COMMUTING ELEMENTS IN GALOIS GROUPS OF FUNCTION FIELDS

by

Fedor Bogomolov and Yuri Tschinkel

Abstract. — We study the structure of abelian subgroups of Galois groups of function fields.

Contents

Introduction

Setup. — We fix a prime number p. Let k be a field of characteristic $\neq p$ and 2. Assume that k does not admit finite extensions of degree divisible by p. Let $K = k(X)$ be the field of functions of an algebraic variety X defined over k and G_K the Galois group of a separable closure of K. The principal object of our study is the group $\Gamma = \Gamma_K$ - the (maximal) pro-p-quotient of the kernel $\mathrm{Ker}(\mathrm{G}_K \to \mathrm{G}_k)$.

Main theorem. — This paper contains a proof of the main theorem from [**2**] describing (topologically) noncyclic subgroups in the abelianization

$$\Gamma^a := \Gamma/[\Gamma,\Gamma]$$

which can be lifted to abelian subgroups of

$$\Gamma^c := \Gamma/[[\Gamma,\Gamma],\Gamma].$$

Let ν be a valuation of K. We denote by K_ν the completion of K with respect to ν, by Γ^a_ν the reduced valuation group and by I^a_ν the abelian inertia group of ν (see Sections 6.1 and 6.2 for the definitions).

THEOREM 1. — *Let F be a noncyclic subgroup of Γ^a. Suppose that it can be lifted to an abelian subgroup of Γ^c. Then there exists a nonarchimedean valuation ν of K such that*

- *F is contained in the abelian reduced valuation group $\Gamma^a_\nu \subset \Gamma^a$ (standard valuation group if the residue field of K_ν has characteristic $\neq p$);*
- *F contains a subgroup F' such that $F' \subset \mathrm{I}^a_v$ and F/F' is topologically cyclic.*

It is easy to see that abelian groups satisfying the conditions of the theorem can be lifted to abelian subgroups of G_K itself. Thus Theorem 1 shows that there are no obstructions to the lifting of abelian subgroups of G_K beyond the first nontrivial level.

Our paper is a contribution to the "anabelian geometry" program, initiated by Grothendieck. For other results in this direction we refer to [**8**], [**10**], [**7**].

Structure of the proof. — By Kummer theory, the elements of Γ^a can be interpreted as k^*-invariant $\mathbb{Z}_p$-valued logarithmic functions on K^*. The quotient space K^*/k^* has a natural structure of an infinite dimensional projective space over k, denoted by $\mathbb{P}(K)$. Consider a pair of (nonproportional) elements f_1, f_2 of Γ^a. They define a map

$$\begin{array}{rrl} \varphi: & \mathbb{P}(K) \to & \mathbb{A}^2(\mathbb{Z}_p) \\ & (v,v') \mapsto & (f_1(v), f_2(v')). \end{array} \tag{1.1}$$

If f_1, f_2 lift to a pair of commuting elements in Γ^c then the restrictions of the corresponding functions to any projective line $\mathbb{P}^1 \subset \mathbb{P}(K)$ are linearly dependent modulo constant functions (see Proposition 5.4.1). Thus every projective line in $\mathbb{P}(K)$ maps into an affine line in $\mathbb{A}^2$. This - together with the logarithmic property of f_1 and f_2 - imposes very strong conditions on the 2-dimensional subspace they span in the space of functions on $\mathbb{P}(K)$. Namely, this subspace contains a special nonzero function which we call an abelian flag function (an AF-function); it corresponds to an inertia element of some reduced valuation subgroup (see Section 6.2 and Section 2 for the definitions). The main problem is to prove the existence of this AF-function.

In Section 2 we define AF-functions and study them on abelian groups of ranks 2 and 3. Let f be a function on a vector space V with values in a set S, $V' \subset V$ a subspace and $f_{V'}$ the restriction of f to V'. A series of reductions leads to the following criterium: f is an (invariant) AF-function on V iff for all 3-dimensional subspaces V' the function $f_{V'}$ is an (invariant) AF-function on V' (3.2.1). Reduction to 2-dimensional subspaces is more problematic. For fields k is of characteristic $\mathrm{char}(k) > 2$ the reduction to dimension 2 can be established without the use of the logarithmic property leading to an easier proof of this case of the main theorem. A similar statement for fields k of characteristic zero requires the logarithmic property. The corresponding proofs are in Section 3.4.

The proof of the main theorem proceeds by contradiction. We assume that the $\mathbb{Z}_p$-span $\langle f_1, f_2\rangle_{\mathbb{Z}_p}$ does not contain an AF-function. The reductions and the logarithmic property imply that there exists a 3-dimensional $V \subset K$, two nonproportional functions $f_1', f_2' \in \langle f_1, f_2\rangle_{\mathbb{Z}_p}$ and a map $h' : \mathbb{Z}_p \to \mathbb{Z}/2$ such that each of the functions $h' \circ f_1', h' \circ f_2', h \circ f_1' + h \circ f_2'$ fails to be AF. In Section 4.2 we find a contradiction to this claim.

Acknowledgements. The first author was partially supported by the NSF. The second author was partially supported by the NSA.

2. Classes of functions

In this section we define certain classes of functions on abelian groups and vector spaces which will be used in the proofs.

2.1. Notations. — Denote by $\mathbb{Z}_{(0)} = \mathbb{Z} \setminus 0$ and by $\mathbb{Z}_{(q)}$ the set of all integers coprime to q. Let $\mathcal{A}_0$ (resp. $\mathcal{A}_q$) be the set of torsion free abelian groups (resp. vector spaces over the finite field $\mathbf{F}_q$, where q is a prime number $\neq 2$). We denote by $\mathrm{rk}(A) \in \{1, ..., \infty\}$ the minimal number of generators of A (as an abelian group). An element $a \in A$ (with $A \in \mathcal{A}_0$) is called primitive if there are no $a' \in A$ and $n \in \mathbb{N}$ such that $a = na'$. We denote by $\langle a_1, ..., a_n \rangle$ the subgroup generated by $a_1, ..., a_n$ and similarly by $\langle B \rangle$ the subgroup generated by elements of a subset $B \subset A$. We denote by $\mathcal{F}(A, S)$ the set of functions on A with values in a set S. We will say that a function $f \in \mathcal{F}(A, S)$ is induced from A/nA if for all primitive x and all $y \in A$ with $x - y = nz$ for some $z \in A$ one has $f(x) = f(y)$. For $B \subset A$ and $f \in \mathcal{F}(A, S)$ we denote by f_B the restriction to B (or simply f if the domain is clear from the context).

Assumption 2.1.1. — *Throughout, all abelian groups are either in $\mathcal{A}_0$ or in $\mathcal{A}_q$.*

2.2. Definitions. — We will work in the following setup:

$$A \subset V \subset K$$

where A is a $\mathbb{Z}$-(resp. $\mathbf{F}_q$-) sublattice of a k-vector space V which is embedded into K.

Definition 2.2.1. — *Let $A \in \mathcal{A}_0$ (resp. $A \in \mathcal{A}_q$) and $f \in \mathcal{F}(A, S)$. We say that f is invariant if*

$$f(na) = f(a)$$

for all $a \in A$ and all $n \in \mathbb{Z}_{(0)}$ (resp. all $n \in \mathbb{Z}_{(q)}$)

Let V be a vector space over k and $f \in \mathcal{F}(V, S)$. We say that f is invariant if

$$f(\kappa v) = f(v)$$

for all $\kappa \in k^*$ and $v \in V$.

An invariant function on $A = \mathbf{F}_q^n$ (minus 0_A) can be considered as a function on $\mathbb{P}^{n-1}(\mathbf{F}_q) = (A \setminus 0)/\mathbf{F}_q^*$. An invariant function on $V \setminus 0$ can be considered as a function on the projective space $\mathbb{P}(V)$ (over k) and we will denote by $\mathcal{F}(\mathbb{P}(V), S) \subset \mathcal{F}(V, S)$ the space of such functions.

Definition 2.2.2 (Filtration). — *Let A be finitely generated and $\mathcal{I}$ a totally ordered set. A (strict)* filtration *on A with respect to $\mathcal{I}$ is a set of subgroups $A_\iota \subset A$ (with $\iota \in \mathcal{I}$) such that*

- *$A = \cup_{\iota \in \mathcal{I}} A_\iota$;*
- *if $\iota < \iota'$ then $A_{\iota'}$ is a proper subgroup of A_ι.*

Notations 2.2.3. — Denote by

$$\overline{A}_\iota := A_\iota \setminus \cup_{\iota' > \iota} A_{\iota'}.$$

Notice that for all $\iota \in \mathcal{I}$ we have $\overline{A}_\iota \neq \emptyset$.

Definition 2.2.4 (AF-functions). — *A function f on a finitely generated group A (as in 2.1.1) is called an* abelian flag *function if*

- *f is invariant;*
- *A has a (strict) filtration by groups (with respect to an ordered set $\mathcal{I}$) such that f is constant on $\overline{A}_\iota$ for all $\iota \in \mathcal{I}$.*

If A is not finitely generated then f is an abelian flag function if $f_{A'}$ is an abelian flag function for every finitely generated subgroup $A' \subset A$.

We denote the set of abelian flag functions by $\mathcal{AF}(A, S)$. This property does not depend on the value of f on the neutral element 0_A. We will identify functions which differ only on 0_A.

Definition 2.2.5. — *Let V be a vector space over k. A function $f \in \mathcal{F}(V, S)$ is called an abelian flag function if*

- *f is invariant;*
- *for all (additive) sublattices $A \subset V$ the restriction $f_A \in \mathcal{AF}(A, S)$.*

Definition 2.2.6 (c-pairs). — *Let A be an abelian group as above and S a ring. We will say that $f_1, f_2 \in \mathcal{F}(A, S)$ form a c-pair if for every subgroup $C \subset A$ of rank 2 one has*

$$\mathrm{rk}(\langle f_1, f_2, 1\rangle_S) \leq 2.$$

Definition 2.2.7 (LF-functions). — *Let V be a unital algebra over k and S an abelian group. A function $f \in \mathcal{F}(V,S)$ is called a* logarithmic *function if*
- *f is invariant;*
- *$f(v \cdot v') = f(v) + f(v')$ for all $v, v' \in V \setminus 0$.*

The set of logarithmic functions will be denoted by $\mathcal{LF}(V,S)$. We shall refer to abelian flag (resp. logarithmic) functions as AF-functions (resp. LF-functions).

2.3. First properties. —

Remark 2.3.1. — Assume that A is *finitely generated.* Then for every $f \in \mathcal{AF}(A,S)$ and every subgroup $B \subset A$ there exists a proper subgroup $B^1_f \subset B^0_f = B$ such that f is constant on the complement $B \setminus B^1_f$. In particular, if $b_0 \in B \setminus B^1_f$ and $b_1 \in B^1_f$ then $f(b_0 + b_1) = f(b_0)$. Thus we can speak about generic elements of B and the generic value of f on B. We obtain a decreasing (possibly finite) $\mathbb{N}$-filtration (A^n_f) on A: A^n_f is the *subgroup* of nongeneric elements in A^{n-1}_f. Notice that an analogous statement for infinitely generated groups is not true, in general (for example, $\mathbb{Q}$ and valuation subgroup for a nonarchimedean valuation).

Lemma 2.3.2. — *Assume that $f \in \mathcal{AF}(A,S)$. Then*
- *for all subgroups $B \subset A$ one has $f_B \in \mathcal{AF}(B,S)$;*
- *if S is a ring then $sf + s' \in \mathcal{AF}(A,S)$ for all $s, s' \in S$;*
- *for every map $h : S \to S'$ one has $h \circ f \in \mathcal{AF}(A,S')$.*

Proof. — Evident from the definition. □

Lemma 2.3.3. — *Let $A \in \mathcal{A}_0$ and $f \in \mathcal{F}(A,S)$. Let $B \subset A$ be a subgroup of finite index. If $f_B \in \mathcal{AF}(B,S)$ then $f \in \mathcal{AF}(A,S)$.*

Proof. — Observe that $nA \subset B$ for some $n \in \mathbb{N}$. By Lemma 2.3.2, $f_{nA} \in \mathcal{AF}(nA,S)$. Now use the invariance of f. □

2.4. Orders. —

Remark 2.4.1. — Let $f \in \mathcal{F}(A, S)$ be such that for every subgroup $B \subset A$ with $\mathrm{rk}(B) \leq 2$ the restriction $f_B \in \mathcal{AF}(B, S)$. Then f defines a partial relation $\tilde{>}_f$ on A as follows: let $b, b' \in A$ with $f(b) \neq f(b')$ and consider the subgroup $B = \langle b, b' \rangle$. One of these elements, say b, is generic in B and the other is not. Then we define $b \tilde{>}_f b'$.

Lemma 2.4.2 (Definition). — *A function $f \in \mathcal{AF}(A, S)$ defines an* order $>_{f,A}$ *on A as follows:*

- *if $f(a) \neq f(a')$ then $a >_{f,A} a'$ iff $a \tilde{>}_f a'$ (that is, $f(a + a') = f(a)$);*
- *if $f(a) = f(a')$ then $a >_{f,A} a'$ iff there exists a $b \in A$ (a separator) such that $f(a) \neq f(b)$ and $a >_{f,A} b >_{f,A} a'$;*
- *finally, $a =_f a'$ if for all a'' we have $a'' >_{f,A} a$ iff $a'' >_{f,A} a'$.*

Notations 2.4.3. — We will write $>_f$ or $>$ and $\tilde{>}$ whenever A and f are clear from the context. We will also use the symbols $\geq$ and $\geq_f$.

Proof. — If $\mathrm{rk}(A) < \infty$, then for every element $a \neq 0$ there exists an $n(a)$ such that $a \in A_f^{n(a)} \setminus A_f^{n(a)+1}$. Then $a > b$ iff $n(a) < n(b)$. For general A, the correctness of the definition and the transitivity of $>$ are checked on finitely generated subgroups of A. For correctness, we assume that $f(a) = f(b)$ and consider the possibility that

$$a \,\tilde{>}\, c \,\tilde{>}\, b \,\tilde{>}\, c' \,\tilde{>}\, a$$

for two separators c, c' (leading to a contradiction). For transitivity, we may need to consider the possibility

$$a > b > c \geq_f a$$

(with separators, if necessary). □

Let A be an abelian group and $f \in \mathcal{AF}(A, S)$. Define the subsets:

$$A_f^\alpha = \{a \in A \,|\, a \geq_f \alpha\}$$

where α is (a representative of) the equivalence class in A with respect to the equivalence relation $=_f$.

