PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 4, December 1993

ON HOMOGENEOUS NILPOTENT GROUPS AND RINGS

GREGORY CHERLIN, DAN SARACINO, AND CAROL WOOD

(Communicated by Maurice Auslander)

ABSTRACT. We give a new framework for the construction of homogeneous nilpotent groups and rings which goes a long way toward unifying the two cases, and enables us to extend previous constructions, producing a variety of new examples. In particular we find ingredients for the manufacture of $2^{\aleph_0}$ homogeneous nilpotent groups "in nature".

INTRODUCTION

An algebraic structure is *homogeneous* if every isomorphism between two of its finitely generated substructures is induced by an automorphism. Solvable homogeneous groups have been classified up to the determination of the homogeneous nilpotent groups of class 2 and exponent 4 [3], which exist in profusion: in [11] $2^{\aleph_0}$ countable examples of such groups are given. Similarly homogeneous rings have been classified up to the determination of the homogeneous rings which consist of the extension of a nilpotent ideal by a multiplicative identity, which also exist in profusion [1], even in the commutative case [12]. The existence of many homogeneous nilpotent groups of exponent four also places certain limitations on the possible extensions of the finite Suzuki 2-group classification to the infinite setting.

In the present paper we will introduce a formalism for carrying out computations of the sort that occur in the constructions of the second and third authors, involving pairs of vector spaces linked by a quadratic map. In the two cases—nilpotent groups and commutative rings—the technical difficulties are connected with the study of free amalgamation in two rather special categories. We propose here to replace those categories by two somewhat simpler categories and to show that all necessary computations can be carried out in those simpler categories. We will then show what the earlier computations look like in our categories and use the setup to generalize these constructions and to give marginally sharper bounds in the cases studied previously. The main point is

Received by the editors January 22, 1991 and, in revised form, March 30, 1992.
1991 *Mathematics Subject Classification*. Primary 03C60; Secondary 03C10, 20F18, 16A22.
Key words and phrases. Amalgamation, bilinear, category, group, homogeneous, nilpotent, ring.
The first author was supported in part by NSF grant DMS 8903006 and prepared the final version of this paper while a guest of the Institute for Advanced Studies, Hebrew University, Jerusalem, during the year on Field Arithmetic, 1991/92. The second author's work was supported by an appointment as J. H. van Vleck Professor at Wesleyan University during the Fall term, 1990.

0002-9939/93 $1.00 + $.25 per page

that the categories in which we work contain less information than the original categories, while retaining everything of importance for the study of homogeneity. A minor point is that the two categories we introduce (one connected with groups, the other with rings) turn out to be two variations on a single theme: the case of nilpotent groups corresponds to working over the finite field $\mathbb{F}_2$, while the commutative rings are associated with the prime fields $\mathbb{F}_p$ for $p > 2$. (It is known that these constructions are impossible for nilpotent groups of odd exponent or for commutative rings of characteristic 2.)

It may be well to review the general method used in [1, 11, 12], which is due in general to Fraissé, but was first applied to problems of this type by Henson. We suppose we have a family $\mathscr{F}$ of algebraic structures closed under isomorphism and substructure, which is uniformly locally finite, closed under arbitrary directed unions, and has the amalgamation property: for any structures A_1, A_2 in $\mathscr{F}$ with a common substructure A_0, there is an amalgam $A \in \mathscr{F}$ of A_1, A_2 over A_0—this means there are embeddings of A_1, A_2 into A that agree on A_0. (We also allow the case $A_0 = \varnothing$ formally; that is, we require any two structures in $\mathscr{F}$ to have a common extension in $\mathscr{F}$.) There are many such classes, but typically the amalgam is far from unique, and for our present purposes it is necessary to assume that some particular amalgamation procedure has been chosen. This notion will be called "free amalgamation", and in practice it is often determined by a universal property. For our purposes it is more important that the amalgamation procedure be explicitly understood, so that computations of the sort described below can actually be carried out. It will be convenient to refer to A_1, A_2 as the "factors" of their free amalgam.

Given such a family $\mathscr{F}$, with a notion of free amalgamation, we then call a structure A *a-indecomposable* if whenever A is embedded into the free amalgam of two structures over a third, the image of the embedding is contained in one of the two factors. Two a-indecomposable structures are *comparable* if there is an embedding of one in the other, and a set of a-indecomposable structures is an *antichain* if no two of them are comparable.

Fraissé's construction, as applied by Henson, amounts to the following: if there is an infinite antichain of finite, a-indecomposable structures in $\mathscr{F}$, then there are $2^{\aleph_0}$ countable homogeneous structures in $\mathscr{F}$. The question as to whether a significant stock of examples can be created by other means is very interesting, but unfortunately we know nothing about this in the cases of interest here, so we will confine ourselves entirely to the problem of constructing infinite antichains of a-indecomposable finite structures.

We now describe the two cases treated in [11, 12], which involve quite well-behaved categories of algebraic systems. Let $\mathscr{G}$ be the category of groups of exponent four in which all involutions are central. Observe that such groups are nilpotent of class two. Let $\mathscr{R}_p$ be the category of commutative nilpotent rings of characteristic p in which any element whose square is 0 annihilates R. Such rings satisfy $R^3 = (0)$. These categories have a notion of free amalgamation characterized by a universal property, and in [11, 12] the necessary antichain of a-indecomposable structures was produced in each of the two cases.

We will associate auxiliary categories of "quadratic structures" with these categories and show that our auxiliary categories are equivalent to the original ones as far as the study of a-indecomposable objects and embeddings is concerned. Working in our new categories of quadratic structures we will find additional antichains of a-indecomposable objects "in nature", derived from quadratic forms over finite fields. For example, it turns out that the Sylow 2-subgroups of the simple groups $\mathrm{PSU}(3, q^2)$ for $q = 2^l$, l prime, form an infinite antichain of a-indecomposable groups of exponent four in which all involutions are central.

In the case of groups the category we use is related to one introduced explicitly by Hughes in [7] in connection with the study of nilpotent groups of class 2. However, the connection between our "linearized" category and the corresponding category of groups is much closer than the connection in [7] for two reasons:

(1) The class of groups is drastically restricted,
(2) We retain more information by using a quadratic form instead of the associated bilinear form (which in characteristic 2 contains much less information).

The result is that we have a functorial correspondence which is 1-1 at the level of isomorphism types of objects, though we lose (i.e., factor out) some morphisms. In some respects our category is closer to the one used by Gruenberg in [6, p. 185].

1. Quadratic structures in characteristic 2

If U, V are vector spaces over the field $\mathbb{F}_2$, we will say that a function $Q: U \to V$ is *quadratic* if the function $\gamma(x, y) = Q(x) + Q(y) + Q(x+y)$ is an alternating bilinear map. We will say that Q is *nondegenerate* if $Q(x) \neq 0$ for $x \neq 0$. This is not one of the usual notions of nondegeneracy, and our definition would not really be adequate over other fields, even of characteristic 2; but this terminology will work well in our context. Observe that a quadratic map Q is uniquely determined by the function γ together with the values of Q on a basis, and these data may be prescribed arbitrarily.

A *quadratic structure* is a structure $(U, V; Q)$ where U, V are vector spaces over the field $\mathbb{F}_2$ and Q is a nondegenerate quadratic map from U to V. For the initial results (Lemmas 1 and 2 below) it is more convenient to refrain from imposing the nondegeneracy condition; in this case we speak of *weak* quadratic structures.

We let $\mathscr{Q}$ be the category of quadratic structures with morphisms

$$(f, g): (U_1, V_1; Q_1) \to (U_2, V_2; Q_2)$$

given by linear maps $f: U_1 \to U_2$, $g: V_1 \to V_2$ respecting the quadratic structure: $gQ_1 = Q_2 f$. $\mathscr{G}$ is the category of groups of exponent four in which every involution is central.

If $G \in \mathscr{G}$, let $V(G) = \Omega_1 ZG$, $U(G) = G/V(G)$, and let $Q_G: U(G) \to V(G)$ be the map induced by squaring in G. Then $\mathscr{M}(G) = (U(G), V(G); Q_G)$ is a quadratic structure. Furthermore, the associated map γ is the one induced by commutation from $G/VG \times G/VG$ to VG. Note that the map from G to $\mathscr{M}(G)$ is actually given by a functor F from $\mathscr{G}$ to $\mathscr{Q}$. The main point is that F throws away very little information, as the next two lemmas show.

