

The brace of a classical group

Wolfgang Rump

Institute for Algebra and Number Theory,

University of Stuttgart

Stuttgart, Germany wolfgang.rump@mathematik.uni-stuttgart.de

Abstract. We exhibit incarnations of *braces* in the context of analytic, algebraic, and finite groups and discuss related old and new problems and conjectures.

Keywords: Brace, 1-cocycle, flat manifold, torsor, quantum Yang-Baxter equation, Chevalley group, nilpotent Lie algebra, RSA structure, p -group.

MSC 2010 classification: Primary: 14L35, 17B45, 22E25, 22E45, 16T25, 22F30. Secondary: 17C36

dedicated to B. V. M.

1 The concept of brace

Let R be a *pseudo-ring* ([10], 1.8.1), that is, R satisfies all properties of a ring except the existence of a unit element. A left ideal I of R is said to be *modular* [36, 7] if there is an element $e \in R$ with $ae - a \in I$ for all $a \in R$. If R is the only modular left ideal, R is said to be a *radical ring*. For example, the Jacobson radical of any (unital) ring is a radical ring. More generally, the *radical* of a pseudo-ring R , the intersection of all modular maximal left ideals (see [39], Lemma 1), is a radical ring. Every radical ring R is a group R° with respect to Jacobson’s circle operation

$$a \circ b := ab + a + b. \tag{1}$$

In particular,

$$a \circ 0 = 0 \circ a = a.$$

The group R° is called the *adjoint group* of R .

Recall that a *1-cocycle* of a right module A over a group G (with right action $a \mapsto a^g$) is a map $d : G \rightarrow A$ which satisfies

$$d(gh) = d(g)^h + d(h)$$

for all $g, h \in G$.

Proposition 1.1. *Let R be a radical ring. The right action $a^b := ab + a$ of R° on the additive group of R makes R into a right R° -module. The identity map $R^\circ \rightarrow R$ is a 1-cocycle.*

Proof. Since $(a + b)^c = (a + b)c + a + b = (ac + a) + (bc + b) = a^c + b^c$ and $(a^b)^c = (ab + a)c + (ab + a) = a(bc + b + c) + a = a^{b \circ c}$, we have

$$(a + b)^c = a^c + b^c, \quad a^{b \circ c} = (a^b)^c \quad (2)$$

for all $a, b, c \in R$. Furthermore, $a^0 = a$. Thus R is a right R° -module. Eq. (1) can be written as

$$a \circ b = a^b + b, \quad (3)$$

which means that the identity map $R^\circ \rightarrow R$ is a 1-cocycle. \square

Now let $d: G \rightarrow A$ be any bijective 1-cocycle, where A is a right G -module. Identifying G with A , we get an abelian group A with a group structure $A^\circ := (A, \circ)$ and a right action $a \mapsto a^b$ of A° on A such that Eqs. (2) and (3) hold. The conditions are partly redundant. It suffices to assume that the abelian group A has a multiplication which satisfies

- (B1) $(a + b)c = ac + bc$
- (B2) $a(bc + b + c) = (ab)c + ab + ac$
- (B3) The map $x \mapsto x^a := xa + x$ is bijective,

so that the circle operation is given by Eq. (1). Note that (B1) and (B2) are equivalent to Eq. (2), while (B3) is an immediate consequence of the group action.

Definition 1. A *(right) brace* is an (additive) abelian group A with multiplication $(a, b) \mapsto ab$ satisfying (B1)-(B3).

Axiom (B2) combines the associativity rule with the left distributive law. Using the right multiplication

$$R_b(a) := ab,$$

it can be written as

$$R_{b \circ c} = R_b \circ R_c$$

which relates the *internal* circle operation $b \circ c$ of A with an *external* circle operation, namely, the circle operation in the endomorphism ring of $(A, +)$.

