Centroids of groups

Serguei Lioutikov
Department of Mathematics and Statistics
McGill University
Montreal, QC H3A 2K6, Canada

Alexei Myasnikov
City College of New York
New York, NY 10031, USA

e-mail: alexei@rio.sci.ccny.cuny.edu

April 7, 2005

1 Introduction

In the first part of this paper for an arbitrary group G we introduce an associative ring with identity $\Gamma(G)$, called the centroid of the group G. This notion is a natural generalization of the ring of endomorphisms to the case of a non–commutative group G, and what is more important, it is an analog of the notion of a centroid from ring theory. Then we describe centroids of various groups, in particular, centroids of free groups, torsion-free hyperbolic groups, free nilpotent groups, and groups of unitriangular matrices $UT_n(R)$ over an arbitrary associative ring R of characteristic zero. Finally, with the description of centroids of free nilpotent groups in hand, we solve affirmatively the rigidity problem for free nilpotent groups posed by F.Grunewald and D.Segal in 1984 [10].

The most natural way to look at the centroid comes from the theory of exponential groups [1, 11, 15, 19, 20], i.e., groups admitting exponents in a ring. We prove that $\Gamma(G)$ is the maximal ring of scalars for the group G: that means that for any $g \in G$, $\gamma \in \Gamma(G)$ the exponent $g^{\gamma} \in G$ is well defined, this action of $\Gamma(G)$ on G is faithful and satisfies some specific axioms (including Lyndon's axioms), and, moreover, $\Gamma(G)$ is the maximal ring with respect to these properties. This resembles the definition of the centroid $\Gamma(K)$ of a ring K as the largest ring of scalars of the ring K.

Constructively, the ring $\Gamma(G)$ is defined as a subring of the near-ring $P(G)$ of all mappings of the group G. Investigation of the near-ring $P(G)$ began with the works of N. Fitting [2] and H.Neumann [22, 23]. H. Neumann used the near–ring $P(G)$ and its subrings in her investigations of varieties of groups. Later, A. Fröhlich [4, 5, 6, 7] applied near-rings of endomorphisms and their links with groups to his study of non–abelian homological algebra.

The results mentioned above gave rise to numerous attempts to construct something similar to "the ring of endomorphisms" for an arbitrary group. It is a well-known fact that over an abelian group G the set of all endomorphisms $End(G)$ forms a ring with respect to the operations of addition $+$ and multiplication $\cdot$:

$$g^{\phi+\psi} = g^{\phi}g^{\psi}, \quad g^{\phi\cdot\psi} = (g^{\phi})^{\psi}, \tag{1}$$

where $g \in G,\ \phi, \psi \in End(G)$. For a non-abelian group G the set $End(G)$ is not a ring, because the sum of two endomorphisms of G is not necessarily an endomorphism of G. Therefore, it is natural to consider more general morphisms over G. It turns out that the set $P(G)$ of arbitrary mappings from G into G forms a near-ring with respect to the operations (1). The subnear-ring $E(G)$ of $P(G)$ generated by the set $End(G)$ may seem to be a good analog of the ring of endomorphisms of a nonabelian group G (in the abelian case $E(G) = End(G)$), except that, in general, it is not a ring. Many authors [12, 25, 24, 18] considered subnear-rings of $E(G)$ generated by different subsets (most often subsemigroups) of $End(G)$. We define $\Gamma(G)$ as the ring which consists of all quasi-endomorphisms of G (i.e. such mappings ϕ that $(xy)^\phi = x^\phi y^\phi$ for commuting $x, y \in G$) that centralize all inner automorphisms of G (very similar to the centroid in ring theory).

In the sections that follow we give a detailed description of centroids of arbitrary CSA-groups, including free groups and torsion-free hyperbolic groups. A similar technique allows us to characterize centroids of free products of groups. Surprisingly enough , the centroid $\Gamma(F)$ of a free non–abelian group F is quite big: $\Gamma(F)$ is an unrestricted direct product of countably many copies of $\mathbf{Z}$.

In Section 5 we describe centroids of finitely generated free nilpotent groups and groups of unitriangular matrices $UT_n(\mathbf{Z})$. In fact, we prove the following result: let N be a non-abelian free nilpotent group of finite rank, R an arbitrary binomial domain, and N^R the free nilpotent R-group introduced by P.Hall [11], then the centroid $\Gamma(N^R)$ is isomorphic to $R \oplus I$, where I is a nilpotent ideal of $\Gamma(G)$. The same also is true for the unitriangular matrix group $UT_n(R)$ over an arbitrary associative ring R of characteristic 0. We then apply these results to solve the above-mentioned rigidity problem of free nilpotent groups. Recall that a torsion-free nilpotent group G is rigid if for any binomial domains R and S the Hall R-completion G^R of G is isomorphic to the Hall S-completion G^S if and only if the rings R and S are isomorphic. We prove that a non-abelian free nilpotent group of finite rank is rigid, which answers the F.Grunewald and D.Segal question from [10]. Notice that the same argument shows that the group $UT_n(\mathbf{Z})$ is rigid (which was already proved by different methods in [10]). Rigidity results form an essential part of the F.Grunewald and D.Segal project aimed to describe torsion-free nilpotent groups up to isomorphism. It seems that centroids give an appropriate tool to deal with rigidity of nilpotent groups. Notice, that in an attempt to carry out this program one may consider centroids relative to the category of nilpotent groups (see [21] for details).

2 Definition of the centroid

To the end of the section, let us fix an arbitrary group G.

Definition 2.1 *A set P with two binary operations $+$ (addition) and $\cdot$ (multiplication) is called a near-ring if P is a group (not necessarily commutative) with respect to the operation $+$, and multiplication is associative and satisfies the left distributivity relation:*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad a, b, c \in P.$$

The following is the principal example of a near-ring. Let $P(G)$ be the set of arbitrary mappings of G into G. The set $P(G)$ with the operations $+$ and

$\cdot$ defined by

$$g^{\phi+\psi} = g^{\phi}g^{\psi}, \quad g^{\phi\cdot\psi} = (g^{\phi})^{\psi}, \qquad \text{for } g \in G, \quad \phi, \psi \in P(G).$$

is *the near-ring of mappings of the group G.*

Note that the mapping $0 : \ G \longrightarrow 1_G$ is a "zero" of the near-ring $P(G)$, the mapping $1_P : \ g \longrightarrow g$ is a "unit" of $P(G)$, and the mapping $-\phi$ is defined according to the rule $g^{-\phi} = (g^{\phi})^{-1}$.

Definition 2.2 *A mapping $\phi \in P(G)$ is called normal if*

$$(h^{-1}gh)^{\phi} = h^{-1}g^{\phi}h$$

for all $g, h \in G$. By $N(G)$ we denote the set of all normal mappings of G.

Clearly, $N(G)$ is a centralizer in $P(G)$ of the set $Inn(G)$ of all inner automorphisms of G. In general, if M and X are subsets of $P(G)$, then the set

$$C_M(X) = \{\phi \in M \ \mid \ \phi \cdot f = f \cdot \phi \ \ \forall f \in X\}$$

is termed *the centralizer of X in M.*

Let us denote by $End(G)$ the monoid of all endomorphisms of G with respect to composition. Later on, subnear-rings will appear as the centralizers of different subsemigroups of $End(G)$.

