CIRM

Numération : mathématiques et informatique

Rencontre organisée par :
Boris Adamczewski, Anne Siegel and Wolfgang Steiner

23-27 mars 2009

Christiaan van de Woestijne

The structure of abelian groups supporting a number system (extended abstract)

Vol. 1, n° 1 (2009), p. 75-79.

<http://acirm.cedram.org/item?id=ACIRM_2009__1_1_75_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

cedram

Texte mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Actes des rencontres du C.I.R.M.
Vol. **1** n° 1 (2009) 75-79

The structure of abelian groups supporting a number system (extended abstract)

Christiaan van de Woestijne

1. Introduction and results

A *number system* is a coherent notation system for numbers. There are many possibilities to define such systems, but in this paper we will consider only generalisations of the *positional* number systems, like the binary and decimal notations. In such systems, one represents numbers by finite expansions of the form

$$a = \sum_{i=0}^{\ell} d_i b^i, \tag{1.1}$$

where the d_i are taken from a finite set of digits, and b is the *base* of the system. For example, taking for b an integer greater than 1 and using digits $\{0, 1, \ldots, b-1\}$, we can represent all natural numbers in the form (1.1), and these representations are in fact unique. However, if we want to represent *all integers* in this form, we must change either the base or the digit set; for example, we can take an integer base b with $b \leq -2$, and digits $\{0, 1, \ldots, |b| - 1\}$.

Looking for the most general sets of "numbers" in which we could possibly represent all elements finitely in the form (1.1) using only a finite digit set, we arrive at the following definitions, which are a generalisation of those given in [7], for example.

Definition 1.2. *A* pre-number system *in an abelian group V is given by an homomorphism $\phi : V \to V$ and a finite set $\mathcal{D} \subseteq V$, such that the elements of $\mathcal{D}$ cover all the cosets of V modulo $\phi(V)$.*

The endomorphism ϕ is called the base *of the pre-number system, and $\mathcal{D}$ is the* digit set*. If $|\mathcal{D}| = |V/\phi(V)|$, we say that $\mathcal{D}$ is* irredundant*, otherwise it is* redundant*.*

A pre-number system $(V, \phi, \mathcal{D})$ is a number system *if every $v \in V$ has a* finite *expansion of the form*

$$v = \textstyle\sum_{i=0}^{\ell-1} \phi^i(d_i)$$

where all d_i are in $\mathcal{D}$ and where ℓ is a positive integer.

If $(V, \phi, \mathcal{D})$ is a number system, we call $\mathcal{D}$ a valid digit set *for the pair (V, ϕ).*

Note that the definition of a pre-number system implies that the image $\phi(V)$ of V under ϕ is a subgroup of *finite index* in V.

Note also that it is possible to define number systems in the same way in non-abelian groups, and examples of this, using crystallographic groups as the underlying group, have been given by Loridant et al. [8]. In this paper, however, we will restrict ourselves to abelian groups.

In order to define more familiar number systems using Definition 1.2, one should think of the group V as the *set of numbers* to be represented, and of the endomorphism ϕ as the *base* of the number system. If the base is just some number b, then define ϕ as the map that multiplies a given element of V by b.

If one takes just $V = \mathbb{Z}$, we recover the well-known b-ary notation of integers, for an integer b with $|b| \geq 2$, if we let ϕ be multiplication by b, and take the digits $\{0, \ldots, |b| - 1\}$.

Text presented during the meeting "Numeration: mathematics and computer science" organized by Boris Adamczewski, Anne Siegel and Wolfgang Steiner. 23-27 mars 2009, C.I.R.M. (Luminy).

More generally, we may take an algebraic integer α as the base, with $V = \mathbb{Z}[\alpha]$ and $\mathcal{D} = \{0, 1, \ldots, |\operatorname{Norm}(\alpha)| - 1\}$. Again, we define ϕ as multiplication by α. This system, if it has the required properties, is a *canonical numeration system* in the terminology of [4, Section 3.1]. In order to have a pre-number system, all the complex embeddings of α must have absolute value greater than 1.