It is convenient to introduce a third category $\mathscr{E}$ whose objects are central extensions

$$\mathbf{1} \to V \to G \to U \to \mathbf{1}$$

with U, V elementary abelian 2-groups and with morphisms given by morphisms of exact sequences (triples of group homomorphisms). The functor $\mathscr{M}$ is the composition of a functor $E: \mathscr{G} \to \mathscr{E}$, which takes a group G in $\mathscr{G}$ to the associated short exact sequence

$$\mathbf{1} \to V(G) \to G \to U(G) \to \mathbf{1},$$

and a functor $\mathscr{M}_*$, which takes the sequence

$$\mathbf{1} \to V \to G \to U \to \mathbf{1}$$

to the weak quadratic structure $(U, V; Q)$ where $Q: U \to V$ is induced by squaring in G. As the functor E takes $\mathscr{G}$ isomorphically onto a full subcategory of $\mathscr{E}$, we work initially with $\mathscr{E}$ and $\mathscr{M}_*$.

We begin by looking at the effect of $\mathscr{M}_*$ on objects.

Lemma 1. *Let U, V be elementary abelian 2-groups. Then:*

(1) *$\mathscr{M}_*$ induces a 1-1 correspondence between equivalence classes of central extensions*

$$\mathbf{1} \to V \to G \to U \to \mathbf{1}$$

and isomorphism types of weak quadratic structures.

(2) *$G \in \mathscr{G}$ iff the corresponding weak quadratic structure is nondegenerate.*

Proof. The second point is clear, so we prove only (1).

We know the central extensions are classified by $H^2(U, V)$ with U acting trivially on V or, more concretely, by normalized 2-cocycles $c: U \times U \to V$, with the cocycle identity

$$c(u_1, u_2) + c(u_1, u_2 + u_3) + c(u_1 + u_2, u_3) + c(u_2, u_3) = 0,$$

and the normalization $c(0, u) = c(u, 0) = 0$, modulo coboundaries $\delta f(u_1, u_2) = f(u_1 + u_2) + f(u_1) + f(u_2)$ where $f: U \to V$ is normalized by $f(0) = 0$. (Since we are working in characteristic 2 we suppress the usual minus signs.) If the extension $\mathbf{1} \to V \to G \to U \to \mathbf{1}$ is represented by the cocycle c then $Q(u) = c(u, u)$.

Our first claim is that every quadratic map Q comes from an extension. We will write down a cocycle c explicitly with $c(u, u) = Q(u)$. Fix an ordered basis (u_i) for U and define

$$c\left(\sum \delta_i u_i, \sum \varepsilon_i u_i\right) = \sum_{i>j} \delta_i \varepsilon_j \gamma(u_i, u_j) + \sum \delta_i \varepsilon_i Q(u_i).$$

One checks that this is a cocycle directly, without using any special properties of the functions Q and γ. One also checks easily that $c(u, u) = Q(u)$, and here the relationship of Q and γ enters in.

For the uniqueness statement, suppose c_1, c_2 are two cocycles corresponding to the same function Q, and consider their difference $c = c_1 - c_2$. Then c satisfies $c(u, u) \equiv 0$, so the corresponding extension has exponent 2 and therefore splits; so c_1, c_2 represent the same extension. □

We now consider the effect of $\mathscr{M}_*$ on morphisms (cf. [6, p. 187, Theorem 1 and the remark following]).

Lemma 2. *Let* (E_i) $\mathbf{1} \to V_i \to G_i \to U_i$ *(for* $i = 1, 2$*) be central extensions with* U_i, V_i *elementary abelian 2-groups, and let* $\mathscr{A}_i = (U_i, V_i; Q_i)$ *be the associated weak quadratic structures. Then:*

(1) *The map* $\mathscr{M}_* : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\mathscr{A}_1, \mathscr{A}_2)$ *is surjective.*
(2) *Taking* $E_1 = E_2 = E$ *and* $\mathscr{A} = \mathscr{M}_*(E)$, *and writing* U, V *for* U_i, V_i, *we have the short exact sequence*

$$\mathbf{1} \to \mathrm{Hom}(U, V) \to \mathrm{Aut}\, E \to \mathrm{Aut}\, \mathscr{A} \to \mathbf{1}.$$

Proof. (1) Let $(f, g) \in \mathrm{Hom}(\mathscr{A}_1, \mathscr{A}_2)$. Then $f : U_1 \to U_2$ and $g : V_1 \to V_2$ and there are induced maps on cohomology:

$$f_*: H^2(U_2, V_2) \to H^2(U_1, V_2), \quad g_* : H^2(U_1, V_1) \to H^2(U_1, V_2).$$

At the level of cocycles these maps are induced by composition with f or g; hence the same applies at the level of the quadratic maps Q (since $Q(u) = c(u, u)$ when Q corresponds to c).

The extensions E_1 and E_2 are represented by cohomology classes α_1 and α_2 in $H^2(U_1, V_1)$ and $H^2(U_2, V_2)$ respectively, and thus $f_*(\alpha_2)$ and $g_*(\alpha_1)$ belong to $H^2(U_1, V_2)$. Now a pair of maps $f : U_1 \to U_2$, $g : V_1 \to V_2$ extends to a morphism from E_1 to E_2 if and only if $f_*(\alpha_2) = g_*(\alpha_1)$ [13, p. 202]. In terms of the associated quadratic maps this means $Q_2 \circ f = g \circ Q_1$, which is exactly what we have assumed.

(2) The surjectivity was proved in part (1). The rest is obvious. □

Now we consider the amalgamation process in $\mathscr{Q}$. Let $\mathscr{M}_0 \hookrightarrow \mathscr{M}_1, \mathscr{M}_2$ be a diagram with embeddings in $\mathscr{Q}$. Let $\mathscr{M}_i = (U_i, V_i; Q_i)$. Let U^*, V^* be the amalgamated direct sums $U_1 \oplus_{U_0} U_2$, $V_1 \oplus_{V_0} V_2$ in the category of vector spaces. Let $\mathscr{M}$ be $(U, V; Q)$ with

$$U = U^*, \qquad V = V^* \oplus (U_1/U_0) \otimes (U_2/U_0),$$

and with $Q : U \to V$ defined by first choosing splittings of U_1, U_2 as $U_0 \oplus U_1'$ and $U_0 \oplus U_2'$, respectively, identifying U_1', U_2' with U_1/U_0, U_2/U_0 and defining

$$Q(u_0 + u_1' + u_2') = Q_0(u_0) + Q_1(u_1') + Q_2(u_2') + \gamma_1(u_0, u_1') + \gamma_2(u_0, u_2') + (u_1' \otimes u_2').$$

Equivalently, $Q \restriction U_i = Q_i$ and $\gamma(u_1', u_2') = u_1' \otimes u_2'$. This is easily seen to be a quadratic map, and since $u_1' \otimes u_2' = 0$ only when one of the factors is zero, the nondegeneracy is also immediate. There are natural maps $\mathscr{M}_1, \mathscr{M}_2 \hookrightarrow \mathscr{M}$ agreeing on $\mathscr{M}_0$, and we claim that $\mathscr{M}$ is a pushout, so let $f_i : \mathscr{M}_i \to \widehat{\mathscr{M}}$ be maps agreeing on $\mathscr{M}_0$ for $i = 1, 2$, where $\widehat{\mathscr{M}} = (\widehat{U}, \widehat{V}; \widehat{Q})$. There are natural maps $f : U \to \widehat{U}$, $g_0 : V^* \to \widehat{V}$ induced by $U_i \to \widehat{U}$, $V_i \to \widehat{V}$. Furthermore relative to the identifications $U_i/U_0 \simeq U_i'$ and the embeddings of U_i' in $\widehat{U}$, there is a map $\hat{\gamma} : U_1' \times U_2' \to \widehat{V}$ inducing a linear map $g_1 : U_1/U_0 \otimes U_2/U_0 \to \widehat{V}$; let $g = g_0 + g_1$. We claim that (f, g) is a morphism, that is, that it preserves Q. On $\mathscr{M}_1, \mathscr{M}_2$ this is certainly the case, so our claim reduces to $g(\gamma(u_1', u_2')) = \hat{\gamma}(fu_1', fu_2')$, which is true by construction since $g(\gamma(u_1', u_2'))$ is just $g_1(u_1' \otimes u_2')$.

We call the quadratic structure $\mathscr{M}$ constructed above the *free amalgam* of $\mathscr{M}_1, \mathscr{M}_2$ over $\mathscr{M}_0$. The following is a reformulation of a result in [10].

