L9 (May 1, 2020) | We prove the last Proposition ①

(namely that: If $K \subset L$ are fields, $(a_n) \subset K$ satisfies for $\forall n \in \mathbb{N}$ the recurrence $a_{n+k} = \sum_{i=0}^{k-1} c_i a_{n+i}$ (1) for some constants $k \in \mathbb{N}_0$ and $c_i \in L$) then $\exists$ constants $k' \in \mathbb{N}_0$ and $c_i' \in K$ s.t. for every $n \in \mathbb{N}$ we have the recurrence $a_{n+k'} = \sum_{i=0}^{k'-1} c_i' a_{n+i}$ (2).

(Proof. (Let $k \in \mathbb{N}$, for $k=0$ the result holds trivially.)(*) We understand the $(k+1)$-tuples L^{k+1} as a vector space over L and use notation for lin. combinations as scalar products: if $\overline{u}, \overline{v} \in L^{k+1}$, then

$$\langle u, v \rangle := \sum_{i=0}^{k} u_i v_i. \qquad \overline{u} = (u_0, \dots, u_k),\ \overline{v} = (v_0, \dots, v_k)$$

(Let $B := \{\overline{a}_n := (a_n, a_{n+1}, \dots, a_{n+k-1}, a_{n+k}) \mid n \in \mathbb{N}\}$, and $\overline{c} := (c_0, c_1, \dots, c_{k-1}, -1_L) \in L^{k+1}$. Then for every $\overline{b} \in B$ we have that $\langle \overline{c}, \overline{b} \rangle \overset{(3)}{=} 0$, which just restates the recurrence (1). Let $d := \dim(B)$ be ~~[illegible]~~ the maximum # of lin. independent (over L) vectors in B. By the relation (3) we

---

(*) True, but not really needed.

have that $d < q+1$ (since $\bar{c} \neq \bar{0}$). Let $B_0 \subset B$ be d lin. indep. vectors in B, $|B_0| = \dim(B_0) = d$. As we know from the linear algebra, every $\bar{b} \in B$ is a lin. combination (over L) of the vectors in B_0. The system $\langle \bar{b}, \bar{x} \rangle = 0_K$, $\bar{b} \in B_0$ (4)

is a system of homogeneous lin. equations with more unknowns $\bar{x} = (x_0, x_1, \dots, x_q)$, $q+1$, than ~~the~~ equations, which are $|B_0| = d < q+1$. By ~~the~~ Lemma L, from the previous lecture and by the assumption that $B_0 \subset K^{q+1}$ (all $a_n \in K$) we have that there exists a solution of (4) in K, $\bar{d} = (d_0, d_1, \dots, d_q) \in K^{q+1}$, that is nontrivial, $\bar{d} \neq \bar{0}_K$. Thus $\forall \bar{b} \in B_0$: $\langle \bar{b}, \bar{d} \rangle = 0$. Because of ..., we in fact have that ... holds for every $\bar{b} \in B$. Let q', $0 \leq q' \leq q$, be the index of the last $\neq 0_K$ term in $\bar{d}$. ~~respectively.~~ ~~We set~~ As $\boxed{\dots}$ for every $\bar{b} \in B$ means that $\forall n \in \mathbb{N}$: $\sum_{i=0}^{r} d_i a_{n+i} = 0_K$) we have that for every $n \in \mathbb{N}$, $a_{n+r'} = \sum_{i=0}^{r'-1} c'_i a_{n+i}$ where

$$c'_i := -\frac{d_{i}}{d_{r'}} \in K \quad (i = 0, 1, \ldots, r'-1)$$

$$= -\frac{d_i}{d_{r'}} \in K.$$ But this is exactly the desired recurrence (2) with coeff-s in K. $\boxtimes$

Remark. the corrections "" in the end of the proof were because of my attempt to get $c'_0 \neq 0_K$, but this is not really required! There is another interesting result on coeff-s of recurrences for LRS, the so called Fatou lemma. I will tell it to you but will not prove it.