Finally, if f is any monic nonconstant univariate polynomial over $\mathbb{Z}$, we can take $(V, \phi, \mathcal{D})$ to be $\mathbb{Z}[X]/(f)$ with multiplication by X, and digits $\{0, 1, \ldots, |f(0)|-1\}$. If this triple satisfies Definition 1.2, the polynomial f is called a *CNS polynomial* in [9]. The problem of characterising all CNS polynomials is as yet unsolved, even for degree 2, in spite of efforts by many authors.

Conforming to the general analogy between rings of integers ($\mathbb{Z}$, or orders in number fields) and orders in function fields of curves over finite fields, it is possible to define number systems in the function field case as well (see [4, Section 3.5] or [10]). The simplest case is where V is the polynomial ring $\mathbb{F}_q[x]$ itself, the base is any nonconstant polynomial $f \in \mathbb{F}_q[x]$, and the digits are simply all polynomials g with degree less than $\deg f$.

The next simplest case results by taking $V = \mathbb{F}_q[y][x]/(P)$, where $P = p_d x^d + \ldots + p_1 x + p_0$ with $p_i \in \mathbb{F}_q[y]$ and $p_d = 1$, taking base x mod P, and taking as digits all $g \in \mathbb{F}_q[y]$ with degree less than $\deg_y(P(0))$. It is proved in [10] that this construction gives a number system if and only if $\max_{1 \le i \le d} \deg(p_i) < \deg(p_0)$.

One notes that in the last cases, V is a torsion group: all elements have additive order p, where p is the characteristic of the field $\mathbb{F}_q$.

The main question of this note is whether we will get something structurally new if we allow *mixed groups*, i.e., base groups V that have both torsion and torsion-free elements.

2. Conditions on the group structure

If a group V has a number system defined on it, this puts quite a number of restrictions on the group structure of V. We will show several such properties in the remainder of this extended abstract.

We use the following concepts and results from the theory of abelian groups; see [5] for more details.

An element x of a group V is *p-divisible* for a prime number p if the equation $py = x$ is solvable in V, and *divisible* if it is p-divisible for all p. The group V itself is p-divisible or divisible if all its elements are. If a group has no divisible elements, it is called *reduced.* Every group can be embedded in a smallest divisible group, called its *divisible hull* or *division group.* For torsion-free V, the divisible hull is equal to $V \otimes \mathbb{Q}$. Every endomorphism $\phi : V \to V$ can be uniquely extended to the divisible hull. Every group splits as a direct sum of a divisible group and a reduced group.

The torsion subgroup of a group V will be written V^{tor}; recall that V/V^{tor} is torsion-free. The *rank* (or *torsion-free rank*) of a group V is defined as the dimension of $V \otimes \mathbb{Q}$ as a $\mathbb{Q}$-vector space, and is written $\operatorname{rk} V$. It is equal to the cardinality of a maximal linearly independent subset of V/V^{tor}. For every prime p, the set of elements of V that have p-power order is a subgroup V_p, called the *p-component* of V. The torsion subgroup V^{tor} of V is the direct sum of the p-components of V for all p. A torsion group is called *bounded* when the orders of its elements are bounded, in other words, when the group has a nontrivial annihilator in $\mathbb{Z}$.

A subgroup W of a V is *pure* in V if, for every $x \in W$ and $n \in \mathbb{Z}$ the equation $ny = x$ is solvable within W whenever it is solvable in V. If V is torsion-free, then W is pure if and only if V/W is torsion-free.

We will say that V *supports a number system* if V is the first component of any number system $(V, \phi, \mathcal{D})$, where we expressly allow redundant digit sets $\mathcal{D}$. The question is, what properties of V can be proved assuming that V supports a number system.

We conjecture the following.

Conjecture 2.1. *Suppose that the abelian group V supports a number system. Then we have*

$$V = W \oplus T,$$

where T is a bounded torsion group and W is torsion-free of finite rank, and has p-divisible quotients for at most finitely many primes p.

Below, we will show some parts of this conjecture, where we leave the full technical details for a future publication. A full proof seems out of reach at the moment, due to the difficulty of classifying torsion-free groups of finite rank; see [2].