Compare this with the Jacobi identity

$$[a, [b, c]] = [[a, b], c] - [[a, c], b]$$

[60] Y. P. Sysak: Products of groups and local nearrings, *Note Mat.* 28 (2008), suppl. n. 2, 177-211

[61] J. Tate, M. Van den Bergh: Homological properties of Sklyanin Algebras, *Invent. Math.* 124 (1996), 619-647

[62] M. Vergne: Cohomologie des algèbres de Lie nilpotentes, Application à l'étude de la variété des algèbres de Lie nilpotentes, *Bull. Soc. Math. France* 98 (1970) 81-116

[63] E. B. Vinberg: Homogeneous cones, *Dokl. Akad. Nauk SSSR* 133:1 (1960) 9-12 = *Soviet Math. Dokl.* 1 (1960), 787-790

[64] E. B. Vinberg: The theory of homogeneous convex cones, *Trudy Moskov. Mat. Obšč.* 12 (1963), 303-358

[65] H.-C. Wang: Two-point homogeneous spaces, *Ann. of Math.* 55 (1952), 177-191

[66] H. Weyl: Über die Gleichverteilung von Zahlen mod. Eins, *Math. Ann.* 77 (1916), 313-352

[67] N. J. Wildberger: A combinatorial construction of G_2 , *J. Lie Theory* 13 (2003), no. 1, 155-165

[68] N. J. Wildberger: A combinatorial construction for simply-laced Lie algebras, *Formal power series and algebraic combinatorics* (Scottsdale, AZ, 2001), *Adv. in Appl. Math.* 30 (2003), no. 1-2, 385-396

The brace of a classical group

This shows that axiom (B2) is quite natural.

The next proposition shows that braces are just equivalent to bijective 1-cocycles.

Proposition 1.2. *Let A be an additive abelian group with a multiplication satisfying (B1). Then A is a brace if and only if Eq. (1) defines a group structure on A .*

Proof. Using (B1), we have $a \circ (b \circ c) = a(b \circ c) + a + (bc + b + c)$ and $(a \circ b) \circ c = (ab + a + b)c + (ab + a + b) + c = (ab)c + ac + bc + ab + a + b + c$. Hence (B2) is equivalent to the associativity of (A, \circ) . Furthermore, (B1) implies that $0c = (0 + 0)c = 0c + 0c$. Hence $0c = 0$, and thus $0 \circ c = c$ for all $c \in A$. Now (B3) states that the map $x \mapsto x \circ a$ is bijective for all $a \in A$. Thus it suffices to show that a semigroup (A, \circ) is a group if the right multiplications are bijective and there is a left unit element. This fact is well known (e. g., [43], I.2). \square

Corollary. *Every bijective 1-cocycle gives rise to a brace, and vice versa.*

Bijective 1-cocycles arise in many different contexts. For example, Etingof and Gelaki [23] use them for the construction of semisimple Hopf algebras.

Like the concept of skew-field which naturally arises from a projective space by the Veilen-Young theorem, braces can be understood geometrically as groups with an extra structure of a principal homogeneous affine space.

Definition 2. Let k be a field. We say that a brace A is *k-linear* or a *k-brace* if its additive group is a k -vector space such that $(\lambda a)b = \lambda(ab)$ holds for $\lambda \in k$ and $a, b \in A$.

k -linear braces were considered by Catino and Rizzo [16] who called them "circle algebras", referring to Jacobson's circle operation. Catino and Rizzo [16] generalize previous work [14] to non-commutative groups by proving that circle algebras are equivalent to affine k -spaces on which a group acts freely and transitively. For arbitrary braces, the correspondence is given as follows. Recall that a *torus* is a set A together with a free transitive right action of a group G . If A is an abelian group such that the implication

$$a - b = c - d \implies ag - bg = cg - dg$$

holds for $a, b, c, d \in A$ and $g \in G$, we call (A, G) an *affine torus*. Equivalently,

$$ag + bg = (a + b)g + 0g$$

for $a, b \in A$ and $g \in G$. The bijection $G \xrightarrow{\sim} A$ with $g \mapsto 0g$ allows us to identify G with A . So the group G induces a group structure (A, \circ) on A with neutral element 0. The equation $(0g)h = 0(gh)$ for $g, h \in G$ then implies that the group action of G on A turns into the right regular representation $a \mapsto a \circ b$ of (A, \circ) . In other words, an affine torsor is equivalent to an abelian group A with a second group structure (A, \circ) , both with neutral element 0, such that the equation

$$a \circ c + b \circ c = (a + b) \circ c + c$$

holds for $a, b, c \in A$. With the multiplication $ab := a \circ b - a - b$, this equation turns into (B1). Therefore, Proposition 1.2 immediately gives