Lemma 2.1 *Let $S \leq End(G)$ be an arbitrary semigroup of endomorphisms of G. Then the centralizer $C_{P(G)}(S)$ of S in $P(G)$ is a subnear-ring in $P(G)$. In particular, $N(G)$ is a near-ring.*

Proof. Let $f \in S, \ \phi, \psi \in C_{P(G)}(S)$, $g \in G$, then

$$(g^f)^{\phi\cdot\psi} = (g^{\phi\cdot\psi})^f, \ (g^f)^{\phi+\psi} = (g^f)^{\phi}(g^f)^{\psi} = (g^{\phi})^f(g^{\psi})^f = (g^{\phi+\psi})^f.$$

□

Lemma 2.2 *1) Let $\phi, \psi \in N(G), \ x, y \in G$. Then $[x, y] = 1$ implies $[x^{\phi}, y^{\psi}] =$* 1;

2) For any set $X \subseteq G$ the centralizer $C_G(X) \subseteq G$ is $N(G)$–invariant. (

Proof. 1) We have:

$$yx^{\phi} = yx^{\phi}y^{-1}y = (yxy^{-1})^{\phi}y = x^{\phi}y.$$

Hence

$$x^{\phi}y^{\psi} = x^{\phi}y^{\psi}x^{-\phi}x^{\phi} = (x^{\phi}yx^{-\phi})^{\psi}x^{\phi} = y^{\psi}x^{\phi}.$$

This proves 1).

2) follows from 1). □

Corollary 2.1 *In the near-ring $N(G)$ the operation of addition $+$ is commutative.*

Proof. For $g \in G, \quad \phi, \psi \in N(G)$ we have:

$$g^{\phi+\psi} = g^{\phi} g^{\psi} = g^{\phi} g^{\psi} g^{-\phi} g^{\phi} = (g^{\phi} g g^{-\phi})^{\psi} g^{\phi} = g^{\psi} g^{\phi} = g^{\psi+\phi},$$

hence $\phi + \psi = \psi + \phi$. $\square$

Near-rings with commutative addition are called *abelian.*

The following example shows that one can represent any abelian near-ring with identity as a subring of $N(G)$ for a properly chosen abelian group G.

Example 2.1 *Let R be an abelian near-ring with identity and $G = R^{+}$ its additive group. Then R acts on G by right multiplications: $g \to ga, \ a \in R, \ g \in G$. This operation gives a monomorphism $R \longrightarrow P(G)$. Due to the fact that the group G is abelian, any mapping of G is normal, i.e., $P(G) = N(G)$.*

Corollary 2.2 *There exists an abelian group G for which $N(G)$ is not a ring.*

Proof. Indeed, according to the previous example, it is sufficient to take an abelian near-ring with 1 which is not a ring. As an example of such near-ring, we can choose the set of all integer polynomials $\mathbf{Z}[x]$ with the standard addition and composition as multiplication. $\square$

Definition 2.3 *A mapping $\phi \in P(G)$ is called a quasi-endomorphism of the group G if for any $x, y \in G$ we have:*

$$[x, y] = 1 \textit{ implies } (xy)^{\phi} = x^{\phi} y^{\phi}.$$

The set of all quasi-endomorphisms of G is denoted by $Q(G)$.

Lemma 2.3 *$Q(G)$ is a semigroup with respect to composition of maps.*

Proof. Indeed, for $x, y \in G, \ \phi, \psi \in Q(G)$ we have

$$[x, y] = 1 \text{ implies } x^{\phi} y^{\phi} = (xy)^{\phi} = (yx)^{\phi} = y^{\phi} x^{\phi}.$$

Hence

$$[x, y] = 1 \text{ implies } (xy)^{\phi \cdot \psi} = (x^{\phi} y^{\phi})^{\psi} = x^{\phi\psi} y^{\phi\psi},$$

i.e., $Q(G)$ is closed under composition. $\square$

Theorem 2.1 *The set $\Gamma(G)$ of all normal quasi-endomorphisms of G is an associative ring with 1. It is called the centroid of the group G.*

Proof. According to the definition, $\Gamma(G) = N(G) \cap Q(G)$ is the intersection of two semigroups, so $\Gamma(G)$ is closed under multiplication. Let us verify that it is closed under addition. Let $\phi, \psi \in \Gamma(G)$. We have already proved that $N(G)$ is a near-ring, hence $\phi + \psi \in N(G)$. Now it suffices to show that $\phi + \psi \in Q(G)$; i.e., $\phi + \psi$ is a quasi-endomorphism of G. Let $x, y \in G$, and $[x, y] = 1$. Then

$$(xy)^{\phi+\psi} = (xy)^{\phi}(xy)^{\psi} = x^{\phi}y^{\phi}x^{\psi}y^{\psi}.$$

But ϕ and ψ are normal, so by Lemma 2.2 the elements y^{ϕ} and x^{ψ} commute. Therefore,

$$x^{\phi}y^{\phi}x^{\psi}y^{\psi} = x^{\phi}x^{\psi}y^{\phi}y^{\psi} = x^{\phi+\psi}y^{\phi+\psi}$$

which, combined with the equality above, proves that $\phi + \psi \in Q(G)$. Consequently, $\Gamma(G)$ is a near-ring; moreover, by Corollary 2.1 addition in $\Gamma(G)$ is commutative. It remains to check that right-hand distributivity holds in $\Gamma(G)$:

$$x^{(\phi+\psi)\theta} = (x^{\phi}x^{\psi})^{\theta} = x^{\phi\theta}x^{\psi\theta} = x^{\phi\theta+\psi\theta}$$

(again, here we used the fact that by Lemma 2.2 x^{ϕ} and x^{ψ} commute). Since this is true for an arbitrary $x \in G$, we have $(\phi + \psi)\theta = \phi\theta + \psi\theta$, and $\Gamma(G)$ is a subring of $P(G)$. Obviously, $1 \in \Gamma(G)$. $\square$

There is an analogy between the construction of the centroid $\Gamma(K)$ of a ring K and the centroid $\Gamma(G)$ of a group G. Namely, $\Gamma(K)$ is the centralizer of the set of all right-hand and left-hand multiplications of K in the semigroup of all endomorphisms $End(K^+)$ of the additive group K^+ of the ring K. Taking instead of the abelian group K^+ a non-abelian group G, instead of the semigroup $End(G)$ its generalization $Q(G)$, we obtain $\Gamma(G)$ as the centralizer of the set of all inner automorphisms of G in the semigroup $Q(G)$. So far this analogy is purely formal. But in the next section we will show that $\Gamma(G)$ is the maximal ring of scalars for G, i.e., $\Gamma(G)$ satisfies the same universal property as the centroid of a ring K.

Observe that if the group G is abelian, then $\Gamma(G) = End(G)$, i.e., $\Gamma(G)$ is indeed a generalization of the ring of endomorphisms to the non–commutative case.

3 Centroid as the maximal ring of scalars

Up to the end of this section, let us fix an arbitrary associative ring with identity A, as well as a group G.

Given an action of A on G, i. e. a mapping $G \times A \to G$, we will write the result of the action of $\alpha \in A$ on $g \in G$ as g^{α}. Consider the following axioms:

1. $g^1 = g,\ g^0 = 1, 1^{\alpha} = 1$;

2. $g^{\alpha+\beta} = g^\alpha g^\beta, \; g^{\alpha\beta} = (g^\alpha)^\beta$;

3. $(h^{-1}gh)^\alpha = h^{-1}g^\alpha h$;

4. $[g,h] = 1 \Longrightarrow (gh)^\alpha = g^\alpha h^\alpha$.

Definition 3.1 *[19, 20] The group G is called an A–exponential group (or an A–group) if an action of the ring A on G satisfying axioms 1)-4) is defined.*

Notice that an arbitrary group is a $\mathbf{Z}$–group; a group of period m is a $\mathbf{Z}/m\mathbf{Z}$–group; a module over a ring A is an abelian A–group and vice versa; D-groups studied by G.Baumslag [1] are $\mathbf{Q}$-groups; exponential nilpotent A–groups over a binomial ring A, introduced by P. Hall [11], are A–groups; an arbitrary pro-p-group is a $\mathbf{Z}_p$–group over the ring of p–adic integers $\mathbf{Z}_p$.

The axiomatic approach to exponential groups first appeared in a paper of R. Lyndon [15]. In his terms, A–groups are those that just satisfy axioms 1)–3). It turns out that this class of groups is too wide to work with; for example, as we show below, there are abelian A-groups in Lyndon's sense which are not A-modules.

