manuscripta math. 95, 349 – 362 (1998)

manuscripta
mathematica

Differential equations with 2-term recursion

Sabine Hoeppner[*]

Mittwegstr. 8, D-45127 Essen, Germany.
e-mail: sabine@exp-math.uni-essen.de

Received: 20 June 1997/ Revised Version: 2 October 1997

Abstract. In this paper we consider linear differential equations with a recursion consisting of two terms. We consider these equations in positive characteristics and in characteristic zero. We will find a new proof for the Grothendieck conjecture for these equations.

1. Introduction

We will investigate linear differential equations

$$y^{(n)} + f_{n-1}y^{(n-1)} + \cdots + f_1 y' + f_0 y = 0 \tag{1}$$

with $f_0, \ldots, f_n \in \mathbf{K}(x)$ where $\mathbf{K} = \mathbf{C}$ or $\mathbf{K} = \mathbf{F}_p$. As usual $y' = \frac{1}{dx}y$ and $y^{(j)}$ is the jth derivative of y.

In the positive characteristic case the derivation is defined formally by $x' = 1$. We call the elements with derivative zero the constants, they are a field. Obviously the field of constants of $\mathbf{C}(x)$ is $\mathbf{C}$, and the field of constants of $\mathbf{F}_p(x)$ is $\mathbf{F}_p(x^p)$. If we talk about linearly independence we mean over the field of constants. By rational solutions we mean solutions in $\mathbf{K}(x)$, by algebraic solutions we mean elements of an algebraic extension of $\mathbf{K}(x)$.

Such an equation (1) in characteristic zero has a finite monodromy group iff it has a finite differential Galois group iff it has a fundamental system of algebraic solutions.

In characteristic p the p-th derivative of all elements of $\mathbf{F}_p(x)$ is zero. So for $p \leq n$ the equation (1) has the same solutions in $\mathbf{F}_p(x)$ as

$$f_{p-1}y^{(p-1)} + \cdots + f_1 y' + f_0 y = 0, \tag{2}$$

[*] Supported by a grant from the DFG.

this means at most $p-1$ linearly independent solutions (if not $f_{p-1} = \cdots = f_0 = 0$). So only if $p > n$ the equation (1) can have a fundamental system of rational solutions modulo p. We will restrict ourselves to this case. If the considered equation has a fundamental system of rational solutions modulo a prime p we will call this prime good, otherwise we call it bad.

In positive characteristic we know that from the existence of k linearly independent algebraic solutions follows the existence of k linearly independent polynomial solutions.

The generalized hypergeometric equation

$$0 = D(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n)y \tag{3}$$

with

$$D(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n) = \\ (\theta + \beta_1 - 1) \ldots (\theta + \beta_n - 1) - x(\theta + \alpha_1) \ldots (\theta + \alpha_n)$$

where $\theta = x\frac{d}{dx}$ and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbf{C}$, was considered by Beukers and Heckman in [BH]. There it has been shown for which parameters the equation has a finite monodromy group (or equivalently a fundamental system of algebraic solutions). For the hypergeometric equation which is (3) with $n = 2$ the same has already been done by Schwarz [Sch]. For the generalized hypergeometric equations the so-called Grothendieck conjecture has been proved by [BH]. The conjecture says:

A linear homogeneous differential equation has a fundamental system of algebraic solutions in characteristic zero if and only if the reduced equation modulo a prime p has a fundamental system of rational solutions for almost all primes.

It is easy to see that a fundamental system of algebraic solutions can be reduced modulo p to a fundamental system of algebraic solutions in characteristic p for almost all primes p. Thus one direction of the conjecture is trivial.

After proving some helpful facts (in section 2) we will first consider the equation (3) (in section 3). We will see for which primes there does not exist a fundamental system of rational solutions although there is a fundamental system of algebraic solutions in characteristic zero. For the hypergeometric equations of order two in standard form (see [BD]) with rational coefficients these are exactly the prime divisors of the order of the differential Galois group and also the prime divisors of the denominators in the equation. This result cannot be extended to the generalized hypergeometric equations.

In the next part (section 4) we will consider the general equation with 2-term recursion. We will see that these equations come from the generalized hypergeometric equation by transformations. With this fact we find a new proof of the Grothendieck conjecture for the equations with 2-term recursion. Another more complicated and also more general proof can be found in the book of Katz [K], where he proves the Grothendieck conjecture for rigid equations.