Lemma 3. *Let* $G_0 \hookrightarrow G_1, G_2$ *be an amalgamation diagram in* $\mathscr{G}$, *associated to the diagram* $\mathscr{M}_0 \hookrightarrow \mathscr{M}_1, \mathscr{M}_2$ *in* $\mathscr{Q}$. *Let* $\mathscr{M}$ *be the free amalgam of* $\mathscr{M}_1, \mathscr{M}_2$ *over* $\mathscr{M}_0$, *and let* G *be the group associated with* $\mathscr{M}$ *in* $\mathscr{G}$. *Then there are embeddings* $G_1, G_2 \hookrightarrow G$ *with respect to which* G *becomes the free amalgam of* G_1, G_2 *over* G_0 *in* $\mathscr{G}$.

Proof. This is not quite contained in Lemma 2. The embeddings $\mathscr{M}_1, \mathscr{M}_2 \hookrightarrow \mathscr{M}$ give rise to embeddings $\iota_i : G_i \hookrightarrow G$ for $i = 1, 2$, and ι_1, ι_2 induce the same embedding of $\mathscr{M}_0$ into $\mathscr{M}$. Hence they have the same image in G and $\iota_2^{-1}\iota_1$ is an automorphism of G_0 which is trivial on $\mathscr{M}_0$, hence induced by an element ϕ of $\operatorname{Hom}(U_0, V_0)$. We can extend ϕ to an element of $\operatorname{Hom}(U, V)$; let α be the corresponding automorphism of G. Then if we replace ι_2 by $\iota_2\alpha$, ι_1 and ι_2 will agree on G_0 and still induce the given embeddings $\mathscr{M}_i \to \mathscr{M}$. Thus at least G serves as a possible amalgam of G_1, G_2 over G_0.

If $\varepsilon_i : G_i \to H$ is another possible amalgam, we have a map $(f, g) : \mathscr{M} \to \mathscr{M}(H)$ commuting with the given embeddings. This map is induced by some homomorphism $h : G \to H$. The maps $h \circ \iota_i$ agree with the ε_i up to automorphisms of G_i trivial on $\mathscr{M}_i$, induced by homomorphisms $\phi_i : U_i \to V_i$. On U_0 the maps ϕ_i coincide with a map $\phi_0 : U_0 \to V_0$, so they define a map $\phi : U = U_1 \oplus_{U_0} U_2 \to V_1 \oplus_{V_0} V_2 \subseteq V$. If we correct the map h by the automorphism corresponding to ϕ, we get a map from G to H whose composition with each ι_i equals the given ε_i. □

Lemma 4. *A group* $G \in \mathscr{G}$ *is a-indecomposable iff the associated quadratic structure* $\mathscr{M}$ *is a-indecomposable in* $\mathscr{Q}$.

Proof. An embedding into a free amalgam in either category can be transferred to a similar embedding in the other category; and the location of the image in one category controls the location of the image in the other category. □

2. Quadratic structures in odd characteristic

In setting up a category $\mathscr{Q}_p$ which controls $\mathscr{R}_p$ in the same way that $\mathscr{Q}$ controls $\mathscr{G}$ we will see that very little changes, though the situation becomes somewhat simpler.

In odd characteristic p we will take our quadratic structures to be of the form $(U, V; \gamma)$ where U, V are vector spaces over the prime field $\mathbb{F}_p$ and $\gamma : U \times U \to V$ is a symmetric bilinear map, and we impose the strong nondegeneracy condition $\gamma(u, u) \neq 0$ for $u \neq 0$, as before. (We could also work with $Q(u) = \frac{1}{2}\gamma(u, u)$ to keep the development closer to the previous case.) This gives rise to a category $\mathscr{Q}_p$ of quadratic structures in characteristic p, with morphisms given by pairs of linear maps (f, g) respecting γ. If we allow $p = 2$ then $\mathscr{Q}_2$ and $\mathscr{Q}$ are quite distinct categories; since $\gamma(u, u)$ would be linear in this case, the nondegeneracy condition turns out to be very restrictive.

Recall that the category $\mathscr{R}_p$ consists of commutative nilpotent rings R of characteristic p in which every element with $x^2 = 0$ annihilates R and that such rings satisfy $R^3 = (0)$. Given a ring $R \in \mathscr{R}_p$, let $V = \operatorname{Ann} R$, $U = R/V$. Let $\gamma : U \times U \to V$ be induced by multiplication. Then $(U, V; \gamma)$ is a quadratic structure, and indeed this correspondence extends to a functor from $\mathscr{R}_p$ to $\mathscr{Q}_p$.

As before we can factor $\mathscr{M}$ through the category $\mathscr{E}_p$ of exact sequences

$$\mathbf{0} \to V \to R \to U \to \mathbf{0}$$

in which R is an $\mathbb{F}_p$-algebra, $R^2 \subseteq V$, $RV = VR = (0)$. There is no advantage in imposing either nondegeneracy or commutativity on these extensions. Accordingly we will take as the class of *weak* quadratic structures all structures $(U, V; Q)$ with $Q : U \times U \to V$ bilinear.

An $\mathbb{F}_p$-algebra extension of this type will be called a *singular* extension (cf. [9, Chapter X, §3]). With U, V fixed, these singular extensions are classified by Hochschild cohomology $H^2(U, V)$, but of such a degenerate type that there is little to be gained from this point of view.

Lemma 5. *Let U, V be elementary abelian p-groups, and view U as an $\mathbb{F}_p$-algebra with trivial multiplication, and V as a trivial U-module. Then:*

(1) *$\mathscr{M}_*$ induces a 1-1 correspondence between equivalence classes of singular extensions*

$$\mathbf{0} \to V \to R \to U \to \mathbf{0}$$

and isomorphism types of weak quadratic structures.

(2) *$R \in \mathscr{R}_p$ iff the corresponding weak quadratic structure $\mathscr{M}(R)$ is a quadratic structure, i.e., Q is symmetric and nondegenerate.*

Proof. (1) This is all immediate, unlike Lemma 1. Given a weak quadratic structure $(U, V; Q)$ let $R = U \oplus V$ with $UV = VU = (0)$ and with multiplication on U defined by γ. Since all extensions under consideration split as abelian groups, and $RV = VR = 0$, the uniqueness is also clear.

(2) As before, this is clear. □

Lemma 6. *Let (E_i) $\mathbf{1} \to V_i \to R_i \to U_i$ be singular extensions with U_i, V_i elementary abelian p-groups carrying trivial ring and module structures, respectively, and let $\mathscr{A}_i = (U_i, V_i; Q_i)$ be the associated weak quadratic structures. Then:*

(1) *The map $\mathscr{M}_*: \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\mathscr{A}_1, \mathscr{A}_2)$ is surjective.*

(2) *Taking $E_1 = E_2 = E$ and $\mathscr{A} = \mathscr{M}_*(E)$ and writing U, V for U_i, V_i, there is the short exact sequence*

$$\mathbf{1} \to \mathrm{Hom}(U, V) \to \mathrm{Aut}\, E \to \mathrm{Aut}\, \mathscr{A} \to \mathbf{1}.$$

Proof. In view of the very simple structure of the rings R_i, this is clear. □

The next step is to describe the operation of free amalgamation in $\mathscr{Q}_p$, which is nearly identical to the construction in $\mathscr{Q}$, taking $\gamma \restriction (U_i \times U_i) = \gamma_i$, and taking $\gamma \restriction (U_1' \times U_2')$ to be essentially the canonical map into the tensor product (after identifying U_i' with U_i/U_0). Then we can return at once to the category $\mathscr{R}_p$:

Lemma 7. *Let $R_0 \hookrightarrow R_1, R_2$ be an amalgamation diagram in $\mathscr{R}_p$, associated to the diagram $\mathscr{M}_0 \hookrightarrow \mathscr{M}_1, \mathscr{M}_2$ in $\mathscr{Q}_p$. Let $\mathscr{M}$ be the free amalgam of $\mathscr{M}_1, \mathscr{M}_2$ over $\mathscr{M}_0$, and let R be the ring associated with $\mathscr{M}$ in $\mathscr{R}_p$. Then there are embeddings $R_1, R_2 \hookrightarrow R$ with respect to which R becomes the free amalgam of R_1, R_2 over R_0 in $\mathscr{R}_p$.*

Finally, as in the case of groups we can read off:

Lemma 8. *A ring $R \in \mathscr{R}_p$ is a-indecomposable iff the associated quadratic structure $\mathscr{M}$ is a-indecomposable in $\mathscr{Q}_p$.*

3. Some antichains in $\mathscr{Q}$ and $\mathscr{Q}_p$

At this point we have an exact correspondence between the a-indecomposable objects in the two categories $\mathscr{G}$ and $\mathscr{Q}$ and a similar correspondence for the two categories $\mathscr{R}_p$ and $\mathscr{Q}_p$, which preserves the relation of embeddability. So the study of antichains of a-indecomposable objects in $\mathscr{G}$ or $\mathscr{R}_p$ can now be transferred completely to $\mathscr{Q}$ or $\mathscr{Q}_p$. For the remainder of the paper we work in $\mathscr{Q}$ and $\mathscr{Q}_p$. We repeat that each infinite antichain in $\mathscr{Q}$ produces $2^{\aleph_0}$ homogeneous nilpotent groups (in $\mathscr{G}$) and each antichain in $\mathscr{Q}_p$ produces $2^{\aleph_0}$ homogeneous nilpotent rings, by the Fraissé technology.