Lemma 2.4.4. — *Assume that* $\mathrm{rk}(A) < \infty$ *and $f \in \mathcal{AF}(A, S)$. Then each A_f^α is a subgroup of A and (A_f^α) is a filtration on A in the sense of Definition 2.2.2. Moreover, f is constant on $\overline{A}_f^\alpha$ for all α.*

Proof. — Evident. □

REMARK 2.4.5. — If $\mathrm{rk}(A) < \infty$ then (A_f^α) coincides with the filtration (A_f^n) introduced in Remark 2.3.1. Notice that the filtration (A_f^α) is not functorial under restrictions. In general, if $f \in \mathcal{AF}(A, S)$ and $B \subset A$ is a proper subgroup then $A_f^\alpha \cap B \neq B_f^\alpha$. In general, for maps $h : S \to S'$ the filtration A_f^α does not coincide with $A_{h\circ f}^\alpha$. However, $A_{h\circ f}^\alpha$ can be reconstructed starting from A_f^α. We will be interested in the case when $S' = \mathbb{Z}/2$.

LEMMA 2.4.6. — *Let $f \in \mathcal{F}(A, S)$ be such that:*

- *for every B with $\mathrm{rk}(B) \leq 2$ the restriction $f_B \in \mathcal{AF}(B, S)$ (by Remark 2.4.1, this defines a partial relation $\tilde{>}$ on A);*
- *$\tilde{>}$ extends to an order $>$ on $A \setminus 0$ (transitivity);*
- *for all $a, a', a'' \in A$ such that $a > a'$ and $a > a''$ one has*

$$a > a' + a''.$$

Then $f \in \mathcal{AF}(A, S)$.

Proof. — Evident. As in Lemma 2.4.4, we obtain a filtration by groups. □

2.5. Rank 2 case. —

EXAMPLE 2.5.1. — A typical AF-function is given as follows. Let p be a prime number and $A = \langle a, a' \rangle$ with

$$\begin{array}{rcl} A_f^{2n} & = & \mathbb{Z}p^n a \oplus \mathbb{Z}p^n a' \\ A_f^{2n+1} & = & \mathbb{Z}p^n a \oplus \mathbb{Z}p^{n+1} a' \end{array}$$

with f taking two values on A: one value on $\overline{A}_f^{2n}$ and a different value on $\overline{A}_f^{2n+1}$.

LEMMA 2.5.2. — *Let $A = \mathbb{Z} \oplus \mathbb{Z}$ and $f \in \mathcal{AF}(A, S)$. Then f is one of the following*

- *f is constant on $A \setminus 0$;*
- *f is constant on $A \setminus \mathbb{Z}a$, for some $a \in A$;*
- *there exists a prime number p and a subgroup C of index p^k (for some $k \geq 0$) such that f is constant on $A \setminus C$ and f_C is as in the Example 2.5.1.*

NOTATIONS 2.5.3. — In the second (resp. the third) case we put

$$p(A) = p(A, f) := 0,$$

$$p(A) = p(A, f) := p.$$

Proof. — Assume that f is nonconstant on $A \setminus 0$. Then there exist two primitive elements $a, a' \in A$ such that $f(a) \neq f(a')$ (and $B := \langle a, a' \rangle$ is a subgroup of finite index in A). Then one of these generators, say a', lies in the subgroup B^1_f. This means that B/B^1_f is a cyclic group. If it is a free cyclic group, then the function f is of the second type.

If it is a finite group then there is a proper subgroup C of finite index in B such that C contains B^1_f and $[C : B^1_f] = p$ (for some prime p). The function f is constant on $C \setminus B^1_f$. Hence $C^1_f = B^1_f$. We have the diagram

$$\begin{array}{ccccccccccc} A & \supset & B & \supset & C & \supset & B^1_f & \supset & B^2_f & & \supset \dots \\ & & & & & & \| & & \| & & \\ & & & & C & \supset & C^1_f & \supset & C^2_f = pC & & \end{array}$$

Indeed, since the generic value of f on pC is equal to the generic value of f on C it is not equal to the generic value of f on C^1_f. It follows that $pC \subset C^2_f$ and since $[C^1_f : pC] = p$ we have $pC = C^2_f$. By invariance, the function f_C is as in the Example 2.5.1. Again by invariance, the index $[A : C]$ is a p-power and f (on A) is of the third type.

□

COROLLARY 2.5.4. — *Let A and f be as in Lemma 2.5.2. Then*

- *f takes at most two values on $A \setminus 0$;*
- *if $na \in A^1_f$ for some n with $\gcd(n, p(A)) = 1$ then $a \in A^1_f$;*
- *if $A = \langle a_1, a_2 \rangle$ and $a_1 - a_2 = p(A)a_3$ ($a_3 \in A$) then $f(a_1) = f(a_2)$;*
- *if $|A/A^1_f| = 2$ and $a \in A$ is primitive then $f(a + 2a') = f(a)$ for all $a' \in A$;*
- *if $|A/A^1_f| > 2$ then A has a basis $\{a_1, a_2\}$ such that all three elements $a_1, a_2, a_1 + a_2$ are generic.*

LEMMA 2.5.5. — *Let $A = \mathbb{Z}/q \oplus \mathbb{Z}/q$ (with q prime) and $f \in \mathcal{AF}(A, S)$. Then f (considered as a function on $\mathbb{P}^1(\mathbf{F}_q)$) is constant on the complement to some point $P \in \mathbb{P}^1(\mathbf{F}_q)$.*

Proof. — See the proof of Lemma 2.5.2. □

LEMMA 2.5.6. — *Let A and $f \in \mathcal{F}(A, \mathbb{Z}/2)$ be such that:*
- *A has a basis (a, b) with $f(a) = f(a+b) \neq f(b)$;*
- *f is invariant (cf. Definition 2.2.4);*
- *f satisfies a functional equation: for all $a', b' \in (A \setminus 0)$ with*

$$f(a') = f(a),\ f(b') = f(b) \text{ and } f(a') = f(a' + b')$$

one has

$$f(ma' + nb') = f(ma' + (n + km)b') \tag{2.1}$$

for all $k, m, n \in \mathbb{Z}$.

Then $f \in \mathcal{AF}(A, \mathbb{Z}/2)$.

Proof. — We have a decomposition $A = A_a \cup A_b$ into two subsets (preimages of $0, 1$). We will generally use the letter a for elements in A_a and b for elements in A_b. Thus $f(a') = f(a) \neq f(b) = f(b')$ for all $a, a', b, b' \in A$.

First we consider the case $A \in \mathcal{A}_q$. By the functional equation,

$$f(a + nb) = f(a)$$

for all $n \in \mathbb{Z}$. By invariance,

$$f(ma + nb) = f(a)$$

for all $m, n \in \mathbb{Z}_{(q)}$. Thus f is constant on $A \setminus A^1_f$ (where $A^1_f = \mathbb{Z}b$).

Now we turn to the case $A \in \mathcal{A}_0$. Denote by $A^1_f = \langle A_b \rangle \subset A$ the subgroup in A generated by elements $b' \in A_b$. We claim that A^1_f is a *proper* subgroup of A (and clearly, $f(a_1) = f(a)$ for all $a_1 \in (A \setminus A^1_f)$).

Consider a pair of elements

$$\begin{aligned} b_1 &= m_1 a + n_1 b, \\ b_2 &= m_2 a + n_2 b. \end{aligned}$$

We can assume that $m_1, m_2 > 0$. Let

$$d_A := \min(\gcd(m_1, m_2))$$

be the minimum over all pairs $(b_1, b_2) \in A_b \times A_b$ (with positive m_1, m_2).

Assume first that there exists a b_1 such that $b_1 = d_A a + n_1 b$ (for some $n_1 \in \mathbb{Z}$). This is impossible for $d_A = 1$, by the functional equation. Now consider the case $d_A > 1$. In this case A^1_f is a proper subgroup of A (since for all $b_2 = m_2 a + n_2 b$ the coefficient m_2 is divisible by d_A and consequently for all $ma + nb \in A^1_f$ the coefficient m is divisible by d_A).

Now assume that there are no such b_1. Choose a pair

$$\begin{aligned} b_1 &= d_A m_1 a + n_1 b, \\ b_2 &= d_A m_2 a + n_2 b \end{aligned}$$

as above (such that $(m_1, m_2) = 1$) and integers $l_1, l_2 \in \mathbb{Z}$ such that $m_1 l_1 + 1 = m_2 l_2$. Then, (using invariance),

$$\begin{aligned} f(d_A r a + e_1 b) &= f(d_A(r+1)a + e_2 b) \\ &= f(b) \end{aligned}$$

for some $e_1, e_2 \in \mathbb{Z}$. Pick the smallest positive r_0 with this property. Then $r_0 > 1$ (since $f(d_A a + nb) = f(a)$ for all n, by assumption) and

$$f(d_A(r_0 - 1)a + nb) = f(a)$$

for all $n \in \mathbb{Z}$. Therefore, (using functional equation and invariance),

$$\begin{aligned} f(a) &= f(d_A(r_0 - 1)a + (2e_1 - e_2)b) \\ &= f((-d_A a + (e_1 - e_2)b) + (d_A r_0 a + e_1 b)) \\ &= f(d_A(r_0 + 1)a + e_2 b) \\ &= f(b), \end{aligned}$$

contradiction.

Thus A^1_f is a proper subgroup of A and $a_1 \in A_a$ for all $a_1 \notin A^1_f$. Now consider the subgroup

$$A^2_f := \langle A^1_f \cap A_a \rangle$$

(generated by $a_2 \in A^1_f$ with $a_2 \in A_a$). We claim that A^2_f is a proper subgroup of A^1_f. (Warning: the conditions of the Lemma are *not* symmetrical with respect to a and b.)

First observe that there exists a basis a', b' of A^1_f such that

$$f(a' + b') = f(b)$$

(otherwise, the subgroup $\langle A_b \rangle$ would be a proper subgroup in A^1_f, contradiction). We fix such a basis and claim that

$$f(ra' + b') = f(b)$$

for all $r \in \mathbb{Z}$. Indeed, if this is not the case then there exists a positive integer $r_0 > 1$ such that

$$\begin{array}{rcl} f(a) & = & f(r_0 a' + b'), \\ f((r_0 - 1)a' + b') & = & f(b). \end{array}$$

Then

$$\begin{aligned} f(a) &= f(a' + ((r_0 - 1)a' + b')) \\ &= f(a' - ((r_0 - 1)a' + b')) \\ &= f((r_0 - 2)a' + b') \end{aligned}$$

(here we used the functional equation, and the invariance). This contradicts the minimality of r_0. Similar argument works for $r < 0$.

Consider the set of pairs

$$\begin{array}{rcl} a_1 & = & m_1 a' + n_1 b' \\ a_2 & = & m_2 a' + n_2 b' \end{array}$$

with positive n_1, n_2 and denote by d_B the smallest $\gcd(n_1, n_2)$ on this set.

Assume that $d_B > 1$ and that there exists an $a_1 = m_1 a' + d_B b'$. Then for every $a_2 = m_2 a' + n_2 b' \in A^1_f$ the coefficient n_2 is divisible by d_B and A^2_f is a proper subgroup.

Now we can assume that

$$f(ma' + d_B b') = f(b)$$

for all $m \in \mathbb{Z}$. Choose a pair a_1, a_2 such that $\gcd(n_1, n_2) = d_B$. Then, (by invariance),

$$\begin{aligned} f(a) &= f(r_1 a' + e d_B b') \\ &= f(r_2 a' + (e+1) d_B b') \end{aligned}$$

for some $r_1, r_2 \in \mathbb{Z}$ and $e > 0$. Pick the smallest $e_0 > 1$ with this property. Then, (using the fact that

$$f((r_2 - r_1)a' + d_B b') = f(b)$$

and the functional equation), we get

$$\begin{aligned} f(a) &= f((r_1 a' + e_0 d_B b') + (r_2 - r_1)a' + d_B b') \\ &= f((2r_1 - r_2)a' + (e_0 - 1) d_B b'). \end{aligned}$$

This contradicts the minimality of e_0.

It follows that the subgroup $A_f^2 \subset A_f^1$ is a proper subgroup and f takes the value $f(b)$ on the complement $A_f^1 \setminus A_f^2$.

Since A_f^2 has a basis (a'', b'') with

$$f(a'') = f(a'' + b'') \neq f(b''),$$

we can apply the inductive step to A_f^2. □

2.6. Rank 3 case: $\mathcal{A}_q$. —

PROPOSITION 2.6.1. — *Let $q > 2$ be a prime number, $A = \mathbb{Z}/q \oplus \mathbb{Z}/q \oplus \mathbb{Z}/q$ and $f \in \mathcal{F}(A, \mathbb{Z}/2)$. Assume that for all subgroups $C \subset A$ with* $\mathrm{rk}(C) \leq 2$ *we have $f_C \in \mathcal{AF}(C, \mathbb{Z}/2)$. Then $f \in \mathcal{AF}(A, \mathbb{Z}/2)$.*

Proof. — We can consider f as a function on $\mathbb{P}(A)$. By Lemma 2.5.5, for every $C \subset A$ with $\mathrm{rk}(C) = 2$ the restriction f_C is either constant on $\mathbb{P}(C) \subset \mathbb{P}(A)$ or constant everywhere except one point. Let L_i be the set of lines $\ell \subset \mathbb{P}(A)$ such that the generic value of f_ℓ is i (for $i = 0, 1$). Assume that f is nonconstant on $\mathbb{P}(A)$. If L_0 is empty then there exists only one point $P \in \mathbb{P}(A)$ with $f(P) = 0$ (otherwise we can draw a line of type L_0 through two such points, and 0 must be the generic value on this line, contradiction). In this case $f \in \mathcal{AF}(A, \mathbb{Z}/2)$. Thus we can assume that both L_0 and L_1 are nonempty and that, for example, $|L_0| \geq |L_1|$. Then $|L_0| \geq (q^2 + q + 1)/2$. Choose an $\ell_1 \in L_1$.

There are two cases: f is constant on $\ell_1 \in L_1$ or f is nonconstant on some line ℓ_1. In both cases there exists at least one point $P \in \ell_1$ such that $f(P) = 1$ and such that there are two distinct lines ℓ_0, ℓ_0' passing through $P \subset \ell_1$.

Indeed, assume in both cases that through every generic point of ℓ_1 there passes only one line of type L_0. In the first case the total number of lines of type L_0 is bounded by $q+1$, contradiction to the assumption that $|L_0| \geq (q^2+q+1)/2$. In the second case, there are at most q lines of type L_0 passing through the nongeneric point and, by assumption, at most 1 line of type L_0 passing through each of the remaining q generic points of ℓ_1 (every line in L_0 intersects ℓ_1 in one point). Thus their number is bounded by $2q < (q^2 + q + 1)/2$, contradiction.