2. Preliminaries

We consider a linear differential equation $f_n y^{(n)} + f_{n-1} y^{(n-1)} + \cdots + f_1 y' + f_0 y = 0$, $f_k \in \mathbf{K}[x]$, $f_n \neq 0$, $gcd(f_0, \ldots, f_n) = 1$. Computing a formal solution means that we put $y = \sum_{k=0}^{\infty} y_k x^k$ with $y_k \in \mathbf{K}$ into the equation. Then we get a recurrence relation for the calculation of the y_k. We are looking for differential equations where every recursion equation contains at most two different y_k. We call the equation an *equation with 2-term recursion with step length* m if the recursion has the following form:

$$\begin{array}{rcrl} & & b_0 y_0 & = 0 \\ & & \vdots & \\ & & b_{m-1} y_{m-1} & = 0 \\ a_m y_0 & + & b_m y_m & = 0 \\ a_{m+1} y_1 & + & b_{m+1} y_{m+1} & = 0 \\ & & \vdots & \\ a_M y_{M-m} & + & b_M y_M & = 0 \\ & & \vdots & \end{array} \tag{4}$$

where $a_m, a_{m+1}, \ldots, b_0, b_1, \ldots \in \mathbf{K}$.

Theorem 1. *The differential equations with 2-term recursion have the form*

$$\begin{aligned} (\gamma_n x^{n+m} - \delta_n x^n) y^{(n)} + (\gamma_{n-1} x^{n+m-1} + \delta_{n-1} x^{n-1}) y^{(n-1)} + \\ \cdots + (\gamma_1 x^{m+1} + \delta_1 x^1) y' + (\gamma_0 x^m + \delta_0) y = 0 \end{aligned} \tag{5}$$

with $\gamma_0, \ldots, \gamma_n, \delta_0, \ldots, \delta_n \in \mathbf{K}$, *or, written with the operator* θ

$$\gamma(\theta + \beta_{n_2}) \ldots (\theta + \beta_1) y - \delta x^m (\theta + \alpha_{n_1}) \ldots (\theta + \alpha_1) y = 0 \tag{6}$$

where $n_1, n_2 \in \mathbf{N}$, $\alpha_1, \ldots, \alpha_{n_1}, \beta_1, \ldots, \beta_{n_2}, \gamma, \delta \in \mathbf{K}$.

Proof. Easy. □

Remark. We assume $(\gamma_0, \ldots, \gamma_n) \neq 0$, $(\delta_0, \ldots, \delta_n) \neq 0$, $\gamma \neq 0$, $\delta \neq 0$, otherwise the recursion is trivial. We can assume $\delta = 1$. The equations (5) and (6) are equivalent, where $n_1 = \max\{\nu | \gamma_\nu \neq 0\}$ and $n_2 = \max\{\nu | \delta_\nu \neq 0\}$. So it is enough to consider in the following the equation (6). By a transformation $\gamma^{1/m} x \to x$ we can remove the γ in (6), so we assume $\gamma = 1$.

Lemma 2. *Let p be a prime number not dividing m. Assume that $Dy = 0$ is a differential equation with 2-term recursion with step length m as in (4), where $a_i \equiv 0 \mod p$ for $i \in \{i_1, \dots, i_k\}$ with $0 < i_1 \leq i_2 \leq \dots \leq i_k \leq mp$, and $b_j \equiv 0 \mod p$ for $j \in \{j_1, \dots, j_k\}$ with $0 \leq j_1 \leq j_2 \leq \dots \leq j_k < mp$, and $i_\mu, j_\nu \equiv 0 \mod m$. Assume further that $a_i \not\equiv 0 \mod p$ for $i \equiv 0 \mod m$ and $i \notin \{i_1, \dots, i_k\}$, and $b_j \not\equiv 0 \mod p$ for $j \equiv 0 \mod m$ and $j \notin \{j_1, \dots, j_k\}$. Then the differential equation has k linearly independent polynomial solutions modulo p iff $j_1 < i_1 \leq j_2 < \dots < i_{k-1} \leq j_k < i_k$ or $i_1 \leq j_1 < i_2 \leq \dots \leq j_{k-1} < i_k \leq j_k$.*

Proof. In the proof a solution means always a polynomial solution modulo p. We see that we have in fact m independent parts of the recursion, namely for $y_0, y_m, y_{2m}, \dots$ for $y_1, y_{m+1}, y_{2m+1}, \dots$ etc. If we have an arbitrary solution of $Dy = 0$ this is the sum of solutions each coming from *one* part of the recursion. If we have a solution y coming from an arbitrary part of the recursion $y = y_i x^i + y_{i+m} x^{i+m} + \dots + y_{i+lm} x^{i+lm}$ we can multiply this solution by x^{rp} for a suitable r and find a solution of the form $y = y_0 + y_m x^m + \dots + y_{\lambda m} x^{\lambda m}$. So from the existence of k linearly independent solutions follows the existence of k linearly independent solutions coming from the recursion for $y_0, y_m, \dots$.