In the present section we give some examples of antichains occurring naturally in $\mathscr{Q}$ and $\mathscr{Q}_p$. In succeeding sections we will combine these examples with the constructions of [11, 12] to get a very rich collection of antichains.

Fix a prime p throughout. For any $d \geq 1$ let F_d, F_{2d} be the finite fields of order p^d, p^{2d} respectively. Let $\mathscr{F}_d^{(p)} = (F_{2d}, F_d; N)$ where $N : F_{2d} \to F_d$ is the norm from F_{2d} to F_d. These will be our examples. (When the superscript p is understood we will often omit it.) If σ generates the Galois group of F_{2d} over F_d, then the associated bilinear map γ is $\mathrm{Tr}(xy^\sigma)$ with Tr the trace. These structures are in $\mathscr{Q}$ for $p = 2$ and in $\mathscr{Q}_p$ for $p > 2$. $\mathscr{F}_d^{(2)}$ corresponds to the Sylow 2-subgroup of $\mathrm{PSU}(3, (2^d)^2)$, which for $d = 1$ is the quaternion group and for $d = 2$ is another homogeneous group.

In our discussion of a-indecomposability we will treat the cases $p = 2$, $p > 2$ separately.

Remark. Suppose $p = 2$. Let $\mathscr{A} = (U, V; Q)$ be the free amalgam of two quadratic structures $\mathscr{A}_1, \mathscr{A}_2$ over a common substructure $\mathscr{A}_0$. Suppose that $u, \tilde{u} \in U$ satisfy:

(1) At least one of $u, \tilde{u}$ lies outside $U_1 \cup U_2$, and both lie outside U_0.
(2) Either $Q(u) = Q(\tilde{u})$, or $\gamma(u, \tilde{u}) = 0$.

Then we may conclude that $\tilde{u} \in u + U_0$.

Lemma 9. *The structure $\mathscr{F}_d^{(2)}$ is a-indecomposable.*

Proof. In $\mathscr{F}_d$ we have the following property: for any two elements $u, \hat{u}$ of F_{2d}, there is an element $\tilde{u}$ such that

$$(*) \qquad \gamma(u, \tilde{u}) = 0 \quad \text{and} \quad N(\tilde{u}) = N(\hat{u}).$$

Suppose that $(f, g) : \mathscr{F}_d^{(2)} \hookrightarrow \mathscr{A}$ embeds $\mathscr{F}_d^{(2)}$ into the free amalgam $\mathscr{A}$ of $\mathscr{A}_1, \mathscr{A}_2$ over $\mathscr{A}_0$. Let $u, \hat{u}$ be two elements of F_{2d}, and suppose that $f(u), f(\hat{u})$ lie outside U_1, U_2. Choosing $\tilde{u}$ as in $(*)$, as $N(\tilde{u}) = N(\hat{u})$ we find $f(\tilde{u})$ also lies outside of U_1, U_2, and hence our foregoing remark implies that $\hat{u} \in u + U_0$. In other words, there is an element $a \in U$ so that $f[F_{2d}]$ is contained in $U_1 \cup U_2 \cup (a + U_0)$.

If $f[F_{2d}]$ is contained in $U_1 \cup U_2$ then as this image is closed under addition, it is contained in one (or both) of the factors. If on the other hand $f[F_{2d}]$ contains an element a not in $U_1 \cup U_2$, then it follows that $f[F_{2d}] = A \oplus \langle a \rangle$ with $A_0 \leq U_0$. Hence on the image of f, γ takes values in $V_1 \oplus_{V_0} V_2$, so that

$Q(a)$ does not lie in the image of γ, since it has a nontrivial component in $U_1/U_0 \otimes U_2/U_0$. However, in $\mathscr{F}_d^{(2)}$ $\gamma(1, x)$ is the trace of x, and the trace is surjective. □

We turn to the proof of a-indecomposability in odd characteristic. In order to formulate a suitable version of our initial remark we need some additional notation. If $\mathscr{A} = (U, V; \gamma)$ is the free amalgam of two quadratic structures $\mathscr{A}_1, \mathscr{A}_2$ in $\mathscr{Q}_p$ over a common substructure $\mathscr{A}_0$, and $u \in U$, we define $u^* \in U/U_0$ as follows. U/U_0 may be identified with $U_1/U_0 \oplus U_2/U_0$. For $u \in U$, let $\bar{u} = (\bar{u}_1, \bar{u}_2)$ be the corresponding element of U/U_0, and let $u^* = (\bar{u}_1, -\bar{u}_2)$.

Remark. Fix $p > 2$. Let $\mathscr{A} = (U, V; \gamma)$ be the free amalgam of two quadratic structures $\mathscr{A}_1, \mathscr{A}_2$ over a common substructure $\mathscr{A}_0$ in $\mathscr{Q}_p$. Suppose that $u, \tilde{u} \in U$ satisfy:

(1) At least one of $u, \tilde{u}$ lies outside $U_1 \cup U_2$, and both lie outside U_0.
(2) $\gamma(u, \tilde{u}) = 0$.

Then $\tilde{u} \in \mathbb{F}_p u^*$.

Lemma 10. *For $p > 2$ the structure $\mathscr{F}_d^{(p)}$ is a-indecomposable.*

Proof. Suppose that $\iota = (f, g) : \mathscr{F}_d^{(p)} \hookrightarrow \mathscr{A}$ embeds $\mathscr{F}_d^{(p)}$ into the free amalgam $\mathscr{A}$ of $\mathscr{A}_1, \mathscr{A}_2$ over $\mathscr{A}_0$. Let $L = \{a \in \mathbb{F}_{2d} : a^\sigma = -a\}$, where σ generates the Galois group of F_{2d} over F_d.

Case 1. Suppose that for some $u \in F_{2d}$, we have $f(u) \in U_1 - U_0$.

(1) For $a \in L$, we have $f(au) \in U_1$.

This follows because $\gamma(u, au) = 0$.

(2) For $a \in L$, we have $f(a^2u) \in U_1$.

If $f(au) \notin U_0$ then this follows from (1). If $f(au) \in U_0$ then $f((a+1)u) \in U_1 - U_0$ and by (1) we have $f(a(a+1)u) \in U_1$, which with (1) yields (2).

Now let $K = \{a \in F_{2d} : f(au) \in U_1\}$. It follows from (2) that K contains the elements of F_d which are not squares in F_d, and as any element of F_d is a sum of two such elements, K contains F_d. At the same time K contains L and $F_d \oplus L = F_{2d}$, so $K = F_{2d}$, as desired.

Of course we may deal similarly with the case in which the image of f meets $U_2 - U_0$.

Case 2. For some $u \in F_{2d}^\times$, $f(u) \in U_0$; and for any $u \in F_{2d}$, if $f(u) \in U_1 \cup U_2$ then $f(u) \in U_0$.

Let $I = \{u \in F_{2d} : f(u) \in U_0\}$ and $R = \{a \in F_{2d} : aI \leq I\}$. Then R is a subring of F_{2d}, and hence a subfield. If $a \in F_{2d}$ has $N(a) = 1$ and $u \in I$, then $N(au) = N(u)$ and $Q(f(au)) = Q(f(u)) \in V_0$, so $f(au) \in U_1 \cup U_2$, and hence $f(au) \in U_0$; so $a \in R$. Thus R contains at least $p^d + 1$ elements, and hence the dimension of R over $\mathbb{F}_p$ is at least $d + 1$; since R is a subfield of F_{2d}, this forces $R = F_{2d}$, as desired.