The main part, and the one which remains to prove, is the question whether the torsion subgroup T of V is indeed a direct summand; in other words, whether the (possibly) mixed group V *splits*. If we knew that only split groups V can support a number system, this knowledge will allow the classification of number systems to follow separate paths of torsion groups and torsion-free groups.

For a general abelian group V, this question has been studied by many authors, starting with Baer [3]; an overview is given in Chapter XIV of [6]. The simplest criteria for splitting unfortunately do not work: from the assumption that V supports a number system, we cannot infer that V^{tor} is bounded, nor that V/V^{tor} is free; either of these would have sufficed for our purpose [6, Theorems 100.1 and 101.1].

We give an example where the torsion-free part W is not finitely generated, and hence is not free. Consider the number system $(\mathbb{Z}[1/2]^+, 5/2, \{-2,-1,0,1,2\})$. To see that this is a number system, one first notes that multiplication by $5/2$ is an endomorphism of the additive group of $\mathbb{Z}[1/2]$, whose image is a subgroup of index 5. Let $a/2^e \in \mathbb{Z}[1/2]$, and let d be the smallest integer (in absolute value) congruent to $a/2^e$ modulo 5; we have $|d| \leq 2$. Then a has a finite expansion if and only if $T(a)$ does, where we define

$$T(a) = \frac{a/2^e - d}{5/2} = \frac{\frac{a-2^e d}{5}}{2^{e-1}}.$$

After repeating this process sufficiently often, we may assume that $a \in \mathbb{Z}$, and showing that the integers have an expansion on base $5/2$ with the given digits is easy (see also [1], with the difference that the presence of negative digits allows negative integers to be represented as well).

The group $\mathbb{Z}[1/2]^+$ is 2-divisible and therefore infinitely generated, and it is clearly not free: any two elements are linearly dependent over $\mathbb{Z}$.

Baer's criterion. The way we propose to prove that a group V supporting a number system must split is Baer's splitting criterion, proved in [3] and cited as Exercises 101.5 and 101.6 in [6].

Theorem 2.2. *(Baer) Let T be a torsion group and W a countable torsion-free group (both abelian). Then every group V with $V^{\mathrm{tor}} \cong T$ and $V/V^{\mathrm{tor}} \cong W$ splits, if and only if:*

(i) *if $p_1, \dots, p_i, \dots$ is an infinite set of different primes for which $p_i T$ is strictly contained in T, then W contains no pure subgroup S of finite rank such that G/S has elements $\neq 0$ divisible by all p_i;*

(ii) *if for some prime p, the reduced part of the p-component of T is unbounded, then W contains no pure subgroup S of finite rank such that G/S has elements $\neq 0$ divisible by all powers of p.*

The first aspect to settle is the cardinality of V.

Lemma 2.3. *If V supports a number system, then V is countable.*

Proof. Let $(V, \phi, \mathcal{D})$ be a number system; then the set $\mathcal{D}^*$ of finite words over the finite alphabet $\mathcal{D}$ maps surjectively to V via the evaluation map $(d_0, d_1, \dots, d_n) \mapsto \sum_{i=0}^n \phi^i(d_i)$. As $\mathcal{D}^*$ is countable, so is V. □

Lemma 2.4. *Every number system $(V, \phi, \mathcal{D})$ induces a number system on V/W for any ϕ-invariant subgroup W of V.*

Proof. Clearly, there is an induced endomorphism $\bar{\phi} : V/W \to V/W$. Having this, we see that every expansion $\sum_{i=0}^n \phi^i(d_i)$ with digits in $\mathcal{D}$ is mapped to an expansion $\sum_{i=0}^n \bar{\phi}^i(d_i + W)$. □

Remark. Note that the induced number system on the quotient will usually have a redundant digit set.