Now we assume that

$$j_1 < i_1 \leq j_2 < \dots < i_{k-1} \leq j_k < i_k. \tag{7}$$

If $b_0 \neq 0$ we get $y_0 = 0$ and from the first equations we find $0 = y_m = y_{2m} = \dots = y_{j_1 - m}$ until we come to $a_{j_1} y_{j_1 - m} + b_{j_1} y_{j_1} = 0$. Because $b_{j_1} = 0$ we can chose y_{j_1} free. (If $b_0 = 0$ we can chose $y_0 = y_{j_1}$ free.) With the next equations we can compute $y_{j_1+m}, y_{j_1+2m}, \dots, y_{i_1 - m}$ uniquely and unequal zero. Then, using $a_{i_1} y_{i_1 - m} + b_{i_1} y_{i_1} = 0$ we see that if $b_{i_1} \neq 0$ (i.e. $i_1 < j_2$) we get $y_{i_1} = 0$ and from this $0 = y_{i_1+m} = y_{i_1+2m} = \dots = y_{j_2 - m}$. Now with $a_{j_2} y_{j_2 - m} + b_{j_2} y_{j_2} = 0$ we see that we can chose y_{j_2} free. If $b_{i_1} = 0$ we get the same immediatly. Continueing we see that for every $b_j = 0$ we can chose y_j free onder the condition that $a_j = 0$ or $y_{j-m} = 0$. But one of these holds because of condition (7). This means that we find k solutions of degree $i_1 - m, i_2 - m, \dots, i_k - m$ where $0 \leq i_1 - m < i_2 - m < \dots < i_k - m < mp$. If p is not a divisor of m these solutions are linearly independent.

We can continue further computing solutions. The parameters a_j, b_j in the recursion depend only on $j \mod p$, in particular $b_{j_1 + pm} = b_{j_1} = 0$. But the solution that we find by chosing $y_{j_1 + pm}$ free is equal the first solution that we found multipied by $x^{mp} y_{j_1 + pm} / y_{j_1}$. Thus the differential equation has exactly k linearly independent solutions.

If $i_1 \leq j_1 < i_2 \leq \dots \leq j_{k-1} < i_k \leq j_k$ we see as above that $0 = y_0 = y_m = y_{2m} = \dots = y_{j_1 - m}$, we can chose y_{j_1} free and find

k solutions of degree $i_2 - m, i_3 - m, \ldots, i_k - m, i_1 + (p-1)m$ where $0 < i_2 - m < i_3 - m < \ldots < i_k - m < i_1 + (p-1)m < i_2 + (m-1)p$. If p does not divide m these solutions are linearly independent.

We have seen that we find exactly one solution for every j with $b_j = 0$ iff $a_j = 0$ or $y_{j-m} = 0$. This means that the interlacing condition for sets with k elements is necessary for k linearly independent solutions. □

Remarks. 1. Instead of the first part of the recursion it is also possible to use every other part. Then one finds a similar condition.

2. If $p = m$ one finds that in one part of the recursion $a_i = a_{i+m} = \cdots$, $b_i = b_{i+m} = \cdots$, because the parameters a_M, b_M depend from $M \mod p$. It follows that the ith part of the recursion gives a nonzero solution iff $a_i = 0$ and $b_i = 0$. So we find k linearly independent solutions iff $a_i \equiv 0 \mod p$ for $i \in \{i_1, \ldots, i_k\}$ and $b_j \equiv 0 \mod p$ for $j \in \{i_1, \ldots, i_k\}$. This means for an order k equation that we can divide it by $x^m + 1$, so we get an equation with two singular points $0, \infty$.
3. If $p|m$ and $p < m$ the variables $y_0, \ldots, y_{p-1}$ occur only in the first equations of the recursion. In this case it is sufficient (and also necessary) to have $b_{i_1} = \cdots = b_{i_k} = 0$ for $i_1 < \cdots < i_k < p$ for k independent solutions. This is independent from $\gamma_0, \ldots, \gamma_n$ in (5).

3. The nth order hypergeometric equation

We consider the equation

$$\begin{aligned} Dy = D(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n)y = \\ (\theta + \beta_1 - 1)\ldots(\theta + \beta_n - 1)y - x(\theta + \alpha_1)\ldots(\theta + \alpha_n)y = 0, \end{aligned} \tag{8}$$

where $\theta = x\frac{d}{dx}$ and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbf{C}$. We can restrict ourselves to rational parameters because only in this case the equation can have finite monodromy group and only in this case the reduced equation can have a fundamental system of polynomial solutions for almost all primes. We know from [Sch] for $n = 2$ and from [BH] for the general case for which $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbf{Q}$ the monodromy group of the equation is finite, and that then the equation has a full set of algebraic solution. We recall some facts from [BH]:

Definition 3. *Let $a_j = \exp 2\pi\sqrt{-1}\alpha_j$ and $b_j = \exp 2\pi\sqrt{-1}\beta_j$ $(j = 1, \ldots, n)$ be two sets of numbers in the unit circle. Suppose $0 \le \alpha_1 \le \alpha_2 \le \ldots \le \alpha_n < 1$, $0 \le \beta_1 \le \beta_2 \le \ldots \le \beta_n < 1$. We say that the sets $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ interlace in the unit circle if and only if either $\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \ldots < \alpha_n < \beta_n$ or $\beta_1 < \alpha_1 < \beta_2 < \alpha_2 < \ldots < \beta_n < \alpha_n$.*