Example 3.1 *Let θ be a non–identity automorphism of the ring A, and M a free A–module with base $\langle x, y\rangle$. We can define a new action $*$ of the ring A on M as follows:*

$$z * \alpha = \begin{cases} z \cdot \theta(\alpha), & z \in xA \cup yA, \\ z \cdot \alpha, & z \notin xA \cup yA. \end{cases}$$

Then the action $*$ of A on M satisfies axioms 1)–3), but if $\alpha_0 \neq \theta(\alpha_0)$, then

$$(x+y) * \alpha_0 = (x+y)\alpha_0 \neq (x+y)\theta(\alpha_0) = x * \alpha_0 + y * \alpha_0,$$

hence axiom 4) doesn't hold.

In fact, all the groups that Lyndon actually dealt with in his paper [15] indeed satisfy axiom 4), i.e., they are A–groups.

Definition 3.2 *Let G be an A-group such that the action of A on G is faithful, i.e., for any nonzero $a \in A$ there exists $g \in G$ such that $g^a \neq 1$. In this case A is called a ring of scalars of G.*

The following proposition shows that G is a $\Gamma(G)$-group and $\Gamma(G)$ is the maximal ring of scalars of G.

Proposition 3.1 *Let G be a group. Then:*

1. *the centroid* $\Gamma(G)$ *is a ring of scalars for* G*; in particular,* G *is a* $\Gamma(G)$*–group;*

2. $\Gamma(G)$ *is the largest ring of scalars of the group* G*; i.e., if* B *is a ring of scalars of* G*, then there is a canonical embedding* $B \hookrightarrow \Gamma(G)$*.*

Proof. For any $\phi \in \Gamma(G)$ and $g \in G$ we define g^{ϕ} as the image of g under the map ϕ. Notice that this action is faithful. Axioms 1) and 2) hold by the very definition of addition and multiplication in $\Gamma(G)$. Axiom 3) holds because all mappings from $\Gamma(G)$ are normal, and axiom 4) holds since $\Gamma(G)$ consists of quasi-endomorphisms of G. It follows that G is a $\Gamma(G)$-group and $\Gamma(G)$ is a ring of scalars of G.

If B is a ring of scalars of G, then B acts faithfully on G and we can define a monomorphism of near-rings $\Phi : B \longrightarrow P(G)$ where $\Phi(b) : G \longrightarrow G$ is the mapping $\Phi(b) : g \rightarrow g^{b}$. By axioms 3) and 4) the mapping $\Phi(b)$ is a normal quasi-endomorphism, hence $\Phi(B) \subset \Gamma(G)$. □

4 Description of centroids of CSA-groups and free products of groups

In this section we describe the centroid of an arbitrary CSA–group, which immediately gives us the structure of centroids of free groups, torsion–free hyperbolic groups, and groups acting freely on Λ–trees. Surprisingly, the centroid of a free non–abelian group F is uncountable: $\Gamma(F) = \overline{\Pi}_{i<\omega}\mathbf{Z}$, the unrestricted direct product of countably many copies of $\mathbf{Z}$. We then describe the structure of the centroid of a free product of two groups G and H. It turns out that

$$\Gamma(G * H) \simeq \Gamma(G) \times \Gamma(H) \times \overline{\Pi}_{i\in I}\mathbf{Z}\ ,$$

where the set of indices I is described in Theorem 4.2 below.

4.1 Preliminary results

In our study of centroids we will frequently use the following important observation:

Lemma 4.1 *Let* G *be an* A*–group. Then for any subset* X *of* G *the centralizer* $C_G(X)$ *is an* A*-subgroup of* G*, in particular, it is* A*–invariant, i.e., for any* $a \in A$

$$C_G(X)^{a} \subset C_G(X).$$

Proof.
For any $x \in X, y \in G, a \in A$ we have

$$[x, y^a] = x^{-1}y^{-a}xy^a = (x^{-1}yx)^{-a}y^a = (y[y, x])^{-a}y^a.$$

So, if $[x, y] = 1$ then $[x, y^a] = 1$. □

Now, let us establish an embedding of $\Gamma(G)$ of an arbitrary group G into a certain Cartesian product.

Proposition 4.1 *Let G be an arbitrary group and let C_i $(i \in I)$ be fixed representatives of the conjugacy classes of the centralizers of all non-trivial elements in G. Then there exists an embedding*

$$\lambda : \Gamma(G) \longrightarrow \overline{\Pi}_{i \in I}\Gamma(C_i).$$

Proof. Let C_i $(i \in I)$ be representatives of the conjugacy classes of the centralizers of all non-trivial elements in G. By Lemma 4.1, all C_i are $\Gamma(G)$-invariant, hence for every $\phi \in \Gamma(G)$ the restriction ϕ_i of ϕ to C_i belongs to $P(C_i)$. Each ϕ_i is a normal quasi-endomorphism of C_i, therefore $\phi_i \in \Gamma(C_i)$. Moreover, the restriction map $\lambda_i : \phi \to \phi_i$ is a homomorphism of rings $\lambda_i : \Gamma(G) \longrightarrow \Gamma(C_i)$. This gives rise to the diagonal homomorphism

$$\lambda : \Gamma(G) \longrightarrow \overline{\Pi}_{i \in I}\Gamma(C_i),$$

where $\lambda = \overline{\Pi}_{i \in I}\lambda_i$. We claim that the homomorphism λ is injective. Let $0 \neq \phi \in \Gamma(G)$. Then there exists an element $g \in G$ such that $g^\phi \neq 1$. Now, some conjugate $h^{-1}gh$ of g belongs to C_i for some i and

$$g^\phi = (h(h^{-1}gh))h^{-1})^\phi = h(h^{-1}gh)^\phi h^{-1} = h(h^{-1}gh)^{\phi_i}h^{-1} \neq 1.$$

therefore, $(h^{-1}gh)^{\phi_i} \neq 1$ and, consequently, $\phi_i \neq 0$. □

If all the centralizers C_i in the proposition above are abelian, then $\Gamma(C_i) = End(C_i)$ and we have the following

Corollary 4.1 *Let G be a group in which all the centralizers of all non-trivial elements of G are abelian. Then there exists an embedding*

$$\lambda : \Gamma(G) \longrightarrow \overline{\Pi}_{i \in I}End(C_i),$$

where C_i $(i \in I)$ are representatives of the conjugacy classes of the centralizers of all non-trivial elements in G.

4.2 Centroids of CSA–groups

Definition 4.1 *[20] A group G is termed a CSA-group if all maximal abelian subgroups in G are malnormal.*

Recall [14] that a subgroup H in a group G is *malnormal* if for any $g \in G$ the condition $H^g \cap H \neq 1$ implies $g \in H$. Below we collect some known results about CSA groups. To do this we need the following

Definition 4.2 *Subgroups A and B of a group G are called conjugate separated if $A^g \cap B = 1$ for any $g \in G$.*

Proposition 4.2 *[20] Let G be a CSA–group. Then the following statements are true:*

1. *Any two maximal abelian subgroups of G either coincide or have trivial intersection;*
2. *Any two maximal abelian subgroups of G are either conjugate or conjugate separated;*
3. *Commutation is an equivalence relation on the set of all non-trivial elements of G;*
4. *The centralizer of any non-trivial element of G is a maximal abelian subgroup of G; conversely, any maximal abelian subgroup of $G \neq 1$ is a centralizer of any of its non-trivial elements.*

Now, we are ready to apply Corollary 4.1 to CSA-groups.

Theorem 4.1 *Let G be an arbitrary CSA–group. Then*

$$\Gamma(G) = \overline{\Pi}_{i \in I} End(C_i),$$

where C_i $(i \in I)$ are representatives of the conjugacy classes of the centralizers of all non-trivial elements in G.