For any pair of points $Q \in \ell_0 \backslash P$, $Q' \in \ell_0' \backslash P$ we have $f(Q) = f(Q') = 0$. The lines through Q, Q' are all of type L_0. Pick a point $P' \in \ell_1$ such that $P \neq P'$ and $f(P') = 1$ (such a point exists since ℓ_1 has at least 3 points and the generic value of f on ℓ_1 is 1). Every line through P' which does not pass through P is of type L_0 (since it intersects ℓ_0, ℓ_0' in distinct points). The family of such lines covers $\mathbb{P}(A) \setminus \ell_1$. It follows that the value of f on $\mathbb{P}(A) \setminus \ell_1$ is 0 and that $f \in \mathcal{AF}(A, \mathbb{Z}/2)$. $\square$

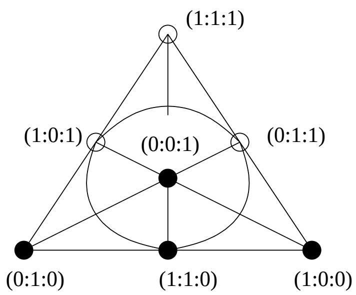
2.7. Exceptional lattices. —

EXAMPLE 2.7.1. — Let $\bar{A} = \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and $\bar{f} \in \mathcal{F}(\bar{A}, \mathbb{Z}/2)$. Assume that for all subgroups $\bar{C} \subset \bar{A}$ of rank 2 one has $f_{\bar{C}} \in \mathcal{AF}(\bar{C}, \mathbb{Z}/2)$ but $\bar{f} \notin \mathcal{AF}(A, \mathbb{Z}/2)$. Then A has a basis $\bar{e}_1, \bar{e}_2, \bar{e}_3$ such that

$$f(\bar{e}_1 + \bar{e}_3) = f(\bar{e}_2 + \bar{e}_3) = f(\bar{e}_1 + \bar{e}_2 + \bar{e}_3) = 0 \neq f(\bar{x})$$

for all other $\bar{x}$ (up to addition of 1 modulo 2).

Indeed, since $\mathbb{P}^2(\mathbb{Z}/2)$ has seven points it suffices to assume that f takes the same value on three of them and a different value on the remaining four. If the three points are on a line we have an AF-function. If not we get the claim. (In particular, such an f contradicts the conclusion of Lemma 2.6.1.)



Any function on $A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ induced from the function on $\bar{A}$ considered above has the property that for every $C \subset A$ of rank ≤ 2 $f_C \in \mathcal{AF}(C, \mathbb{Z}/2)$.

We give another example of a function on $\mathbb{Z}^3$ with the same property.

EXAMPLE 2.7.2. — We keep the notations of Example 2.7.1. Choose a basis e_1, e_2, e_3 of $A = \mathbb{Z}^3$. Consider the projection $A \to \bar{A} = A/2A$, taking e_j to $\bar{e}_j$. The function f is defined by its values on primitive elements

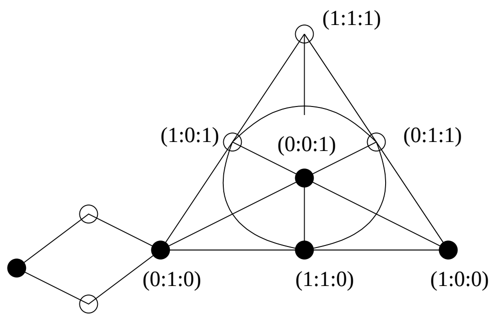
$$a = n_1e_1 + n_2e_2 + e_3n_3.$$

If $(n_1, n_2, n_3) \neq (0, 1, 0)$ modulo 2 then

$$f(a) = \bar{f}(\bar{a})$$

(where $\bar{f}$ was defined in Example 2.7.1). Otherwise,

$$f(n_1e_1 + n_2e_2 + n_3e_3) = \begin{cases} 0 & \text{if} \quad n_1 = 0 \mod 4 \\ 1 & \text{if} \quad n_1 = 2 \mod 4 \end{cases}$$



2.8. Rank 3 case: $\mathcal{A}_0$. —

Let A be an abelian group and $f \in \mathcal{F}(A, \mathbb{Z}/2)$. We have a decomposition of the set $A = A_a \cup A_b$ (preimages of 0 or 1, respectively). We will say that A has a *special basis* (with respect to f) if $A = \langle a_1, a_2, b_1 \rangle$ with

$$a_1, a_2, a_1 + b_1, a_2 + b_1 \in A_a, \quad b_1 \in A_b.$$

Proposition 2.8.1. — *Let $A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ and $f \in \mathcal{F}(A, \mathbb{Z}/2)$. Assume that A has a special basis (with respect to f) and that for every subgroup C with* $\mathrm{rk}(C) \leq 2$ *one has $f_C \in \mathcal{AF}(C, \mathbb{Z}/2)$. Then there is a proper subgroup $A^1 \subset A$ such that f is constant on $A \setminus A^1$.*

Proof. — The proof is subdivided into a sequence of Lemmas.

Lemma 2.8.2. — *Assume A has a special basis $\{a_1, a_2, b_1\}$. Then A does not have a basis $\{b_1, b_2, b_3\}$ with $b_1, b_2, b_3 \in A_b$.*

Proof. — Assume the contrary. Then

$$C := \langle a_1 + e_1 b_1, a_2 + e_1' b_1\rangle = \langle b_2, b_3\rangle$$

for some $e_1, e_2' \in \mathbb{Z}$. We know that

$$f(a_1 + e_1 b_1) = f(a_2 + e_1' b_1) = f(a)$$

for all e_1, e_1'. Contradiction to, for example, 2.5.2: C cannot have such pairs of generators. $\square$

LEMMA 2.8.3. — *Assume that A has a special basis $\{a_1, a_2, b_1\}$. Then*

$$\langle A_b\rangle \subset A$$

is a proper subgroup.

Proof. — Consider the projection

$$\mathrm{pr} \,:\, A \to \hat{A} := A/\langle b_1\rangle.$$

Assume that there exists an element

$$b = n_1 a_1 + n_2 a_2 + m_1 b_1 \in A_b$$

such that $\hat{b} = n_1 a_1 + n_2 a_2$ is primitive in $\hat{A} = \langle a_1, a_2\rangle$. Then it is part of a basis $\{\hat{x}, \hat{b}\}$ of $\hat{A}$. Take any x in the preimage $\mathrm{pr}^{-1}(\hat{x})$. Then

$$A = \langle x, b, b_1\rangle.$$

By Lemma 2.8.2, $x \notin A_b$, so we will denote it by a. Assume that

$$a + mb + m_1 b_1 \in A_b$$

for some $m, m_1 \in \mathbb{Z}$. This contradicts 2.8.2, since

$$A = \langle a + mb + m_1 b_1, b, b_1\rangle.$$

.

Consider the set R of all $r \in \mathbb{N}$ such that

$$b_r := ra + mb + m_1 b_1 \in A_b$$

(for some $m, m_1 \in \mathbb{Z}$). We have seen that $r > 1$. We claim that $r, r' \in R$ implies that $g := \gcd(r, r') \in R$. Indeed, assume the contrary and choose $l, l' \in \mathbb{Z}$ so that $g = lr - l'r'$. By invariance, $lb_r, l'b_{r'} \in A_b$. In the subgroup $B := \langle b_r, b_{r'}\rangle$ the element $a_g := lb_r - l'b_{r'} \in A_a \cap B$ is nongeneric. This implies that

$$b_r - na_g \in A_b \cap B$$

for all n. This leads to a contradiction and the claim follows. Thus we have proved that for all $b' \in A_b$ the corresponding coefficients n_1' are either zero or have a common divisor > 1. Consequently, $\langle A_b\rangle$ is a proper subgroup.

Now we assume that $\mathrm{pr}(A_b)$ does not contain primitive elements of $\langle a_1, a_2\rangle$, in other words: for all primitive $a \in \langle a_1, a_2\rangle$ and all $m_1 \in \mathbb{Z}$ one has

$$a + m_1 b_1 \in A_a.$$

For two pairs of (a, m_1) and (a', m_1') with primitive a, a' such that

$$\langle a_1, a_2\rangle = \langle a, a'\rangle$$

consider the subgroups

$$\begin{array}{rcl} D & := & \langle a, m_1 b_1\rangle \\ D' & := & \langle a', m_1' b_1\rangle \end{array}$$

and assume that both $p = p(D), p' = p(D') \neq 0$.

We claim that $p = p'$. Indeed, assume the contrary. By Lemma 2.5.2, there exist integers k, k' such that

$$f(qa + m_1 b_1) = f(q'a' + m_1' b_1) = f(b_1),$$

where $q = p^k, q' = p'^{k'}$ for some $k, k' \in \mathbb{N}$. Now consider the group

$$E := \langle qa + m_1 b_1, q'a' + m_1' b_1\rangle.$$

For all $n_1 \in \mathbb{Z}$ coprime to p' and all $n_1' \in \mathbb{Z}$ coprime to p the element

$$n_1(qa + m_1 b_1) + n_1'(q'a' + m_1' b_1) = n_1 qa + n_1' q'a' + (n_1 m_1 + n_1' m_1')b_1 \in A_a,$$

(since $\mathrm{pr}(A_b)$ does not contain primitive elements). The subset of such elements cannot be contained in a proper subgroup of E. On the other hand, it has to be: both generators of E are in A_b and $f \in \mathcal{AF}(E, \mathbb{Z}/2)$. Contradiction to the assumption that $p \neq p'$. Since for any pair of primitive a, a' generating a sublattice of finite index in $\langle a_1, a_2\rangle$ there exists a primitive element a_0 such that

$$\langle a, a_0\rangle = \langle a', a_0\rangle = \langle a_1, a_2\rangle$$

we conclude that for the corresponding D as above either $p(D) = 0$ or $p(D) = p$ for some fixed prime p.

To finish the proof of the lemma, consider an element

$$na + m_1 b_1 \in A_b$$

for some $n > 1$, some primitive $a \in \langle a_1, a_2 \rangle$ and some m_1 (coprime to $n > 1$). There are two possibilities: either n is zero or n is divisible by a fixed prime p (which is independent of the coefficients). It follows that $\langle A_b \rangle \subset A$ is a proper subgroup. $\square$

This concludes the proof of Proposition 2.8.1 $\square$

PROPOSITION 2.8.4. — *Let $A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ and $f \in \mathcal{F}(A, \mathbb{Z}/2)$. Assume that A does not have a special basis (with respect to f) and that for all subgroups $C \subset A$ of rank 2 one has $f_C \in \mathcal{AF}(C, \mathbb{Z}/2)$. Then f (up to addition of 1 modulo 2) is*

Case 1: as in Example 2.7.1 or

Case 2: as in Example 2.7.2.

Proof. — Assume first that for all subgroups $C \subset A$ of rank 2 the function f is either constant on $C \setminus 0$ or $|C/C_f^1| = 2$. Then f is induced from $A/2A$. Indeed, consider the subgroup $C := \langle x, y \rangle$ (with $x \in A$ primitive and y nonproportional to x). It suffices to consider the case when f is nonconstant and thus $|C/C_f^1| = 2$. By Corollary 2.5.4, if $x - y = 2z$ we have

$$f(x) = f(y),$$

so that f is induced from $A/2A$.

Now we assume that there exists a subgroup C of rank 2 such that $|C/C_f^1| > 2$ and f has generic value, say $f(a)$ on C. By Corollary 2.5.4, we can choose a basis $C = \langle a_1, a_2 \rangle$ such that all three $a_1, a_2, a_1 + a_2 \in A_a$. We will fix such a basis. For any $d \in A$ such that $\langle d, C \rangle = A$ consider the shift $d + C \subset A$.

1. We claim that both

$$(d + C) \cap A_a \neq \emptyset \text{ and } (d + C) \cap A_b \neq \emptyset.$$

Indeed, assume this is not so and choose, in the first case, some element $b \in d + C$. Then $\{b + a_1, b + a_2, a_1\}$ is a special basis of A. In the second case, for any $a \in d + C$ we get a special basis $\{a, a_1, b_1\}$, (where $b_1 \in A_b$ is some nongeneric element in C). Contradiction.

For any pair of generators $\{a_1', a_2'\}$ of C (without the assumption that $a_1' + a_2' \in A_a$) we have:

2. (Forbidden triangle.) There are no $b \in (d+C) \cap A_b$ such that both

$$b + a_1', b + a_2' \in A_a.$$

Indeed, $\{a_1', a_2', b\}$ would be a special basis for A.

3. (Forbidden square.) There are no $b \in (d+C) \cap A_b$ such that all three

$$b + a_1', b + a_2', b + a_1' + a_2' \in A_b.$$

Indeed, $\{b, b + a_1', a_2'\}$ would be a special basis for A.

4. Choose any element $b \in d + C$ and consider the subset $\{b + na_1\}$ (with $n \in \mathbb{N}$). Than there are two possibilities: either $b + na_1 \in A_b$ for all $n \in \mathbb{N}$ or there exists an $n_0 > 0$ such that

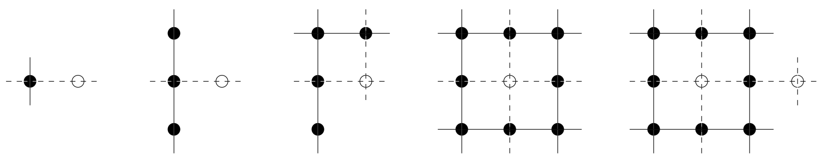
$$b + n_0 a_1 \in A_b \text{ and } b + (n_0 + 1)a_1 \in A_a.$$

Let us consider the second case: rename $b + n_0 a_1$ to b.

Then $b + a_1 \in A_a$. By 2, $b + a_2, b - a_2 \in A_b$. By 2 and by our assumption that $a_1 + a_2 \in A_a$, we have $b + a_1 + a_2 \in A_b$. By 2 (applied to $b - a_2$), we have $b + a_1 - a_2 \in A_b$; similarly,

$$b + 2a_1, b + 2a_1 - a_2, b + 2a_1 + a_2 \in A_b.$$

By 3, applied to $b + a_1 - a_2$, we have $b + 3a_1 \in A_a$.



Clearly, a pattern is emerging: we can rename $b + 2a_1$ to b and repeat the argument. Further, notice the symmetry with respect to a_1 and a_2, as well as the symmetry with respect to ± 1. In conclusion, we have:

For any $a_3 \in A_a$ such that $\langle a_1, a_2, a_3 \rangle = A$ we have

$$n_1 a_1 + n_2 a_2 + a_3 \in A_a$$

iff both n_1 and n_2 are divisible by 2.

