Pascal's triangle, normal rational curves, and their invariant subspaces

Johannes Gmainer *

August 20, 1999

Abstract

Each normal rational curve Γ in $\mathrm{PG}(n, F)$ admits a group $\mathrm{P\Gamma L}(\Gamma)$ of automorphic collineations. It is well known that for characteristic zero only the empty and the entire subspace are $\mathrm{P\Gamma L}(\Gamma)$–invariant. In case of characteristic $p > 0$ there may be further invariant subspaces. For $\#F \geq n + 2$, we give a construction of all $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces. It turns out that the corresponding lattice is totally ordered in special cases only.

1 Introduction

If the (commutative) ground field F of a projective space $\mathrm{PG}(n, F)$ has characteristic zero, then only the trivial subspaces are fixed by the group $\mathrm{P\Gamma L}(\Gamma)$ of automorphic collineations of a normal rational curve Γ. However, in case of non-zero characteristic there may be further $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces. A well known example is the intersecting point of the tangents of a conic, the so-called *nucleus*, in a projective plane of characteristic two.

In the present paper we show that every non–trivial $\mathrm{P\Gamma L}(\Gamma)$–invariant subspace is included in the nucleus of a normal rational curve, which is the intersection of all osculating hyperplanes. Our results are valid, if the ground field has sufficiently many elements ($\#F \geq n+2$). However, in case of a small ground field the problem is more complicated, since $\mathrm{P\Gamma L}(\Gamma)$ needs not be isomorphic to $\mathrm{P\Gamma L}(2, F)$.

Note, that normal rational curves are just specific examples of Veronese varieties. In case of non–zero characteristic all Veronese varieties with empty nucleus have been determined independently by H. Timmermann [9], [10], A. Herzer [6], and H. Karzel [8]. In [10] and [4] one can find an explicit formula for the

*Research supported by the Austrian National Science Fund (FWF), project P–12353–MAT, and by the City of Vienna (Hochschuljubiläumsstiftung der Stadt Wien), project H–39/98.

dimension of the nucleus of a normal rational curve; in [3] this is generalized to arbitrary Veronese varieties. The term *nucleus* can be extended in the following way [4]: Define the intersection over all k–dimensional osculating subspaces of the curve Γ to be a *k–nucleus*. Obviously, these subspaces are further examples of $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces.

In the present paper we give a construction of all $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces of a normal rational curve Γ with the usual parametric representation

$$\Gamma = \{F(1, t, \ldots, t^n) \mid t \in F \cup \{\infty\}\}. \tag{1}$$

Note that ∞ yields the point $F(0, \ldots, 0, 1)$. We show that in case of $\#F \geq n+2$ each $\mathrm{P\Gamma L}(\Gamma)$–invariant subspace $\mathcal{U}$ is spanned by points P_λ ($\lambda \in \Lambda$) of the standard basis. In Theorem 2 we characterize those index sets $\Lambda \subset \{0, 1, \ldots, n\}$ which yield invariant subspaces in terms of two closure operators.

In Section 3 we give examples of non–trivial index sets $\Lambda = \Lambda(I_1, \ldots, I_L; i, b)$. It turns out that their construction is closely related to Pascal's triangle modulo $\mathrm{char}\, F = p$ and, on the other hand, to the representation of the integer $b := n+1$ in base p.

The lattice of all $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces is investigated in Section 4. We show that the invariant subspaces constructed in Section 3 are exactly the *irreducible* elements of the lattice.

2 Necessary and sufficient conditions

Let $\mathrm{PG}(n, F)$ be the n–dimensional projective space on F^{n+1}, where $n \geq 2$ and F is a (commutative) field with $\#F \geq n+2$. In this section the characteristic ($\mathrm{char}\, F$) of the ground field is arbitrary.

We put $\mathrm{P\Gamma L}(\Gamma)$ for the group of all collineations fixing the normal rational curve (1) as a set and $\mathrm{PGL}(\Gamma)$ for the subgroup of all projective collineations in $\mathrm{P\Gamma L}(\Gamma)$. Due to $\#F \geq n+2$, $\mathrm{PGL}(\Gamma)$ and $\mathrm{PGL}(2, F)$ are isomorphic transformation groups on Γ and $\mathrm{PG}(1, F)$, respectively; cf. [5] and [7, 307–308].

The collineations induced by matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

where $a \in F \setminus \{0\}, t \in F$, generate the group $\mathrm{PGL}(2, F)$, cf. [1, 320–321]. So the projective collineations induced by matrices of the form

$$A_a = \mathrm{diag}\,(1, a, \ldots, a^n) \tag{2}$$

$$
B = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \tag{3}
$$

$$
C_t = \begin{pmatrix} \binom{0}{0} & 0 & 0 & \dots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \dots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \dots & \binom{n}{n} \end{pmatrix} \tag{4}
$$

generate $\mathrm{PGL}(\Gamma)$.

The automorphic collineations arising from (2) form a subgroup G_A of $\mathrm{P\Gamma L}(\Gamma)$. In an analogous manner the subgroup G_C is the set of all collineations induced by matrices (4).

THEOREM 1 *Let Γ be the normal rational curve (1) in $\mathrm{PG}(n, F)$ and $\#F \geq n+2$. A subspace $\mathcal{U}$ is G_A–invariant if and only if $\mathcal{U}$ is spanned by points P_λ $(\lambda \in \Lambda)$ of the standard basis.*

Proof. For all cases of $\operatorname{char} F$ we are able to find an element $\alpha \in F$ with the powers $\alpha^0, \alpha^1, \dots, \alpha^n$ being mutually different. If $\operatorname{char} F = 0$, the element $\alpha = 2$ is appropriate. For $\operatorname{char} F = p > 0$ we have to distinguish three possibilities.
1) For a finite field $F = GF(q)$ the multiplicative group is cyclic with a generating element α. As $\#F \geq n+2$, the powers $\alpha^0, \alpha^1, \dots, \alpha^n$ are mutually different.
2) If $\#F = \infty$ and $GF(q) \subset F$ for $q \geq n+2$, the same argument holds.
3) Now let $\#F = \infty$ and $q \leq n+1$ maximal, so that $GF(q) \subset F$. Each $\alpha \in F \setminus GF(q)$ is transcendental over F, because otherwise the field $F(\alpha)$ would have finite degree over F and q would not be maximal. Again, the powers $\alpha^0, \alpha^1, \dots, \alpha^n$ are mutually different.