Proof. Let $\lambda : \Gamma(G) \longrightarrow \overline{\Pi}_{i \in I} End(C_i)$ be the embedding from Corollary 4.1. We claim that λ is onto. Choose an arbitrary $\phi = \overline{\Pi}_{i \in I} \phi_i \in \overline{\Pi}_{i \in I} End(C_i)$. Each such ϕ acts on C_i as the endomorphism ϕ_i, and we can extend this action to the union

$$Z_i = \bigcup_{g \in G} C_i^g$$

of all conjugates of C_i by the rule

$$(g^{-1}xg)^{\phi_i} = g^{-1}x^{\phi_i}g \quad (x \in C_i).$$

This action is well-defined, since the centralizers of non-trivial elements in G either coincide or have trivial intersection. Notice that for any $i \neq j$ we have $Z_i \cap Z_j = 1$, therefore the union

$$\bigcup_{i \in I} \phi_i = \psi$$

gives rise to a well-defined mapping on G. From the definition of ψ one can see that ψ is a normal quasi-endomorphism of G, i.e. $\psi \in \Gamma(G)$. Obviously, $\lambda(\psi) = \phi$. □

Corollary 4.2 *1. Let F_n be a free group on n generators. Then*

$$\Gamma(F_n) = \overline{\Pi}_{i \in I} \mathbf{Z} \ ,$$

where I is an infinite countable set.

2. Let G be a torsion-free hyperbolic group. Then

$$\Gamma(G) = \overline{\Pi}_{i \in I} \mathbf{Z} \ .$$

3. Let F^A be a free A-group (see [19, 20]) over an associative unitary ring A of characteristic 0. Then $\Gamma(F^A)$ is an unrestricted Cartesian product of infinitely many copies of the ring of endomorphisms of the additive group A^+ of the ring A:

$$\Gamma(F^A) = \overline{\Pi}_{i \in I} End_{\mathbf{Z}}(A^+),$$

where I is the set of representatives of the conjugacy classes of the centralizers of all non-trivial elements in F^A.

Proof. In the case of a free group F it suffices to notice that all centralizers C_i of non-trivial elements in F are infinite cyclic, hence $\mathrm{End}(C_i) \simeq \mathbf{Z}$.

If G is a torsion-free hyperbolic group, then the centralizers of all non-trivial elements are infinite cyclic [8]. This implies, in particular, that G is a CSA-group [20]. Now the statement follows from the theorem above.

In the paper [20] the free A-group F^A over a ring A was described in terms of HNN-extensions. It was proved there that F^A is a CSA-group, and that the centralizers of non-trivial elements are isomorphic to the additive group A^+ of the ring A. □

The following theorem clarifies the structure of the centroids of free products of groups.

Theorem 4.2 *Let G and H be arbitrary groups, then*

$$\Gamma(G * H) = \Gamma(G) \times \Gamma(H) \times \overline{\Pi}\mathbf{Z},$$

where the unrestricted direct product is taken over all the conjugacy classes of the centralizers of elements in $G * H$ which are not conjugate to an element of G or H.

Proof. If G or H is trivial then the statement of the theorem is obvious. So we can assume that both G and H are non-trivial.

We begin by recalling several properties of free products of groups (see details in [14]).

It follows from the Kurosh Subgroup Theorem that every proper centralizer in $G*H$ is either infinite cyclic or conjugate to a centralizer in one of the factors.

From The Conjugacy Theorem for Free Products (see [14]) we have that G and H are malnormal and conjugate separated in $G * H$.

Let C_i $(i \in I)$ be the complete set of representatives of the conjugacy classes of the centralizers of elements in $G * H$ which are not conjugate to an element of G or H. Notice that if $i \neq j$ then $C_i \cap C_j = 1$. Indeed, suppose $C_i = gp(x), C_j = gp(y)$ and $1 \neq z \in C_i \cap C_j$, then the subgroup $gp(x, y)$ has a non-trivial center, and hence by the subgroup theorem $gp(x, y)$ is cyclic. That implies that x and y commute, hence $C_i = C_j$.

Define a homomorphism of rings

$$\xi : \Gamma(G) \times \Gamma(H) \times \overline{\Pi}_{i \in I}\mathbf{Z} \longrightarrow \Gamma(G * H)$$

as follows. Let $\phi \in \Gamma(G) \times \Gamma(H) \times \overline{\Pi}_{i\in I}\mathbf{Z}$. Then $\phi = (\sigma, \delta, f)$ where $\sigma \in \Gamma(G), \delta \in \Gamma(H), f \in \overline{\Pi}_{i\in I}\mathbf{Z}$ (we think of f as a function $f : I \to \mathbf{Z}$). Now we define a mapping $\xi(\phi) : G * H \to G * H$ according to the following three cases. Take an arbitrary $g \in G*H$. Then either g is in a conjugate of C_i for some i or it is conjugate to some element in G or else it is conjugate to some element in H. Suppose first that g is in a conjugate of some C_{i_0}. As we mentioned above, this g does not belong to any other C_j, therefore the number i_0 is uniquely determined by g. In this case put

$$g^{\xi(\phi)} = g^{f(i_0)}.$$

If g is in a conjugate of G, say $g = z^{-1}az$, $(a \in G)$, then put

$$g^{\xi(\phi)} = z^{-1}a^{\sigma}z.$$

Similarly, if g is in a conjugate of H, say $g = z^{-1}bz$, $(b \in H)$, then define

$$g^{\xi(\phi)} = z^{-1}b^{\delta}z.$$

The mapping $\xi(\phi)$ is well-defined and by construction it is a normal quasi-endomorphism, hence $\xi(\phi) \in \Gamma(G * H)$. One can check directly that ξ is a ring homomorphism.

We claim that ξ is an isomorphism. To show that ξ is onto, consider an arbitrary mapping $\psi \in \Gamma(G * H)$. For any non-trivial $g \in G$ the centralizer $C(g)$ of g in $G*H$ is contained in G; since this centralizer is $\Gamma(G*H)$-invariant, we have that $g^\psi \in G$, and consequently, $G^\psi \subset G$. Thus the restriction ψ_G of ψ to G belongs to $\Gamma(G)$. Similarly, the restriction ψ_H of ψ to H belongs to $\Gamma(H)$. Again, each centralizer C_i is ψ-invariant and cyclic; therefore the restriction of ψ to C_i acts on C_i as the multiplication by a given integer, say n_i. Define a function $f_\psi : I \to \mathbf{Z}$ by $f_\psi(i) = n_i$. Now, for $\phi = (\psi_G, \psi_H, f_\psi)$ we have $\xi(\phi) = \psi$. Thus ξ is onto.

To show that ξ is a monomorphism consider an arbitrary

$$\phi = (\sigma, \delta, f) \in \Gamma(G) \times \Gamma(H) \times \overline{\Pi}\mathbf{Z}$$

and assume that $\xi(\phi) = 0$. Then $\sigma = 0, \delta = 0, f = 0$, i.e., $\phi = 0$. □

5 Centroids of nilpotent groups

5.1 Centroids of free nilpotent groups

Let G be a group. By

$$G = G_1 \geq G_2 \geq \dots$$

we denote the lower central series of G, here $G_{i+1} = [G_i, G]$. The upper central series of G is denoted by

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

where $Z_{i+1}(G)$ is the preimage in G of the center $Z(G/Z_i(G))$ under the canonical epimorphism $G \to G/Z_i(G)$. The subgroup $Z_1(G)$ is the center of G and we often write simply $Z(G)$ instead of $Z_1(G)$.

We begin with the following lemma.

Lemma 5.1 *Let G be an arbitrary group. For every $g, h \in G, \phi \in \Gamma(G)$ such that $[g, [g, h]] = 1$ the following equality holds*

$$[g^\phi, h] = [g, h]^\phi.$$

Proof. Observe that if $[g, [g, h]] = 1$, then g and $h^{-1}gh$ commute (since $h^{-1}gh = g[g, h]$). Therefore,

$$[g^\phi, h] = g^{-\phi}h^{-1}g^\phi h = g^{-\phi}(h^{-1}gh)^\phi = (g^{-1}(h^{-1}gh))^\phi = [g, h]^\phi.$$

□

Corollary 5.1 *Let $g, h \in G, \phi \in \Gamma(G)$. If $[g, h] \in Z(G)$ then*

$$[g^\phi, h] = [g, h^\phi] = [g, h]^\phi.$$

Corollary 5.2 *The following statements are true for an arbitrary group G:*

1. *$Z(G)$ is a $\Gamma(G)$-subgroup of G;*

2. *$Z_2(G)$ is a $\Gamma(G)$-subgroup of G.*

Proof. If $z \in Z(G)$, then $[z, g] = 1$ for any $g \in G$. Hence by the lemma above for any $\phi \in \Gamma(G)$ we have $[z^\phi, g] = [z, g]^\phi = 1$, therefore $z^\phi \in Z(G)$. This proves 1).