Theorem 4. ([BH], prop. 3.2. and th. 4.8.) *Suppose the parameters $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are as in definition 3, and say*

$$\mathbf{Q}(a_1, \dots, a_n, b_1, \dots, b_n) = \mathbf{Q}(\exp(2\pi\sqrt{-1}/h))$$

for some $h \in \mathbf{N}$. Then the monodromy group of $D(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)y = 0$ is finite iff for each $k \in \mathbf{N}$ with $gcd(k, h) = 1$ the sets $\{a_1^k, \dots, a_n^k\}$ and $\{b_1^k, \dots, b_n^k\}$ interlace on the unit circle.

We want to consider these equations modulo a prime p.

3.1. Bad primes for the generalized hypergeometric equation

Inserting $y = \sum_{l=0}^{\infty} y_l x^l$ into (8) we get a 2-term recursion for the y_l's. It is $(\theta + \beta - 1)y = \sum_{l=0}^{\infty}(l + \beta - 1)y_l x^l$ and so $(\theta + \beta_1 - 1)\dots(\theta + \beta_n - 1)y = \sum_{l=0}^{\infty}\prod_{j=1}^{n}(l + \beta_j - 1)y_l x^l$. We see that in the recursion (4) $a_l = -\prod_{j=1}^{n}(l + \alpha_j - 1)$ and $b_l = \prod_{j=1}^{n}(l + \beta_j - 1)$. Now $a_l \equiv 0 \mod p$ iff $l \equiv -\alpha_j + 1 \mod p$ for a j, and $b_l \equiv 0 \mod p$ iff $l \equiv -\beta_j + 1 \mod p$ for a j. It follows

Corollary 5. *We set $\overline{\alpha_i} \equiv \alpha_i \mod p$, $\overline{\alpha_i} \in \{0, \dots, p-1\}$ for $i = 1, \dots, n$ and $\overline{\beta_j} \equiv \beta_j \mod p$, $\overline{\beta_j} \in \{0, \dots, p-1\}$ for $j = 1, \dots, n$. The hypergeometric equation has n linearly independent solutions modulo a prime p iff we have $\overline{\alpha_1} < \overline{\beta_1} \le \overline{\alpha_2} < \dots \le \overline{\alpha_n} < \overline{\beta_n}$ or $\overline{\beta_1} \le \overline{\alpha_1} < \overline{\beta_2} \le \dots < \overline{\beta_n} \le \overline{\alpha_n}$, perhaps after renumbering of the α's and β's.*

Proof. It follows immediately using lemma 2 with $m = 1$. □

Theorem 6. *Let $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ be the parameters of the equation (8), assume that they are written with common denominator ν. Assume further that the equation has a fundamental system of algebraic solutions in characteristic zero. Then for a prime p greater than the maximum of the differences of the numerators of $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ the reduced equation has a fundamental system of solutions in $\mathbf{F}_p(x)$.*

Proof. We first assume that $\alpha_i, \beta_i \ge 0$ for all i and write $\alpha_i = \frac{A_i}{\nu}$ and $\beta_i = \frac{B_i}{\nu}$. Now we consider the integers $\tilde{p}$ with $0 < \tilde{p} < \nu$, $gcd(\tilde{p}, \nu) = 1$ and the primes p with $p \equiv \tilde{p} \mod \nu$. There is a $c_{i,\tilde{p}} \in \mathbf{N}$, $0 \le c_{i,\tilde{p}} < \nu$ such that $\nu | (c_{i,\tilde{p}}\tilde{p} + A_i)$, then it follows $\overline{\alpha_i} = (c_{i,\tilde{p}}p + A_i)/\nu$, if $p > A_i$ for every i, $\overline{\alpha_i}$ defined as in corollary 5. Similar we find a $d_{i,\tilde{p}}$ for β_i for every i. Now we know that the equation modulo p has a fundamental system of solutions in $\mathbf{F}_p(x)$ for almost every prime. So we can choose a prime $\Pi \equiv \tilde{p} \mod \nu$ with this property, $\Pi > max\{A_1, \dots, A_n, B_1, \dots, B_n\}$. Because of corollary 5 for the set $\{\overline{\alpha_1}, \dots, \overline{\alpha_n}, \overline{\beta_1}, \dots, \overline{\beta_n}\}$ holds $\overline{\alpha_1} < \overline{\beta_1} \le \overline{\alpha_2} <$

$\overline{\beta_2} \leq \cdots \leq \overline{\alpha_n} < \overline{\beta_n}$ or $\overline{\beta_1} \leq \overline{\alpha_1} < \overline{\beta_2} \leq \cdots < \overline{\beta_n} \leq \overline{\alpha_n}$ if we write the $\overline{\alpha_i}$'s and the $\overline{\beta_i}$'s modulo Π as elements of $\{0, \ldots, \Pi - 1\}$ (perhaps after renumbering). Then the same follows for the corresponding c_i's and d_i's. Now we consider any prime with $p \equiv \tilde{p} \mod \nu$ with p greater than the maximum of the numerators. Then the $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ modulo p as elements of $\{0, \ldots, p-1\}$ are in the same order as the α_i's and the β_i's modulo Π as elements of $\{0, \ldots, \Pi - 1\}$, because the A_i's, B_i's are to small to disturb the order.