Now we investigate the collineation given by the matrix $A_\alpha = \operatorname{diag}(1, \alpha^1, \dots, \alpha^n)$. As the eigenvalues are mutually different, exactly the points of the standard basis are fixed by the induced collineation. So, if $\mathcal{U}$ is spanned by base points, we certainly get $G_A(\mathcal{U}) = \mathcal{U}$.

On the other hand, let the subspace $\mathcal{U}$ be G_A–invariant. If $\dim \mathcal{U} \in \{-1, 0, n\}$, the assertion is either already shown or trivial. So, consider a k–dimensional

($1 \le k \le n-1$) invariant subspace $\mathcal{U}$ and choose two hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$, spanned by points of the standard basis, such that

$$\mathcal{U}_1 := \mathcal{U} \cap \mathcal{H}_1 \neq \mathcal{U} \cap \mathcal{H}_2 =: \mathcal{U}_2, \quad \dim \mathcal{U}_i = k-1.$$

As $G_A(\mathcal{U}) = \mathcal{U}$ and $G_A(\mathcal{H}_i) = \mathcal{H}_i$, also the subspaces $\mathcal{U}_i$ ($i = 1,2$) are G_A–invariant. However, by the induction hypothesis, each $\mathcal{U}_i$ is spanned by points of the standard basis and, by $\mathcal{U} = \mathcal{U}_1 \vee \mathcal{U}_2$, so is $\mathcal{U}$. $\square$

REMARK 1 From now on we know that in case of $\#F \ge n+2$ an invariant subspace can be written as $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$, so that finding invariant subspaces means characterizing the appropriate sets $\Lambda \subset \{0, \ldots, n\}$.

Before we are able to characterize the subspaces $\mathcal{U}$ which are also G_C–invariant, we need some preparations.

DEFINITION 1 *Given* char F *and a non–negative integer n, then define for $j \in \mathbb{N} := \{0, 1, \ldots\}$:*

$$\Omega(j) := \{m \in \mathbb{N} \mid 0 \le m \le n, \binom{m}{j} \not\equiv 0 \pmod{\operatorname{char} F}\}. \tag{5}$$

Moreover, put $\Omega(J) := \bigcup_{j \in J} \Omega(j)$ for every subset $J \subset \{0, \ldots, n\}$.

Note, that $\Omega(\emptyset) = \emptyset$. As the sets $\Omega(j)$ are crucial for the rest of the paper, they have to be investigated thoroughly. If char $F = 0$, we get $\Omega(j) = \{m \in \mathbb{N} \mid j \le m \le n\}$. In case of characteristic $p > 0$, the following lemma of LUCAS, cf. [2, 364], is very helpful:

$$\binom{m}{j} \equiv \prod_{\sigma=0}^{\infty} \binom{m_\sigma}{j_\sigma} \pmod{p}. \tag{6}$$

Here j_σ and m_σ are the digits of the representations of j and m in base p. Now, $\binom{m}{j} \not\equiv 0$ modulo p, if and only if $j_\sigma \le m_\sigma$ for all σ.

This gives rise to a half order $\preceq_F$ on $\mathbb{N}$. We have

$$j \preceq_F m \quad :\Leftrightarrow \quad j_\sigma \le m_\sigma \text{ for all } \sigma \in \mathbb{N}. \tag{7}$$

LEMMA 1 *For fixed n and given* char F *the following antitonicity holds:*

$$i_1 \preceq_F i_2 \Leftrightarrow \Omega(i_1) \supset \Omega(i_2) \tag{8}$$

Here $\preceq_F$ is the above mentioned half order for char $F = p$*, and the canonical half order " $\le$ " in case of characteristic zero.*

Proof. The case of char $F = 0$ is trivial, whereas the assertion in case of char $F = p$ is a consequence of (5) and (7). $\square$

The mapping Ω is a closure operator on the set $\{0, 1, \ldots, n\}$, because for arbitrary elements A and B of the power set of $\{0, 1, \ldots, n\}$ the following three conditions hold:

$$\begin{array}{rcl} A & \subset & \Omega(A) \\ \Omega(\Omega(A)) & = & \Omega(A) \\ A \subset B & \Rightarrow & \Omega(A) \subset \Omega(B) \end{array}$$

Now we characterize those G_A–invariant subspaces that are also G_C–invariant.

LEMMA 2 *A subspace* $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$ *is* G_C*–invariant if and only if the following condition holds:*

$$j \in \Lambda \Rightarrow \Omega(j) \subset \Lambda$$

Proof. If $j \in \Lambda$, we investigate the j–th column of a matrix (4) in the general case ($t \neq 0$). As $\mathcal{U}$ is spanned by base points, it is G_C–invariant if and only if the condition

$$\binom{m}{j} \not\equiv 0 \pmod{\operatorname{char} F} \quad \Rightarrow \quad m \in \Lambda$$

holds. However, $\binom{m}{j} \not\equiv 0 \pmod{\operatorname{char} F} \Leftrightarrow m \in \Omega(j)$. $\square$

If $\mathcal{U}$ is $\mathrm{PGL}(\Gamma)$–invariant, it has to be invariant under the collineation B in (3), which leads us to the next lemma.

LEMMA 3 *A subspace* $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$ *is invariant under the collineation* B *if and only if the following symmetry–condition holds:*

$$j \in \Lambda \quad \Leftrightarrow \quad j^* := n - j \in \Lambda \quad \forall j \in \{0, 1, \ldots, n\}. \tag{9}$$

Proof. This condition is an immediate consequence of the structure of the matrix B in (3). $\square$

In analogy to the operator Ω we may define another closure operator Σ, also called "the symmetry operator", on the power set of $\{0, 1, \ldots, n\}$:

$$\Sigma(A) := \bigcup_{a \in A} \{a, a^*\} \tag{10}$$

Now we are able to formulate the main theorem for invariant subspaces.