By definition $Z_2(G) = \{z \in G | [z, g] \in Z(G) \text{ for every } g \in G\}$. By the lemma above for any $z \in Z_2(G), g \in G$, and $\phi \in \Gamma(G)$ we have

$$[z^\phi, g] = [z, g]^\phi \in Z(G),$$

which shows that $z^\phi \in Z_2(G)$. □

From now on we will assume that G is *a finitely generated non-abelian free nilpotent group of class c with basis $x_1, \ldots, x_m$*. in this case $G_i = Z_{c-i+1}(G)$ for each $i = 1, \ldots, c$ and each subgroup G_i is isolated in G, i.e., for any $g \in G$ and any integer $n \neq 0$, if $g^n \in G_i$, then $g \in G_i$.

Notice that every non-trivial element $g \in G$ has a unique maximal root in G, i.e., the unique element $g_0 \in G$ such that $g = g_0^m$, where m is the greatest positive integer for which the equation $g = x^m$ has a solution in G.

We presume that the following proposition is known, but we need the proof to be able to describe centralizers of elements in an arbitrary free nilpotent R-group at the end of this section.

Proposition 5.1 *Let G be a free nilpotent group of class c. If $g \in G_i - G_{i+1}$, then*

$$C_G(g) = \langle g_0 \rangle \cdot G_{c-i+1},$$

where g_0 is the maximal root of g modulo G_{c-i+1} (and $g_0 = 1$ if $g \in G_{c-i+1}$).

Proof. Let $g \in G_i - G_{i+1}$, $v \in G_j - G_{j+1}$, and $[g, v] = 1$. If $j \geq c - i + 1$, then $v \in \langle g_0 \rangle \cdot G_{c-i+1}$. Suppose now that $j < c - i + 1$. Then by corollary 5.12 in [16] the following holds: $i = j$ and for some element $w \in G_i$ we have $gG_{i+1} = w^p G_{i+1}$ and $vG_{i+1} = w^q G_{i+1}$. It follows that $g^q v^{-p} \in G_{i+1}$ and still $[g, g^q v^{-p}] = 1$. By the argument above $g^q v^{-p} \in G_{c-i+1}$, and hence $g^q G_{c-i+1} = v^p G_{c-i+1}$. The nilpotent group G/G_{c-i+1} is torsion-free, therefore the canonical images of the g and v in G/G_{c-i+1} are powers of one and the same element, so they are powers of $g_0 G_{c-i+1}$. This implies that v is a power of g_0 modulo G_{c-i+1}, as desired.

□

Lemma 5.2 *For every $\varphi \in \Gamma(G)$ there exists $n_\varphi \in \mathbf{Z}$ such that*

1. *if $g \in G$, but $g \notin G_2$, then $g^\varphi = g^{n_\varphi}$ modulo $Z(G)$;*
2. *if $z \in Z(G)$, then $z^\varphi = z^{n_\varphi}$.*

Proof. We show first that $x_i^\varphi = x^{n_\varphi}$ for every basic element x_i. By Proposition 5.1

$$C_G(x_i) = \langle x_i \rangle \cdot Z(G), \quad C_G(x_i x_j) = \langle x_i x_j \rangle \cdot Z(G)$$

for every $i, j = 1, \dots, m$. Fix an arbitrary $\varphi \in \Gamma(G)$. Since centralizers of elements are $\Gamma(G)$-invariant, for every $i, j = 1, \dots, m$ we have:

$$x_i^\varphi = x_i^{n_i} z_i, \quad (x_i x_j)^\varphi = (x_i x_j)^{n_{ij}} z_{ij}$$

for some integers n_i, n_{ij} and some elements $z_i, z_{ij} \in Z(G)$. Let us show that $n_1 = n_i$ for all $i = 1, \dots, m$. Indeed, let

$$u = [x_i, \underbrace{x_1, x_1, \dots, x_1}_{c-2}].$$

Then u is a basic commutator of weight $c-1$. Then by corollary 5.1

$$[u, x_i x_1]^\varphi = ([u, x_i][u, x_1])^\varphi = [u, x_i]^\varphi [u, x_1]^\varphi = [u, x_i^\varphi][u, x_1^\varphi] = \tag{2}$$

$$= [u, x_i^{n_i}][u, x_1^{n_1}] = [u, x_i]^{n_i} [u, x_1]^{n_1}.$$

On the other hand,

$$[u, x_i x_1]^\varphi = [u, (x_i x_1)^\varphi] = [u, (x_i x_1)^{n_{i1}}] = [u, x_i x_1]^{n_{i1}} = [u, x_i]^{n_{i1}} [u, x_1]^{n_{i1}}. \tag{3}$$

Since $[u, x_i]$ and $[u, x_1]$ are basic commutators, we deduce from 2 and 3 that $n_i = n_{i1} = n_1$. Put $n_\varphi = n_1$.

The next step is to prove that $z^\varphi = z^{n_\varphi}$ for every $z \in Z(G)$. Since $Z(G)$ is an abelian group it suffices to show that this equality holds for generators of $Z(G)$. The center $Z(G)$ is generated by simple commutators of weight c in the generators $x_1, \dots, x_n$. We have

$$[x_{i_1}, \dots, x_{i_{c-1}}, x_{i_c}]^\varphi = [x_{i_1}, \dots, x_{i_{c-1}}, x_{i_c}^\varphi] = [x_{i_1}, \dots, x_{i_{c-1}}, x_{i_c}^{n_\varphi}] = [x_{i_1}, \dots, x_{i_{c-1}}, x_{i_c}]^{n_\varphi},$$

which proves the statement.

Now we show that $g^\varphi = g^{n_\varphi}$ modulo $Z(G)$ for all elements g in G but not in G_2 which are not proper powers modulo $Z(G)$. By Proposition 5.1, $C_G(g) = \langle g \rangle \cdot Z(G)$. Thus, $g^\varphi = g^{n_{g,\varphi}} z_{g,\varphi}$, where $n_{g,\varphi} \in \mathbf{Z}$ and $z_{g,\varphi} \in Z(G)$. We need to show that $n_{g,\varphi} = n_\varphi$. Since $g \notin G_2$, there exists an element $u \in Z_2(G)$ such that $1 \neq [g, u] \in Z(G)$. In this case $[g, u]^\varphi = [g, u]^{n_\varphi}$. On the other hand,

$$[g, u]^\varphi = [g^\varphi, u] = [g^{n_{g,\varphi}}, u] = [g, u]^{n_{g,\varphi}}.$$

Since the center of a free nilpotent group is a free abelian group, this implies that $n_{g,\varphi} = n_\varphi$.

Now let $g \in G$ be an arbitrary element which does not belong to G_2. Then $g = g_0^k z$, where g_0 is not a proper power modulo $Z(G)$ and $z \in Z(G)$. Then,

$$(g_0^k z)^\varphi = (g_0^k)^\varphi z^\varphi = (g_0^\varphi)^k z^{n_\varphi} = (g_0^{n_\varphi} z_{g_0,\varphi})^k z^{n_\varphi} = (g_0^k z)^{n_\varphi} z_{g_0,\varphi}^k,$$

which completes the proof of the lemma. □

Definition 5.1 *Let*

$$I = \{\varphi \in \Gamma(G) \mid n_\varphi = 0\}.$$

The center $Z(G)$ is a $\Gamma(G)$-subgroup of G, hence for every $\phi \in \Gamma(G)$ the restriction ϕ^* of ϕ to $Z(G)$ belongs to $\Gamma(Z(G))$. Denote by

$$\tau : \Gamma(G) \longrightarrow \Gamma(Z(G))$$

the corresponding ring homomorphism $\tau(\phi) = \phi^*$. The definition above implies that $I = ker(\tau)$.