Now we consider the general case. If we add a rational number to all α's and β's we get a parallel shift of all these numbers. Such a shift does not change the interlacing condition from corollary 5 of the α's and β's. So instead of $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ we consider $\alpha_1 - c, \ldots, \alpha_n - c, \beta_c, \ldots, \beta_n - c$, where $c = min\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n\}$. Now the theorem follows from the first part of the proof, using corollary 5. □

So we see that the set of candidates for bad primes is finite for every hypergeometric equation. With the following theorem we see that these primes have a very special property, if the parameters $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ are in the interval $(0, 1]$.

Theorem 7. *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in (0, 1]$ again be the parameters of equation (8), written with common denominator ν. If the interlacing condition (definition 3) is satisfied and the equation does not have n linearly independent polynomial solutions modulo a prime p then there exist i, j such that $\alpha_i \equiv \beta_j \mod p$.*

Proof. Choose f such that $p^f - 1$ is divisible by ν. Any fraction ξ with denominator ν and in $(0, 1]$ can be written in the form

$$\xi = \frac{a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}}{p^f - 1}$$

where the a_i are integers with $0 \leq a_i \leq p - 1$. Note that $\xi \equiv -a_0 \mod p$. Consider the map $T : (0, 1] \to (0, 1]$ given by multiplication with p^f and reduction modulo 1. We find,

$$T(\xi) = \frac{a_1 + \cdots + a_{f-1} p^{f-2} + a_0 p^{f-1}}{p^f - 1}.$$

We abbreviate this by

$$T(\xi) = a_0(\xi) \frac{p^{f-1}}{p^f - 1} + \delta(\xi)$$

and note that $0 \leq \delta(\xi) < 1/p$. Let η be another fraction with denominator ν. Then $T(\xi) > T(\eta)$ implies that

$$(a_0(\xi) - a_0(\eta)) \frac{p^{f-1}}{p^f - 1} + \delta(\xi) - \delta(\eta) \geq \frac{1}{\nu}.$$

Hence

$$a_0(\xi) - a_0(\eta) > (p - p^{1-f})(\frac{1}{\nu} - \frac{1}{p}) > -1.$$

So we observe that $T(\xi) > T(\eta)$ implies $a_0(\xi) \geq a_0(\eta)$ and when $p > \nu$ we even have $a_0(\xi) > a_0(\eta)$.

Now by the validity of the interlacing condition we can index the α_i, β_j such that $T(\alpha_n) < T(\beta_n) < \cdots < T(\alpha_1) < T(\beta_1)$ or $T(\beta_n) < T(\alpha_n) < \cdots < T(\beta_1) < T(\alpha_1)$. Let us look at the first case.

The above considerations imply that when $p > \nu$ the mod p ordering of the α's and β's looks like

$$-\alpha_n < -\beta_n < \cdots < -\alpha_1 < -\beta_1.$$

Hence the equation has n linearly independent solutions modulo p. When $p < \nu$, the best we can do is

$$-\alpha_n \leq -\beta_n \leq \cdots \leq -\alpha_1 \leq -\beta_1.$$

So, when the equation has less than n linearly independent solutions this is because $\alpha_i \equiv \beta_i \mod p$ for some i. □

Remark: From the proof we get also that the bad primes are smaller than ν. This bound is a little bit greater than the result from theorem 6 but this proof does not use the general fact that there are only finitly many bad primes. Using the result of theorem 7, we can find the same bound as in theorem 6, but only for parameters in $(0, 1]$. Because $(p - p^{1-f})(\frac{1}{\nu} - \frac{1}{p}) \to \infty$ for $p \to \infty$ we can also find a bound for bad primes for the general case $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_n \in \mathbf{Q}$ instead of $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_n \in (0, 1]$. But the statement of theorem 7 does not hold in general. To construct a counterexample, one can use theorem 4. From this follows that the finiteness of the monodromy group depends from the $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_n$ modulo 1. So adding integers to some of these numbers, we can get any order of the numbers modulo *one* prime p and also the mentioned counterexample.