THEOREM 2 (main theorem) *If* F *has at least* $n + 2$ *elements, then the* $\mathrm{P\Gamma L}(\Gamma)$*–invariant subspaces can be characterized in the following way:*

1. *The subspace $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda\}]$ with $\Lambda \subset \{0, 1, \ldots, n\}$ is spanned by base points of the standard frame of reference.*

2. *The symmetry–condition $\Sigma(\Lambda) \subset \Lambda$ holds.*

3. *The set Λ has the closure property $\Omega(\Lambda) \subset \Lambda$.*

Proof. Note, that PGL(Γ) is generated by the 3 types of collineations induced by (2),(3), and (4). Due to $\#F \geq n + 2$, we may apply Theorem 1, Lemma 2, and Lemma 3 to find out that the above theorem characterizes the PGL(Γ)–invariant subspaces. However, PGL(Γ) is a subgroup of PΓL(Γ) and each collineation $\kappa \in \mathrm{P\Gamma L}(\Gamma)$ can be written as a product $\kappa = \kappa_1 \circ \kappa_2$; here $\kappa_1 \in \mathrm{PGL}(\Gamma)$ and κ_2 is fixing each point of the standard frame of reference. Thus each PGL(Γ)–invariant subspace is also κ_2–invariant and therefore PΓL(Γ)–invariant. □

REMARK 2 The trivial subspaces $\mathcal{U} = \emptyset$ and $\mathcal{U} = \mathcal{P}$ are certainly PΓL(Γ)–invariant and the corresponding trivial index sets are $\Lambda = \emptyset$ and $\Lambda = \{0, 1, \ldots, n\}$. We easily show that in case of char $F = 0$ these subspaces are the only ones:

$$\exists\, j \in \Lambda \overset{\Omega}{\Rightarrow} n \in \Omega(j) \overset{\Sigma}{\Rightarrow} 0 \in \Lambda \overset{\Omega}{\Rightarrow} \Omega(0) = \{0, \ldots, n\} \subset \Lambda.$$

Thus we are going to concentrate on the case char $F > 0$ for the rest of the paper. The main theorem enables us to decide for given dimension n, whether a given index set Λ represents a PΓL(Γ)–invariant subspace, or not. However, we aim at a construction of all appropriate sets Λ, which we are going to give in the following section.

3 Examples of invariant subspaces

Throughout this section the projective space PG(n, F) has fixed dimension n and prime–number characteristic $p = \operatorname{char} F$. For $j \in \{0, 1, \ldots, n\}$ the symmetric index $n - j$ is written as j^*. The representation of a non–negative integer $b \in \mathbb{N}$ in base p has the form

$$b = \sum_{\sigma=0}^{\infty} b_\sigma p^\sigma =: \langle b_\sigma \rangle. \tag{11}$$

We are going to construct index sets Λ, for which the last two conditions of the main theorem hold. As Ω and Σ are both closure operators, suitable sets Λ can be created in the following way:

The starting point is a set $J_0 := \{j_0\}$. Now compute $\Omega(J_0)$ and $J_1 := \Sigma(\Omega(J_0))$. If $J_0 = J_1$ we have found a suitable set $\Lambda := J_1$. Otherwise, repeat the two operations from above to get J_2 and so on. As Ω and Σ are closure operators acting on a finite set, there exists an index α, so that $J_{\alpha+1} = J_\alpha$ and the construction is successful. We are going to follow up this idea later on; cf. Theorem 6.

Right now, our starting point are sets of the form $\Lambda = \bigcup_\sigma \Omega(\sigma)$ with the property $\Sigma(\Lambda) = \Lambda$. Later on we are able to show that these sets Λ are exactly those that we get by the above mentioned method.

Right at the beginning we have to give some definitions and notations:

DEFINITION 2 *Given an expansion of the form (11) we define the function $V(i,b)$ as follows:*

$$\begin{array}{rrcl} V(i,b): & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ & (i,b) & \mapsto & \sum_{\sigma=0}^{i-1} b_\sigma p^\sigma \end{array} \tag{12}$$

From now on, the second argument $b := n+1$ of the function V is constant. Note, that for variable i the values $V(i,b)$ are not necessarily different, but we need a consistent description of these values. Let $N_1 < N_2 < \ldots < N_d$ be the positions of the non–zero digits of b in base p. Then we have

$$V(i,b) = 0 \quad \text{if} \quad i \le N_1 \tag{13}$$

$$V(i,b) = b = n+1 \quad \text{if} \quad i \ge N_d + 1 \tag{14}$$

and for all $\alpha \in \{1,2,\ldots,d-1\}$ the relation

$$V(N_\alpha+1,b) = V(N_\alpha+2,b) = \ldots = V(N_{\alpha+1},b) < V(N_{\alpha+1}+1,b).$$

REMARK 3 Observe that (13) and (14) describe the trivial index sets $\Omega(0) = \{0,1,\ldots,n\}$ and $\Omega(n{+}1) = \emptyset$, in which we are no longer interested, cf. Remark 2.

With the settings from above, the different values of $V(i,b)$ besides 0 and $n+1$ are denoted by $V(N_2,b),\ldots,V(N_d,b)$. Each $V(i,b)$ will lead us to a $\mathrm{P\Gamma L}(\Gamma)$–invariant subspace.