Proposition 1.3. *Every brace can be viewed as an affine torsor, and every affine torsor arises in this way.*

Braces can also be characterized in terms of triply factorized groups. I am grateful to Bernhard Amberg who told me that such a connection was observed by Y. Sysak (see [60], Theorem 18). Note first that every right module A over a group G gives rise to a semidirect product $S := G \ltimes A$, such that the elements of S are multiplied by the rule $(g, a)(h, b) = (gh, a^h + b)$, with $g, h \in G$ and $a, b \in A$. The groups G and A can be regarded as subgroups of S , and the operation of G on A is given by conjugation: $a^g = g^{-1}ag$. Thus a right G -module A is completely described by a group S with a subgroup G and an abelian normal subgroup A such that $S = GA$ and $G \cap A = 1$.

Now any map $d: G \rightarrow A$ with $d(1) = 0$ is determined by its graph $H := \{gd(g) \mid g \in G\}$, a subset of S with $HA = S$ and $H \cap A = 1$, and vice versa. It is easy to check that H is a subgroup if and only if d is a 1-cocycle. The kernel of d is $G \cap H$, and d is surjective if and only if $GH = S$. Since braces are tantamount to bijective 1-cocycles, we obtain

Proposition 1.4. *Up to isomorphism, there is a one-to-one correspondence between braces and groups S with subgroups G, H and an abelian normal subgroup A such that $S = GA = HA = GH$ and $G \cap A = H \cap A = G \cap H = 1$.*

2 The origin of braces

The construction of quantum groups is based on the *quantum Yang-Baxter equation*, an equation for an operator $R \in \text{End}(V \otimes V)$ on a vector space V . On the threefold tensor product $V \otimes V \otimes V$, the operator R gives rise to partial operators R^{ij} , acting on the i th and j th component (in this order) for distinct $i, j \in \{1, 2, 3\}$ and leaving the third component fixed. Then the equation reads

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}. \quad (4)$$

- [37] E. Jespers, J. Okniński: Monoids and Groups of I-Type, *Algebr. Represent. Theory* 8 (2005), 709-729
- [38] D. Joyce: Compact Riemannian 7-manifolds with holonomy G_2 , I, II, *J. Differential Geom.* 43 (1996), no. 2, 291-328, 329-375
- [39] I. Kaplansky: Dual rings, *Ann. of Math.* 49 (1948), 689-701
- [40] W. Killing: Über die Clifford-Kleinschen Raumformen, *Math. Ann.* 39 (1891), 257-270
- [41] M. Koecher: Positivitätsbereiche im R^n , *Amer. J. Math.* 97 (1975), 575-596
- [42] G. Laffaille: Quantum binomial algebras, *Colloquium on Homology and Representation Theory* (Spanish) (Vaquerías, 1998). *Bol. Acad. Nac. Cienc. (Córdoba)* 65 (2000), 177-182
- [43] S. Lang: *Algebra*, Revised third edition, *Graduate Texts in Mathematics*, 211, Springer-Verlag, New York, 2002
- [44] M. Lazard: Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sci. Ecole Norm. Sup.* 71 (1954), 101-190
- [45] G. A. Margulis: Free completely discontinuous groups of affine transformations, *Dokl. Akad. Nauk SSSR* 272 (1983), no. 4, 785-788
- [46] G. A. Margulis: Complete affine locally flat manifolds with a free fundamental group, *Automorphic functions and number theory*, II. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* 134 (1984), 190-205
- [47] L. Markus: *Cosmological models in differential geometry*, mimeographed notes, University of Minnesota, 1962
- [48] A. Medina, Y. Khakimdjanyov: Groupes de Lie nilpotents à structure affine invariante à gauche, *Transform. Groups* 6 (2001), no. 2, 165-174
- [49] J. Milnor: On fundamental groups of complete affinely flat manifolds, *Advances in Math.* 25 (1977), no. 2, 178-187
- [50] C. M. Ringel: Hall algebras and quantum groups, *Invent. Math.* 101 (1990), no. 3, 583-591
- [51] C. M. Ringel: Hall polynomials for the representation-finite hereditary algebras, *Adv. Math.* 84 (1990), no. 2, 137-178
- [52] W. Rump: A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation, *Adv. Math.* 193 (2005), no. 1, 40-55
- [53] W. Rump: Braces, radical rings, and the quantum Yang-Baxter equation, *J. Algebra* 307 (2007), no. 1, 153-170
- [54] W. Rump: Generalized radical rings, unknotted biquandles, and quantum groups, *Colloq. Math.* 109 (2007), no. 1, 85-100
- [55] W. Rump: Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation, *J. Algebra Appl.* 7 (2008), no. 4, 471-490
- [56] W. Rump: Addendum to "Generalized radical rings, unknotted biquandles, and quantum groups" (*Colloq. Math.* 109 (2007), 85-100) [MR2308827], *Colloq. Math.* 117 (2009), no. 2, 295-298
- [57] W. Rump: Classification of cyclic braces, *J. Pure Appl. Algebra* 209 (2007), no. 3, 671-685
- [58] J. Scheuneman: Translations in certain groups of affine motions, *Proc. Amer. Math. Soc.* 47 (1975), 223-228
- [59] D. Segal: The structure of complete left-symmetric algebras, *Math. Ann.* 293 (1992), no. 3, 569-578