Now we want to consider an example from No. 1 of table 8.3 in [BH]. For $n \geq 4$ we have the following parameters of equation 8:

$$\{\alpha_1, \ldots, \alpha_n\} = \{\frac{1}{n+1}, \frac{2}{n+1}, \cdots, \frac{n-1}{n+1}, \frac{n}{n+1}\}$$

and

$$\{\beta_1, \ldots, \beta_n\} = \{0, \frac{1}{j}, \frac{2}{j}, \cdots, \frac{j-1}{j}, \frac{1}{n+1-j}, \frac{2}{n+1-j}, \cdots, \frac{n-j}{n+1-j}\}$$

with $\gcd(j, n+1) = 1$ and $j < n+1$. For $p \leq n$ it is not meaningful to consider the differential equation with these parameters because the order of the equation is n, and for $p = n+1$ it is of course also not meaningful. But we can show:

Lemma 8. *For $p > B = max\{nj - (n+1), n(n+1-j) - (n+1)\}$ the equation (8) with*

$$(\alpha_1, \ldots, \alpha_n) = (\frac{1}{n+1}, \frac{2}{n+1}, \cdots, \frac{n-1}{n+1}, \frac{n}{n+1})$$

and

$$(\beta_1, \ldots, \beta_n) = (0, \frac{1}{j}, \frac{2}{j}, \cdots, \frac{j-1}{j}, \frac{1}{n+1-j}, \frac{2}{n+1-j}, \cdots, \frac{n-j}{n+1-j})$$

with $\gcd(j, n+1) = 1$ *and* $j < n+1$ *modulo p has n linearly independent solutions over $\mathbf{F}_p(x^p)$.*

Furthermore all primes for which one of the differences $\alpha_i - \beta_k \equiv 0 \mod p$ are bad.

Proof. We use theorem 7. In our example we have $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in [0,1)$ instead of $\in (0,1]$, but reading the proof of theorem 7 we can change to the other intervall. So we have to look for i, k such that the difference $\alpha_i - \beta_k \equiv 0 \mod p$. Alternatively we can consider the equivalences $ij - k(n+1) \equiv 0 \mod p$ for $1 \leq i \leq n$ and $1 \leq k \leq j-1$ and the equivalences $i(n+1-j) - l(n+1) \equiv 0 \mod p$ for $1 \leq i \leq n$ and $1 \leq l \leq (n-j)$. Of course $ij \neq k(n+1)$ and $i(n+1-j) \neq l(n+1)$ for all i, k, l, thus every prime p greater than the maximal difference is good. This maximal difference is exactly B.

For the second statement we consider $\frac{i}{n+1}$. There is a $\iota \in \{1, \ldots, n\}$ such that $(n+1) | (\iota p + i)$, then $\overline{\frac{i}{n+1}} = \frac{\iota p + i}{n+1}$. Then $\overline{\frac{n+1-i}{n+1}} = p + 1 - \overline{\frac{i}{n+1}}$. Considering the β_k we can find something similar. Thus if we order the $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ as $\overline{\beta_1} \leq \overline{\alpha_1} \leq \overline{\beta_2} \leq \ldots \leq \overline{\beta_n} \leq \overline{\alpha_n}$ (after renumbering) we find that from equality $\overline{\beta_\rho} = \overline{\alpha_\rho}$ for a $\rho \in \{1, \ldots, n\}$ (which does not matter following corollary 5) follows equality $\overline{\alpha_\sigma} = \overline{\beta_{\sigma+1}}$ for a $\sigma \in \{1, \ldots, n-1\}$ which makes the prime bad following corollary 5. $\square$

Remark. The No.1 from the table in [BH] does not mean only one equation but the set of all equations with parameters $k\alpha_1 + i_1, \ldots, k\alpha_n + i_n; k\beta_1 + j_1, \ldots, k\beta_n + j_n$ or $k\beta_1 + j_1, \ldots, k\beta_n + j_n; k\alpha_1 + i_1, \ldots, k\alpha_n + i_n$ where

$i_1, \dots, i_n, j_1, \dots, j_n$ are integers, $gcd(k, \nu) = 1$ and ν is the common denominator of the parameters,

$$\{\alpha_1, \dots, \alpha_n\} = \{\frac{1}{n+1}, \frac{2}{n+1}, \dots, \frac{n-1}{n+1}, \frac{n}{n+1}\}$$

and

$$\{\beta_1, \dots, \beta_n\} = \{0, \frac{1}{j}, \frac{2}{j}, \dots, \frac{j-1}{j}, \frac{1}{n+1-j}, \frac{2}{n+1-j}, \dots, \frac{n-j}{n+1-j}\}$$

with $\gcd(j, n+1) = 1$ and $j < n+1$, $n \geq 4$. Considering all these equations we see that if the parameters are in $[0, 1)$ then they are the same as in lemma 8. So for this kind of parameters we get the same bound for the primes to be good as in the lemma. For the general equation with parameters in $\mathbf{Q}$ we have of course more bad primes.