5. We claim that for any primitive $x \in C$ and $c \in C$ we have $f(x+4c) = f(x)$. Indeed, consider the lattice

$$E := \langle x, a_3 + 2c \rangle.$$

In E, we have two sublattices of index 2:

$$\begin{array}{rcl} E' & := & \langle a_3 + 2c, a_3 + 2c + 2x \rangle \\ E'' & := & \langle a_3 + 2c + x, a_3 + 2c - x \rangle. \end{array}$$

The generic values of f on these sublattices are different (by 4). It follows that one of them is equal E^1_f. By Corollary 2.5.4, we have $f(x + 2y) = f(x)$ for every $y \in E$, in particular

$$f(x + 2a_3 + 4c) = f(x).$$

Now consider the lattice

$$G := \langle x', a_3 \rangle,$$

where $x' = x + 4c$, and the sublattices

$$\begin{array}{rcl} G' & := & \langle a_3, a_3 + 2x' \rangle \\ G'' & := & \langle a_3 + x', a_3 - x' \rangle. \end{array}$$

Both have index 2 in G and have different generic values. If follows that $|G/G^1_f| = 2$. In particular,

$$f(x' + 2a_3) = f(x + 4c + 2a_3) = f(x + 4c).$$

Combining with the result for E we get our claim. It follows that for every sublattice $C \subset A$ of rank 2 $p(C) = 2$ and, moreover, that $|C/C^1_f|$ is equal to 2 or 4. If $|C/C^1_f| = 2$ for every subgroup C of rank 2 we get a contradiction to our assumption (this leads to Case 1).

6. We can assume that $|C/C^1_f| = 4$. We claim that f is as in Case 2. First of all,

$$f(n_1a_1 + n_2a_2 + m_3a_3) = f(n_1a_1 + n_2a_2 + a_3)$$

for all odd m_3 (equal to $f(a_3)$ iff $n_1 = n_2 = 0$ modulo 2, by 4). Next, $f(2m_3a_3 + c) = f(c)$ for all $m_3 \in \mathbb{Z}$ and all primitive $c \in C$. Since

$$f_C(x + 4c) = f(x)$$

for all primitive x and all $c \in C$ we conclude that either f_C is constant, or induced from $C/2C$ or as in Case 2. The first two possibilities contradict our assumptions on C. $\square$

3. Reductions

3.1. Reduction of S. —

LEMMA 3.1.1. — *Let $f \in \mathcal{F}(A, S)$. Assume that for all $h : S \to \mathbb{Z}/4$ the function $h \circ f \in \mathcal{AF}(A, \mathbb{Z}/4)$. Then $f \in \mathcal{AF}(A, S)$.*

Proof. — The invariance is obvious (if $f(na) \neq f(a)$ for some n, a then define h so that $h \circ f(na) \neq h \circ f(a)$, leading to a contradiction). Assume that there exist elements $a, b \in A$ such that $f(a), f(b)$ and $f(a+b)$ are pairwise distinct. Define h such that

$$\begin{array}{lcl} h \circ f(a) & = & 0, \\ h \circ f(b) & = & 1, \\ h \circ f(a+b) & = & 2. \end{array}$$

Then, by Lemma 2.4.2, $h \circ f \notin \mathcal{AF}(A, \mathbb{Z}/4)$, contradiction. We see that for any $a, b \in A$ with $f(a) \neq f(b)$ either $f(a+b) = f(a)$ or $f(a+b) = f(b)$. This defines a partial relation $\tilde{>}$ on A (as in Remark 2.4.1).

We need to check that $\tilde{>}$ can be extended to an order on A. Let $a, a' \in A$ be such that $f(a) = f(a')$. If there is no $b \in A$ such that $f(b) \neq f(a)$ then f is constant and thus $\in \mathcal{AF}(A, S)$. If for all such $b \in A$ we have $a \tilde{>} b$ and $a' \tilde{>} b$ then $a =_f a'$. Otherwise, b is a separator and we can assume that $a \tilde{>} b \tilde{>} a'$. Assume that for some other separator b' we have $a' \tilde{>} b' \tilde{>} a$. Let

$$\begin{array}{lcl} h \circ f(a) & = & 0, \\ h \circ f(b) & = & 1 \end{array}$$

and put (if $f(b) \neq f(b')$)

$$h \circ f(b') = 2.$$

By assumption, $h \circ f \in \mathcal{AF}(A, \mathbb{Z}/4)$, contradiction (we use that either $f(a) = f(a+b)$ or $f(b) = f(a+b)$, etc). Thus we have a correctly defined relation $>$ on A.

Now we check the transitivity of $>$. Assume that we have elements $a, b, c \in A$ such that $a >_f b > c$. Assume that $c \geq a$. If the values of f on a, b, c are pairwise distinct, put

$$\begin{aligned} h \circ f(a) &= 0, \\ h \circ f(b) &= 1, \\ h \circ f(c) &= 2. \end{aligned}$$

Since $h \circ f \in \mathcal{AF}(A, S)$ we get a contradiction. If $f(a) = f(b)$, let a' be their separator; if $f(b) = f(c)$ let b' be their separator and if $f(c) = f(a)$, let c' be their separator: $c \geq c' \geq a$. Then there is a map $h : S \to \mathbb{Z}/4$ such that $h \circ f \notin \mathcal{AF}(A, \mathbb{Z}/4)$, contradiction.

Finally, we need to check that if $a > b$ and $a > b$, then $a > b + c$. Again, we can introduce separators, if necessary, and proceed as above.

To conclude we apply Lemma 2.4.6. $\square$

Lemma 3.1.2. — *Let A be a finitely generated group, S a finite set and $f \in \mathcal{F}(A, S)$. Assume that for all $h : S \to \mathbb{Z}/2$ one has $h \circ f \in \mathcal{AF}(A, \mathbb{Z}/2)$. Then $f \in \mathcal{AF}(A, S)$.*

Proof. — As above, the invariance of f is obvious. Following the proof of Lemma 3.1.1, observe that for all $a, b \in A$ with $f(a) \neq f(b)$ either $f(a+b) = f(a)$ or $f(a+b) = f(b)$. Thus we have a partial relation $\tilde{>}$ on these pairs as in 2.4.1.

Let $h : S \to \mathbb{Z}/2$ be a nonconstant map and

$$S(h) := \{s \in S \mid \exists\, a \in A \setminus A^1_{h \circ f} \text{ with } f(a) = s\}.$$

Let h_0 be a map such that

$$|S(h_0)| = \min_h(|S(h)|).$$

We can assume that $S = \{1, ..., n\}$ and that $S(h_0) = \{1, ..., k_0\}$.

Assume that $1 < k_0 < n$. Let $a_1, ..., a_{k_0}$ be some elements in $A \setminus A^1_{h_0 \circ f}$ with $f(a_j) = j$. Then, for all $j \in S(h_0)$ and all $i \notin S(h_0)$ we have $a_j > x_i$ for all $x_i \in A$ with $f(x_i) = i$.

Let h' be the map sending each element in $\{n, 2, ..., k_0\}$ to 0 and each element in $\{1, k_0+1, ..., n-1\}$ to 1. One of the values is generic for $h' \circ f$. Assume that 0 is the generic value for $h' \circ f$. Then $a_n \notin A \setminus A^1_{h' \circ f}$ (indeed, if a_n were generic then $a_n > x_1$ for all x_1 with $f(x_1) = 1$, contradiction to the previous). But then $|S(h')| \leq k_0 - 1$, contradiction to the minimality of k_0.

Assume that 1 is the value of a generic element for $h' \circ f$. Similarly, the elements a with $f(a) \in \{k_0 + 1, ..., n-1\}$ cannot be generic for $h' \circ f$. It follows that generic elements for $h' \circ f$ are mapped to $1 \in S$. Contradiction to the assumption that $1 < k_0$.

If $k_0 = 1$ then

$$A^1 := \{a \in A \mid f(a) \neq 1\}$$

is a proper subgroup and f is constant on $A \setminus A^1$. Applying the same argument to A^1 we obtain a filtration (A^n) such that f is constant on $\overline{A}^n$ for all $n \in \mathbb{N}$. □

3.2. Reduction of the rank. —

LEMMA 3.2.1. — *Let A be an abelian group and $f \in \mathcal{F}(A, S)$. If for all subgroups $B \subset A$ with* $\mathrm{rk}(B) \leq 3$ *the restriction $f_B \in \mathcal{AF}(B, S)$ then $f \in \mathcal{AF}(A, S)$.*

Proof. — By definition, it suffices to consider finitely generated A. Invariance of f is clear. By Lemmas 3.1.1 and 3.1.2, it suffices to assume $S = \mathbb{Z}/2$. As in Remark 2.4.1 and in the proof of Lemma 3.1.1, we can define a partial relation $\tilde{>}$ on A, which by assumption and by Lemma 2.4.2 extends to an order on subgroups of rk ≤ 3 (see Lemma 2.4.2). We will denote the induced order on subgroups $C \subset A$ by $>_C$. We need to show that this order extends compatibly to A. Notice that for $C \subset D \subset A$ the order $>_D$ is stronger than the order $>_C$.

We have a decomposition of $A = A_a \cup A_b$ (preimages of $0, 1$). As in the proof of Lemma 2.5.6, we will use the letter a (resp. b) for elements in A_a (resp. A_b). The proof is subdivided into a sequence of Sublemmas.

SUBLEMMA 3.2.2. — *(Correctness) There are no a, a' and b, b' such that*

$$a \tilde{>} b \tilde{>} a' \tilde{>} b' \tilde{>} a.$$

Proof. — Introducing the subgroups

$$\begin{aligned} C &:= \langle a, b, a' \rangle \\ D &:= \langle a', b', a \rangle \\ M &:= \langle b, b', a + a' \rangle \\ N &:= \langle b', a' + b, a \rangle \end{aligned}$$

we obtain

$$a >_C b + a' >_C a' \text{ and } a' >_D b' + a >_D a.$$

It follows that

$$f(a+a') = f(a+a'+b) = f(a), \tag{3.1}$$

$$f(a'+a+b') = f(a'), \tag{3.2}$$

$$f(b+a') = f(b) \tag{3.3}$$

By Equations 3.1 and 3.2, neither b nor b' can be generic in M. Thus $a+a' >_M b, b'$ and

$$f(a+a'+b+b') = f(a+a') = f(a). \tag{3.4}$$

On the other hand, in N, the element a is not generic: $f(a+b') = f(b')$. Since $f(b+a') = f(b)$ and $f(b+a'+a) = f(a)$ (by 3.1) and since a is not generic, the element $b+a'$ cannot be generic. It follows that b' is generic in N and

$$f(b' + (b+a') + a) = f(b'),$$

contradiction to 3.4. □

The sublemma implies that we can extend $\tilde{>}$ to a relation $>$ on the whole A.

Sublemma 3.2.3. — *(Transitivity) If $x > y > z$ then $x > z$.*

Proof. — We have to consider 4 cases:

Case 1. $a > b > a'$. Transitivity follows from the definition.

Case 2. $a > b > b'$. Let a' be the separator. Assume $f(b'+a) = f(b)$. Then $b' > a$ and we have a contradiction to Sublemma 3.2.2. Thus $f(b'+a) = f(a)$ and $a > b'$.

Case 3. $a > a' > b'$. Let b be the separator. Again, if $b' > a$ we get a contradiction to Sublemma 3.2.2.

Case 4. $a > a' > a''$. Denote by b the separator between a and a'. We have $a > b > a' > a''$. Applying case 2 (with a's and b's interchanged), we get $b > a''$. Thus $a > a''$ (by the definition). □

Sublemma 3.2.4. — *(Additivity) If $x, y, z \in A$ and $x > y$ and $x > z$ then $x > y + z$.*

Proof. — We are looking at the following cases:

Case 1. $a > b, b'$. Neither b nor b' can be generic in the subgroup $\langle a, b, b'\rangle$. Thus a is generic and the claim follows.

Case 2. $a > b$ and $a > b' > a'$. Then

$$f(b' \pm a') = f(b') \text{ and } f(a + b' + a') = f(a).$$

Case 2.1. $f(b + a') = f(b)$. Consider the subgroup $\langle a, b + a', b\rangle$. The element b cannot be generic since $f(a + b) = f(a)$. It follows that $b + a'$ cannot be generic since

$$f(b + a' - b) = f(a') \neq f(b + a').$$

Thus a is the generic element and $a > b + a'$.

Case 2.2. $f(b + b') = f(b)$. Apply Case 1: $a > (b + b') - (b' - a')$.

Case 2.3. $f(b + a') = f(a)$, $f(b + b') = f(a)$. Consider the subgroup $\langle b, b', a'\rangle$. The element a' cannot be generic since $f(a' + b') = f(b')$. The element b cannot be generic since $f(b + a') = f(a)$. Finally, b' cannot be generic since $f(b + b') = f(a)$. Contradiction.

Case 3. $a > b' > a'$ and $a > b'' >_f a''$.

Case 3.1. $f(b' + a'') = f(b')$. Consider $\langle a, b', a''\rangle$: b' is nongeneric, therefore, a'' is also nongeneric - it follows that a is generic and that $a > b' + a''$. Consider $\langle a, b', a'\rangle$: again a is generic and b', a' are nongeneric, thus $a > (a' - b')$. Now we can apply case 1 or 2, depending on the value of $f(a' - b')$.

Case 3.2. By symmetry, we can assume that both

$$f(b' + a'') = f(a' + b'') = f(a).$$

Combining with the assumption of Case 3 we obtain

$$a'' > b' > a' > b'' > a'',$$

contradiction to Sublemma 3.2.2. □

Now we apply Lemma 2.4.6 to conclude the proof of Lemma 3.2.1. □

3.3. The exceptional case. —

LEMMA 3.3.1. — *Let $A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ and $f \in \mathcal{F}(A, S)$ be a function such that*

- *for every rank 2 sublattice $C \subset A$ we have $f_C \in \mathcal{AF}(C, S)$;*

- *$f \notin \mathcal{AF}(A, S)$;*
- *f does not have a special basis.*

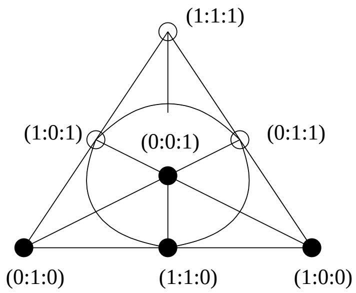
Then f takes exactly two values on A. Moreover, f is either as in Example 2.7.1 or as in Example 2.7.2.

Proof. — We can assume that $f : A \to S$ is surjective. By Lemma 3.1.2, there exists an

$$h : S \to \mathbb{Z}/2 = \{\circ, \bullet\}$$

such that $h \circ f \notin \mathcal{AF}(A, \mathbb{Z}/2)$. By Proposition 2.8.4, $h \circ f$ is either of the first or the second type.