THEOREM 3 *The sets of the form $\Lambda = \Omega(V(i,b))$ are symmetric.*

Proof. We have to investigate, if $j^* \in \Lambda$ for each index $j \in \Lambda$. The digits of j in base p satisfy:

$$\begin{array}{rcll} j_\alpha & \in & \{0,1,\ldots,p-1\} & 0 \le \alpha \le N_1 - 1 \\ j_{N_1} & > & n_{N_1} & \\ j_\beta & \ge & n_\beta & N_1 + 1 \le \beta \le i-1 \\ j_i & \in & \{0,1,\ldots,p-1\} & \end{array}$$

For the symmetric index $j^* = n - j$ we get digits:

$$\begin{array}{rcll} j^*_\alpha & = & n_\alpha - j_\alpha & 0 \leq \alpha \leq N_1 - 1 \\ j^*_{N_1} & > & n_{N_1} & \\ j^*_\beta & \geq & n_\beta & N_1 \leq \beta \leq i-1 \end{array}$$

With these inequalities the assertion $j^* \in \Omega(V(i,b))$ is shown. □

Note, that $n_\alpha = p - 1$ in case of $0 \leq \alpha \leq N_1 - 1$ and that for $N_1 \leq \beta \leq i - 1$ there is always a "carry" in the p–adic addition $j_\beta + j^*_\beta$.

The following example illustrates the general situation:
With $p = 5$ and $n = 1424 = \langle 2,1,1,4,4\rangle$ we get $n + 1 = b = 1425 = \langle 2,1,2,0,0\rangle$. The interesting values $V(i,b)$ are

$$\begin{array}{rcl} V(3,b) & = & \langle 2,0,0\rangle \\ V(4,b) & = & \langle 1,2,0,0\rangle \end{array}$$

We get $\Omega(V(4,b)) = \{j = \langle j_4, j_3, j_2, j_1, j_0\rangle \mid j \leq n, j_2 \geq 2, j_3 \geq 1\}$. The digits of the symmetric index j^* are:

$$\begin{array}{rcl} n_0 - j_0 = 4 - j_0 & = & j^*_0 \\ n_1 - j_1 = 4 - j_1 & = & j^*_1 \\ j_2 = 2 & \Leftrightarrow & j^*_2 = 4 \\ j_2 = 3 & \Leftrightarrow & j^*_2 = 3 \\ j_2 = 4 & \Leftrightarrow & j^*_2 = 2 \\ j_3 = 1 & \Leftrightarrow & j^*_3 = 4 \\ j_3 = 2 & \Leftrightarrow & j^*_3 = 3 \\ j_3 = 3 & \Leftrightarrow & j^*_3 = 2 \\ j_3 = 4 & \Leftrightarrow & j^*_3 = 1 \end{array}$$

However, the values $V(i,b)$ are just the starting points for the construction of all invariant subspaces, and that is why further values $V(I_1, \ldots, I_L; i, b)$ are defined.

DEFINITION 3 *Given a set $\{0, 1, \ldots, i\}$ we consider for $\sigma = 1, 2, \ldots, L$ subsets of the form $I_\sigma := \{i_\sigma, i_\sigma + 1, \ldots, i_\sigma + k_\sigma\}$. With the conditions*

$$\begin{array}{rcll} i_\sigma, k_\sigma & \in & \mathbb{N} & \sigma = 1, \ldots, L \qquad (15) \\ i_\sigma + k_\sigma & \leq & i_{\sigma+1} - 2 & \sigma = 1, \ldots, L-1 \qquad (16) \\ i_L + k_L & \leq & i - 2 & \qquad (17) \\ b_{i_\sigma} & > & 0 & \sigma = 1, \ldots, L \qquad (18) \\ b_{i_\sigma + k_\sigma + 1} & < & p - 1 & \sigma = 1, \ldots, L \qquad (19) \end{array}$$

we define

$$V(I_1,\ldots,I_L;i,b) := V(i,b) - \sum_{\sigma=1}^{L}\sum_{\mu=0}^{k_\sigma} b_{i_\sigma+\mu}\, p^{i_\sigma+\mu} + \sum_{\sigma=1}^{L} p^{i_\sigma+k_\sigma+1}. \qquad (20)$$

For each I_σ we have a system $\mathcal{T}(I_\sigma)$ of subsets:

$$\mathcal{T}(I_\sigma) := \{T_{\sigma;t_\sigma} = \{i_\sigma, i_\sigma+1,\ldots,i_\sigma+t_\sigma\} \mid t_\sigma = -1,0,\ldots,k_\sigma\} \qquad (21)$$

The value $t_\sigma = -1$ describes the empty set and $\mathcal{T}(I_1\times\ldots\times I_L)$ is a shorthand for the product $\mathcal{T}(I_1)\times\ldots\times\mathcal{T}(I_L)$.

Now we check, if we can apply Definition 3 to $(T_1,\ldots,T_L)\in\mathcal{T}(I_1\times\ldots\times I_L)$ to obtain a number $V(T_1,\ldots,T_L;i,b)$. Of course, this is only possible, if all the conditions in Definition 3 are fulfilled, in other words $t_\sigma \geq 0$ and $b_{i_\sigma+t_\sigma+1} < p-1$ for all $\sigma\in\{1,2,\ldots,L\}$. This means that all sets T_σ have to be non–empty. However, we want to get

$$V(\ldots,T_{\alpha-1},T_\alpha,T_{\alpha+1},\ldots;i,b) = V(\ldots,T_{\alpha-1},T_{\alpha+1},\ldots;i,b),$$

if a set T_α is empty, and so Definition 3 has to be modified in the following sense: "Take an L-tuple $(T_1,\ldots,T_L)\in\mathcal{T}(I_1\times\ldots\times I_L)$. If there are empty sets T_α, then ignore these sets and apply Definition 3 to the remaining tuple with only non–empty sets."

Again, a short example for illustration: We consider $p=2$ and $b=372=\langle 1,0,1,1,1,0,1,0,0\rangle$. Taking $V(8,b)=\langle 0,1,1,1,0,1,0,0\rangle$ as a starting point, it is not possible to generate a value $V(I_1,I_2,I_3;8,b)$: As the conditions in Definition 3 imply $i_2\geq i_1+2$, $i_3\geq i_2+2$ and $b_{i_\mu}>0$, the only permissible triple (i_3,i_2,i_1) and (k_3,k_2,k_1) are $(6,4,2)$ and $(0,0,0)$. However, we are not allowed to define $V(\{2\},\{4\},\{6\};8,b)$ due to $b_{i_2+k_2+1}=b_5=p-1=1$.