Notice that every integer n gives rise to a mapping $\psi_n : g \to g^n$ which belongs to $\Gamma(G)$. We will identify the ring of integers $\mathbf{Z}$ with the corresponding subring in $\Gamma(G)$ under the embedding $n \to \psi_n$. Now we can formulate the following

Lemma 5.3 *I is an ideal in $\Gamma(G)$ and $\Gamma(G) \simeq \mathbf{Z} \bigoplus I$.*

Proof. We have mentioned already that $I = ker(\tau)$, hence I is an ideal in $\Gamma(G)$. So we need only to prove that $\Gamma(G) \simeq \mathbf{Z} \bigoplus I$.

By definition, $\varphi \in I$ if and only if $n_\varphi = 0$, so $\mathbf{Z} \cap I = 0$. Let $\varphi \in \Gamma(G)$ and $z \in Z(G)$. Then

$$z^{\varphi - n_\varphi} = z^{n_\varphi} \cdot z^{-n_\varphi} = 1.$$

Therefore $\varphi - n_\phi \in I$, and $\Gamma(G) = \mathbf{Z} \bigoplus I$. □

Lemma 5.4 *Let g be an arbitrary element from G_i such that $g \notin G_{i+1}$. Then the following hold:*

1. *if $i \geq c/2$, then $g^\varphi = g^{n_\varphi}$ modulo G_{i+1};*

2. *if $i < c/2$ then $g^\varphi = g^{n_\varphi}$ modulo G_{c-i+1}.*

Proof. We prove the first part of this lemma by induction on i. If $i = c$, then the statement holds by Lemma 5.2, part 2. Let $i \geq c/2$ and let g be an arbitrary element from G_i which does not belong to G_{i+1}. Then for every $x \in G$ we have $[g,x] \in G_{i+1}$ and hence by induction

$$[g,x]^{\varphi} = [g,x]^{n_\varphi} \quad modulo\ G_{i+2}.$$

Observe that g^{-1} commutes with $x^{-1}gx$ since

$$[g^{-1}, x^{-1}gx] = [g^{-1}, [g,x]] \in G_{2i+1} \subset G_{c+1} = 1.$$

Therefore

$$[g,x]^{\varphi} = (g^{-1}x^{-1}gx)^{\varphi} = g^{-\varphi}(x^{-1}gx)^{\varphi} = g^{-\varphi}x^{-1}g^{\varphi}x = [g^{\varphi}, x].$$

This implies that

$$[g^{\varphi}, x] = [g,x]^{\varphi} = [g^{n_\varphi}, x] \quad modulo\ G_{i+1}.$$

Thus, for any $x \in G$ we have $[g^{\phi - n_\varphi}, x] \in G_{i+2}$, and consequently, $g^{\phi - n_\varphi} \in G_{i+1}$. Part 1 of the lemma follows.

Now, let us prove part 2. Suppose $i < c/2$. For any $x \in G_{c-i}$ we have $[g,x] \in Z(G)$, so

$$[g^{\varphi - n_\varphi}, x] = [g,x]^{\varphi - n_\varphi} = 1.$$

This implies that $g^{\varphi - n_\varphi} \in G_{i+1}$. Observe that $[g, g^{\varphi - n_\varphi}] = 1$, hence by Proposition 5.1 we have

$$g^{\varphi - n_\varphi} \in G_{i+1} \cap C_G(g) = G_{c-i+1}$$

(we used here that $i < c/2$ and hence $i+1 < c-i+1$). $\square$

Corollary 5.3 *Let G be a free nilpotent group of finite rank. Then $Z_i(G)$ is $\Gamma(G)$-invariant for each i.*

Theorem 5.1 *If G is a non-abelian free nilpotent group of class c, then $\Gamma(G) = \mathbf{Z} \bigoplus I$, and $I^d = 0$, where d is the smallest integer such that $d > c/2$.*

Proof. This theorem follows directly from Lemma 5.3 and Lemma 5.4. $\square$

Analyzing the proof of the theorem above, one can see that the argument works also for free nilpotent R-groups in the sense of P. Hall [11]. Recall that an integral (commutative) domain R of characteristic 0 is termed a *binomial domain* if for any $r \in R$ and $n > 0$ the equation

$$r(r-1)\dots(r-n+1) = n!x$$

has a solution in R. Now, following P.Hall [11] we describe the R-completion G^R of an arbitrary torsion-free finitely generated nilpotent group G.

An ordered set of elements $a_1, \ldots, a_n \in G$ is called a Mal'cev basis for G if every element g of G can be uniquely expressed in the form

$$g = a_1^{t_1(g)} \ldots a_n^{t_n(g)},$$

where $t_1(g), \ldots, t_n(g) \in \mathbf{Z}$ and the subgroups $G_i = < a_i, \ldots, a_n >$ form a central series

$$G = G_1 \geq G_2 \geq \ldots$$

in the group G. The numbers $t_i(g)$'s are called *the coordinates* of g with respect to the given basis $a_1, \ldots, a_n$.

A. Mal'cev [17] proved that such basis exists in every torsion-free nilpotent group G (see also [11]). Moreover, he proved that the multiplication and exponentiation in G can be defined coordinate-wise by some polynomials $f_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$ and $h_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$ $(i = 1, \ldots, n)$ with rational coefficients. Namely, for any elements $u, v \in G$ and an integer λ the following holds for each $i = 1, \ldots, n$

$$t_i(uv) = f_i(t_1(u), \ldots, t_n(u), t_1(v), \ldots, t_n(v)), \tag{4}$$

$$t_i(u^\lambda) = h_i(t_1(u), \ldots, t_n(u), \lambda). \tag{5}$$

Now let

$$G^R = \{a_1^{r_1} \ldots a_n^{r_n} | r_i \in R\},$$

where $a_1^{r_1} \ldots a_n^{r_n}$ is just a formal product of this type.

If $u = a_1^{r_1} \ldots a_n^{r_n} \in G^R$, then elements $t_i(u) = r_i \in R$ $(i = 1, \ldots, n)$ are called *coordinates* of u. Now we can define multiplication and R-exponentiation on G^R by the formulas (4) and (5) (assuming in the latter that λ is an arbitrary element in R). This turns G^R into a nilpotent R-group. Notice that if N is a free nilpotent group of class c with basis $x_1, \ldots, x_m$, then N^R is a free nilpotent R-group (in the P.Hall category of nilpotent R-groups) of class c and with basis $x_1, \ldots, x_m$.

Analogues of Proposition 5.1 and Lemmas 5.2, 5.3 and 5.4 also hold for the free nilpotent R-group $G = N^R$. To explain this, denote by F the field of fractions of the integral domain R. It follows from the P.Hall construction above that $G = N^R$ canonically embeds into $H = N^F$. The same argument as above implies that if $g \in H_i - H_{i+1}$ then

$$C_H(g) =< g >_F H_{c-i+1}.$$

This translates into the group $G = N^R$ as follows: if $g \in G_i - G_{i+1}$ and $[g, u] = 1$, then either $u \in G_{c-i+1}$ or $g^\alpha G_{c-i+1} = u^\beta G_{c-i+1}$ for some $\alpha, \beta \in R$. Observe that another way to prove this is to use Mal'cev's correspondence between free nilpotent F-groups and free nilpotent Lie F-algebras (see for example [26]).