Case 3. For all $u \in F_{2d}^\times$, $f(u) \notin U_1 \cup U_2$.

Fix $u \in F_{2d}^\times$. For $a \in L$, as $\gamma(u, au) = 0$, we have $au \in \mathbb{F}_p u^*$. If $d > 1$ then $|L| > |\mathbb{F}_p|$ and we can find $a, b \in L$ distinct with $(a - b)u \in U_0$, a contradiction. If $d = 1$ we have a basis $1, t$ for F_{2d} with $\gamma(1, t) = 0$ and $Q(t) = -\varepsilon \in \mathbb{F}_p$ with ε a nonsquare in $\mathbb{F}_p$. If $f(1) = u$ then we have

$\overline{f(t)} = \alpha u^*$ for some $\alpha \in \mathbb{F}_p$, and then examining the coefficient of $Q(u)$ and of $Q(f(t))$ in $U_1/U_0 \otimes U_2/U_0$, we find $\alpha^2 = \varepsilon$, a contradiction. □

Now with p any fixed prime, we look for antichains among the quadratic structures $\mathscr{F}_d^{(p)}$. For the remainder of this section we will write $\mathscr{F}_d$ for $\mathscr{F}_d^{(p)}$. Our analysis of embeddings between two such structures depends on the following.

Lemma 11. *Let A, B be two abelian groups, and let $f: A \to B$ be a* 1-1 *function satisfying*

$$f(a-b) = \pm(f(a) - f(b)) \quad \textit{for all } a, b \in A,$$

where the sign may depend on the choice of a and b. Assume that A is not an elementary abelian 2-group. Then f is a homomorphism.

Proof. Taking $a = b$ yields

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

Fix $c \in A$ with

(2) $$2c \neq 0.$$

As $f(-c) = \pm f(c)$ we find:

(3) $$\text{If } 2c \neq 0 \text{ then } f(-c) = -f(c).$$

As $f(c) = f(2c - c) = \pm(f(2c) - f(c))$ we find:

(4) $$\text{If } 2c \neq 0 \text{ then } f(2c) = 2f(c).$$

For any $b \in A$, using $c + b = b - (-c)$ yields

(5) $$f(c+b) = \pm(f(c) + f(b)).$$

In fact we claim

(6) $$f(c+b) = f(c) + f(b) \quad \text{for all } b \in A.$$

Suppose that $f(c+b) \neq f(c) + f(b)$, that is,

($6^\perp$) $$f(c+b) = -f(c) - f(b) \neq f(c) + f(b).$$

Then

$$f(b) = f((c+b) - c) = \pm(f(c+b) - f(c)) = \pm(2f(c) + f(b)).$$

If $f(b) = 2f(c) + f(b)$ then $0 = 2f(c) = f(2c)$, a contradiction. If $f(b) = -(2f(c) + f(b))$ then the inequality in ($6^\perp$) is contradicted. Thus ($6^\perp$) is untenable, and (6) holds.

Now suppose $d \in A$ and

(7) $$2d = 0.$$

Then $2(c+d) \neq 0$, so for $b \in A$ we find $f(c+d+b) = f(c+d) + f(b) = f(c) + f(d) + f(b)$, $f(c+d+b) = f(c) + f(d+b)$; hence,

(8) $$f(d+b) = f(d) + f(b) \quad \text{for all } b \in A.$$

As (6), (8) together cover all cases, f is a homomorphism. □

With more patience one can get the same conclusion when A is an elementary abelian 2-group of rank at least three.

Lemma 12. *The structure $\mathscr{F}_d$ embeds into the structure $\mathscr{F}_{d'}$ if and only if d' is an odd multiple of d.*

Proof. If d' is an odd multiple of d then the fields F_d, F_{2d} are contained naturally in $F_{d'}$, $F_{2d'}$, and the norm from $F_{2d'}$ to $F_{d'}$ restricts to give the norm from F_{2d} to F_d.

Suppose now that $f : \mathscr{F}_d \to \mathscr{F}_{d'}$ is an embedding induced by injections $f_1 : F_{2d} \to F_{2d'}$ and $f_2 : F_d \to F_{d'}$ which preserve the additive structure. For $a \in F_{2d'}^{\times}$ the pair of maps $\alpha_1 : F_{2d'} \to F_{2d'}$ and $\alpha_2 : F_{d'} \to F_{d'}$ given by multiplication by a and $N(a)$ respectively define an automorphism of $\mathscr{F}_{d'}$. As such automorphisms act transitively on the nonzero vectors of $F_{2d'}$, we may assume that $f_1(1) = 1$, hence taking norms also $f_2(1) = 1$. Let A, B be the kernels of the norm maps from F_{2d} to F_d and from $F_{2d'}$ to $F_{d'}$ respectively. On A and B we have the law

$$N(x+y) = 2 + \mathrm{Tr}(xy^{-1}).$$

Hence from $f_2(N(x+y)) = N(f_1(x) + f_1(y))$ we get

$$2 + \mathrm{Tr}(f_1(xy^{-1})) = 2 + \mathrm{Tr}(f_1(x)f_1(y)^{-1}).$$

Taking $a = f_1(xy^{-1})$, $b = f_1(x)f_1(y)^{-1}$, we find $\mathrm{Tr}a = \mathrm{Tr}b$, $N(a) = N(b) = 1$, and hence a is b or b^{-1}. Thus the triple $(A, B, f_1 \upharpoonright A)$ satisfies the hypotheses of the previous lemma (written there in additive notation) and f_1 is a homomorphism on A. In particular $|A|$ divides $|B|$, and from this it follows easily that d' is an odd multiple of d. We can go a little further: since f_1 respects addition and A generates F_{2d} additively, it follows that f_1 is a field embedding. Since f respects the norm, it again follows that d' is an odd multiple of d. □

As a byproduct of this argument, we see that the automorphism group of $\mathscr{F}_d$ is the semidirect product of F_{2d} with the Galois group of F_{2d} over the prime field, and that all embeddings from $\mathscr{F}_d$ into $\mathscr{F}_{d'}$ are conjugate under $\mathrm{Aut}\,\mathscr{F}_{d'}$. The first statement could also be made to follow from Kantor's [8]; for this remark we thank Simon Thomas.

Corollary. *With p fixed, let X be the set of prime numbers, or the set of powers of 2, and let $\mathscr{X}$ be $\{\mathscr{F}_d^{(p)} : d \in X\}$. Then $\mathscr{X}$ is an infinite antichain of a-indecomposable quadratic structures.*

As an immediate consequence of this corollary, we may construct $2^{\aleph_0}$ countable homogeneous nilpotent groups of class 2 and exponent 4, none of which contains a quaternion subgroup. From one point of view this is a disappointment: a priori it seemed possible that such a restriction would lead to a decent structure theorem.

The foregoing construction gives an alternate route to the main result of [11, 12]. In the remainder of the present paper we will combine our antichain with the ones produced in [11, 12] to get much richer antichains of a-indecomposable structures, that are naturally represented as 2-parameter families of a-indecomposable structures.

4. More antichains in $\mathscr{Q}$

We take $p = 2$ throughout the present section. We will make use of the orthogonal direct sum of a family of quadratic structures $\mathscr{M}_i = (U_i, V_i; Q_i)$,

$\overset{\perp}{\bigoplus}_i\mathscr{M}_i = (\bigoplus_i U_i, \bigoplus_i V_i; \overset{\perp}{\bigoplus} Q_i)$ where by definition $\overset{\perp}{\bigoplus} Q_i(\sum_i u_i) = \sum_i Q_i(u_i)$ for $u_i \in U_i$. If $Q = \overset{\perp}{\bigoplus}_i Q_i$ then the associated bilinear γ satisfies $\gamma(U_i, U_j) = 0$ for $i \neq j$, so these spaces are orthogonal in the sense of γ. It should be noted that the orthogonal direct sum is indeed again nondegenerate. In a similar vein, if $u \in U$ then $u^\perp$ denotes the kernel of $\gamma(u, \cdot)$.

Let $\mathscr{M} = (U, V; Q)$ be a fixed finite a-indecomposable quadratic structure of characteristic 2, which we will call the *initial* structure, and fix a decomposition of U as $\langle u \rangle \oplus U'$. We are going to build an infinite series of a-indecomposable structures $\mathscr{M}_n$ associated with $\mathscr{M}$. In some cases the structures $\mathscr{M}_n$ will form an antichain for large enough n. We do not have a good general criterion for this, but we will show by an abstract argument that there are no "nice" embeddings between the $\mathscr{M}_n$ and use ad hoc considerations to show in special cases that all embeddings are nice, in the appropriate sense.

