$ are sent to $\mathbb{Z}_p$.

Step 2. We now regard $v, w \in \mathbb{Z}_p^d$ and $A \in \mathrm{GL}_d(\mathbb{Z}_p)$ because $\Delta \in \mathbb{Z}_p^*$). So we think of $A : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$, as a linear and invertible map.

Step 3. Notice that if we reduce mod p, we get

$$\overline{A} : \mathbb{F}_p^d \to \mathbb{F}_p^d.$$

We still have linearity – but we also have invertibility because $\Delta \in \mathbb{Z}_p^*$. Thus $\overline{A} \in \mathrm{GL}_d(\mathbb{F}_p)$. Since $|\mathrm{GL}_d(\mathbb{F}_p)| < \infty$, there exists $N \geq 1$ so that $\overline{A}^N = I \in \mathrm{GL}_d(\mathbb{F}_p)$. Hence $A^N \equiv I \pmod p$, so $A^N(x_1, \ldots, x_d) \equiv (x_1, \ldots, x_d) \pmod p$. So if we let $f_1, f_2, \ldots, f_d$ be linear forms in $x_1, \ldots, x_d$ such that $A^N(x_1, \ldots, x_d) := (f_1(x_1, \ldots, x_d), \ldots, f_d(x_1, \ldots, x_d))$. Then $f_i(x_1, \ldots, x_d) \equiv x_i \pmod p$ Thus we can let $A^N = F$ in Theorem 22.3.

Step 4. Let $i \in \{0, 1, \ldots, N-1\}$. Let

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_d \end{bmatrix} = A^i v = A^i \begin{bmatrix} c_1 \\ \vdots \\ c_d \end{bmatrix} \in \mathbb{Z}_p^d.$$

Then

$$A^{Nn+i}(v) = A^{Nn}A^i v = (A^N)^n \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_d \end{bmatrix} = F^n(\beta_1, \ldots, \beta_d).$$

By Theorem 22.3, there exist $g_1, \ldots, g_d : \mathbb{Z}_p \to \mathbb{Z}_p$ analytic so that $F^n(\beta_1, \ldots, \beta_d) = (g_1(n), \ldots, g_d(n))$. So

$$f(Nn+i) = w^T A^{Nn+i} v = w^T F^n(\beta_1 \ldots, \beta_d) = \begin{bmatrix} b_1 & \cdots & b_d \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_d \end{bmatrix} = \sum_{i=1}^{d} b_i g_i(n).$$

<u>Step 5</u>. Let

$$h(z) = \sum_{i=1}^{d} b_i g_i(z).$$

Notice that for all sufficiently large n, we have $h(n) = 0 \Leftrightarrow f(Nn+i) = 0$. By Strassman's theorem, either $h(z) \equiv 0$ or it has finitely many zeros in $\mathbb{Z}_p$. Thus, we can conclude that either $f(Nn+i) = 0$ for all sufficiently large n or there can only exist finitely many n for which $f(Nn+i) = 0$. SML now follows. □

24. Dynamical Mordell-Lang Conjecture

Definition 24.1. Let X be a quasi-projective variety over $\mathbb{C}$. We will say that X is an *algebraic group* if X is a group such that $M : X \times X \to X$ defined as $(x, y) \mapsto xy$ and $i : X \to X$ defined as $x \mapsto x^{-1}$ are morphisms.

Example 24.2. $C^* = \mathbb{A}^1 \setminus \{0\}$ is an algebraic group. And note that

$$\mathbb{A}^1 \setminus \{0\} \cong V(xy - 1 = 0) \subseteq \mathbb{A}^2_{\mathbb{C}},$$

and such group is called an *affine algebraic group*. More generally, $(\mathbb{C}^*)^n$ is an affine algebraic group.

Example 24.3 (Elliptic curves). Elliptic curves are projective algebraic groups, and in particular are examples of *abelian varieties*

Definition 24.4. An *abelian variety* A is a projective, connected algebraic group. To put it another way, abelian varieties are *complete* connected algebraic groups. Note that X closed implies that $\pi : X \times Y \to Y$ is a closed map for all varieties Y.

Example 24.5. $\mathrm{GL}_n(\mathbb{C}) \subseteq \mathbb{A}^{n^2} \setminus V(\Delta = 0)$, where

$$\Delta(x_{11}, \ldots, x_{nn}) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)}.$$

Then $\mathrm{GL}_n(\mathbb{C})$ is an affine algebraic group, and $\mathrm{GL}_n(\mathbb{C}) \cong V(\Delta t = 1) \subseteq \mathbb{A}^{n^2} \times \mathbb{A}^1$.