Let us consider the first case. By Example 2.7.1, $h \circ f$ is given by



Let L be a line (=rank 2 lattice in C) reducing to the line through $(0:0:1)$ and $(0:1:1)$ modulo 2 and $P \in L$ be a point in

$$(h \circ f)^{-1}((0:0:1)).$$

By Corollary 2.5.4, an AF-function takes only two values on a lattice of rank 2. Since $f_L \in \mathcal{AF}(L, S)$ the value $f(P)$ is generic for L. Thus for every point Q on L in

$$(h \circ f)^{-1}((0:1:0)) \text{ and } (h \circ f)^{-1}(0:0:1)$$

we have

$$f(P) = f(Q).$$

Take any line L' which modulo 2 passes through $(0:0:1)$ and $(1:1:0)$. The value of f on the point of intersection $L \cap L'$ is $f(P)$. Since $f(P')$ is the generic value for L' for every point P' on L' in the preimage of $h \circ f((0:0:1))$ we have $f(P') = f(P)$. Moreover, $f(P') = f(Q')$ for every Q' in the preimage $h \circ f((1:1:0))$ in L'. Therefore, for *any* line L (resp. L'') such that the reduction modulo 2 passes through $(0:0:1)$ and $(0:1:1)$ (resp. $(0:0:1)$ and $(1:1:0)$) the generic value is $f(P)$. In particular, for every point R in the preimage of $(1:1:0)$ we have $f(R) = f(P)$.

Now consider the preimages of the points

$$(1:0:1),\ (1:1:1),\ (0:1:1).$$

Every one of those is generic for some rank 2 sublattice in A. Since these lattices intersect, we can apply the same reasoning as above. It follows that f can take only two values on A and, moreover, that f is induced from $A/2A$.

The second case is treated similarly. □

3.4. Checking the AF-property. — We summarize the discussion of the previous sections:

PROPOSITION 3.4.1. — *Let $A \in \mathcal{A}_q$, S a set and $f \in \mathcal{F}(A, S)$. Assume that $q > 2$ and that for all subgroups $C \subset A$ of rank ≤ 2 one has $f_C \in \mathcal{AF}(C, S)$. Then $f \in \mathcal{AF}(A, S)$.*

Proof. — By Lemma 3.2.1 it suffices to consider the case when $\mathrm{rk}(A) = 3$. Assume that $f \notin \mathcal{AF}(A, S)$. By Lemma 3.1.2, there exists a map $h : S \to \mathbb{Z}/2$ such that $h \circ f \notin \mathcal{AF}(A, \mathbb{Z}/2)$. By Lemma 2.6.1, there exists a subgroup $C \subset A$ of rank 2 such that $h \circ f_C \notin \mathcal{AF}(C, \mathbb{Z}/2)$. In particular, $f_C \notin \mathcal{AF}(C, S)$. □

PROPOSITION 3.4.2. — *Let k be a field of $\mathrm{char}(k) = 0$ and K/k an extension. Let S be a ring such that $2s \neq 0$ for all $s \in S$. Assume that $f \in \mathcal{LF}(K, S)$ and that for all $\mathbb{Z}$-submodules $C \subset K$ of rank ≤ 2 one has $f_C \in \mathcal{AF}(C, S)$. Then $f \in \mathcal{AF}(K, S)$.*

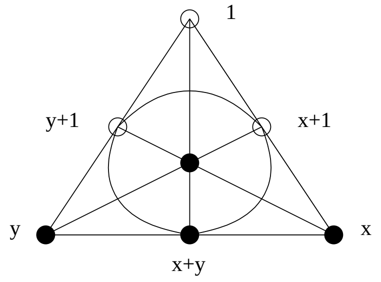
Proof. — Assume otherwise. Then, by Lemma 3.2.1, there exists a submodule $C \subset K$ of rank 3 such that $f_C \notin \mathcal{AF}(C, S)$. Moreover, there exists a map $h : S \to \mathbb{Z}/2$ such that $h \circ f_C \notin \mathcal{AF}(C, \mathbb{Z}/2)$. By Proposition 2.8.1, we can assume that C does not have a special basis (by restricting to a proper subgroup). Then, by Proposition 2.8.4, $h \circ f_C$ has the form described in Example 2.7.1 or 2.7.2. In both cases, f_C itself takes exactly two values.

Up to addition of a constant (and shifting C using the logarithmic property, if necessary), we can assume that f takes the values 0 and s (for some $s \in S \setminus 0$) and that

$$f(1) = 0.$$

Moreover, (in both cases!) there exist elements $x, y \in C \subset K$ such that

$$f(x) = f(y) = f(x+y) = f(x+y+1) = s,$$
$$f(x+1) = f(y+1) = 0.$$



Consider the sublattices in K

$$\begin{array}{rcl} D & := & \langle xy, y, 1\rangle; \\ E & := & \langle xy, 1, x+y\rangle. \end{array}$$

Using the logarithmic property we find that

$$f(xy) = 2s,\ f(y) = s,\ f(1) = 0.$$

By Lemma 3.3.1, f_D is an AF-function. Using the transitivity of the induced order on D we see that

$$1 >_D y >_D xy.$$

In particular, since $f(1) \neq f(xy)$, for any subgroup of K containing 1 and xy we have $1 > xy$. Similarly, on E the function f_E also takes 3 values. Therefore (by Lemma 3.3.1), $f_E \in \mathcal{AF}(E, S)$ and the induced order gives

$$x + y >_E 1 >_E xy$$

(by transitivity of the order relation on E). It follows that

$$f(x + y + xy + 1) = f(x + y) = s.$$

On the other hand, (using the logarithmic property),

$$f(x+y+xy+1) = f((x+1)(y+1)) = f(x+1) + f(y+1) = 0.$$

Contradiction. $\square$

4. AF-functions and geometry

ASSUMPTION 4.0.3. — *Throughout R is $\mathbb{Q}$, $\mathbb{Z}_p$ or $\mathbb{Z}/p$.*

4.1. Affine geometry. — Let k be a field and V a (possibly infinite dimensional) vector space over k, with an embedding of k as $k \cdot 1$. For every pair

$$f_1, f_2 \in \mathcal{F}(\mathbb{P}(V), R)$$

we have a map

$$\begin{array}{rccc} \varphi = \varphi_{f_1,f_2} : & \mathbb{P}(V) & \to & \mathbb{A}^2(R) \\ & v & \mapsto & (f_1(v), f_2(v)). \end{array}$$

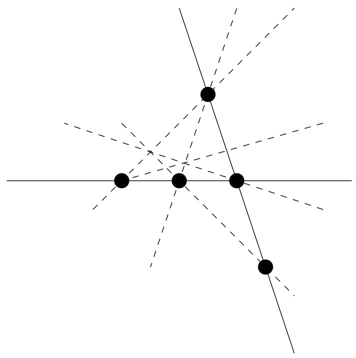
REMARK 4.1.1. — If f_1, f_2 form a c-pair (see Definition 2.2.6) then the image of every line in $\mathbb{P}(V)$ under φ_{f_1,f_2} is contained in a line in $\mathbb{A}^2(R)$.

PROPOSITION 4.1.2. — *If $f_1, f_2 \in \mathcal{F}(\mathbb{P}(V), R)$ form a c-pair then for every 3-dimensional k-vector space $V' \subset V$ there exists an affine line $\mathbb{L}_{V'} \subset \mathbb{A}^2$ and a point $d_{V'} \in \mathbb{A}^2(R)$ such that*

$$\varphi(\mathbb{P}(V')) \subset d_{V'} \cup \mathbb{L}_{V'}(R).$$

Proof. — Assume that $\varphi(\mathbb{P}(V'))$ contains 4 distinct points $\overline{p}_1, ..., \overline{p}_4$. Denote by $\overline{\ell}_{ij}$ the line through $\overline{p}_i$ and $\overline{p}_j$. Then the lines intersect in $\mathbb{A}^2(R)$ and the intersection point of these lines is contained in $\varphi(\mathbb{P}(V'))$. Indeed, denote by $\ell_{ij} \subset \mathbb{P}(V')$ the line passing through a pair of points p_i, p_j contained in $\varphi^{-1}(\overline{p}_i)$ (resp. $\varphi^{-1}(\overline{p}_j)$) and assume, for example, that $\overline{\ell}_{12} \cap \overline{\ell}_{34} = \emptyset$. The lines ℓ_{12} and ℓ_{34} intersect (or coincide) in $\mathbb{P}(V')$. The point of intersection is contained in the image. Thus the lines $\overline{\ell}_{12}, \overline{\ell}_{34}$ intersect and the image of $\mathbb{P}(V)$ contains the intersection point.

Now we can assume that $\varphi(\mathbb{P}(V'))$ contains at least 5 points $\overline{p}_j$, such that $\overline{p}_1, \overline{p}_2, \overline{p}_3 \in \overline{\ell} \in \mathbb{A}^2_R$ and $\overline{p}_4, \overline{p}_5 \notin \overline{\ell}$ and such that the line through $\overline{p}_4, \overline{p}_5$ intersects $\overline{\ell}$ in $\overline{p}_3$.



The goal is to show that drawing lines in $\mathbb{A}^2$ through the points of intersections of the existing lines one can produce 2 new pairs of points in $\mathbb{A}^2(R)$ such that the corresponding lines are parallel, leading to a contradiction.

First we assume that R is $\mathbb{Q}$ or $\mathbb{Z}/p$. Compactify $\mathbb{A}^2$ to $\mathbb{P}^2$ by adding a line ℓ_∞. After a projective transformation of $\mathbb{P}^2$ (with coefficients in R) we can assume that the points are given by

$$(1:0:1),\ (0:0:1),\ (0:1:1),\ (1:0:0),\ (0:1:0).$$

We use standard affine coordinates (z_1, z_2) on $\mathbb{A}^2$ and corresponding projective coordinates $(z_1 : z_2)$ on ℓ_∞. The set $\varphi(\mathbb{P}(V'))$ has the following properties:

- if $(z_1, z_2) \in \varphi(\mathbb{P}(V'))$ then $(z_1 : z_2) \in \ell_\infty$ is also contained in $\varphi(\mathbb{P}(V'))$.
- if $(z_1, z_2) \in \varphi(\mathbb{P}(V'))$ then $(z_1, 0)$, $(0, z_2)$ are also in $\varphi(\mathbb{P}(V'))$.
- if $(z_1, z_2) \in \varphi(\mathbb{P}(V'))$ then $(z_1 : z_2 : 0) \in \varphi(\mathbb{P}(V'))$ and $(z_1/z_2, 0) \in \varphi(\mathbb{P}(V'))$.
- if $(z_1, 0)$, $(z_2, 0) \in \varphi(\mathbb{P}(V'))$ then $(z_1 + z_2, 0) \in \varphi(\mathbb{P}(V'))$.
- if $(z, 0) \in \varphi(\mathbb{P}(V'))$ then $(0, z) \in \varphi(\mathbb{P}(V'))$.

To check the listed properties it suffices to compute the coordinates of the points of intersection of appropriate lines. For example, the first property follows from the fact that $(z_1 : z_2) \in \ell_\infty$ is the intersection of ℓ_∞ with the line through $(0, 0)$ and $(z_1, z_2) \in \mathbb{A}^2$. For the second, observe that $(z_1 : 0 : 1)$ can be obtained as the intersection of the line through $(0 : 0 : 1)$ and $(1 : 0 : 1)$ with the line through $(z_1 : z_2 : 1)$ and $(0 : 1 : 0)$, etc.

In particular, $\varphi(\mathbb{P}(V'))$ contains a subset of points (z_1, z_2), where z_1, z_2 are generated from coordinates of points in $\varphi(\mathbb{P}(V')) \cap (\mathbb{P}^2 \setminus \ell_\infty)$ by the above procedures. For $R = \mathbb{Q}$ or $R = \mathbb{Z}/p$, the set $\varphi(\mathbb{P}(V'))$ contains $\mathbb{A}^2(R) \cup \ell_\infty(R) = \mathbb{P}^2(R)$. In particular, one can find two lines in $\mathbb{P}(V')$ such that their images don't intersect in $\mathbb{A}^2$, contradiction.

Now we show how to extend this argument to $R = \mathbb{Z}_p$. As before, we assume that $\varphi(\mathbb{P}(V'))$ contains 5 points as in the picture above. One can choose a coordinate system such that $\varphi(\mathbb{P}(V'))$ contains the points $(1,0), (0,0), (0,1), (z_1, 0)$ and $(0, z_2)$ with $z_1, z_2 \in \mathbb{Q}_p$. Then it also contains some point (z_1', z_2') with *nonzero* coordinates $z_1', z_2' \in \mathbb{Q}_p$. The (projective) transformation $\mathcal{T}$ moving

$$(1,0), (0,0), (0,1) \ \mapsto (\infty, 0), (0,0), (0,\infty)$$

is given by

$$(w_1, w_2) = (\frac{z_1}{1-(z_1+z_2)}, \frac{z_2}{1-(z_1+z_2)})$$

and its inverse $\mathcal{T}^{-1}$ by

$$(z_1, z_2) = (\frac{w_1}{1+w_1+w_2}, \frac{w_2}{1+w_1+w_2}).$$

Apply the reasoning of the first part to $(w_1', w_2') := \mathcal{T}((z_1', z_2'))$. First we find that $\varphi(\mathbb{P}(V'))$ contains the points $(w_1', 0), (0, w_2')$, then that it contains all points of the form $(w_1'/2^{m_1}, w_2'/2^{m_2})$ for some $m_1, m_2 \in \mathbb{N}$, then that it contains all points $(r_1 w_1'/2^{m_1}, r_2 w_2'/2^{m_2})$ with $r_1, r_2 \in \mathbb{N}$, and, finally, that it contains all points with coordinates $(e_1 w_1', e_2 w_2')$ for arbitrary $e_1, e_2 \in \mathbb{Q}$.

To arrive at a contradiction it suffices to produce a pair of rational numbers e_1, e_2 such that

$$\mathcal{T}^{-1}((e_1 w_1', e_2 w_2')) \notin \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

Clearly, (for any $w_1', w_2' \in \mathbb{Q}_p$) we can find $e_1, e_2 \in \mathbb{Q}$ such that

$$\frac{e_1 w_1'}{1 + e_1 w_1' + e_2 w_2'} \notin \mathbb{Z}_p.$$

This concludes the proof. $\square$

REMARK 4.1.3. — Proposition 4.1.2 is wrong for $R = \mathbb{Q}_p$.