In an analogous manner we are restricted to $i_1=2$ in defining a value $V(I_1,I_2;8,b)$. For i_2 we may choose $i_2=4$, but then again have to decide on $k_2=2$ due to (19). We get $V(\{2\},\{4,5,6\};8,b)=\langle 1,0,0,0,1,0,0,0\rangle$. The subsets $(T_1,T_2)\in\mathcal{T}(I_1\times I_2)$, for which we are able to define $V(T_1,T_2;8,b)$ are $(\{2\},\emptyset)$, $(\emptyset,\{4,5,6\})$ and $(\emptyset,\emptyset)$:

$$\begin{aligned} V(\{2\};8,b) &= \langle 0,1,1,1,1,0,0,0\rangle \\ V(\{4,5,6\};8,b) &= \langle 1,0,0,0,0,1,0,0\rangle \\ V(8,b) &= \langle 0,1,1,1,0,1,0,0\rangle \end{aligned}$$

After all these preparations, the indices $V(I_1,\ldots,I_L;i,b)$ will lead us to further non–trivial PΓL(Γ)–invariant subspaces.

THEOREM 4 *For each* $(T_1, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$*, such that* $V(T_1, \ldots, T_L; i, b)$ *is defined, there exists a number* $j \in \Omega(V(I_1, \ldots, I_L; i, b))$*, with*

$$\begin{array}{lcll} j^* & \in & \Omega(V(T_1, \ldots, T_L; i, b)) & \textit{but} \\ j^* & \notin & \Omega(V(S_1, \ldots, S_L; i, b)) & \textit{for all } (S_1, \ldots, S_L) \in \\ & & & \quad \mathcal{T}(I_1 \times \ldots \times I_L) \setminus (T_1, \ldots, T_L) \end{array}$$

Proof. With $T_\mu := T_{\mu; t_\mu}$ for all $\mu \in \{1, 2, \ldots, L\}$, we are going to choose $j \in \Omega(V(I_1, \ldots, I_L; i, b))$, such that $j^* = V(T_1, \ldots, T_L; i, b)$. Define j in terms of its digits in base p:

$$\begin{array}{llcll}
 & j_\alpha & = & n_\alpha = p-1 & 0 \le \alpha \le N_1 - 1 \\
\underline{\text{iff } i_1 > N_1} & \left\{ \begin{array}{l} j_\beta \\ j_{i_1} \end{array} \right. & \begin{array}{c} = \\ = \end{array} & \begin{array}{l} p-1 \\ n_{i_1} - 1 \end{array} & N_1 \le \beta \le i_1 - 1 \\
\underline{\text{iff } i_1 = N_1} & j_{i_1} & = & n_{i_1} & \\
 & j_\gamma & = & n_\gamma & i_1 + 1 \le \gamma \le i_1 + t_1 \\
 & j_\delta & = & p-1 & i_1 + t_1 + 1 \le \delta \le i_2 - 1 \\
 & j_{i_2} & = & n_{i_2} - 1 & \\
 & j_\gamma & = & n_\gamma & i_2 + 1 \le \gamma \le i_2 + t_2 \\
 & j_\delta & = & p-1 & i_2 + t_2 + 1 \le \delta \le i_3 - 1 \\
 & & \vdots & & \\
 & j_{i_L} & = & n_{i_L} - 1 & \\
 & j_\gamma & = & n_\gamma & i_L + 1 \le \gamma \le i_L + t_L \\
 & j_\delta & = & p-1 & i_L + t_L + 1 \le \delta \le i - 1 \\
 & j_i & = & n_i - 1 & \\
 & j_\gamma & = & n_\gamma & i + 1 \le \gamma \le N_d
\end{array}$$

In case of $t_\sigma = -1$ we simply omit the line $j_{i_\sigma} = n_{i_\sigma} - 1$, respectively $j_{i_1} = n_{i_1}$ (if $t_1 = -1$ and $i_1 = N_1$).

For the symmetric index j^* we get:

$$\begin{array}{llcll}
 & j^*_\alpha & = & 0 & 0 \le \alpha \le N_1 - 1 \\
\underline{\text{iff } i_1 > N_1} & \left\{ \begin{array}{l} j^*_{N_1} \\ j^*_\beta \end{array} \right. & \begin{array}{c} = \\ = \end{array} & \begin{array}{l} n_{N_1} + 1 \\ n_\beta \end{array} & N_1 + 1 \le \beta \le i_1 - 1
\end{array}$$

$$
\begin{array}{rcll}
j^*_{i_1} &=& 0 & \\
j^*_\gamma &=& 0 & i_1+1 \le \gamma \le i_1+t_1 \\
j^*_{i_1+t_1+1} &=& n_{i_1+t_1+1}+1 & \\
j^*_\delta &=& n_\delta & i_1+t_1+2 \le \delta \le i_2-1 \\
j^*_\gamma &=& 0 & i_2 \le \gamma \le i_2+t_2 \\
j^*_{i_2+t_2+1} &=& n_{i_2+t_2+1}+1 & \\
j^*_\delta &=& n_\delta & i_2+t_2+2 \le \delta \le i_3-1 \\
&\vdots&& \\
j^*_\gamma &=& 0 & i_L \le \gamma \le i_L+t_L \\
j^*_{i_L+t_L+1} &=& n_{i_L+t_L+1}+1 & \\
j^*_\delta &=& n_\delta & i_L+t_L+2 \le \delta \le i-1
\end{array}
$$