Fact 1 (Important fact)**.** *Any affine algebraic group is* linear*, i.e., isomorphic to a Zariski-closed subgroup of some* $\mathrm{GL}_n(\mathbb{C})$*.*

Fact 2. *If G is an algebraic group and N is a normal and closed subgroup of G, then G/N can be given the structure of an algebraic group.*

Example 24.6. Let $G = \mathrm{GL}_n(\mathbb{C})$, and let

$$Z = \left\{ \begin{bmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{bmatrix} : a \in \mathbb{C}^* \right\} \cong \mathbb{C}^*.$$

Then $G/Z = \mathrm{PGL}_n(\mathbb{C})$.

Theorem 24.7 (Chevalley's structure theorem). *Let G be a connected algebraic group over $\mathbb{C}$. Then there exists a* unique *normal (or characteristic) closed affine algebraic subgroup N such that G/N is an abelian variety, i.e., the sequence*

$$1 \to N \to G \to A \to 0$$

(N affine, hence linear; and A abelian variety, hence an abelian group under addition) is exact.

Definition 24.8. G is a *semi-abelian variety* if

$$0 \to (\mathbb{C}^*)^n \to G \to A \to 0$$

is an exact sequence. We remark also that G is an abelian group, and that $(\mathbb{C}^*)^n$ is an affine algebraic variety.

Definition 24.9. The collection of *constructible sets of subsets of Y* denote the smallest collection of subsets of Y containing open sets closed under finite unions and complements.

Theorem 24.10. *If X and Y are quasi-projective varieties and $f : X \to Y$ is a morphism, then $f(X)$ is constructible.*

24.1. **Group actions.**

Remark 29. If G is an algebraic group and X is a quasi-projective variety, then $f : G \times X \to X$ defined as $f(g, x) = g \cdot x$ is a group action if f is a a morphism and $e_G \cdot x = x$ for all x, and we have $(gh)x = g(hx)$ for all $g, h \in G, x \in X$.

24.2. **On Mordell-Lang conjecture.**

Theorem 24.11 (Vojta-Faltings-Hrushovski-Buium-Voloch, et al.). *Let G be a semi-abelian variety over $\mathbb{C}$, and let $\Gamma \leq G$ be a finitely-generated (abelian)subgroup and let $Y \subseteq G$ be Zariski-closed. Then*

$$Y \cap \Gamma = \bigcup_{i=1}^{r} (y_i + N_i),$$

and there exists $r \geq 0$ such that $N_1, \ldots, N_r \subseteq \Gamma$ and $y_i + N_i$'s are cosets of N_i.

Proof. Beyond the scope of this course. □

Corollary 24.12. *Let X be an irreducible, smooth projective curve defined over a number field F (finite-degree extension over $\mathbb{Q}$). Then if K is a finite-degree extension over F and the genus of X is at least 2, then $\#X(K)$ is finite, where $X(K) = \mathbb{P}^n(K) \cap X$. Note that there is an inclusion map $X \hookrightarrow \mathbb{P}^n_c (\supseteq \mathbb{P}^n(K) = \{[a_0 : \cdots a_n] : a_0, \ldots, a_n \in K\})$.*

Definition 24.13. Let X be an irreducible projective surge. Then a point $x \in X$ is *smooth* if $\mathcal{O}_{X,x}$ is a principal ideal domain (PID). If every $x \in X$ is smooth, then X is smooth.

In general, if X is irreducible with dimension d and $x \in X$ is smooth, then $\dim_k \mathcal{M}_{X,x}/\mathcal{M}_{X,x}^2 = d$, where $k = \mathcal{O}_{X,x}/\mathcal{M}_{X,x}$.

Definition 24.14. Let X be an irreducible smooth curve over $\mathbb{C}$. A *divisor* on X is a formal (finite) $\mathbb{Z}$-linear combination of points of X

$$\operatorname{Div}(X) = \left\{ \sum_{p \in X} n_p[p] : n_p \in \mathbb{Z}, n_p = 0 \text{ for all but finitely many } p \right\}.$$

If $f \in \mathbb{C}(X) = \mathcal{O}_{X,X}$ then we can talk about zeroes and poles of f. If $x \in X$ then we can view $\mathbb{C}(X) = \operatorname{Frac}(\mathcal{O}_{X,x})$ ($\mathcal{O}_{X,x}$ is a PID), so $\mathcal{M}_{X,x} = (\pi_x)$. Then we can write $f = \pi^s u$ with $s \in \mathbb{Z}, u \in \mathcal{O}_{X,x}^*$.