Let $\mathscr{A}_i = (U_i, V_i; Q_i)$ be a sequence of isomorphic copies of $\mathscr{M}$. Correspondingly write $U_i = \langle u_i \rangle \oplus U_i'$. Let $T^n = \bigoplus_{i \leq n} U_n$, $W^n = \bigoplus_{i \leq n} V_n$. Set $U^{0,n} = A^n \oplus T^n$ where $A^n = \langle a_1, \dots, a_n \rangle$ is an additional n-dimensional space, and set $V^{0,n} = B^n \oplus C^n \oplus W^n$ where $B^n = \langle b_1, \dots, b_n \rangle$ and $C^N = \langle c_2, \dots, c_n \rangle$ are supplementary spaces of dimensions n and $n-1$ respectively. Define $Q^{0,n}$ as follows:

(1) $$Q^{0,n} = \overset{\perp}{\bigoplus} Q_i \quad \text{on } T^n;$$

(2) $$Q^{0,n}(a_i) = \gamma^{0,n}(a_i, u_i) = b_i;$$

(3) $$\gamma^{0,n}(a_i, a_j) = c_j \quad \text{for } i < j;$$

(4) $$\gamma^{0,n}(a_i, u_j) = (0) \quad \text{for } i \neq j, \qquad \gamma^{0,n}(a_i, U_j') = (0) \quad \text{for all } i, j.$$

Finally we define $\mathscr{M}_n = (U^n, V^n; Q^n)$ as follows:

$$U^n = U^{0,n}; \qquad V^n = V^{0,n}/\langle \textstyle\sum_i b_i, \sum_i c_i \rangle; \qquad Q^n \text{ is induced by } Q^{0,n}.$$

We will continue to give the same names to elements of V^n that we gave to their preimages in $V^{0,n}$; since we work exclusively in $\mathscr{M}_n$, it follows for example that $\sum_i b_i$ should now be considered to be 0.

Lemma 13. *For $n \geq 3$, $\mathscr{M}_n$ is a quadratic structure.*

Proof. It is necessary to check that Q^n is nondegenerate. Observe that for $n = 2$ we find $Q(a_1 + a_2) = b_1 + b_2 + c_2 = 0$, so that $\mathscr{M}_2$ is degenerate. If $a \in A^n$ and $t \in T^n$ then $Q(a+t) \in (B^n \oplus C^n) + Q(t)$, so if $Q(a+t) = 0$ then $t = 0$ and $Q(a) = 0$. In particular, since the B^n-component of $Q(a)$ is 0, either $a = 0$ or $a = \sum_{i \leq n} a_i$. But in the second case $Q(a) = c_2 + c_4 + \cdots \neq 0$ since $n \geq 3$. $\square$

Lemma 14. *Suppose that the initial quadratic structure $\mathscr{M}$ is a-indecomposable. Then the derived structures $\mathscr{M}_n$ are also a-indecomposable.*

Proof. Let $\mathscr{N}$ be the free amalgam of two structures $\mathscr{N}_1, \mathscr{N}_2$ over a common substructure $\mathscr{N}_0$, and suppose $\iota = (f, g)$ is an embedding of $\mathscr{M}_n$ into $\mathscr{N}$. Each copy $\mathscr{A}_i$ of $\mathscr{M}$ in $\mathscr{M}_n$ is carried by ι into one or the other factor of

$\mathcal{N}$. However, the various copies of $\mathcal{M}$ are orthogonal in $\mathcal{M}_n$ (with respect to γ), whereas in the free amalgam elements of different factors can be orthogonal only if one of them lies in the common part $\mathcal{N}_0$. It follows that $\iota[\overset{\perp}{\bigoplus}_i \mathcal{A}_i]$ is wholly contained in (at least) one of the two factors, which we may take to be $\mathcal{N}_1$.

The next step is to check that $f(a_i)$ lies in one or the other factor, for each i. If $f(u_i)$ is in $\mathcal{N}_0$ then this follows from the relation $Q^n(a_i) = \gamma^n(a_i, u_i)$. If $f(u_i)$ is not in $\mathcal{N}_0$ then the relations $\gamma^n(a_j, u_i) = 0$ for $j \neq i$ force all u_j to lie in $\mathcal{N}_1$ for $j \neq i$; but then $\sum_k Q^n(a_k) = 0$ forces $f[Q^n(a_i)]$ to lie in $\mathcal{N}_1$, and hence $f(a_i)$ is in one of the two factors, in view of the definition of Q in the free amalgam.

So now each element $f(a_i)$ lies in one of the two factors. Suppose that two elements $f(a_i)$ and $f(a_j)$ do not lie in the same factor and $i < j$. If $j < k$ then as $\gamma(a_i, a_k) = \gamma(a_j, a_k)$ and each of these three elements lies in one factor or the other, we get a contradiction, in view of the structure of the free amalgam. It follows that we must have $j = n$ and that all $f(a_i)$ lie in the same factor for $i < n$. But now the relation $\sum_i \gamma(a_i, a_{i+1}) = 0$ yields a contradiction after applying f. □

Lemma 15. *Let $\iota = (f, g)$ be an embedding of $\mathcal{M}_m$ into $\mathcal{M}_n$ such that $f[A^m] \subseteq A^n$, where $m, n \geq 3$. Then $m = n$, and $f \restriction A^m$ is induced by a permutation of the coordinates (if $n > 3$, this is at worst a transposition of (1), (2)).*

Proof. Let $f(a_i) = \sum_i \delta_{ik} a_k$ and let $f(u_i) \equiv \sum_i \varepsilon_{ik} u_k \mod A^n \oplus \bigoplus_i U_i'$, with coefficients $\delta, \varepsilon \in \mathbb{F}_2$. Look at the B-components of the relations derived by applying ι to $Q(a_i) = \gamma(a_i, u_i)$ and $\gamma(a_i, u_j) = 0$ for $i \neq j$. These are $\sum \delta_{ik} b_k = \sum_i \delta_{ik} \varepsilon_{ik} b_k$ and $\sum \delta_{ik} \varepsilon_{jk} b_k = 0$, both interpreted in V^n. In other words:

(1) Either $\delta_{ik}\varepsilon_{ik} = \delta_{ik}$ for all k, or else $\delta_{ik}\varepsilon_{ik} = \delta_{ik} + 1$ for all k.
(2) Either $\delta_{ik}\varepsilon_{jk} = 0$ for all k, or else $\delta_{ik}\varepsilon_{jk} = 1$ for all k.

We will now eliminate the second alternative in both cases. We fix i. If for some k we have $\delta_{ik} = 0$ then the second alternative is untenable in both cases, regardless of the choice of j. Suppose now that for our fixed i, $\delta_{ik} = 1$ for all k. Then for all j (including i) conditions (1), (2) state that $\varepsilon_{jk} = \varepsilon_j$ is independent of k. We will show further that $\varepsilon_j = 1$ for $j \neq i$. If to the contrary $\varepsilon_j = 0$ for some $j \neq i$, then (1) says that also $\delta_{jk} = \delta_j$ is independent of k. But this means that $f(a_j)$ is either 0 or $f(a_i)$, a contradiction. So indeed $\varepsilon_j = 1$ for all $j \neq i$. As $n \geq 3$, for any i' we can apply (2) with some $j \neq i, i'$ to conclude that $\delta_{i'k}$ is also independent of k, yielding the same contradiction as above.

Thus conditions (1), (2) reduce to

$$\delta_{ik}\varepsilon_{ik} = \delta_{ik}, \quad \delta_{ik}\varepsilon_{jk} = 0 \qquad \text{for all } k, \text{ when } i \neq j.$$

For $i \leq m$, if we define $S_i = \{k : \delta_{ik} = 1\}$, it follows that the sets S_i are pairwise disjoint. Then the equation derived from $\sum Q^n(a_i) = 0$ by applying ι forces the S_i to cover $\{1, \ldots, n\}$, by considering its B-component, and it forces the sets S_i to be singletons, by considering the C-component and bearing in mind that the sets are disjoint. Since $\{1, \ldots, n\}$ can be covered by m disjoint singletons, $m = n$, and $f \restriction A^m$ is induced by a permutation of the coordinates. For the final statement, assume $n > 3$, and let d_i be the number of distinct nonzero values assumed by the function $\gamma(a_i, a_j)$ as j varies. For any $i > 1$, this is $n - i + 1$, and for $i = 1$ it is $n - 1$. Thus we can at worst permute a_1, a_2. □

Now fix $d > 1$. Taking $\mathcal{F}_d$ as the initial structure, construct the sequence $\mathcal{M}_n^{(d)}$ of associated a-indecomposable structures as described above. For the antichain property it will be important that in $\mathcal{F}_d$ two sets of the form $u^\perp$ with $u \in F_{2d}^\times$ either coincide or meet in (0).