[15] Y. Carrière: Autour de la conjecture de L. Markus sur les variétés affines, Invent. Math. 95 (1989), no. 3, 615-628

[16] F. Catinio, R. Rizzo: Regular subgroups of the affine group and radical circle algebras, Bull. Aust. Math. Soc. 79 (2009), no. 1, 103-107

[17] A. Cayley, Esq.: On the Theory of the Analytical Forms called Trees, Philos. Magazine, Series 4, XXVIII (1857), 172-176, <http://dx.doi.org/10.1080/14786445708642275>

[18] F. Cedo, E. Jespers, Eric: A. del Rio: Involutive Yang-Baxter groups, Trans. Amer. Math. Soc. 362 (2010), no. 5, 2541-2558

[19] T. de Cat, K. Dèkimppe, P. Igodet: Translations in simply transitive affine actions of Heisenberg type Lie groups, Linear Algebra Appl. 359 (2003), 101-111

[20] F. Chapoton, M. Livernet: Pre-Lie algebras and the rooted trees operad, Internat. Math. Res. Notices 8 (2001), 393-408

[21] A. Connes, D. Kreimer: Hopf algebras, renormalization and noncommutative geometry, Comm. Math. Phys. 199 (1998), no. 1, 203-242

[22] V. G. Drinfeld: On some unsolved problems in quantum group theory, in: Quantum Groups (Leipzig), Lecture Notes in Math. 1510, Springer-Verlag, Berlin, 1992, 1-8

[23] P. Etingof, S. Gelaki: A method of construction of finite-dimensional triangular semisimple Hopf algebras, Math. Research Letters 5 (1998), 551-561

[24] P. Etingof, T. Schedler, A. Solovlev: Set-theoretical solutions to the quantum Yang-Baxter equation, Duke Math. J. 100 (1999), 169-209

[25] D. Fried, W. M. Goldman: Three-dimensional affine crystallographic groups, Adv. in Math. 47 (1983), no. 1, 1-49

[26] D. Fried: Flat spacetimes, J. Differential Geom. 26 (1987), no. 3, 385-396

[27] D. Fried, W. M. Goldman: Three-dimensional affine crystallographic groups, Adv. in Math. 47 (1983), no. 1, 1-49

[28] T. Gateva-Ivanova: Noetherian properties of skew polynomial rings with binomial relations, Trans. Amer. Math. Soc. 343 (1994), no. 1, 203-219

[29] T. Gateva-Ivanova: A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation, J. Math. Phys. 45 (2004), 3828-3838

[30] the International Algebra Conference, Regularity of skew-polynomial rings with binomial relations, Talk at the International Algebra Conference, Miskolc, Hungary, 1996

[31] T. Gateva-Ivanova: Quadratic algebras, Yang-Baxter equation, and Artin-Schelter regularity, Adv. Math. 230 (2012), no. 4-6, 2152-2175

[32] T. Gateva-Ivanova, M. Van den Bergh: Semigroups of I-type, J. Algebra 206 (1998), 97-112