Definition 24.15. If $s > 0$, then we say f has a zero of order s at x. If $s < 0$, then we say f has a pole of order $-s$ at x, and from now on define $v_x(f) = s$.

25. November 14: pre-Dynamical Mordell-Lang

Let X be an irreducible smooth projective curve. Recall that we defined $\operatorname{Div}(X)$ to be the set of all (formal) $\mathbb{Z}$-linear combinations of $[P]$, where $P \in X$. If $f \in \mathbb{C}(X)^* = \operatorname{Frac}(\mathcal{O}_{X,x})$ (note that $\mathcal{O}_{X,x} \supseteq \mathcal{M}_{X,x} = (\pi)$, and $f = \pi^s u$ with $u \in \mathcal{O}_{X,x}^*$, define $v_x(f) = s$. Then

$$v_x(fg) = v_x(f) + v_x(g). \tag{12}$$

Define

$$\operatorname{div}(f) := \sum_{P \in X} v_p(f)[P],$$

which is a finite sum. By (12) we have $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$ and $\operatorname{div}(1/f) = -\operatorname{div}(f)$. In particular, $\operatorname{div} : \mathbb{C}(X)^* \to \operatorname{Div}(X)$.

Definition 25.1. $\operatorname{Cl}(X) := \operatorname{Div}(X)/\operatorname{div}(\mathbb{C}(X)^*)$.

Example 25.2. $\operatorname{Cl}(\mathbb{P}^1) \cong \mathbb{Z}$ via an isomorphism $\sum n_p[p] \mapsto \sum n_p$.

Example 25.3. For curves, we have a surjective map $\deg : \operatorname{Cl}(X) \to \mathbb{Z}$, and we define $\ker(\deg) =: \operatorname{Cl}^0(X)$. Then the following sequence is a short exact sequence:

$$0 \to \operatorname{Cl}^0(X) \to \operatorname{Cl}(X) \to \mathbb{Z} \to 0.$$

Proposition 25.4. $\operatorname{Cl}^0(X)$ *is an abelian variety of dimension g, where g is a genus of X.*

The inclusion map $X \hookrightarrow \mathbb{P}^n$ is defined over a number field K. If $Q \in X(L)$, where L is an infinite-degree extension over K. Then the map $X \to \operatorname{Cl}^0(X)$ defined by $P \mapsto \underbrace{[P] - [Q]}_{\deg 0}$ induces(?) an inclusion map $X(L) \hookrightarrow \operatorname{Cl}^0(X)(L)$.

Theorem 25.5 (Mordell-Weil-Lang-Néron theorem)**.** *Let A be an abelian variety (defined over K, some finitely-generated extension of $\mathbb{Q}$). Let L be a finitely-generated extension of k. Then $A(L)$ form a finitely-generated abelian group.*

Theorem 25.6 (Faltings' theorem)**.** *X is irreducible smooth projective curve of genus ≥ 2. Then $\#X(K) < \infty$, where K is a finitely-generated extension over $\mathbb{Q}$.*

Proof. There is an inclusion map from X to A, and pick a K-finitely-generated extension L so that X has an L-point. Then $X(L) \hookrightarrow A(L)$ is an inclusion map also, and $A(L)$ is an abelian group. If $i : X \to A$ then $Y := i(X) \subseteq A$, and let $\Gamma = A(L)$. Then by Mordell-Lang, we have

$$X(L) \subseteq \Gamma \cap Y = \bigcup_{i=1}^{r} (z_i + N_i),$$

so it is enough to show that all N_i's are finite.