4.2. Projective geometry. —

PROPOSITION 4.2.1. — *Let k be any field and V a 3-dimensional vector space over k. Assume that $f_1, f_2 \in \mathcal{F}(\mathbb{P}(V), \mathbb{Z}/2)$ are such that*

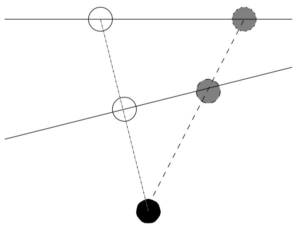
$$\varphi(\mathbb{P}(V)) \subset \{\overline{p}_{12}, \overline{p}_{13}, \overline{p}_{23}\} \subset \mathbb{A}^2(\mathbb{Z}/2),$$

where $\overline{p}_{12} = (0,0), \overline{p}_{13} = (1,0)$ and $\overline{p}_{23} = (0,1)$. Assume further that for all 2-dimensional vector spaces $V' \subset V$ the image $\varphi(\mathbb{P}(V'))$ is contained in at most two of these points. Then at least one of the functions f_1, f_2 or $f_3 = f_1 + f_2$ is an AF-function on every 2-dimensional subspace $V' \subset V$.

NOTATIONS 4.2.2. — Denote by $P_{ij} \subset \mathbb{P}(V)$ the preimage of $\overline{p}_{ij}$. Let T_i be the set of lines $t \subset \mathbb{P}(V)$ such that $\varphi(t) \subset \{\overline{p}_{ij}, \overline{p}_{ik}\}$.

The proof of Proposition 4.2.1 is subdivided into a sequence of lemmas.

LEMMA 4.2.3. — *Let t_i, t_i' be two lines in T_i. Every point p_{jk} defines a projective isomorphism between $t_i \cap P_{ij}$ and $t_i' \cap P_{ij}$.*



Proof. —

$\square$

LEMMA 4.2.4. — *If there exists a line $t_i \in T_i$ such that the number of points in $t_i \cap P_{ij}$ is ≤ 1 then either f_1, f_2 or f_3 is a GF-function on V.*

Proof. — First of all, if one of the sets P_{ij} is empty then one of the functions f_1, f_2, f_3 is the constant function, hence a flag function.

Assume that this is not the case and that there exists a line t_i such that $t_i \cap P_{ij} = \emptyset$. By assumption, there exist points of all three types. We can draw a line t_j through some points of type P_{ij} and P_{jk}. The line t_j intersects t_i in a point, which must be a point of type P_{ik}. Thus the line t_i contains points of all three types, contradiction.

Finally, assume that there exists a line t_i such that $t_i \cap P_{ij}$ consists of exactly one point. There are two possibilities: there are at least two lines of type T_j or there is exactly one line of type T_j. In the first case Lemma 4.2.3, shows that *all* lines of type T_j contain exactly one point of type P_{ij}. This means that there is only one point of type P_{ij} in $\mathbb{P}(V)$ (otherwise, we could draw a line through two of those points; this line cannot by of type T_i nor of type T_j). It follows that f_k is an AF-function on V (delta function).

Assume now that there exists exactly one line of type T_j. The complement to this line contains *only* points of type P_{ik}. It follows that f_j is an AF-function on $\mathbb{P}(V)$. □

Thus we can assume that there are at least 3 points of each type (which do not lie on a line) and that there are at least two lines of each type and that for every line $t_i \in T_i$ the set $t_i \cap P_{ij}$ has at least two elements.

Definition 4.2.5. — *We call the points $p_{ij}, p'_{ij} \in t_i$* related *if there exists a point p^0_{ij} such that the line joining p^0_{ij} and p_{ij} and the line joining p^0_{ij} and p'_{ij} are both of type T_j.*

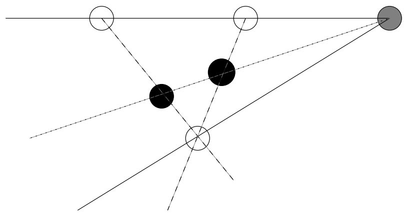
Lemma 4.2.6. — *If there exists a line $t_i \in T_i$ containing two nonrelated points $p_{ij}, p'_{ij} \in t_i$ then for every $t_j \in T_j$ passing through p_{ij} or p'_{ij} all points in $t_i \cap P_{ij}$ are related.*

Proof. — Consider this line t_i with two nonrelated points p_{ij}, p'_{ij}. Let $t_j \in T_j$ be any line passing through p_{ij}. Let p''_{ij} be an arbitrary point in $t_i \cap P_{ij}$, distinct from p_{ij}. Since p_{ij}, p'_{ij} are not related the line through p''_{ij} and p'_{ij} has to be of type T_i. It follows that all points of type P_{ij} on t_j are related through p'_{ij}. □

Lemma 4.2.7. — *Assume that $p_{ij}, p'_{ij} \in t_i$ are related. For every point $p_{ik} \in t_i$ there exists a projective automorphism $m_{ik} : t_i \to t_i$ such that*

- $m_{ik}(t_i \cap P_{ij}) = t_i \cap P_{ij}$;
- *the unique fixed point of m_{ik} is p_{ik};*
- $m_{ik}(p_{ij}) = p'_{ij}$.

Proof. — Consider the triangle spanned by $p_{ij}, p'_{ij} \subset t_i$ and p^0_{ij}. Draw a line t'_i through $p_{ik} \in t_i$ and p^0_{ij}. Pick a point p_{jk} on the line t_j through p_{ij} and p^0_{ij} and draw a line t_k through p_{jk} and p_{ik}. Denote by p'_{jk} the point of intersection of t_j with the line through p'_{ij} and p^0_{ij}. Using the points p_{jk} and p'_{jk} as centers for the projective isomorphism between the line joining t_i and the line t'_i, we obtain the projective automorphism m_{ik}.



□

Lemma 4.2.8. — *Assume that there exists a line t_i such that all points $p_{ij} \in t_i$ are related. Then all three functions f_1, f_2, f_2 are AF-functions on all lines of type T_i.*

Proof. — The function f_i is constant on lines of type T_i, hence an AF-function. The function $f_j + f_k$ is constant on (the fixed line) t_i. Let us show that f_j is an AF-function on t_i.

By Lemma 4.2.7, for any pair of related points p_{ij}, p'_{ij} and any point p_{ik} on a projective line of type t_i there exists a projective automorphism (transvection) with a single fixed point p_{ik} moving p_{ij} to p'_{ij}. Introduce coordinates on $\mathbb{P}^1$ such that $p_{ik} = (0:1)$, $p_{ij} = (1:0)$ and $p'_{ij} = (1:1)$. A unipotent lifting of the automorphism m_{ij} to $\mathrm{GL}(V) = \mathrm{GL}_2(k)$ can be written in the form

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

In this basis $f(e_1) = f(e_1 + e_2) = 1$ and $f(e_2) = 0$. Consequently, f satisfies the conditions of Lemma 2.5.6. (Notice that the points p_{ik} on t_i need not be related. This leads to the nonsymmetric shape of the functional equation 2.1.) Now we apply Lemma 2.5.6.

To conclude that f_1, f_2, f_3 are AF-functions on *all* lines of type T_i we use the projective isomorphism preserving both sets $t_i \cap P_{ij}$ and $t_i \cap P_{ik}$ (introduced in Lemma 4.2.3). □

Proof. — (of Proposition 4.2.1) We may assume that we are not in the situation of Lemma 4.2.4. If for all $i = 1, 2, 3$ and all lines t_i of type T_i

all points in $t_i \cap P_{ij}$ or all points in $t_i \cap P_{ik}$ are related then all three functions f_1, f_2, f_3 are AF-functions on t_i.

Assume there is a t_i and two points $p_{ij}, p'_{ij} \in t_i \cap P_{ij}$ which are not related. By Lemma 4.2.6 and Lemma 4.2.8, f_1, f_2, f_3 are AF-functions on all lines of type T_j. There are two cases: there exist two nonrelated points in $t_i \cap P_{ik}$ or not. In the first case, f_1, f_2, f_3 are AF-functions on all lines of type T_k. In the second case f_1, f_2, f_3 are AF-functions on lines of type T_i. If, for example, all three functions are AF-functions on lines of type T_j and T_k then the function f_i (being constant on lines of type T_i) is an AF-function on *all* lines in $\mathbb{P}(V)$. This concludes the proof. □

4.3. Logarithmic functions. — We keep the assumptions of 4.0.3.

PROPOSITION 4.3.1. — *Let k be a field of characteristic $\neq 2$ and K/k an extension. Assume that $f_1, f_2 \in \mathcal{LF}(K, R)$ form a c-pair (see 2.2.6 for the definition). Assume that the linear space $\langle f_1, f_2\rangle_R$ does not contain a (nonzero) AF-function. Then there exists a 3-dimensional $V \subset K$ such that for* every *(nonzero) $f' \in \langle f_{1,V}, f_{2,V}\rangle_R$ we have $f' \notin \mathcal{AF}(V, R)$.*

Proof. — For $\mathrm{char}(k) > 2$ we use Proposition 3.4.1 and for $\mathrm{char}(k) = 0$ Proposition 3.4.2. Since $f_1 \notin \mathcal{AF}(K, R)$ there exists a 2-dimensional subspace $V' \subset K$ such that $f_{1,V'} \notin \mathcal{AF}(V', R)$. Since

$$\mathrm{rk}\, \langle f_{1,V'}, f_{2,V'}, 1\rangle \leq 2$$

we have $f_{2,V'} - \mu_1 f_{1,V'} = \mu_2$ (for some $\mu_1, \mu_2 \in R$). Since

$$f_2 - \mu_1 f_1 \notin \mathcal{AF}(K, R),$$

by Section 3.4, there exists a 2-dimensional W' such that

$$f_{2,W'} - \mu_1 f_{1,W'} \notin \mathcal{AF}(W', R).$$

Choose some k-basis in $V' = \langle x_1, x_2\rangle$ and $W' = \langle y_1, y_2\rangle$ (with $x_j, y_j \in K^*$). Let $V = \langle x_1, x_2, y_2 y_1^{-1} x_1\rangle$. Then for every pair of $(\lambda_1, \lambda_2) \neq (0, 0)$

$$\lambda_1 f_1 + \lambda_2 (f_2 - \mu_1 f_1) \notin \mathcal{AF}(V, R).$$

Indeed, for pairs with $\lambda_1 \neq 0$ consider the restriction to V'. For pairs $(0, \lambda_2)$ with $\lambda_2 \neq 0$ consider the restriction to (a shift of) W' and use the invariance and the logarithmic property of f. □

LEMMA 4.3.2. — *Let k be a field of characteristic $\neq 2$, K/k an extension and $V \subset K$ a 3-dimensional vector space over k. Consider a c-pair $f_1, f_2 \in \mathcal{F}(\mathbb{P}(V), R)$. Assume that there are no nonzero AF-functions $f \in \langle f_1, f_2 \rangle_F$. Then there exist nonconstant (and nonproportional) functions $f_1', f_2' \in \langle f_1, f_2, 1 \rangle_R$ and a map $h' : R \to \mathbb{Z}/2$ such that neither of the three functions*

$$\begin{gathered} h' \circ f_1', \\ h' \circ f_2', \\ h' \circ f_1' + h' \circ f_2' \end{gathered}$$

is an AF-function on V.

Proof. — By 4.1.2, we know that

$$\varphi_{f_1,f_2}(\mathbb{P}(V)) \subset d_V \cup \mathbb{L}_V.$$

After a linear change of coordinates (over R) we can assume that

$$\varphi_{\tilde{f}_1,\tilde{f}_2}(\mathbb{P}(V)) = (0,1) \cup \{x - \text{axis}\},$$

where

$$\begin{aligned} \tilde{f}_1 &= \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3, \\ \tilde{f}_2 &= \mu_1 f_1 + \mu_2 f_2 + \mu_3 \end{aligned}$$

and

- $\tilde{f}_1(0) = \tilde{f}_2(0) = 0$;
- $\tilde{f}_2$ takes only two values;
- $\tilde{f}_2(v) = 0$ if $\tilde{f}_1(v) \neq 0$;
- $\tilde{f}_1(v) = 0$ if $\tilde{f}_2(v) \neq 0$.

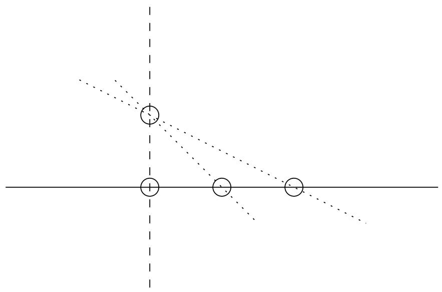
Let h be such that $h \circ \tilde{f}_1 \notin \mathcal{AF}(V, Z/2)$. We can assume that $h(0) = 0$. Let $v_1 \in V$ be such that $h \circ \tilde{f}_1(v_1) \neq 0$. After rescaling (and a corresponding rescaling of h), we can assume that $\tilde{f}_1(v_1) = 1$ and that $h(1) = 1$. Since $\tilde{f}_2$ takes only the values $0, 1$ we have

$$h \circ \tilde{f}_2 = \tilde{f}_2 \notin \mathcal{AF}(V, Z/2).$$

Notice that the last two properties imply that

$$h \circ (\tilde{f}_1 + \tilde{f}_2) = h \circ \tilde{f}_1 + h \circ \tilde{f}_2. \tag{4.1}$$

The lines in $\mathbb{P}(V)$ can be subdivided into 3 classes according to their image under $\varphi_{\tilde{f}_1,\tilde{f}_2}$.



The function $\tilde{f}_1$ is obviously constant on lines in $\mathbb{P}(V)$ whose image is contained in the y-axis, $\tilde{f}_2$ is constant on lines mapping to the x-axis and $\mu\tilde{f}_1 + \tilde{f}_2$ (with $\mu \neq 0$) is constant on the lines mapping to $\mu x + y = 1$. We call the lines of the first type T_1-lines, the lines of the second type T_2-lines and all other T_3-lines.