It is obvious that we have $j^* = V(T_1, \ldots, T_L; i, b) \in \Omega(V(T_1, \ldots, T_L; i, b))$.
It remains to show that $V(T_1, \ldots, T_L; i, b) \in \Omega(V(S_1, \ldots, S_L; i, b))$ if and only if $(S_1, \ldots, S_L) = (T_1, \ldots, T_L)$: So we assume that there exists Y with $S_Y \neq T_Y$ and $V(T_1, \ldots, T_L; i, b) \in \Omega(V(S_1, \ldots, S_L; i, b))$. There are two possibilities, i) $s_Y < t_Y$ and ii) $s_Y > t_Y$.
i) If $s_Y = -1$, we have $h_{i_Y} \ge b_{i_Y} > 0$ for all $h \in \Omega(V(S_1, \ldots, S_L; i, b))$, whereas $V(T_1, \ldots, T_L; i, b)_{i_Y} = 0$. Otherwise ($s_Y \ge 0$) we have $h_{i_Y+s_Y+1} > b_{i_Y+s_Y+1}$, but $V(T_1, \ldots, T_L; i, b)_{i_Y+s_Y+1} = 0 \le b_{i_Y+s_Y+1}$, which is always a contradiction.
ii) Similarly $h_{i_Y+s_Y+1} > b_{i_Y+s_Y+1}$, but $V(T_1, \ldots, T_L; i, b)_{i_Y+s_Y+1} = b_{i_Y+s_Y+1}$, if $t_Y = -1$; and otherwise $h_{i_Y+s_Y+1} > b_{i_Y+s_Y+1}$, but $V(T_1, \ldots, T_L; i, b)_{i_Y+s_Y+1} = b_{i_Y+s_Y+1}$, which is again a contradiction. □

Theorem 4 tells us that starting with $\Omega(V(I_1, \ldots, I_L; i, b))$, the smallest set which might pass the conditions of the main theorem is

$$\Lambda(I_1, \ldots, I_L; i, b) := \bigcup \Omega(V(T_1, \ldots, T_L; i, b)), \tag{22}$$

taking the union over all L-tuples $(T_1, \ldots, T_L) \in \mathcal{T}(I_1 \times \ldots \times I_L)$. In fact, these sets $\Lambda(I_1, \ldots, I_L; i, b)$ meet the symmetry–condition of the main theorem. This will be proved by the help of the following two lemmas.

LEMMA 4 *Let j be an element of $\Lambda(I_1, \ldots, I_L; i, b)$. Then we have*

$$j \quad \notin \quad \Omega(V(T_1, \ldots, T_L; i, b))$$

for all

$$(T_1, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, \ldots, I_L))$$

if and only if

$$\nu_\mu \quad := \quad \max\{\alpha \in \{0, 1, \ldots, k_\mu\} \mid j_{i_\mu+\alpha} < b_{i_\mu+\alpha}\} \tag{23}$$

exists for all $\mu \in \{1, 2, \ldots, L\}$ and

$$\min\{\beta \in \{\nu_\mu+1, \ldots, k_\mu+1\} \mid j_{i_\mu+\beta} > b_{i_\mu+\beta}\} \quad = \quad k_\mu + 1. \tag{24}$$

Proof. Assume $j \in \Lambda(I_1, \ldots, I_L; i, b)$ and $j \notin \Omega(V(T_1, \ldots, T_L; i, b))$ for all $(T_1, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, \ldots, I_L))$. If there were $Y \in \{1, 2, \ldots, L\}$ with $j_{i_Y+\alpha} \geq b_{i_Y+\alpha}$ for $\alpha = 0, 1, \ldots, k_Y$, then we would get the contradiction $j \in \Omega(V(I_1, \ldots, I_{Y-1}, \emptyset, I_{Y+1}, \ldots, I_L; i, b))$. So the maximum ν_μ exists for all indices. Now assume, that for $Y \in \{1, 2, \ldots, L\}$ we have

$$\min\{\beta \in \{\nu_Y + 1, \ldots, k_Y + 1\} \mid j_{i_Y+\beta} > b_{i_Y+\beta}\} =: t_Y + 1 < k_Y + 1.$$

However, this results in $j \in \Omega(V(I_1, \ldots, I_{Y-1}, T_Y, I_{Y+1}, \ldots, I_L; i, b))$ with $(T_Y \neq I_Y)$, which is also a contradiction.

Now let us have $j \in \Lambda(I_1, \ldots, I_L; i, b)$ with conditions (23) and (24). Assume to the contrary that $j \in \Omega(V(T_1, \ldots, T_L; i, b))$ with $(T_1, \ldots, T_L) \neq (I_1, \ldots, I_L)$. So there exists $Y \in \{1, 2, \ldots, L\}$ with $T_Y \neq I_Y$. Note that an element $h \in \Omega(V(T_1, \ldots, T_L; i, b))$ fulfills:

$$\begin{aligned} h_{i_Y+t_Y+1} &> b_{i_Y+t_Y+1} \\ h_{i_Y+\alpha} &\geq b_{i_Y+\alpha} \qquad t_Y + 2 \leq \alpha \leq k_Y + 1 \end{aligned}$$

However, the inequality $j_{i_Y+\nu_Y} < b_{i_Y+\nu_Y}$ in the case $\nu_Y \geq t_Y + 1$, respectively the identity $j_{i_Y+t_Y+1} = b_{i_Y+t_Y+1}$ in case of $\nu_Y < t_Y + 1 < k_Y + 1$ leads to an absurdity. □

LEMMA 5 *Let $j \in \Lambda(I_1, \ldots, I_L; i, b)$ and*

$$j \notin \Omega(V(T_1, \ldots, T_L; i, b))$$

for all

$$(T_1, \ldots, T_L) \in (\mathcal{T}(I_1 \times \ldots \times I_L) \setminus (I_1, \ldots, I_L)).$$

Then the symmetric index j^* has the same properties.