3.2. The bad primes for the standard equations of order two

As an illustration we will consider now the standard hypergeometric equations of order 2

$$L_{\lambda,\mu,\nu}(y) = y'' + (\frac{\alpha}{x^2} + \frac{\beta}{(x-1)^2} + \frac{\zeta}{x(x-1)})y = 0 \tag{9}$$

where $4\alpha = 1 - \lambda^2, 4\beta = 1 - \mu^2, 4\zeta = \lambda^2 + \mu^2 - \nu^2 - 1$ and $(\lambda, \mu, \nu) = (\frac{1}{2}, \frac{1}{3}, \frac{1}{3})$ or $(\lambda, \mu, \nu) = (\frac{1}{2}, \frac{1}{3}, \frac{1}{4})$ or $(\lambda, \mu, \nu) = (\frac{1}{2}, \frac{1}{3}, \frac{1}{5})$ or $(\lambda, \mu, \nu) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{n})$. These are the standard hypergeometric equations with the tetrahedral group of order 24, the octahedral group of order 48, the icosahedral group of order 120 and the dihedral group of order $2n$ resp. as the differential Galois-group (see [BD]).

We will see that the bad primes for these equations are exactly the divisors of the group order.

We start with the first of the equations for $p > 3$:

$$0 = y'' + \frac{32x^2 - 27x + 27}{144x^2(x-1)^2}y. \tag{10}$$

We want to show that the equation has 2 linearly independent solutions in $\mathbf{F}_p(x)$ for all p. For this we transform the equation in the following way. Let γ be a solution of (10) and $\xi' = c\xi$. Then $\gamma\xi$ solves

$$y'' - 2cy' + by = 0 \tag{11}$$

with

$$b = \frac{32x^2 - 27x + 27}{144x^2(x-1)^2} - c' + c^2.$$

We choose $c = -\frac{Ax+B}{2x(x-1)}$ with $B = -2$ and $A = \frac{10}{3}$, then we get the following equation:

$$0 = y'' + \frac{\frac{10}{3}x - 2}{x(x-1)}y' + \frac{64x - 9}{48x^2(x-1)}y \tag{12}$$

and from this we get

$$\begin{aligned} 0 &= 48x^2(x-1)y'' + (160x^2 - 96x)y' + (64x - 9)y \\ &= 48((\theta + \frac{1}{4})(\theta + \frac{3}{4})y - x(\theta+1)(\theta + \frac{4}{3})y). \end{aligned} \tag{13}$$

For $p > 9$ we see that the equation has 2 linearly independent solutions over $\mathbf{F}_p(x^p)$ because of theorem 6. For smaller primes we have to consider the order of $1, \frac{4}{3}, \frac{5}{4}, \frac{7}{4}$ modulo p.. By computation we see that the order is as in corollary 5, so also for $p = 5$ and 7 the equation has 2 linearly independent solutions.

Now we consider the second equation for $p > 3$:

$$y'' + \frac{135x^2 - 115x + 108}{576x^2(x-1)^2}y = 0. \tag{14}$$

We transform it to

$$(576x^3 - 576x^2)y'' + (1872x^2 - 1104x)y' + 5(144x - 17)y = 0. \tag{15}$$

This is

$$576((\theta + \frac{5}{24})(\theta + \frac{17}{24})y - x(\theta + 1)(\theta + \frac{5}{4})y) = 0. \tag{16}$$

Now for primes greater than 17 there are 2 linearly independent solutions because of theorem 6, for smaller primes p we compute $\frac{5}{24}, \frac{17}{24}, 0, \frac{1}{4}$ modulo p. Then we see the same with corollary 5.

Now we consider the third equation for $p > 5$:

$$0 = y'' + \frac{864x^2 - 739x + 675}{3600x^2(x-1)^2}y. \tag{17}$$

We can transform the equation and get

$$0 = (3600x^3 - 3600x^2)y'' + (11520x^2 - 6720x)y' + (4320x - 451)y \tag{18}$$

and this is

$$3600((\theta+\frac{11}{60})(\theta+\frac{41}{60})y - x(\theta+1)(\theta+\frac{6}{5})y) = 0. \tag{19}$$

Again, for primes greater than 41 there are 2 linearly independent solutions because of theorem 6, for smaller primes p we compute $\frac{11}{60}, \frac{41}{60}, 0, \frac{1}{5}$ modulo p. Then we see the same with corollary 5.

Finally we consider the equation (9) with $(\lambda, \mu, \nu) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{n})$. We get

$$y'' + \frac{4x^2n^2 - 4n^2x + 3n^2 - 4x^2 + 4x}{16x^2(x-1)^2n^2} y = 0.$$

We transform it to:

$$\begin{aligned} 4n^2x^2(x-1)y'' + 2nx(6nx + 2x - 3n - 2)y' \\ + (4n^2x + 4nx - 1 - n)y = 0. \end{aligned}$$

This is

$$-4n^2((\theta+\frac{1}{2n})(\theta+\frac{n+1}{2n}) - x(\theta+1)(\theta+\frac{2n+2}{2n})) = 0.$$

Now we have to compare $\beta_1 - 1 = \frac{1}{2n}, \beta_2 - 1 = \frac{n+1}{2n}$ and $\alpha_1 - 1 = 0, \alpha_2 - 1 = \frac{2}{2n}$ modulo a prime p. There is a unique $l_1 \in \{1, \dots, 2n-1\}$ such that l_1p+1 is divisible by $2n$. Similar there are $l_2, l \in \{1, \dots, 2n-1\}$ such that $l_2p + n + 1$ and $lp + 2$ are divisible by $2n$. Assume that we have found l_1.