Lemma (P. Fatou, 1906)

If $(a_n) \subset \mathbb{Z}$, a sequence of integers, satisfies for $\forall n \in \mathbb{N}$ the recurrence $a_{n+r} = \sum_{i=0}^{r-1} c_i a_{n+i}$ for some constants $r \in \mathbb{N}_0$

④ and $c_i \in \mathbb{Q}$, then $\exists$ constants $k' \in \mathbb{N}_0$ and and $c_i' \in \mathbb{Z}$ s.t. for $\forall n \in \mathbb{N}$ we have the recurrence $a_{n+k'} = \sum_{i=0}^{k'-1} c_i' a_{n+i}$.

Remarks

~~The~~ A proof of the F. lemma can be found in the book *Enumer. Combinatorics, Vol. 1*, of R.P. Stanley, it is an exercise there. The F. lemma(*) show(s) that for integral LRS we can WLOG assume that also the recurrence coeff-s are integers. The proof is actually harder than the previous one, so it is really a "lemma". If you (today, May 8, 2020) ask Wikipedia about the F. lemma, it returns as an answer another Fatou's lemma, on (Lebesgue) integration. But we are smarter than Wikipedia. I also remark that both in the previous Prop. and the F. lemma we actually have that $k' \le k$.

There is another result on LRS, linear recurrence sequences, which

(*) and the previous proposition.

I like very much but cannot give a proof for it (as it is hard and relies on the p-adic numbers which I do not have time to introduce).

Recall that a <u>power sum $S(x)$</u> is:

$$S(x)=\sum_{i=1}^{r} p_i(x)\alpha_i^x \text{ where } r\in\mathbb{N}_0,\ p_i\in\mathbb{C}[x] \text{ are}$$

$\neq 0$ and the $\alpha_i\in\mathbb{C}$ too and are mutually distinct.

We call $S(x)$ <u>non-degenerate</u> if no ratio $\frac{\alpha_i}{\alpha_j}$, $i\neq j$, is a root of 1 (i.e. $\forall i,j,k\in\mathbb{N}$, $i\neq j$: $\left(\frac{\alpha_i}{\alpha_j}\right)^k\neq 1$). Else $S(x)$ is <u>degenerate</u>. For example, the p. sum $S(n)=2^n-(n+1)(-2)^n$ (in variable n now) is degenerate. For a p. sum $S(x)$ we denote by Z_S its <u>zero set</u>, as a function $S:\mathbb{N}\to\mathbb{C}$, i.e. $Z_S:=\{n\in\mathbb{N}\mid S(n)=0\}$.

Degenerate power sums may have infinite Z_S even when $S(x)\neq 0$: $S(x)=1^x+(-1)^x$ has $Z_S=\{1,3,5,\dots\}=$ all odd numbers. But for non-deg. p. sum this cannot happen:

⑥ $\boxed{\text{Theorem (the SML theorem)}}$ If $S(x)$ is a $\neq 0$ and non-degenerate power sum, then its zero set $Z_S = \{n \in \mathbb{N} \mid S(n) = 0\}$ is finite!

Remarks. The theorem holds in fact more generally for p. sums over any field K with characteristic 0 (instead of just $\mathbb{C}$) but, remarkably, not when $char(K) = p$. **Exercise** Let $K = \mathbb{Z}_p(x)$ be, for a prime p, the field of rational functions (ratios of polynomials) with coeff-s in $\mathbb{Z}_p$. Then for the power sum $S = S(y)$ (over K) given by

$$\boxed{S = S(y) = (x+1)^y - x^y - 1^y}$$

(note that S has now variable y, not x) we have that

$$Z_S = \{p^n \mid n \in \mathbb{N}_0\} = \{1, p, p^2, p^3, \ldots\}.$$

The "SML" refers to ~~the~~ T. Skolem, K. Mahler and Ch. Lech who proved the theorem for ~~respectively~~ $K = \mathbb{Q}, \overline{\mathbb{Q}}$ (the algebraic numbers) and any K with $char(K) = 0$, respectively.