Corollary 2.5. *If V supports a number system, then so does V/V^{tor}.*

Proof. The torsion subgroup V^{tor} is invariant under any endomorphism of V, so the lemma is applicable whenever we have a number system $(V, \phi, \mathcal{D})$. □

Lemma 2.6. *If V supports a number system and is a torsion group, then V is bounded.*

Proof. Let $(V, \phi, \mathcal{D})$ be a number system, and let $x \in V$ have the expansion $x = \sum_{i=0}^{n} \phi^i(d_i)$, with $d_i \in \mathcal{D}$. The order of $\phi^i(d_i)$ divides that of d_i, and the order of a sum in V divides the least common multiple of the orders of the summands. This means that the order of x is bounded by the l.c.m. of the orders of the digits. □

Lemma 2.7. *If V supports a number system and is torsion-free, then* $\operatorname{rk} V$ *is finite.*

Proof. Let $(V, \phi, \mathcal{D})$ be a number system on V, and let $D = [V : \phi(V)]$. Then for every $x \in V$, we have $Dx \in \phi(V)$. In particular, if $d \in \mathcal{D}$, then $Dd = \phi(d')$ for some $d' \in V$. By our assumption, there exists a finite expansion

$$d' = \sum_{i=0}^{\ell-1} \phi^i(d_i) \quad (d_i \in \mathcal{D})$$

of length ℓ, so that

$$Dd = \phi(d') = \sum_{i=1}^{\ell} \phi^i(d_{i-1}).$$

Let $L \in \mathbb{N}$ be such that all Dd, for $d \in \mathcal{D}$, have expansions of length at most L, and consider the finitely generated subgroup

$$W = \langle \phi^i(d) \mid d \in \mathcal{D}, 0 \le i \le L-1 \rangle \subseteq V.$$

Then $\phi(W)$ contains $\phi^i(d)$ for all $d \in \mathcal{D}$ and $1 \le i \le L$, so it also contains Dd for all $d \in \mathcal{D}$. By the linearity of ϕ, we find that $DW \subseteq \phi(W)$.

Passing to divisible hulls, we see that $W \otimes \mathbb{Q} \subseteq \phi(W) \otimes \mathbb{Q}$, and because $\dim(\phi(W) \otimes \mathbb{Q}) = \operatorname{rk}(\phi(W)) \le \operatorname{rk}(W) = \dim(W \otimes \mathbb{Q})$, the inclusion is in fact an equality. Because furthermore $\phi(W) \otimes \mathbb{Q} = \phi(W \otimes \mathbb{Q})$ for torsion-free W, we find that $W \otimes \mathbb{Q}$ is invariant under the corresponding extension of ϕ. In particular, $\phi^i(d)$, for every $i \ge 0$ and every $d \in \mathcal{D}$ is contained in $W \otimes \mathbb{Q}$, and by assumption this means that $V \subseteq W \otimes \mathbb{Q}$. Because W is finitely generated, this shows that V has finite rank, and in fact $\operatorname{rk} V \le L \cdot |\mathcal{D}|$. □

Remark. This proof is due to Ryotaro Okazaki.

The following result shows that part (i) of Baer's criterion is always satisfied for groups supporting a number system. The proof uses the theory of types, as well as the fact that by the previous lemma, the endomorphism on V/V^{tor} induced by ϕ is a restriction of a $\mathbb{Q}$-linear map on a finite-dimensional $\mathbb{Q}$-vector space.

Lemma 2.8. *If V supports a number system, then no torsion-free quotient of V has elements $\neq 0$ that are divisible by p, without being p-divisible, for infinitely many distinct primes p.*

The final result is a first approximation of a proof of part (ii) of Baer's criterion. First, we show that if V supports a number system, it can be covered by the images of successive application of the endomorphism ϕ to the subgroup of V generated by the digits; if V is torsion-free, this subgroup is free.

Lemma 2.9. *Let $(V, \phi, \mathcal{D})$ be a number system. Let W be the subgroup of V generated by $\mathcal{D}$, and define $V_0 = W$, $V_{i+1} = V_i \oplus \phi(V_i)$ for $i = 1, 2, \ldots$. Then*

$$\cup_{i=0}^{\infty} V_i = V.$$

Proof. Trivial. □

Next, we show that for one of the archetypal nonsplitting mixed groups, we can prove that endomorphisms that cover the torsion free quotient as described in the lemma do not lift to the mixed group, showing that the mixed group does not support a number system.