[33] M. Gershenhaber: The cohomology structure of an associative ring, Ann. of Math. 78 (1963), 267-288

[34] U. Hirzebruch: Über Jordan-Algebren und kompakte Riemannsche symmetrische Räume vom Rang 1, Math. Z. 90 (1965), 339-354

[35] H. Hopf: Zum Clifford-Kleinschen Raumproblem, Math. Ann. 95 (1926), 313-339

[36] N. Jacobson: Structure of rings, American Mathematical Society Colloquium Publications, vol. 37, American Mathematical Society, Providence, R. I., revised ed., 1964

Drinfel'd [22] initiated the study of *set-theoretic solutions*, where the operator R is induced by a map $X \times X \rightarrow X \times X$ for some basis X of V . If the inverse of R is obtained by conjugating R with a twist $(x, y) \mapsto (y, x)$, then R is said to be of *untwisted non-degenerate* if the component maps $x \mapsto x_{\#}$ and $y \mapsto x_{\#}$

$$R(x, y) = (x_{\#}, x_{\#} y)$$

(5) given by a square-free non-degenerate unitary map $R: X \times X \rightarrow X \times X$ and constants $a_{xy} \in k^{\times}$. In 1994, Gateva-Ivanova introduced a special class of quantum binomial algebras and called them *binomial skew polynomial rings* [28]. The term "quantum binomial algebra" was attached to them by Laflamme [42] who verified that the algebras up to $|X| \leq 6$ satisfy the quantum Yang-Baxter equation. A *binomial skew polynomial ring* A is given by a finite set $X = \{x_1, \dots, x_n\}$ of generators and quadratic relations $x_j x_i = a_{ij} x_i x_j$ with $i < j < i' < j'$ for all pairs $i < j$ such that each pair (i', j') occurs on the right-hand side of a relation and the overlaps $x_k x_j x_i$ with $k > j > i$ do not give rise to new relations. In other words, A has a PBW-basis of ordered monomials $x_1^{n_1} \cdots x_n^{n_n}$ [9]. It is known that the quantum binomial algebras associated to solutions R of the quantum Yang-Baxter equation are (left and right) noetherian domains [28]. They are Koszul

we introduced a concept [52] closely related to that of a brace. Here is the point where braces arise. To prove Gateva-Ivanova's conjecture, Yang-Baxter equation comes from a quantum binomial algebra. Conversely, every square-free non-degenerate unitary solution R of the quantum Yang-Baxter equation. Gateva-Ivanova conjectured [30] that Bergh [32] proved that the operator R of any binomial skew polynomial ring satisfies the quantum Yang-Baxter equation. Gateva-Ivanova and van den

nomial algebra A satisfies the quantum Yang-Baxter equation if and only if A has finite global dimension and a PBW basis [31]. Gateva-Ivanova and van den Schelder [2] as well as Auslander-regular and Cohen-Macaulay [32]. It is now known that the operator R of a finitely generated quantum binomial algebra of polynomial growth, and they are regular in the sense of Artin and

left multiplications $L_x: X \rightarrow X$ with $L_x(y) := x \cdot y$ are bijective and

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)$$

holds for all $x, y, z \in X$. A cycle set X is *non-degenerate* if the square map $x \mapsto x \cdot x$ is bijective. If this map is the identity, we call X *square-free*.

By [52], Theorem 2, every finite cycle set is non-degenerate. The connection with the quantum Yang-Baxter equation (QYBE) rests upon the inverse $y \mapsto y^x$ of the left multiplication L_x :

Proposition 2.1 ([52]). *Every non-degenerate cycle set X gives rise to a non-degenerate unitary solution (5) of the QYBE with ${}^x y = x^y \cdot y$. Conversely, every non-degenerate unitary solution of the QYBE arises from a non-degenerate cycle set. Under this bijection, square-free cycle sets correspond to square-free solutions.*

In terms of cycle sets, Gateva-Ivanova's conjecture admits a simple reformulation.

Definition 4. A cycle set X is *decomposable* if there is a non-trivial partition $X = X_1 \sqcup X_2$ with $x \cdot x_i \in X_i$ for all $x \in X$ and $x_i \in X_i$.

The conjecture is then equivalent to the statement of the following

Theorem 2.2 ([52]). *Any square-free cycle set X with $1 < |X| < \infty$ is decomposable.*

Now braces can be viewed as particular cycle sets.