Lemma 16. *Let $f : \mathcal{M}_m^{(d)} \hookrightarrow \mathcal{M}_n^{(d')}$ be an embedding. Then $f[A^m] \leq A^n$.*

Proof. Let π_k be the projection of U^n onto the kth component U_k of T^n and $\tau_k = \pi_k f : U_m^{(d)} \to U_k$. Let $t_{i,k} = \tau_k(a_i)$, $t'_{i,k} = \tau_k(u_i)$. Our goal is to prove that each $t_{i,k} = 0$.

Suppose first that for some k, there are at least two distinct i, j with $t_{i,k}, t_{j,k} \neq 0$. Since $\gamma^n(t_{i,k}, t'_{i,k}) = Q^n(t_{i,k}) \neq 0$, we see that $t'_{i,k}$ (and similarly $t'_{j,k}$) are also nonzero. We have $\gamma^m(a_j, u_i) = 0$, so $\gamma^n(t_{j,k}, t'_{i,k}) = 0$. If $t_{i,k}^\perp = t_{j,k}^\perp$ then $\gamma^n(t_{i,k}, t'_{i,k}) = 0$, a contradiction. As this is impossible, we conclude that $t_{i,k}^\perp \cap t_{j,k}^\perp = (0)$. But then as $\gamma^m(a_i, U'_i) = \gamma^m(a_j, U'_i) = 0$, we find that $\tau_k[U'_i] = 0$. On the other hand there is also an equation of the form $\gamma^m(u_i, u'_i) = Q(u_i)$ holding in U_i with $u'_i \in U'_i$, yielding $\gamma(t_{i,k}, 0) = Q(t_{i,k})$, a contradiction.

Our conclusion therefore is that for fixed k, there is at most one term $t_{i,k}$ not equal to 0. Then the equation $\sum_i Q^m(a_i) = 0$ shows that all of these terms vanish, as claimed. □

So all of this proves:

Proposition. *For each d, the series $\mathcal{M}_n^{(d)}$ derived from the initial quadratic structure $\mathcal{F}_d$ is an infinite antichain of a-indecomposable quadratic structures over $\mathbb{F}_2$.*

Actually the result is a little stronger, because in the proof of Lemma 14 we never use the hypothesis that $\mathcal{M}_m$, $\mathcal{M}_n$ are derived from the *same* initial structure.

Lemma 17. *Let $f : \mathcal{M}_m^{(d)} \hookrightarrow \mathcal{M}_n^{(d')}$ be an injection with $m, n \geq 3$. Then d' is an odd multiple of d.*

Proof. By Lemma 15, we know that $m = n$ and f is induced by a permutation of the coordinates, hence without loss of generality we may take f to be the identity on A^n. It then follows easily that f takes $T_n^{(d)}$ into $T_n^{(d')}$.

Under this hypothesis, the last part of the proof of Lemma 15 shows that the u_i are fixed modulo $A^n \oplus \bigoplus_i U'_i$, and since $\gamma^n(a_j, u_i) = 0$ for $i \neq j$, it follows easily that they are fixed modulo $\bigoplus_i U'_i$ as well. Let $\pi : T_n^{(d')} \to F_{2d}$, $\psi : W^n \to F_d$ be induced by the projections onto the first coordinate. We claim that $(\pi f, \psi f)$ embeds $\mathcal{F}_d$ into $\mathcal{F}_{d'}$. It suffices to check that πf is injective.

Let L be the kernel of πf on $U_1^{(d)}$. Observe that if $u, \tilde{u} \in U_1^{(d)}$ with $u \in L$ and $Q(u) = Q(\tilde{u})$, then $\tilde{u} \in L$. Thinking of L as an $\mathbb{F}_2$-subspace of F_{2d}, this means it is closed under multiplication by elements in the kernel K of the norm to F_d, as well as addition of course. But any element $a \in F_d$ can be written as the sum of two elements of the form $x + x^{-1}$ for some $x \in K$, hence L is a vector space over F_d. As L is closed under multiplication by K, it must be (0) or F_{2d}, and we know by looking at u_1 that the latter possibility may be excluded. □

Proposition. *Let a set D of integers be chosen so that for $d \in D$, no nontrivial odd multiple of d lies in D. Then the set of derived structures $\{\mathscr{M}_n^{(d)} : d \in D, n \geq 3\}$ is an antichain.*

The relative freedom we have to construct such antichains suggests the following.

Conjecture. *Let $\mathscr{X}$ be a finite set of a-indecomposable quadratic structures. Then there is an infinite antichain $\mathscr{A}$ of finite a-indecomposable quadratic structures, such that no structure in $\mathscr{X}$ embeds in any structure in $\mathscr{A}$.*

5. More antichains in $\mathscr{Q}_p$ for p odd

A prime $p > 2$ is fixed throughout. We begin with the abstract portion of the construction, based on an initial a-indecomposable quadratic structure $\mathscr{M}$ with a distinguished decomposition of U as $\langle u \rangle \oplus U'$ and leading to a derived series $\mathscr{M}_n$ of a-indecomposable quadratic structures which may or may not constitute an antichain.

So we introduce $\mathscr{A}_i = (U_i, V_i; \gamma_i)$, u_i, U_i', T^n, W^n, A^n, B^n, C^n, T^n, W^n as in §3, and set $U^{0,n} = A^n \oplus T^n$, $V^{0,n} = B^n \oplus C^n \oplus W^n$. To define the quadratic map $Q_n : U^{0,n} \to V^{0,n}$ we use the same defining conditions (1)–(4) that were used in §4. Finally, we take $U^n = U^{0,n}$, and we modify $V^{0,n}$ as follows (this is the most subtle point of the whole enterprise, copied over from [12]):

$$V^n = V^{0,n} \Big/ \left(\sum_{1 \leq i \leq n} b_i , \sum_{2 \leq i \leq n} (-1)^i c_i \right).$$

We write $B(u)$ for $Q(u, u)$ (and similarly B_n, etc.).

We note that the next lemma uses the condition $p > 2$.

Lemma 18. *Assume that $n \geq 4$, or $n = 3$ and $p > 3$. Then $\mathscr{M}_n$ is a quadratic structure.*

Proof. It is necessary to check that Q^n is nondegenerate. Observe that for $n = 2$ we find

$$Q(a_1 + a_2) = b_1 + b_2 + 2c_2 = 0,$$

so that $\mathscr{M}_2$ is degenerate, and that for $n = 3$, $p = 3$ we find

$$Q(a_1 + a_2 + a_3) = 2(c_2 + 2c_3) = 0.$$

If $a \in A^n$ and $t \in T^n$ then $Q(a+t) \in (B^n \oplus C^n) + Q(t)$, so if $Q(a+t) = 0$ then $t = 0$ and $Q(a) = 0$. In particular, since the B^n-component of $Q(a)$ is 0, $a = \alpha \sum_{i \leq n} \varepsilon_i u_i$ with $\alpha \in F_p$, $\varepsilon_i = \pm 1$. If $\alpha \neq 0$ then $Q(a) = 2\alpha^2 \sum_{i<j} \varepsilon_i \varepsilon_j c_j$. Normalizing by $\varepsilon_1 = 1$, we find

$$Q(a) = \varepsilon_2 c_2 + (1 + \varepsilon_2)\varepsilon_3 c_3 + (1 + \varepsilon_2 + \varepsilon_3)\varepsilon_4 c_4 + \cdots ;$$

inspection of the first two coefficients shows that $\varepsilon_2 = 1$ and the characteristic must be 3, in which case ε_3 is also 1, and the next coefficient vanishes. □

Lemma 19. *Suppose that the initial quadratic structure $\mathcal{M}$ is a-indecomposable. Then the derived structures $\mathcal{M}_n$ are also a-indecomposable.*

Proof. Not a word needs to be changed in the proof of Lemma 14, given that $Q(u)$ is taken to mean $\gamma(u, u)$, until the very last line, where some minus signs must be inserted in keeping with the current setup. □

Lemma 20. *Let $\iota = (f, g)$ be an embedding of $\mathcal{M}_m$ into $\mathcal{M}_n$ such that $f[A^m] \subseteq A^n$, where $m, n \geq 3$. Then $m = n$, and $f \restriction A^m$ is induced by a permutation of the coordinates (if $n > 3$, this is at worst a transposition of $(1), (2)$).*

Proof. Let $f(a_i) = \sum_i \delta_{ik} a_k$ and let $f(u_i) \equiv \sum_i \varepsilon_{ik} u_k \bmod A^n \oplus \bigoplus_i U_i'$, with coefficients $\delta, \varepsilon \in \mathbb{F}_p$.