Proof. As the index j meets the conditions of the lemma, we have:

$$\begin{aligned}
& j_\alpha \in \{0, 1, \ldots, p-1\} && 0 \leq \alpha \leq N_1 - 1 \\
\underline{\text{iff } i_1 > N_1} \quad & \begin{cases} j_{N_1} > n_{N_1} \\ j_\beta \geq n_\beta \end{cases} && N_1 + 1 \leq \beta \leq i_1 - 1 \\
& j_{i_1+k_1+1} > n_{i_1+k_1+1} \\
& j_\delta \geq n_\delta && i_1 + k_1 + 2 \leq \delta \leq i_2 - 1 \\
& j_{i_2+k_2+1} > n_{i_2+k_2+1} \\
& j_\delta \geq n_\delta && i_2 + k_2 + 2 \leq \delta \leq i_3 - 1 \\
& \vdots \\
& j_{i_L+k_L+1} > n_{i_L+k_L+1} \\
& j_\delta \geq n_\delta && i_L + k_L + 2 \leq \delta \leq i - 1
\end{aligned}$$

As a result we get $j_\alpha^* = n_\alpha - j_\alpha = p-1-j_\alpha$ with $0 \leq \alpha \leq N_1 - 1$, and for the other digits of j^* the same inequalities are valid, as above. This gives

$$j^* \in \Omega(V(I_1, \ldots, I_L; i, b)) \subset \Lambda(I_1, \ldots, I_L; i, b).$$

With the notations in Lemma 4 and fixed $\mu \in \{1, 2, \ldots, L\}$ there are two possibilities: Either there is a "carry" in the addition

$$j_{i_\mu+\nu_\mu-1} + j^*_{i_\mu+\nu_\mu-1} = n_{i_\mu+\nu_\mu-1},$$

or there is not. It turns out, that in both cases we get

$$\begin{array}{rcl} \nu_\mu^* & = & \max\{\alpha \in \{0, 1, \ldots, k_\mu\} \mid j^*_{i_\mu+\alpha} < n_{i_\mu+\alpha}\} \geq \nu_\mu \\ k_\mu + 1 & = & \min\{\beta \in \{\nu_\mu^* + 1, \ldots, k_\mu + 1\} \mid j^*_{i_\mu+\beta} > n_{i_\mu+\beta}\}, \end{array}$$

and with Lemma 4 we obtain the assertion. □

With the aid of these two lemmas we are now able to formulate

THEOREM 5 *The subspaces* $\mathcal{U} = [\{P_\lambda \mid \lambda \in \Lambda(I_1, \ldots, I_L; i, b)\}]$ *are invariant under the group* $\mathrm{P\Gamma L}(\Gamma)$ *of automorphic collineations.*

Proof. As $\Lambda(I_1, \ldots, I_L; i, b)$ is a union of sets $\Omega(V(*, b))$, we just have to investigate, if the symmetry–condition of Theorem 2 holds. Given $j \in \Lambda(I_1, \ldots, I_L; i, b)$, there exists one and only one L-tuple $(T_1, \ldots, T_L)$ with

$$j \in \Omega(V(T_1, \ldots, T_L; i, b)) \qquad \text{and} \qquad \sum_{\mu=1}^{L} \# T_\mu \quad \longrightarrow \quad \text{minimum}.$$

i) If this minimum equals 0 or, in other words, $j \in \Omega(V(i, b))$, then we get $j^* \in \Omega(V(i, b))$ by Theorem 3.
ii) For a positive value of this minimum, we only write down non–empty sets and get an H-tuple $(T_{i_1}, \ldots, T_{i_H})$ with $H \leq L$ and $T_{i_\mu} \neq \emptyset$ $(\mu = 1, 2, \ldots, H)$. Now we apply Lemma 5 to the set $(T_{i_1} \times \ldots \times T_{i_H})$, which completes the proof. □

4 The lattice of the invariant subspaces

If we want to determine the lattice of all $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces, it is sufficient to characterize those "irreducible" elements, which cannot be written as a non–trivial sum of invariant subspaces. As the lattice has only finitely many elements, each "non–irreducible" subspace can be constructed as a sum of "irreducible" ones.

THEOREM 6 *The subspaces of the form*

$$\mathcal{U} := [\{P_\lambda \mid \lambda \in \Lambda(I_1, \dots, I_L; i, b)\}]$$

are exactly the non–trivial irreducible invariant subspaces.

Proof. We are going to follow up the idea explained at the beginning of Section 3. For every index j in the set $\{0, 1, \dots, n\}$ we construct the minimal index set Λ with $\Omega(\Lambda) = \Lambda$ and $\Sigma(\Lambda) = \Lambda$. If $\binom{n}{j} \not\equiv 0 \pmod p$, we get

$$j \in \Lambda \overset{\Omega}{\Rightarrow} n \in \Omega(j) \overset{\Sigma}{\Rightarrow} 0 \in \Lambda \overset{\Omega}{\Rightarrow} \Omega(0) = \{0, \dots, n\} \subset \Lambda, \tag{25}$$

the entire space, a trivial irreducible invariant subspace.

Now take j with $\binom{n}{j} \equiv 0 \pmod p$ and define:

$$\begin{array}{llcl}
\text{iff } j_{N_1} \le n_{N_1} & i_1 & := & N_1 \\
\text{iff } j_{N_1} > n_{N_1} & i_1 & := & \min\{\alpha \in \{N_1+1, \dots, N_d\} \mid j_\alpha < n_\alpha\} \\
 & i_1 + k_1 + 1 & := & \min\{\beta \in \{i_1+1, \dots, N_d\} \mid j_\beta > n_\beta\} \\
 & i_2 & := & \min\{\gamma \in \{i_1+k_1+2, \dots, N_d\} \mid j_\gamma < n_\gamma\} \\
 & i_2 + k_2 + 1 & := & \min\{\delta \in \{i_2+1, \dots, N_d\} \mid j_\delta > n_\delta\} \\
 & & \vdots & \\
 & i := i_{L+1} & := & \min\{\omega \in \{i_L+k_L+2, \dots, N_d\} \mid j_\omega < n_\omega\}
\end{array}$$