Now, the argument in Lemmas 5.3 and 5.4 goes through without any changes. Let us show how to prove the analogue of Lemma 5.2. To formulate the analogue one needs just to replace $n_\varphi \in \mathbf{Z}$ by $n_\varphi \in R$. Then the first part of the proof (i.e., $n_i = n_1 = n_\varphi$ for all i) works readily for the analog. To prove that $z^\varphi = z^{n_\varphi}$, observe that the argument in the lemma holds if we can prove that each $\varphi \in \Gamma(G)$ acts on $Z(G)$ as an R-endomorphism. To show this it suffices to prove that φ acts as an R-homomorphism on R-generators of $Z(G)$, for example, on all simple commutators of weight c in the generators $x_1, \ldots, x_n$. Now for any $r \in R$ the following holds:

$$([x_{i_1}, \ldots, x_{i_{c-1}}, x_{i_c}]^r)^\varphi = [x_{i_1}, \ldots, x_{i_{c-1}}^r, x_{i_c}]^\varphi = [x_{i_1}, \ldots, x_{i_{c-1}}^r, x_{i_c}^\varphi] =$$

$$[x_{i_1}, \ldots, x_{i_{c-1}}, x_{i_c}^\varphi]^r = ([x_{i_1}, \ldots, x_{i_{c-1}}, x_{i_c}]^\varphi)^r,$$

which proves the statement and the second part of the lemma. To finish the proof, let us consider an arbitrary $g \in G - G_2$. Since the centralizer of g in G is invariant under $\Gamma(G)$, we have that

$$(g^\varphi)^\alpha = g^\beta z$$

for some $\alpha, \beta \in R$ and $z \in Z(G)$. Since $g \notin G_2$, there exists an element $u \in Z_2(G)$ such that $1 \neq [g, u^\alpha] \in Z(G)$. In this case

$$[g, u^\alpha]^\varphi = [g, u^\alpha]^{n_\varphi} = [g^{n_\varphi}, u^\alpha] = [g, u]^{n_\varphi \alpha}.$$

On the other hand,

$$[g, u^\alpha]^\varphi = [g^\varphi, u^\alpha] = [(g^\varphi)^\alpha, u] = [g^\beta, u] = [g, u]^\beta.$$

Since the center of a free nilpotent R-group is a free abelian R-group (i.e., free R-module), this implies that $\alpha n_\varphi = \beta$. But then

$$(g^\varphi)^\alpha = g^\beta z = (g^{n_\varphi})^\alpha z$$

and since R-roots are unique in the quotient group $G/Z(G)$ we have $g^\varphi = g^{n_\varphi}$ *modulo* $Z(G)$, as desired. This finishes the proof of the lemma.

Summarizing the discussion above, we have the following result.

Theorem 5.2 *Let R be a binomial domain and G a finitely generated non-abelian free nilpotent group of class c. Then $\Gamma(G^R) = R \bigoplus I$, and $I^d = 0$, where d is the smallest integer such that $d > c/2$.*

5.2 Centroid of $UT_n(R)$

Now we will prove that the centroid of $G = UT_n(\mathbf{Z}), n \geq 3$, has a structure similar to the structure of the centroid of a finitely generated free nilpotent group.

By $t_{ij}, i < j$ we denote the elements of G having 1's on the main diagonal and in column j of row i, and 0's everywhere else.

The center of G is the cyclic group generated by t_{1n}. Since the center of G is Γ-invariant, we can define a ring homomorphism $\tau : \Gamma(G) \to \mathbf{Z}, \varphi \mapsto n_\varphi$, where $n_\varphi \in \mathbf{Z}$ is such that $t_{1n}^\varphi = t_{1n}^{n_\varphi}$.

Note that any integer n can be viewed as an element of $\Gamma(G)$: n takes elements to their n^{th} power.

Lemma 5.5 *$\Gamma(G) \simeq \mathbf{Z} \bigoplus I$, where $I = ker(\tau) \lhd \Gamma(G)$.*

Proof. Any $\varphi \in \Gamma(G)$ can be written uniquely in the form $\varphi = n_\varphi + (\varphi - n_\varphi)$, where $n_\varphi \in \mathbf{Z}$ and $\varphi - n_\varphi \in I$. Also, it is easy to see that $\mathbf{Z} \cap I = \{0\}$, which completes the proof. □

Lemma 5.6 *$I^n = 0$.*

Proof. The elements t_{ij} constitute a Mal'cev basis for G, and every element $g \in G$ can be written uniquely in the form: $g = t_{12}^{\alpha_{12}} t_{23}^{\alpha_{23}} \dots t_{1n}^{\alpha_{1n}}$. Let us fix an arbitrary element $\varphi \in I$ and write the image of g under φ in the form: $g^\varphi = t_{12}^{\beta_{12}} t_{23}^{\beta_{23}} \dots t_{1n}^{\beta_{1n}}$. We will prove the lemma by showing that if $\alpha_{ij} = 0$ for all $j :\ 1 < j < N$ and for all $i :\ 1 \leq i < j$, then $\beta_{ij} = 0$ for all $j :\ 1 < j \leq N$ and for all $i :\ 1 \leq i < j$.

Before we begin the proof, let us point out the following useful identity:

$$[ab, c] = [a, c]^b [b, c] = [a, c][a, c, b][b, c] \tag{6}$$

First, let us assume that $\alpha_{12} \neq 0$. We can think of g as $g = ab$, where $a = t_{12}^{\alpha_{12}}$ and $b = t_{23}^{\alpha_{23}} t_{34}^{\alpha_{34}} \cdots t_{1n}^{\alpha_{1n}}$. Then, using identity 6,

$$[g, t_{2n}] = [t_{12}^{\alpha_{12}}, t_{2n}]^b [b, t_{2n}]$$

Since all factors $t_{ij}^{\alpha_{ij}}$ in b are such that $i < n$ and $j > 2$, we have $[b, t_{2n}] = 1$, so

$$[g, t_{2n}] = [t_{12}^{\alpha_{12}}, t_{2n}]^b = ([t_{12}, t_{2n}]^{\alpha_{12}})^b = (t_{1n}^{\alpha_{12}})^b,$$

but $t_{1n}^{\alpha_{12}} \in Z(G)$, hence $[g, t_{2n}] = t_{1n}^{\alpha_{12}} \in Z(G)$. Then by Lemma 5.1 $1 = [g, t_{2n}]^\varphi = [g^\varphi, t_{2n}] = t_{1n}^{\beta_{12}}$, which implies $\beta_{12} = 0$.

Suppose now that $\alpha_{ij} = 0$ for all j with $1 < j < N$ and all i with $1 \leq i < j$. For j and i as above, we will prove by induction on j that $\beta_{ij} = 0$. By the induction hypothesis, $\beta_{ik} = 0$ for all $k < j$, $i < k$.

Since all $\alpha_{ij} = 0$ for $j < N$, we have $1 = [g, t_{jn}]$, and therefore $1 = [g, t_{jn}]^\varphi = [g^\varphi, t_{jn}]$.

Write g^φ in terms of the Mal'cev basis: $g^\varphi = t_{12}^{\beta_{12}} t_{23}^{\beta_{23}} \cdots t_{1n}^{\beta_{1n}}$. By the induction hypothesis, the first non-trivial term in this product is $t_{j-1,j}^{\beta_{j-1,j}}$; let us denote it by a_1 and the rest of the product by b_1. Then by the second part of identity 6, we have

$$1 = t_{j-1,n}^{\beta_{j-1,j}} [t_{j-1,n}^{\beta_{j-1,j}}, b_1][b_1, t_{jn}]$$

Note that the second factor vanishes due to the fact that b_1 does not contain t_{ik} with $k < j$ by the induction hypothesis. Thus we simply have

$$1 = t_{j-1,n}^{\beta_{j-1,j}} [b_1, t_{jn}].$$

We now turn our attention to the commutator $[b_1, t_{jn}]$. Write $b_1 = a_2 t_{j-2,j} b_2$, where a_2 commutes with t_{jn}.