Suppose that some $|N_i| = \infty$. Without loss of generality, let $|N_1| = \infty$. Then since $z_1 + N_1 \subseteq \Gamma \cap Y$ it follows that $Y \supseteq z_1 + N_1$. Then we have $X \cong Y \cong Y - z_1 \supseteq N_1$. If $Z := Y - z_1 \cong X$ then $Z \supseteq N_1$, hence $Z \supseteq \overline{N_1}$, and $\overline{N_1}$ is contained in A. If E is a connected component of identity of $\overline{N_1}$, then $Z \supseteq E$. Then we have an inclusion map from $\iota : E \hookrightarrow Z \cong X$, where E is an irreducible elliptic curve of genus 1 and X is an irreducible smooth curve of genus $g \geq 2$. This is a contradiction, by Riemann-Hurwitz (whatever that theorem is...). □

26. November 14: Dynamical Mordell-Lang

Suppose that X is an abelian variety over $\mathbb{C}$, and let

$$\Gamma = \langle g_1^{\pm 1}, g_2^{\pm 1}, \dots, g_r^{\pm 1} \rangle \subseteq X,$$

with $Y \subseteq X$ closed. Then by Mordell-Lang, we have $\Gamma \cap Y = \bigcup_{i=1}^{r} (z_i + N_i)$.

Remark 30. Each $g \in X$ gives a translation automorphism

$$\tau_g : X \to X$$

with $\tau_g(x) = g + x$. Note that $\tau_{(-g)} \circ \tau_g(x) = -g + g + x = x$. Notice that Γ corresponds to an abelian subgroup

$$H = \langle \tau_{g_1}^{\pm 1}, \dots, \tau_{g_r}^{\pm 1} \rangle \subseteq \mathrm{Aut}(X).$$

Definition 26.1. Given a quasi-projective variety X, with $H \leq \mathrm{Aut}(X)$ and $x \in X$, we define the *orbit of x under H*

$$H_x := \{\varphi(x) : \varphi \in H\} \subseteq X.$$

If we go back to the abelian variety case X with $x = O_x$ and $H = \langle \tau_{g_1}, \dots, \tau_{g_r} \rangle$, we have

$$\begin{aligned} H \cdot x &= \{\tau_{g_1}^{i_1} \circ \cdots \circ \tau_{g_r}^{i_r}(O) : i_1, \dots, i_r \in \mathbb{Z}\} \\ &= \{i_1 g_1 + \cdots + i_r g_r : i_1, \dots, i_r \in \mathbb{Z}\} = \Gamma. \end{aligned}$$

Therefore,

$$\bigcup_{i=1}^{r} \tau_{z_i} \tilde{N}_i x = \bigcup_{i=1}^{x} (z_i + N_i) = \Gamma \cap Y = (H \cdot x) \cap Y,$$

where $\tilde{N}_i = \langle \tau_h : h \in N_i \rangle \subseteq H$.

Conjecture (Dynamical Mordell-Lang: the first attempt)**.** *Let X be an irreducible complex quasi-projective variety, and let $H \subseteq \operatorname{Aut}(X)$ be a finitely-generated abelian subgroup with $x \in X$ and $Y \subseteq X$ closed. Then*

$$Hx \cap Y = \sum_{i=1}^{r} \tau_i N_i x$$

with $N_i \leq H$ and $\tau_i \in H$.

Unfortunately, this conjecture is false!

Example 26.2. Let $X = \mathbb{A}^2$ and $\sigma(x, y) = (x+1, y)$ and $\tau(x, y) = (x, 2y)$. Then $\mathbb{Z}^2 \cong \langle \sigma, \tau \rangle \subseteq \operatorname{Aut}(\mathbb{A}^2)$. If we let $x = (0, 1)$ and $H = \langle \sigma, \tau \rangle$ with $Y = \Delta = V(y = x) \subseteq \mathbb{A}^2$, then the orbit

$$Hx = \{(a, 2^b) : a, b \in \mathbb{Z}\},$$

so

$$Hx \cap Y = \{(2^b, 2^b) : b \geq 0\}.$$

In particular,

$$Hx \cap Y = \{\sigma^{2^b} \tau^b(x) : b \geq 0\},$$

which is an infinite set. If it contains some $\mu N x$ with $N \leq H \cong \mathbb{Z}^2$ and $N \supseteq \langle \sigma^c \tau^d \rangle$ and $\mu = \sigma^e \tau^f$. So if it contains $\mu N x$ with N infinite, then there exist c, d, e, f with $(c, d) \neq (0, 0)$ such that it contains

$$(\sigma^{e+cn} \tau^{f+dn})(x) = ((e + cn, 2^{f+dn}) : n \geq 0),$$

and these cannot all be on Y.

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1
E-mail address: hsyang@uwaterloo.ca