Notice that $\tilde{f}_3$ restricted to the T_i-lines coincides with $\tilde{f}_i$ for $i = 1, 2$. By assumption, $\tilde{f}_3 \notin \mathcal{AF}(V, R)$, and by the results in Section 3.4, there exists a line $\ell_3 \subset \mathbb{P}(V)$ such that $\tilde{f}_3 \notin \mathcal{AF}(\ell_3, R)$. If ℓ_3 is of type T_1 or T_2 then h as above solves our problem. Thus we can assume that all three functions $\tilde{f}_1, \tilde{f}_2$ and $\tilde{f}_3$ are AF-functions on all lines of type T_1 and T_2. Consider a line ℓ_3 of type T_3 such that $\tilde{f}_3 \notin \mathcal{AF}(\ell_3, R)$. Then $\varphi(\ell_3) \subset \mu x + y = 1$, (with $\mu \neq 1$). That is, on ℓ_3 we have

$$\begin{array}{rcl} \mu\tilde{f}_1 + \tilde{f}_2 & = & 1 \\ \tilde{f}_1 + \tilde{f}_2 & = & \tilde{f}_3 \end{array}$$

It follows that all 3 functions $\tilde{f}_1, \tilde{f}_2, \tilde{f}_3 \notin \mathcal{AF}(\ell_3, R)$. Now we change coordinates again, making ℓ_3 the new coordinate axis (in addition to the x-axis). We put

$$\begin{array}{rcl} f_1' & = & \mu\tilde{f}_1 + \tilde{f}_2 - 1 \\ f_2' & = & -\tilde{f}_2 \\ f_3' & = & f_1' + f_2'. \end{array}$$

Now we can apply the argument above: find an h' such that

$$h' \circ f_1' \notin \mathcal{AF}(V, \mathbb{Z}/2);$$

(after rescaling, if necessary) one can assume that

$$h' \circ f_2' = f_2',$$

(with $f'_2 = \lambda \tilde{f}_2$ for some nonzero λ). Since $(f'_1 + f'_2)$ restricted to $\ell_3 = \{f'_1 = 0\}$ is equal to f'_2, which is not AF on ℓ_3, (by our assumption that $\tilde{f}_2$ is not AF on ℓ_3), we conclude that

$$h' \circ (f'_1 + f'_2) \notin \mathcal{AF}(\ell_3, \mathbb{Z}/2).$$

By the same reasoning as above (see 4.1) we have

$$h' \circ (f'_1 + f'_2) = h' \circ f'_1 + h \circ f'_2.$$

This finishes the proof. □

4.4. Existence of AF-functions. —

PROPOSITION 4.4.1. — *Let K/k be an extension of fields. Assume that $f_1, f_2 \in \mathcal{LF}(K, R)$ form a c-pair. Then $\langle f_1, f_2 \rangle_R$ contains an AF-function.*

Proof. — We can assume that $f_1, f_2, 1$ are linearly independent on $\mathbb{P}(K)$. (Otherwise some linear combination is constant, hence an AF-function.)

Assume that $\langle f_1, f_2 \rangle_R$ does not contain an AF-function. By Proposition 4.3.1 combined with Lemma 4.3.2, there exist a 3-dimensional $V \subset K$, functions $f'_1, f'_2 \in \mathcal{F}(\mathbb{P}(V), R)$ and a map $h : R \to \mathbb{Z}/2$ such that

$$h \circ f'_1, h \circ f'_2, h \circ f'_3 = h \circ f'_1 + h \circ f'_2 \notin \mathcal{AF}(V, \mathbb{Z}/2).$$

These functions satisfy the assumptions of Proposition 4.2.1. We obtain a contradiction to its statement. □

5. Galois theory

5.1. Groups. — Let G be a (topological) group with unit $0 = 0_G$ and $g, g' \in G$. Denote by $[g, g']$ their commutator and by

$$G = G^{(0)} \supset G^{(1)} \supset ...$$

the lower central series: $G^{(i)}$ is the (closed) subgroup generated by $[g_i, g_0]$, where $g_i \in G^{(i)}$ and $g_0 \in G^{(0)}$. Denote by $G^a = G/G^{(1)}$ the abelianization of G, by $G^c = G/G^{(2)}$ the second quotient - it is a central extension of G^a - and by $G^{1,2} = G^{(1)}/G^{(2)}$. Let

$$\psi_c : G \to G^c, \qquad \psi_a : G \to G^a, \qquad \psi_{ca} : G^c \to G^a$$

be the quotient homomorphisms (we have $\psi_a = \psi_{ac} \circ \psi_c$).

LEMMA 5.1.1. — *Let G be a (profinite) group and $\psi : G \to A$ a (continuous) surjective homomorphism onto a finite group A. Assume that $\alpha \in H^2(A, \mathbb{Z}/p^n)$ is a class such that*

$$\psi^*(\alpha) = 0 \in H^2(G, \mathbb{Z}/p^n).$$

Then there exists a (continuous) homomorphism $\tilde{\psi} : G^c \to A$ such that $\tilde{\psi} \circ \psi_c = \psi$ and

$$\tilde{\psi}^*(\alpha) = 0 \in H^2(G^c, \mathbb{Z}/p^n).$$

We write $G(p^n)$ for the subgroup of G generated by g^{p^n} with $g \in G$ (for abelian groups and their central extensions, the product of p^n-th powers is a p^n-th power). For any profinite group G we denote by G_p its maximal pro-p-quotient. Notice that for any profinite group G we have $(G^a)_p = (G_p)^a$ and $(G^c)_p = (G_p)^c$.

5.2. Fields. —

ASSUMPTION 5.2.1. — *Fix a prime p. We assume that* $\mathrm{char}(k) \neq p$ *and that k does not admit finite separable extensions of degree divisible by p.*

Let K be a field over k. It has a structure of a vector space over k and therefore, K^*/k^* a structure of a projective space over k, though infinite-dimensional. We continue to denote this space by $\mathbb{P}(K)$ and by $\mathcal{F}(\mathbb{P}(K), \mathbb{Z}_p)$ the space of $\mathbb{Z}_p$-valued functions on $\mathbb{P}(K)$.

In Section 2.2 we defined the set $\mathcal{LF}(K, \mathbb{Z}_p)$. We now consider the topological space $\mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$. As a set it coincides with $\mathcal{LF}(K, \mathbb{Z}_p)$. The basis of the topology is given by $U_{E^*,n}$, where E^* is a finitely generated subgroup of K^*/k^* and $n \in \mathbb{N}$ - a function f is in $U_{E^*,n}$ if f is equal to 0 modulo p^n on E^*.

NOTATIONS 5.2.2. — For any k-vector space $V \subset K$ (not necessarily closed under multiplication in K) and $f \in \mathcal{F}(\mathbb{P}(K), \mathbb{Z}_p)$ we denote by f_V the restriction of f to $\mathbb{P}(V) = (V \setminus 0)/k^*$ (sometimes we will denote by the same symbol the restriction of f to V). For a finite set of functions $f_j \in \mathcal{F}(\mathbb{P}(K), \mathbb{Z}_p)$ we denote by $\langle f_1, ..., f_n \rangle$ the $\mathbb{Q}_p$-vector space they span in $\mathcal{F}(\mathbb{P}(K), \mathbb{Z}_p)_{\mathbb{Q}_p}$.

5.3. Galois groups. — Let K be a field as in Section 5.2. Denote by G_K the Galois group of a separable closure of K. It is a profinite compact topological group (we refer to [**11**] for basic facts concerning profinite groups). In general, the group G_K has a rather complicated structure. We will be interested in

$$\mathrm{G}_{K/k} := \mathrm{Ker}(\mathrm{G}_K \to \mathrm{G}_k),$$

more precisely, in the pro-p-group $\Gamma^c := (\mathrm{G}^c_{K/k})_p$ and its abelianization $\Gamma^a := (\mathrm{G}^a_{K/k})_p$. The group Γ^a is a torsion free abelian pro-p-group (by our assumptions on k).

Lemma 5.3.1. — *One has a (noncanonical) isomorphism of topological groups*

$$\Gamma^a \simeq \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p).$$

Proof. — Since K contains all p-power roots of 1 we can choose an identification between $\mathbb{Z}_p$ and $\mathbb{Z}_p(1)$. Then, by Kummer theory, we have a nondegenerate pairing

$$\Gamma^a/\Gamma^a(p^n) \times K^*/(K^*)^{p^n} \to \mathbb{Z}/p^n,$$

given by

$$(\sigma, \kappa) \mapsto \sigma(\kappa)/\kappa$$

for $\sigma \in \Gamma^a/\Gamma^a(p^n)$ and $\kappa \in K^*$. We derive an isomorphism (of topological groups)

$$\Gamma^a = \mathrm{Hom}(\hat{K}^*, \mathbb{Z}_p)$$

(where $\hat{K}^*$ is the completion of K^* with respect to subgroups of p-power index). Moreover, every such homomorphism is trivial on k^*, since k^* does not admit finite extensions of degree divisible by p, by assumption. Thus, in our case, the latter group is isomorphic to $\mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$, (since K^* is dense in $\hat{K}^*$).

More explicitely, two elements of the Galois group Γ^a coincide if for all n their actions on all cyclic p^n-degree extensions of K coincide. Thus the resulting map

$$\Gamma^a/\Gamma^a(p^n) \to \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}/p^n)$$

is a monomorphism.

Conversely, every element of $\mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$ defines an element of Γ^a. Any homomorphism $\chi : K^*/k^* \to \mathbb{Z}_p$ defines a compatible set of elements of $\Gamma^a/\Gamma^a(p^n)$ for all abelian extensions of K of degree p^n. Thus Γ^a and $\mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$ are isomorphic as topological groups.

(We use the fact that the group K^*/k^* has no torsion, by assumptions on k. Therefore, the map

$$\mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}/p^{n+1}) \to \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}/p^n)$$

corresponding to the projection $\mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^n$ is surjective and we obtain an isomorphism between projective limits.) □

We consider K as a vector space over k, with a canonical embedding of k as a 1-dimensional subspace $k \cdot 1$. Every finite-dimensional subspace $V \subset K$ which contains k (as a subspace) defines a subfield K_V of K (generated by elements of a basis of V over k). Denote by G_V the Galois group of the (separable) closure of K_V. We have canonical maps

$$\Gamma^c_K \to \Gamma^c_V \text{ and } \Gamma^a_K \to \Gamma^a_V.$$

If V is 2-dimensional then K_V is isomorphic to $k(t)$, (where $1, t$ generate V over k).

Lemma 5.3.2. — *Let $V \subset K$ be 2-dimensional. Then*

$$H^2(\mathrm{G}_V, \mathbb{Z}/p^n) = 0$$

for all $n \geq 1$.

Proof. — One has

$$K_2(k(V)) = \sum_{\nu} k^*_\nu$$

where the sum is over all codimension 1 points of $k(V)$. By our assumptions on k, the group k^*_ν is p-divisible as well. Now we apply the theorem of Merkuriev-Suslin (see [**6**])

$$H^2(\mathrm{G}_V, \mathbb{Z}/p^n) = K_2(k(V))/p^n = 0.$$

□

Remark 5.3.3. — For $K = k(t)$ the irreducible divisors are parametrized by $\mathbb{P}^1_k = \mathbb{P}(V)$. In general, if $\dim V \geq 3$ then the transcendence degree of K_V over k is > 1 (and $\leq \dim V - 1$) and the description of Γ^a_V is complicated since there are many more irreducible divisors - they cannot be parametrized by an algebraic variety.

5.4. Commuting pairs. — If $[\tilde{f}_1, \tilde{f}_2] = 0$ for some lifts to Γ^c of elements $f_1, f_2 \in \Gamma^a$ then this commutator vanishes for all lifts. In this case we will call the pair f_1, f_2 a *commuting pair* (c-pair, since the following Proposition shows that it is indeed a c-pair in the sense of Definition 2.2.6). Natural c-pairs in Γ^a arise from valuations of fields.

PROPOSITION 5.4.1. — *If f_1, f_2 are a c-pair then for all 2-dimensional subspaces $V \subset K$ (not necessarily containing k) we have*

$$\dim\langle f_{1,V}, f_{2,V}, 1\rangle \leq 2.$$

Proof. — First assume that V contains k. We have the following diagram

$$\begin{array}{ccccccc} \mathrm{G}_K & \to & \mathrm{G}_K^c & \to & \Gamma_K^c & \to & \Gamma_K^a \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathrm{G}_V & \to & \mathrm{G}_V^c & \to & \Gamma_V^c & \to & \Gamma_V^a \end{array}$$

Lemma 5.3.2 implies that for all surjective continuous homomorphisms

$$\Gamma_V^a \to A$$

onto a finite abelian group A and any cocycle $\alpha \in H^2(A, \mathbb{Z}/p^n)$ its image in $H^2(\mathrm{G}_V, \mathbb{Z}/p^n)$ is zero. By Lemma 5.1.1, it is already zero in $H^2(\mathrm{G}_V^c, \mathbb{Z}/p^n)$. If α is nonzero in $H^2(Z, \mathbb{Q}/\mathbb{Z})$ then we can conclude that its image in $H^2(\Gamma_V^c, \mathbb{Z}/p^n)$ is zero. This means that there exists a finite group B which is a central extension of A and a surjective continuous homomorphism

$$\Gamma_V^c \to B$$

such that

$$H^2(A, \mathbb{Z}/p^n) \to 0 \in H^2(B, Z/p^n).$$

Assuming that f_1, f_2 are nonproportional in Γ_V^a we construct an A with a nonzero cocycle $\alpha \in H^2(A, \mathbb{Q}/\mathbb{Z})$ as follows. Since f_1, f_2 are nonproportional there exists a sublattice of $k(V)$ of the form $\langle x, x+1\rangle$ such that f_1, f_2 remain nonproportional on this lattice. Thus the vectors $\hat{f}_1 = (f_1(x), f_1(x+1))$ and $\hat{f}_2 = (f_2(x), f_2(x+1))$ define a rank 2 lattice $\hat{A} \subset \mathbb{Z}_p \oplus \mathbb{Z}_p$ and we have a surjective homomorphism $\Gamma_V^a \to \hat{A}$. Then there exists an n such that the reduction A of $\hat{A}$ modulo p^n is a subgroup of index $< p^n$ in $\mathbb{Z}/p^n \oplus \mathbb{Z}/p^n$ This implies that there exists a nonzero cocycle $\alpha = \alpha(f_1, f_2) \in H^2(A, \mathbb{Z}/p^n)$ mapping to a nonzero element in $H^2(A, \mathbb{Q}/\mathbb{Z})$ (by the condition on $\det(\hat{f}_1, \hat{f}_2)$ modulo p^n). Thus we have surjective maps

$$\Gamma_V^c \to B \to A$$

where B is a finite group such that α maps to 0 in $H^2(B, \mathbb{Z}/p^n)$.

The group B contains images of $\tilde{f}_1, \tilde{f}_2 \in \Gamma_K^c$ and

$$\tilde{A} = \langle \tilde{f}_1, \tilde{f}_2 \rangle \subset B$$

surjects onto A. The cocycle $\alpha \in H^2(A, \mathbb{Q}/\mathbb{Z})$ maps to a nonzero element in $H^2(\tilde{A}, \mathbb{Q}/\mathbb{Z})$ but to zero in $H^2(B, \mathbb{Q}/\mathbb{Z})$. Contradiction. It follows that the restrictions of f_1, f_2 to V are proportional.