Using identity 6 again, we see that

$$[b_1, t_{jn}] = [t_{j-2,j} b_2, t_{jn}] = t_{j-2,n}^{\beta_{j-2,j}} [t_{j-2,n}^{\beta_{j-2,j}}, b_2][b_2, t_{jn}] = t_{j-2,n}^{\beta_{j-2,j}} [b_2, t_{jn}]$$

by the same argument as before. This yields

$$1 = t_{j-1,n}^{\beta_{j-1,j}} t_{j-2,n}^{\beta_{j-2,j}} [b_2, t_{jn}]$$

Proceeding in the same fashion, we obtain

$$1 = t_{j-1,n}^{\beta_{j-1,j}} t_{j-2,n}^{\beta_{j-2,j}} \cdots t_{1,n}^{\beta 1,j}.$$

Because the elements t_{ij} constitute a Mal'cev basis for G, this implies that $\beta_{ij} = 0$ for all $i < j < N$.

Note that $[g, t_{Nn}] = t_{N-1\ n}^{\beta_{N-1\ N}} t_{N-2\ n}^{\beta_{N-2\ N}} t_{1n}^{\beta_{1N}}$. Moreover, $[t_{1j}, [g, t_{Nn}]] = t_{1n}^{\alpha_{jN}} \in Z(G)$. Since $[g, [g, t_{Nn}]] = 1$, by Lemma 5.1 we have $1 = [t_{1j}, [g, t_{Nn}]]^\varphi = [t_{1j}, [g^\varphi, t_{Nn}]] = t_{1n}^{\beta_{jN}}$. Therefore, $\beta_{jN} = 0$ for every $j < N$. This concludes the proof of the lemma. □

Theorem 5.3 *If $G = UT_n(\mathbf{Z})$, then $\Gamma(G) = \mathbf{Z} \bigoplus I$, and $I^n = 0$.*

Proof. This theorem follows directly from lemmas 5.5 and 5.6. □

It is easy to see that lemmas 5.5 and 5.6 continue to be valid if we replace the ring of integers $\mathbf{Z}$ by an arbitrary associative ring R of characteristic 0 (the same argument). This allows us to formulate the following theorem:

Theorem 5.4 *If $G = UT_n(R)$, then $\Gamma(G) = R \bigoplus I$, and $I^n = 0$.*

6 The rigidity problem

Definition 6.1 *A torsion-free nilpotent group G is called* rigid *if $G^R \simeq G^S$ implies $R \simeq S$ for any two binomial domains R and S of characteristic 0.*

In [10] F.Grunewald and D.Segal proved that $UT_n(\mathbf{Z})$ ($n \geq 3$) is rigid, and formulated the following problem:

Problem 6.1 *Is a finitely generated non-abelian free nilpotent group N rigid?*

Using the structure of the centroid of the free nilpotent R-group N^R obtained in the previous section, we can answer this question affirmatively.

Theorem 6.1 *Every finitely generated non-abelian free nilpotent group N is rigid.*

Proof. Suppose that $N^R \simeq N^S$. Then their centroids are also isomorphic, so $\Gamma(N^R) \simeq \Gamma(N^S)$, and from our description of centroids we obtain that $R \oplus I_1 \simeq S \oplus I_2$, where I_1 and I_2 are as in Theorem 5.2.

We now claim that I_1 is an ideal containing all nilpotent elements in $\Gamma(N^R)$. Indeed, all elements of I_1 are nilpotent by Theorem 5.4. If $r \in R,\ r \neq 0$, then $(r+i)^n = r^n + j \neq 0$, since $r^n \neq 0$. Similarly, I_2 contains all nilpotent elements of $\Gamma(N^S)$.

Denote by f the isomorphism between $R \oplus I_1$ and $S \oplus I_2$. Since the image of a nilpotent element under f is again nilpotent, $f(I_1) = I_2$. Therefore, f induces an isomorphism $\bar{f} : R \oplus I_1/I_1 \longrightarrow S \oplus I_2/I_2$, that implies $R \simeq S$. $\square$

Finally, we observe that according to Theorem 5.4, the centroid of the group $UT_n(R)$ is isomorphic to $R \oplus I$, where I is a nilpotent ideal. Moreover, $UT_n(\mathbf{Z})^R \simeq UT_n(R)$. Thus our method offers an alternative proof of the fact that $UT_n(\mathbf{Z})$ is rigid for every $n \geq 3$.

References

[1] Baumslag G. *Some aspects of groups with unique roots.* Acta Math., 1960, 104, p.217-303.

[2] Fitting H. *Die Theorie der Automorphismenringe abelscher Gruppen und ihr analogon bei nichtcommutativen Gruppen.* Math. Ann., 1933, 107, p. 514-543.

[3] Fröhlich A. *Distributively generated near-rings.* Proc. Lond. Math. Soc., 1958, 8, p. 76-108.

[4] Fröhlich A. *On groups over a.d.g. near-rings.* Quart. J. Math. (Oxford) (2) II, 1960, p. 193-228.

[5] Fröhlich A. *Non-abelian homological algebra. I. Derived functors and satellites.* Proc. Lond. Math. Soc. II, 1961, p. 239-275.

[6] Fröhlich A. *Non-abelian homological algebra. II. Varieties.* Proc. Lond. Math. Soc., 1962, 12, p. 1-28.

[7] Fröhlich A. *Non-abelian homological algebra. III. The functors EXT and TOR.* Proc. Lond. Math. Soc., 1962, 12, p. 739-768.

[8] Ghys E., P. de la Harpe *Sur les groupes hyperboliques d'apres Mikhael Gromov.* Progress in Mathematics, 83, 1990.

[9] Gildenhuys D., Kharlampovich O., Myasnikov A. *CSA–groups and separated free constructions.* Bulletin of the Australian Math. Soc., 1995, v. 52, 1, p. 63-84.

[10] Grunewald F., Segal D. *Reflections on the classification of torsion-free nilpotent groups* Group Theory: essays for Philip Hall, 1984, p. 121-158.

[11] Hall P. *Nilpotent groups.* Canad. Math. Congress, Edmonton, 1957.

[12] Heerema N. *Sums of normal endomorphisms.* Trans. Amer. Math. Soc., 1957, 84, p. 137-147.

[13] Kargapolov M.I., Merzljakov Ju.I. *Fundamentals of the Theory of Groups.*

[14] Lyndon R., Paul E. Schupp *Combinatorial Group Theory.* Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[15] Lyndon R. *Groups with parametric exponents.* Trans. Amer. Math. Soc., 1960, 96, p. 518-533.

[16] Magnus W., Karras A., Solitar D. *Combinatorial group theory.* Interscience publ., 1966.

[17] Mal'cev A.I. *Nilpotent torsion-free groups.* Izvestia Akad. Nauk USSR, Ser.Mat., 1949, 13 , p. 9-32.

[18] Meldrum J.D.P. *Near-rings and their links with groups.* Pitman, London, 1985.

[19] Myasnikov A.G., Remeslennikov V.N. *Exponential groups 1: Foundations of the theory and tensor completions.* Siberian Math. J., 1995, v.5.

[20] Myasnikov A.G., Remeslennikov V.N. *Exponential groups 2: Extensions of centralizers and tensor completion of CSA–groups.* Int. Journal of Algebra and Computation, 1996, v.6, N.6, p. 687-711.

[21] Myasnikov A. *Structure of models and criteria of decidability of complete theories of finite-dimensional algebras.* Izvest. Akademii Nayk USSR, ser. math., 1989, v.53,2, p. 379-397.

[22] Neumann H. *Near-rings connected with free groups* Proc. Intern. Confer., Amsterdam II (1954), p. 46-47.

[23] Neumann H. *On varieties of groups and their associated near-rings* Math. Z., 1956, 65 , p. 36-69.

[24] Pilz G. *Near-rings.* North-Holland / American Elsevier. Amsterdam, 1983.

[25] Robinson D.A. *Sums of normal semi-endomorphisms.* Amer. Math. Month., 1963, 70, p. 537-539.

[26] Warfield R.B. *Nilpotent groups.* Lect. Notes in Math., 513, Springer-Verlag, Berlin, Heidelberg, New York, 1976.