Definition 5. A cycle set A with an abelian group structure is called *linear* if it satisfied the equations

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad (6)$$

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c). \quad (7)$$

Here the equation of Definition 3 is contained in Eq. (6) by the symmetry of $a + b$. Note that Eqs. (6) and (7) can be viewed as recipes to reduce the sums in expressions like $(a_1 + \dots + a_n) \cdot (b_1 + \dots + b_m)$. The inverse $b \mapsto b^a$ of the left multiplication $b \mapsto a \cdot b$ coincides with the corresponding operation of a brace:

Proposition 2.3. *Every linear cycle set is a brace, and vice versa.*

Proof. Passing to the inverse operation, Eq. (6) turns into the first equation in (2), which is equivalent to (B1). As to Eq. (7), the substitution $b \mapsto b^a$ yields $(a + b^a) \cdot c = b \cdot (a \cdot c)$. By $c \mapsto (c^b)^a$, the equation turns into $(b^a + a) \cdot (c^b)^a = c$, that is, $(c^b)^a = c^{b^a+a}$. This is the second equation of (2), equivalent to (B2). The bijectivity of the left multiplication is just (B3). QED

Thus, every brace is a cycle set. Conversely, every cycle set gives rise to a brace, and this close relationship is deeply connected with the mechanism of the QYBE.

prime numbers 2, 3, 5, and 7. In order to make use of Lazard's correspondence [44], one has to choose $p \geq 11$. Lazard's correspondence refines the Malcev correspondence which relates torsion-free radicable nilpotent groups, that is, groups with unique k -th roots, to nilpotent Lie \mathbb{Q} -algebras. This simply works since exponentials have finitely many terms in the nilpotent case. The group operation is uniquely given by the Baker-Campbell-Hausdorff formula. Since p exceeds the nilpotency class, \mathbb{Q} can be replaced by the finite field \mathbb{F}_p . So Burde's example yields a p -group G of order p^{10} with nilpotency class 9. Suppose that G is the adjoint group of a brace A . The 1-cocycle $G \rightarrow A$ would then lead to a complete RSA structure of \mathfrak{g} via Lazard's correspondence. As \mathfrak{g} is 10-dimensional, this gives an 11-dimensional faithful representation of \mathfrak{g} . In particular, the RSA structure would yield a bijective 1-cocycle of \mathfrak{g} . For the adjoint representation, this can be ruled out for all p .

To remove any doubts that a finite p -group need not be IYB, all 10-dimensional representations have to be taken into account. At present, notwithstanding the special structure of \mathfrak{g} , we are not able to do this by hand.

References

- [1] H. Abels, G. Margulis, G. Soifer: The Auslander conjecture for dimension less than 7, [arXiv:1211.2525v4](#) [[math.GR](#)]
- [2] M. Artin, W. F. Schelter: Graded algebras of global dimension 3, *Adv. in Math.* 66 (1987), no. 2, 171-216
- [3] L. Auslander: An exposition of the structure of solvmanifolds, I, Algebraic theory, *Bull. Amer. Math. Soc.* 79 (1973), no. 2, 227-261
- [4] L. Auslander: The structure of complete locally affine manifolds, *Topology* 3 (1964), suppl. 1, 131-139
- [5] L. Auslander: Simply transitive groups of affine motions, *Amer. J. Math.* 99 (1977), no. 4, 809-826
- [6] L. Auslander, L. Markus: Holonomy of flat affinely connected manifolds. *Ann. of Math.* 62 (1955), 139-151
- [7] E.-A. Behrens: Ring theory, Translated from the German by Clive Reis, Pure and Applied Mathematics, Vol. 44, Academic Press, New York-London, 1972
- [8] Y. Benoist: Une nilvariété non affine, *J. Differential Geom.* 41 (1995), no. 1, 21-52
- [9] G. M. Bergman: The diamond lemma for ring theory, *Adv. in Math.* 29 (1978), no. 2, 178-218
- [10] N. Bourbaki: Algebra I, Chapters 1-3, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998
- [11] D. Burde: Affine structures on nilmanifolds, *Internat. J. Math.* 7 (1996), no. 5, 599-616
- [12] D. Burde: Left-symmetric algebras, or pre-Lie algebras in geometry and physics, *Cent. Eur. J. Math.* 4 (2006), no. 3, 323-357
- [13] D. Burde, F. Grunewald: Modules for certain Lie algebras of maximal class, *J. Pure Appl. Algebra* 99 (1995), no. 3, 239-254
- [14] A. Caranti, F. Dalla Volta, M. Sala: Abelian regular subgroups of the affine group and radical rings, *Publ. Math. Debrecen* 69 (2006), no. 3, 297-308