The index j' with

$$\begin{array}{lllll}
 & j'_\alpha & = & n_\alpha = p-1 & 0 \le \alpha \le N_1 - 1 \\
\underline{\text{iff } i_1 > N_1} & \left\{ \begin{array}{l} j'_\beta \\ j'_{i_1} \end{array} \right. & \begin{array}{c} = \\ = \end{array} & \begin{array}{l} p-1 \\ n_{i_1} - 1 \end{array} & N_1 \le \beta \le i_1 - 1 \\
\underline{\text{iff } i_1 = N_1} & j'_{i_1} & = & n_{i_1} & \\
 & j'_\gamma & = & n_\gamma & i_1 + 1 \le \gamma \le i_1 + k_1 \\
 & j'_\delta & = & p-1 & i_1 + k_1 + 1 \le \delta \le i_2 - 1 \\
 & j'_{i_2} & = & n_{i_2} - 1 & \\
 & j'_\gamma & = & n_\gamma & i_2 + 1 \le \gamma \le i_2 + k_2 \\
 & j'_\delta & = & p-1 & i_2 + k_2 + 1 \le \delta \le i_3 - 1 \\
 & & \vdots & & \\
 & j'_{i_L} & = & n_{i_L} - 1 & \\
 & j'_\gamma & = & n_\gamma & i_L + 1 \le \gamma \le i_L + k_L \\
 & j'_\delta & = & p-1 & i_L + k_L + 1 \le \delta \le i - 1 \\
 & j'_i & = & n_i - 1 & \\
 & j'_\gamma & = & n_\gamma & i + 1 \le \gamma \le N_d
\end{array}$$

has the properties

$$\begin{array}{rcl} j' & \in & \Omega(j) \\ j'^{*} & = & V(I_1, \ldots, I_L; i, b). \end{array}$$

So we get $\Lambda = \Lambda(I_1, \ldots, I_L; i, b)$, and due to Theorem 4 and Theorem 5 the corresponding subspace is $\mathrm{P\Gamma L}(\Gamma)$–invariant and irreducible. Note, that for each $V(I_1, \ldots, I_L; i, b)$, which can be defined by (20), we find an appropriate j, so that the above construction is possible. □

Having determined all irreducible invariant subspaces in the ambient space of a normal rational curve, it is a natural question to ask, in which cases the accompanying lattice is totally ordered.

THEOREM 7 *Let the positions of the non-zero digits of* $b := n+1$ *in base* p *be denoted by* $N_1, N_2, \ldots, N_d$*. Then the lattice of the* $\mathrm{P\Gamma L}(\Gamma)$*–invariant subspaces is totally ordered if and only if one of the following cases occurs:*

1. $d \in \{1, 2\}$.
2. $d \geq 3, N_d - N_1 = d-1,$ *and* $N_2 = \ldots = N_{d-1} = p-1$.

Proof. We are going to discuss all the cases of $d \geq 1$:
1) If $d = 1$, the representation of n in base p has the form $\langle n_Y, p-1, \ldots, p-1\rangle$. Only if $b_{N_1} = 1$ we get $Y = N_1 - 1$, in all other cases Y equals N_1. By formula (6) we get $\binom{n}{j} \not\equiv 0 \pmod p$ for all $j \in \{0, 1, \ldots, n\}$. With (25) merely the trivial subspaces are $\mathrm{P\Gamma L}(\Gamma)$–invariant. If $d = 2$, the only index sets Λ that can be constructed according to Definition 3 and formula (22) are of the form $\Lambda(I_1; N_2, b)$ with $I_1 = \{N_1, \ldots, i_1 + k_1\}$. As $i_1 = N_1$ is constant, the lattice is totally ordered.
2) $d \geq 3$: i) Assume $N_d > N_1 + d - 1$ or $N_d = N_1 + d - 1$ and that there is an $\alpha \in \{2, 3, \ldots, d-1\}$ with $b_{N_\alpha} < p - 1$. In both cases there exists an index Y, with $N_1 < Y < N_d$ and $b_Y < p - 1$. Now put $I_1 := \{N_1, \ldots, Y-1\}$, to get

$$\Lambda(N_2, b) \underset{\not\supset}{\not\subset} \Lambda(I_1; N_d, b).$$

ii) In the case $N_d - N_1 = d-1$ and $N_2 = \ldots = N_{d-1} = p-1$, the only non–trivial index sets we may construct are

$$\Lambda(N_2, b) \subset \Lambda(N_3, b) \subset \ldots \subset \Lambda(N_d, b),$$

which completes the proof. □

In conclusion we give according to $\operatorname{char} F = p$ the minimal dimension n, so that the lattice of $\mathrm{P\Gamma L}(\Gamma)$–invariant subspaces is not totally ordered:

1. $p = 2$: $b = \langle 1, 0, 1, 1\rangle = 11$, which means $n = p^3 + p = p(p^2+1)$.
2. $p \geq 3$: $b = \langle 1, 1, 1\rangle$, so $n = p(p+1)$.

References

[1] Benz, W., *Vorlesungen über Geometrie der Algebren*, Springer, Berlin Heidelberg New York, 1973.

[2] Brouwer, A.E., and Wilbrink, H.A., *Block designs*, in Handbook of incidence geometry, Buekenhout, F., ed., Elsevier, Amsterdam, 1995, ch. 8, pp. 349–382.

[3] Gmainer, J., and Havlicek, H., *A dimension formula for the nucleus of a Veronese variety.* submitted.

[4] Gmainer, J., and Havlicek, H., *Nuclei of normal rational curves.* J. Geom., in print.

[5] Havlicek, H., *Die automorphen Kollineationen nicht entarteter Normkurven*, Geom. Dedicata, 16 (1984), pp. 85–91.

[6] Herzer, A., *Die Schmieghyperebenen an die Veronese–Mannigfaltigkeit bei beliebiger Charakteristik*, J. Geom., 18 (1982), pp. 140–154.

[7] Hirschfeld, J.W.P., and Thas, J.A., *General Galois geometries*, Oxford University Press, Oxford, 1991.

[8] Karzel, H., *Über einen Fundamentalsatz der synthetischen algebraischen Geometrie von W. Burau und H. Timmermann*, J. Geom., 28 (1987), pp. 86–101.

[9] Timmermann, H., *Descrizioni geometriche sintetiche di geometrie proiettive con caratteristica* $p > 0$, Ann. Mat. Pura Appl., IV. Ser. 114, (1977), pp. 121–139.

[10] Timmermann, H., *Zur Geometrie der Veronesemannigfaltigkeit bei endlicher Charakteristik*, Habilitationsschrift, Univ. Hamburg, 1978.