Our first claim is that for every i, there is at least one index k for which $\delta_{ik} = 0$.

Suppose that i is fixed, and for all k we have $\delta_{ik} \neq 0$. Choose indices i', j so that i, i', j are all distinct. From the equation $\gamma_m(a_i, u_j) = 0$, by considering the B-component after applying ι, we deduce that $\delta_{ik}\varepsilon_{jk} = \alpha$ is independent of k. Similarly $\delta_{i'k}\varepsilon_{jk} = \beta$ is independent of k. If $\alpha = 0$ then all ε_{jk} vanish, contradicting $Q^m(a_j) = \gamma^m(a_j, u_j)$. So $\alpha \neq 0$ and hence all ε_{jk} are nonzero, forcing $\delta_{i'k}$ to be a constant multiple of δ_{ik}, so that $f(a_i)$ and $f(a_{i'})$ commute, a contradiction.

Now examine the B-components of the equations $Q^m(a_i) = \gamma^m(a_i, u_i)$ and $\gamma(a_i, u_j) = 0$ for $i \neq j$. These state

$$\delta_{ik}^2 = \delta_{ik}\varepsilon_{ik} + \alpha_i, \qquad \delta_{ik}\varepsilon_{jk} = \beta_{ij},$$

with $\alpha_i, \beta_{ij} \in \mathbb{F}_p$ independent of k. As some δ_{ik} is 0, we find that α_i, β_{ij} are all zero. When $\delta_{ik} \neq 0$ these equations then become

$$\delta_{ik} = \varepsilon_{ik}, \qquad \varepsilon_{jk} = 0.$$

Therefore, if we let $S_i = \{k : \delta_{ik} \neq 0\}$, the sets S_i are disjoint as i varies. Now we apply the relation $\sum_i Q^m(a_i) = 0$ (or rather, the relation we get by applying ι to this). Looking at the B-component we find that the sets S_i cover $\{1, \ldots, n\}$, and then looking at the C-component, bearing in mind that we know the sets are disjoint, we find that they are singletons. The claim then follows. □

Now fix d. Taking $\mathcal{F}_d$ as the initial structure, construct the sequence $\mathcal{M}_n^{(d)}$ of associated a-indecomposable structures as described above. For the antichain property it will be important that in $\mathcal{F}_d$ two sets of the form $u^\perp$ with $u \in F_{2d}^\times$ either coincide or meet in (0).

Lemma 21. *Let $f : \mathcal{M}_m^{(d)} \hookrightarrow \mathcal{M}_n^{(d')}$ be an embedding. Then $f[A^m] \leq A^n$.*

Proof. Let π_k be the projection of U^n onto the kth component U_k of T^n, and $\tau_k = \pi_k f : U_m^{(d)} \to U_k$. Let $t_{i,k} = \tau_k(a_i)$, $t'_{i,k} = \tau_k(u_i)$. Our goal is to prove that each $t_{i,k} = 0$. As in the proof of Lemma 16, if k is fixed so that $t_{i,k} \neq 0$ for some i, then there are at least two indices $i < j$ for which $t_{i,k}, t_{j,k} \neq 0$, and for any such i, j, k we have $t_{i,k}^\perp \cap t_{j,k}^\perp = (0)$. If there is a third index j' for which $t_{j',k}$ is also nonzero, then similarly $t_{j,k}^\perp \cap t_{j',k}^\perp = (0)$

and hence $t'_{i,k} = 0$, a contradiction. We may therefore suppose that $t_{i,k}$, $t_{j,k}$ are nonzero, with $i < j$, and that $t_{j',k} = 0$ for any other index j'. Now from the conditions $\sum_{i<m} \gamma(a_i, a_{i+1}) = 0$ and $\gamma(a_i, a_j) = \gamma(a_{j-1}, a_j)$, by applying f and then looking at the kth coordinate, we find that $\gamma(t_{i,k}, t_{j,k}) = 0$. Since $\gamma(t'_{i,k}, t_{j,k}) = 0$, we conclude $\gamma(t_{i,k}, t'_{i,k}) = 0$, a contradiction. □

So all of this proves:

Proposition. *For each d, the series $\mathcal{M}_n^{(d)}$ derived from the initial quadratic structure $\mathcal{F}_d$ is an infinite antichain of a-indecomposable quadratic structures over $\mathbb{F}_p$.*

Actually the result is a little stronger, because in the proof of Lemma 19 we never use the hypothesis that $\mathcal{M}_m$, $\mathcal{M}_n$ are derived from the *same* initial structure. Arguing as in §4 we get:

Lemma 22. *Let $f : \mathcal{M}_m^{(d)} \hookrightarrow \mathcal{M}_n^{(d')}$ be an injection with $m, n \geq 3$. Then d' is an odd multiple of d.*

As before, we may conjecture that there is an infinite antichain meeting an arbitrary finite set of negative constraints.

One final comment. Though we defined the notion of quadratic structures differently in the two cases—even or odd characteristic—both notions make sense formally in all characteristics. The alternating version, associated with groups, gives rise to infinite antichains of a-indecomposable structures in all characteristics but only yields groups in characteristic 2, while the symmetric version, associated with rings, yields rings in all characteristics but only gives rise to infinite antichains of a-indecomposable structures in odd characteristics. Thus circumstances conspire to keep the two cases well apart.

References

1. C. Berline and G. Cherlin, *QE rings in characteristic p*, Logic Year 1979/80 (M. Lerman et al., eds.), Lecture Notes in Math., vol. 859, Springer, New York, 1980, pp. 16–31.
2. M. Boffa, A. Macintyre, and F. Point, *The quantifier elimination problem for rings without nilpotent elements and for semisimple rings*, Model Theory of Algebra and Arithmetic (L. Pacholski et al., eds.), Lecture Notes in Math., vol. 834, Springer, New York, 1980, pp. 20–30.
3. G. Cherlin and U. Felgner, *Homogeneous solvable groups*, J. London Math. Soc. (2) **44** (1991), 102–120.
4. G. Cherlin and U. Felgner, *Quantifier eliminable groups*, Logic Colloquium 1980 (van Dalen, ed.), North-Holland, Amsterdam, 1982, pp. 69–81.
5. R. Fraissé, *Sur l'extension aux relations de quelques propriétés des ordres*, Ann. Sci. École Norm. Sup. (4) **71** (1954), 363–388.
6. K. Gruenberg, *Cohomological topics in group theory*, Lecture Notes in Math., vol. 143, Springer, New York, 1970.
7. N. J. S. Hughes, *The use of bilinear mappings in the classification of groups of class* 2, Proc. Amer. Math. Soc. **2** (1951), 742–747.
8. W. Kantor, *Linear groups containing a Singer cycle*, J. Algebra **62** (1980), 232–234.
9. S. Mac Lane, *Homology*, Grundlehren Math. Wiss., vol. 114, Springer, New York, 1963.
10. D. Saracino, *Amalgamation bases for nil-2 groups*, Algebra Universalis **16** (1982), 47–62.
11. D. Saracino and C. Wood, *QE nil-2 groups of exponent* 4, J. Algebra **76** (1982), 337–352.

12. ———, *QE commutative nil rings*, J. Symbolic Logic **49** (1984), 644–651.

13. E. Weiss, *Cohomology of groups*, Pure Appl. Math., vol. 34, Academic Press, New York, 1969.

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903
E-mail address: `cherlin@math.rutgers.edu`

Department of Mathematics, Colgate University, Hamilton, New York 13346-1398
E-mail address: `dsaracino@colgateu.bitnet`

Department of Mathematics, Wesleyan University, Middletown, Connecticut 06459-0128
E-mail address: `cwood@eagle.wesleyan.edu`