Definition 2.10. [6, Chap. XIV, Sec. 100, Example 3] *For some prime p, let $T_p = \oplus_{i=1}^{\infty} \langle a_i \rangle$, where for each $i = 1, 2, \ldots$, the element a_i is torsion of order p^{2i}. Also for each i, define*

$$b_i = (0, \ldots, 0, a_i, pa_{i+1}, p^2 a_{i+2}, \ldots) \in \prod_{i=1}^{\infty} \langle a_i \rangle.$$

Now let $A_p = \langle T_p, b_1, b_2, \ldots \rangle$.

Lemma 2.11. *For each p, the torsion part T_p of the group A_p is not a direct summand.*

Proof. The b_i, as defined above, are of infinite order and satisfy $pb_{i+1} = b_i - a_i$ for $i = 1, 2, \ldots$. Using these relations, it is readily checked that T_p is the torsion part of A_p.

If we had $A_p = T_p \oplus G$ for some subgroup G of A_p, then because $pb_{i+1} \equiv b_i \mod T_p$, the group G would be p-divisible, contrary to the fact that $\prod\langle a_i\rangle$ has no p-divisible subgroups $\neq 0$. □

Theorem 2.12. *Let p be a prime, and define the group A_p as in Definition 2.10. Then the image of the natural map* $\mathrm{End}(A_p) \to \mathrm{End}(A_p/T_p) \cong \mathbb{Z}[1/p]$ *is just* $\mathbb{Z}$.

This result has an immediate bearing on the existence of number systems.

Theorem 2.13. *Let p be a prime, and let the group A_p be as in Definition 2.10. Then A_p does not support a number system.*

Proof. Let ϕ be an endomorphism of A_p whose image has finite index in A_p, and suppose $(A_p, \phi, \mathcal{D})$ is a number system for some finite subset $\mathcal{D} \subseteq A_p$.

By Lemma 2.4, we have an induced number system on the torsion free quotient $A_p/T_p \cong \mathbb{Z}[1/p]^+$. In particular, the powers of the induced endomorphism $\overline{\phi}$ fill up the whole group $\mathbb{Z}[1/p]^+$, as described in Lemma 2.9. If $\overline{\phi}$ is multiplication by n/p^e, we clearly must have $e \geq 1$ for this to happen. But this contradicts Theorem 2.12. □

We hope to prove an analogous result for any nonsplit group of torsion-free rank 1, using the classification of rank-1 mixed groups given in [6, Section 104]. For higher ranks, such a classification seems to be nowhere in sight, and we expect that a full proof of our conjecture will have to wait for further progress in this direction.

Acknowledgements

The research leading to this paper was supported by the Austrian Science Foundation FWF, project S9606, which is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory."

References

[1] Shigeki Akiyama, Christiane Frougny, and Jacques Sakarovitch. Powers of rationals modulo 1 and rational base number systems. *Israel J. Math.*, 168:53–91, 2008.

[2] David M. Arnold. *Finite rank torsion free abelian groups and rings*, volume 931 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1982.

[3] Reinhold Baer. The subgroup of the elements of finite order of an abelian group. *Ann. of Math. (2)*, 37(4):766–781, 1936.

[4] Guy Barat, Valérie Berthé, Pierre Liardet, and Jörg Thuswaldner. Dynamical directions in numeration. *Ann. Inst. Fourier (Grenoble)*, 56(7):1987–2092, 2006.

[5] László Fuchs. *Infinite abelian groups. Vol. I.* Pure and Applied Mathematics, Vol. 36. Academic Press, New York, 1970.

[6] László Fuchs. *Infinite abelian groups. Vol. II.* Academic Press, New York, 1973. Pure and Applied Mathematics. Vol. 36-II.

[7] Attila Kovács. *Radix expansion in lattices.* PhD thesis, Eötvös Loránd University, Budapest, 2001.

[8] Benoit Loridant, Jun Luo, and Jörg M. Thuswaldner. Topology of crystallographic tiles. *Geom. Dedicata*, 128:113–144, 2007.

[9] A. Pethő. On the periodic expansion of algebraic numbers. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 18:167–174, 1999.

[10] Klaus Scheicher and Jörg M. Thuswaldner. Digit systems in polynomial rings over finite fields. *Finite Fields Appl.*, 9(3):322–333, 2003.

Institut für Mathematik B, Technische Universität Graz, 8010 Graz, Austria • c.vandewoestijne@tugraz.at