Now we turn to the general case. For any 2-dimensional subspace $V \subset K$ and $x \in V \setminus 0$ consider the 2-dimensional space V' over k consisting of elements of the form $v' = x^{-1}v$ with $v \in V$. The space V' contains k and, therefore, $f_{1,V'} = \lambda f_{2,V'}$ for some $\lambda \in k$. Thus

$$f_1(v) + f_1(x^{-1}) = f_1(x^{-1}\, v) = \lambda f_2(x^{-1}\, v) = \lambda(f_2(x^{-1}) + f_2(v)),$$

for all $v \in V$, i.e., $\dim\langle f_{1,V}, f_{2,V}, 1\rangle \leq 2$. $\square$

6. Valuations

6.1. Notations. — A *scale* is a commutative totally ordered group (we will use the notations $>$ and $\geq$). Let K be a field and

$$\nu \,:\, K^* \to \mathcal{I}_\nu$$

a surjective homomorphism onto a scale $\mathcal{I}_\nu$. It is called a nonarchimedean valuation if

$$\nu(x+y) \geq \min(\nu(x), \nu(y)),$$

with an equality if $\nu(x) \neq \nu(y)$. The group $\mathcal{I}_\nu$ is called the scale of the valuation. We consider only nonarchimedean valuations and call them simply valuations.

A valuation ν can be extended to K by $\nu(0) = \infty > \iota$ for all $\iota \in \mathcal{I}_\nu$. It defines a topology on K. We denote by K_ν the completion of K with respect to this topology. The sets

$$\mathcal{O}_{\nu,\iota} = \{x \in K \mid \nu(x) \geq \iota\}$$

are additive subgroups. We call the subring $\mathcal{O}_\nu = \mathcal{O}_{\nu,\nu(1)}$ the *valuation ring* of ν. Denote by $\mathfrak{m}_\nu = \{x \mid \nu(x) > \nu(1)\}$ the *valuation ideal* (it is a maximal ideal in $\mathcal{O}_\nu$); by $\mathcal{O}_\nu^* = \mathcal{O}_\nu \setminus \mathfrak{m}_\nu$ the set of invertible elements and by $\mathrm{K}_\nu = \mathcal{O}_\nu/\mathfrak{m}_\nu$ the *residue field* of $\mathcal{O}_\nu$. We have a multiplicative decomposition $\mathcal{O}_\nu^*/(1+\mathfrak{m}_\nu) = \mathrm{K}_\nu^*$. Here $1+\mathfrak{m}_\nu$ is the multiplicative subgroup of $\mathcal{O}_\nu^*$ consisting of elements of the form $(1+m)$, $m \in \mathfrak{m}_\nu$.

6.2. Inertia group. — Let K and ν be as above. We have a natural embedding $\Gamma^a_{K_\nu} \to \Gamma^a_K$. Its image is called the *abelian valuation group*.

Definition 6.2.1. — *Denote by*

$$\Gamma^a_\nu \subset \Gamma^a_K = \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$$

the subgroup of those functions which are trivial on $(1+\mathfrak{m}_\nu)$. *This group will be called the* abelian reduced valuation group.

Definition 6.2.2. — *Denote by*

$$\mathrm{I}^a_\nu \subset \Gamma^a_\nu \subset \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$$

the subgroup of those functions $z^\chi_\nu \in \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$ *such that*

$$z^\chi_\nu(\kappa) = \chi(\nu(\kappa))$$

for some homomorphism

$$\chi : \mathcal{I}_\nu \to \mathbb{Z}_p$$

and all $\kappa \in K^*$. *This group will be called the* abelian inertia group of ν. *The elements* z^χ_ν *are called* inertia elements *of* ν.

Of course, for all $\kappa, \kappa' \in K^*$ we have

$$z^\chi_\nu(\kappa \cdot \kappa') = z^\chi_\nu(\kappa) + z^\chi_\nu(\kappa')$$

and, since k contains all p-power roots, we have $\chi(\nu(k^*)) = 0$.

Remark 6.2.3. — If $\mathrm{char}(\mathrm{K}_\nu) \neq p$ then Γ^a_ν coincides with the abelian valuation group ([**13**]). Otherwise, Γ^a_ν is its proper subgroup.

6.3. Valuations and flag functions. —

EXAMPLE 6.3.1. — Let ν be a valuation on $K = k(X)$ which is trivial on k. Let z_ν^X be an inertia element of ν. It is a function on K^*, invariant under k^*. We can extend it arbitrarily to K, for example by $z_\nu^X(0) = 0$. Then z_ν^X is an abelian flag function on K (considered as a vector space over k).

EXAMPLE 6.3.2. — Let X be an algebraic variety defined over $k = \mathbb{Q}$, with good reduction X_p at p. Let ν be a divisorial valuation on the reduction $X_p \otimes \overline{\mathbf{F}}_p$. This valuation extends to a valuation on $K = \overline{\mathbb{Q}}(X)$, with values in $\mathbb{Q} \times \mathbb{Z}$. Any character of $\mathbb{Z}$ which is trivial on $\mathbb{Q}$ defines an inertia element z_ν^X, which can be considered as a function on K. This is an abelian flag function: for every finite dimensional subspace in K the corresponding filtration by groups consists of modules over p-integers in $\overline{\mathbb{Q}}$.

EXAMPLE 6.3.3. — Let K be field with a valuation ν, $\mathcal{O}_\nu$, $\mathfrak{m}_\nu$, K_ν as above. Let $\bar{V}$ be an n-dimensional vector space over K_ν and $\bar{f}$ an AF-function on $\mathbb{P}(\bar{V})$ (with respect to K_ν). Define f on $\mathcal{O}_\nu^n$, extending f trivially over the cosets $\mathcal{O}_\nu/\mathfrak{m}_\nu$. Consider the restriction of f to the subset

$$V_{\mathcal{O}} := \mathcal{O}_\nu^n \setminus (\mathfrak{m}_\nu \mathcal{O}_\nu)^n.$$

Put $V = K^n$ and consider the orbit space $(V \setminus 0)/K^*$. Every orbit has a representative in $V_{\mathcal{O}}$. Thus f defines an AF-function on $\mathbb{P}(V)$ (with respect to K).

THEOREM 6.3.4. — *Let $f \in \mathcal{LF}(K, \mathbb{Z}_p) \cap \mathcal{AF}(K, \mathbb{Z}_p)$. Then there exists a valuation ν on K with scale $\mathcal{I}_\nu$ and a map $\tilde{f} : \mathcal{I}_\nu \to \mathbb{Z}_p$ such that $f(\kappa) = \tilde{f} \circ \nu(\kappa)$ for all $\kappa \in K$.*

Proof. — An AF-function defines a filtration $(K_\alpha^f)_{\alpha \in \mathcal{A}}$. The logarithmic property of f implies that the ordered set $\mathcal{A}$ is an ordered group (a scale). The map $\nu : K \to \mathcal{A}$ is a homomorphism. Every K_α^f is a subgroup under addition. Since f is constant on $\overline{K}_\alpha^f$ it follows that ν is a nonarchimedean valuation and that f can be factored as claimed. □

Corollary 6.3.5. — *Assume that f satisfies the conditions of Theorem 6.3.4 and let v be the associated valuation. Consider the groups*

$$\mathcal{O}_v := \{\kappa \in K \mid f(\kappa) \geq f(1)\}$$

$$\mathfrak{m}_v := \{\kappa \in K \mid f(\kappa) > f(1)\}.$$

Then $\mathcal{O}_v/\mathfrak{m}_v$ is a field and $\mathcal{O}_v \setminus \mathfrak{m}_v$ consists of invertible elements in $\mathcal{O}_v$.

Proof. — For any $x \in K^*$ the sets $\overline{K}_f^{\alpha}$ are shifted (bijectively) under multiplication by x. In particular, if there is an element $y \in \overline{K}_f^{\alpha}$ such that $xy \in \overline{K}_f^{\alpha}$ then for all $y' \in \overline{K}_f^{\alpha}$ the element xy' is also in $\overline{K}_f^{\alpha}$. The set $\mathcal{O}_v \setminus \mathfrak{m}_v$ contains both x and $1 \cdot x$ (for any $x \in \mathcal{O}_v \setminus \mathfrak{m}_v$). Thus for all $x \in \mathcal{O}_v \setminus \mathfrak{m}_v$ there exists an inverse in $\mathcal{O}_v \setminus \mathfrak{m}_v$. □

6.4. AF-functions on Γ^a. —

Proposition 6.4.1. — *Assume that $f_1, f_2 \in \Gamma^a = \mathcal{LF}^{\mathrm{top}}(K, \mathbb{Z}_p)$ are linearly independent (over $\mathbb{Q}_p$) and that they form a c-pair. Then there exists a valuation ν of K such that the $\mathbb{Z}_p$-linear span of f_1, f_2 contains an inertial element $z_\nu^\chi \in \mathrm{I}_\nu^a$. Moreover, for all $\lambda_1, \lambda_2 \in \mathbb{Q}_p$ the restriction of $\lambda_1 f_1 + \lambda_2 f_2$ to $1 + \mathfrak{m}_v$ is identically 0.*

Proof. — By Proposition 4.4.1, the $\mathbb{Z}_p$-linear span of f_1, f_2 contains an AF-function. By Theorem 6.3.4 and definitions in Section 6.2, there exists a valuation ν on K such that this AF-function is equal to z_ν^χ for some inertia element $z_\nu^\chi \in \mathrm{I}_\nu^a$.

Let f be any function in the $\mathbb{Q}_p$-linear span of f_1, f_2. Since both f and z_ν^χ are multiplicative, it suffices to consider them on $\mathcal{O}_v$. By definition, $z_\nu^\chi = 0$ on

$$\mathcal{O}_\nu^* = \mathcal{O}_\nu \setminus \mathfrak{m}_\nu$$

First observe that for $m \in \mathfrak{m}$ with $z_\nu^\chi(m) \neq 0$ we have $f(1+m) = 0$. Indeed, consider the sublattice $C = \langle 1, m \rangle$. Since z_ν^χ is nonconstant on C and since it forms a c-pair with f, we conclude that f is proportional to z_ν^χ on this space. Thus $f(1+m) = z_\nu^\chi(1+m) = 0$ as claimed.

Now assume that $z_\nu^\chi(m) = 0 = z_\nu^\chi(1)$. Then (since z_ν^χ is an AF-function) there exists an $m_1 \in \mathfrak{m}$ with $z_\nu^\chi(m_1) \neq 0$ and $1 > m_1 > m$.

Consider the subgroup $\langle m_1, m\rangle$ with generic element m_1 and put $m_2 = m_1 - m$. Then $z_\nu^\chi(m') = z_\nu^\chi(m_2) \neq 0$ and

$$f(1+m_1) = f(1-m_2) = 0.$$

By Corolllary 6.3.5, we have

$$m_3 := \frac{1}{1+m_1-m_2} \in \mathcal{O}_v \setminus \mathfrak{m}_v.$$

Further, by the logarithmic property,

$$0 = f(1+m_1) + f(1-m_2) = f(1+m_1-m_2) + f(1-m_1m_2m_3).$$

Since

$$z_\nu^\chi(m_1) + z_\nu^\chi(m_2) = 2z_\nu^\chi(m_1) \neq 0$$

(as z_ν^χ takes values in $\mathbb{Z}_p$) and $z_\nu^\chi(m_3) = 0$ (as $m_3 \in \mathcal{O}_v^*$) we have that

$$f(1-m_1m_2m_3) = 0.$$

This concludes the proof. □

Corollary 6.4.2. — *If f_1, f_2 satisfy the conditions of 6.4.1 then there is a valuation ν such that $\langle f_1, f_2\rangle$ lies in the abelian reduced valuation group Γ_ν^a of ν.*

The subgroup of Γ^a generated by f_1, f_2 contains a cyclic subgroup generated by the inertial element z_ν^χ and the quotient of $\langle f_1, f_2\rangle$ by the subgroup generated by AF-elements has at most one topological generator. An analogous statement is true for liftable abelian groups of higher rank.

Lemma 6.4.3. — *Let $f_1, \dots f_n \in \mathcal{LF}(K, \mathbb{Z}_p)$ be linearly independent functions. Suppose that for every i, j the functions f_i, f_j form a c-pair. Then the group F (topologically) generated by $f_1, \dots f_n$ contains a closed subgroup F' consisting of AF-functions such that F/F' is topologically cyclic.*

Proof. — If all f_j are AF-functions then every $\mathbb{Z}_p$-linear combination of f_j is an AF-function. (Indeed, for every 2-dimensional $V \subset K$ and any pair f_i, f_j the restrictions $\mathrm{rk}\,\langle f_{i,V}, f_{j,V}\rangle \leq 2$. Now apply results from 3.4)

Assume that f_1 is not an AF-function. By Proposition 4.4.1, there exist $\lambda_{1j}, \lambda_j \in \mathbb{Z}_p$ such that $\lambda_{1j}f_1 + \lambda_j f_j$ is an AF-function. These functions generate a $\mathbb{Z}_p$-submodule F'' of corank 1, such that F/F'' is a direct sum of a torsion module and a rank one $\mathbb{Z}_p$-module. The torsion elements correspond to AF-functions. Denote by F' the module generated by F'' and (the preimages of) these torsion elements. Then F' consists of AF-functions and F/F' is (topologically) cyclic. $\square$

COROLLARY 6.4.4. — *The subgroup F' generated by AF-elements corresponds to the inertia subgroup of some valuation ν'. The lemma implies that every liftable noncyclic abelian group lies in some reduced valuation group and contains a group of corank one consisting of inertial elements.*

References

[1] Fedor A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Izv. Akad. Nauk SSSR **51(2)**, (1988), 485–516.

[2] F. A. Bogomolov, *Abelian subgroups of Galois groups*, Izv. Akad. Nauk SSSR **55(1)**, (1991), 1–41.

[3] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Proc. of Tokyo Satellite conference ICM-90 Analytic and Algebraic Geometry (1991), 26–52.

[4] F. A. Bogomolov, *Stable cohomology of groups and algebraic varieties*, Math. Sbornik SSSR **185**, (1992), 1–27.

[5] J. W. S. Cassels, A. Fröhlich (eds.), *Algebraic number theory. Proceedings of the conference held at the University of Sussex, Brighton, September 1–17, 1965.* Academic Press, London-New York, (1986).

[6] A. S. Merkur'ev, A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR **46**, (1982), 1011–1046.

[7] S. Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. Math. **138**, (1999), no. 2, 319–423.

[8] F. Pop, *Glimpses of Grothendieck's anabelian geometry*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser. **242**, Cambridge Univ. Press, Cambridge, (1997), 113–126.

[9] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Ann. of Math. **139(1)**, (1994), 145–182.

[10] F. Pop, *Alterations and birational anabelian geometry*, Resolution of singularities (Obergurgl, 1997), 519–532, Progr. Math. **181**, Birkhäuser, Basel, (2000).

[11] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, (1994).

[12] A. A. Suslin, *Algebraic K-theory and the norm residue homomorphism*, VINITI (J. Soviet Math.) **25**, (1984) Moscow (1985), 115–207.

[13] O. Zariski, P. Samuel, *Commutative Algebra*, Springer-Verlag (1958).