Case 1. Let $l_1 < n$. If $p \neq n+1$ then we see that $l = 2l_1$ and $l_2 = l_1 + n$. We get that $\alpha_1 - 1 < \beta_1 - 1 < \alpha_2 - 1 < \beta_2 - 1$ if we consider the numbers as elements of $\{0, \dots, p-1\}$. If $p = n+1$ we get $\beta_2 - 1 = \alpha_1 - 1 < \beta_1 - 1 < \alpha_2 - 1$ and the differential equation has 2 linearly independent solutions modulo p.

Case 2. Obviously $l_1 \neq n$, so we consider now $l_1 > n$. Then we find $l_2 = l_1 - n$ and $l = 2(l_1 - n)$. Now we have to compare $l_1p+1, (l_1-n)p+n+1$ and $2(l_1-n)p+2$. Because $l_1 < 2n$ we see that $l_1p+1 > 2(l_1-n)p+2$, and for $p > n-1$ we can also see that $2(l_1-n)p+2 > (l_1-n)p+n+1$. For $p \leq n-2$ we use that $\frac{l_1p+1}{2n} \geq \frac{p+1}{2}$, so l_1 has to be greater than or equal to $\frac{n-1}{p} + n$, and using this fact we find that $2(l_1-n)p+2 \geq (l_1-n)p+n+1$ for every p. Now we have $\alpha_1 < \beta_2 \leq \alpha_2 < \beta_1$, and as in the other case the differential equation has 2 linearly independent solutions modulo p for every p that not devides n. We get

Theorem 9. *The standard hypergeometric equations of order 2 (see (9)) have for all primes p not dividing the denominators of the coefficients of the equation two linearly independent solutions modulo p.*

Remark. This result does not hold for the generalized hypergeometric equations of order n. Let's consider the example with $\alpha_1 = \frac{3}{14}$, $\alpha_2 = \frac{5}{14}$, $\alpha_3 = \frac{13}{14}$, $\beta_1 = 0$, $\beta_2 = \frac{1}{4}$, $\beta_3 = \frac{3}{4}$. Then the bad primes are: 3,5,13,19.

4. The general equation with 2-term recursion

The following theorem shows that all equations with 2-term recursion come from a hypergeometric equation by transformations:

Theorem 10. *Transforming the equation*

$$(\theta_x + b_{n_2}) \dots (\theta_x + b_1)y - x(\theta_x + a_{n_1}) \dots (\theta_x + a_1)y = 0 \qquad (20)$$

by $z^m \to x$, *then we get*

$$(\theta_z + mb_{n_2}) \dots (\theta_z + mb_1)y - z^m(\theta_z + ma_{n_1}) \dots (\theta_z + ma_1)y = 0. \qquad (21)$$

Proof. Easy. □

In the following we will assume that the prime p does not divide m. Then equation (20) has a fundamental system of polynomial solutions modulo p iff (21) has such a system. Furthermore in characteristic 0 (20) has a fundamental system of algebraic solutions iff (21) has such a system. If equation (20) has a fundamental system of polynomial solutions modulo p then $n_1 = n_2$, we assume this and write $n_1 = n_2 = n$. Because there is this connection between (20) and (21) for almost all prime characteristics and for characteristic zero we get the following:

Lemma 11. *For the equation*

$$(\theta_x + b_n) \dots (\theta_x + b_1)y - x^m(\theta_x + a_n) \dots (\theta_x + a_1)y = 0 \qquad (22)$$

the Grothendieck conjecture is true.

Now the following corollary follows:

Corollary 12. *For all equations with 2-term recursion the Grothendieck conjecture is true.*

Acknowledgements. I would like to thank Marius van der Put, Frits Beukers and Jacques-Arthur Weil for a lot of helpful discussions. Especially I thank Frits Beukers for the proof of theorem 7 and Jacques-Arthur Weil for doing some experiments with maple. Furthermore I thank the Department of Mathematics of the University of Groningen for the possibility to work here.

References

[BD] F. Baldassarri and B. Dwork: On second order linear differential equations with algebraic solutions, Amer. J. Math. **101**, (1979), 42–76

[BH] F. Beukers and G. Heckman: Monodromy for the hypergeometric function $F_{n,n+1}$, Invent. math **95**, 325–354 (1989)

[K] N.M. Katz: Rigid local systems, Princeton University Press, 1996

[Sch] H.A. Schwarz: Über diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe einer algebraischen Funktion ihres vierten Elementes darstellt. Crelle J. **75**, 292–335 (1873)