is given by a matrix $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$. For a positive integer m , an easy calculation shows that

$$1 + \gamma + \gamma^2 + \cdots + \gamma^{m-1} = \begin{pmatrix} 0 & m \\ m & 2 \end{pmatrix}.$$

Hence $1 + \gamma + \gamma^2 + \cdots + \gamma^{p-1} = 0$, a contradiction.

$$\square \square \square$$

Example 5. For $p = 2$, there is a unique brace A with cyclic adjoint group

and the Klein four-group as additive group. Assume that the adjoint group is generated by a . Then $b := a^2 = a \circ a \notin \{0, a\}$. Hence $A = \mathbb{F}_2 a \oplus \mathbb{F}_2 b$. Furthermore, $b^2 = b \circ b = 0$ and $a \circ b = 0$ and $a \circ a = a \circ a \circ a = a + b$. Hence $ab = ba = 0$, and thus A is a unique radical ring.

12 Nilpotent braces

Let \mathfrak{g} be a filiform \mathbb{K} -linear Lie algebra of dimension $n > 1$. Benoist [8] has

shown that the minimal dimension $\mu(\mathfrak{g})$ of a faithful \mathfrak{g} -module satisfies $\mu(\mathfrak{g}) \geq n$. He constructed a filiform Lie algebra \mathfrak{n} of dimension 11 with $\mu(\mathfrak{n}) > 12$. So there cannot be an RSA structure, as this would require a faithful representation of dimension 12 (see also [13]). In particular, this disproves Milnor's second conjecture.

Vergne [62] has shown that filiform Lie algebras of dimension ≥ 8 are de-

formations of the *standard graded filiform* Lie algebra $L(n) = \mathbb{K}e_0 \oplus \cdots \oplus \mathbb{K}e_n$ with non-zero brackets $[e_i, e_j] = e_{i+1}$ for $i \in \{1, \dots, n-1\}$. Burde [11] replaced Benoist's example by a family of 10-dimensional Lie algebras, given as deformation of $L(9)$. The simplest one[†] seems to be $L(9)$ with additional non-zero brackets

$$\begin{aligned} [e_1, e_2] &= e_4 + e_5 & [e_1, e_3] &= e_5 + e_6 & [e_1, e_4] &= 2e_6 + 3e_7 + 25e_8 \\ [e_1, e_5] &= 3e_7 + 5e_8 + 50e_9 & [e_1, e_6] &= 7e_8 + 5e_9 & [e_1, e_7] &= 14e_9 \\ [e_1, e_8] &= -e_9 & [e_2, e_3] &= -e_6 - 2e_7 - 25e_8 & [e_2, e_4] &= -e_7 - 2e_8 - 25e_9 \\ [e_2, e_5] &= -4e_8 & [e_2, e_6] &= -7e_9 & [e_2, e_7] &= e_9 \\ [e_3, e_4] &= 3e_8 - 2e_9 & [e_3, e_5] &= 3e_9 & [e_3, e_6] &= -e_9 \\ [e_4, e_5] &= e_9. \end{aligned}$$

As in the previous examples, the verification that every faithful module must be of dimension > 11 is based on computer calculations.

Postponing the task of finding an independent proof, let us sketch how such examples can be transformed into finite braces with a p -group as adjoint group. Note first that the structure constants of the above Lie algebra are integral, involving the

[†]We owe thanks to D. Burde who pointed out that a condition was missing in the example on our slides for the AGTA-conference (Porto Cesareo 2013) which was given by a monomial basis.

Theorem 2.4 ([52, 53]). *Via Eqs. (6) and (7), the operation \cdot of a non-degenerate cycle set X admits a unique extension to the free abelian group $\mathbb{Z}(X)$ such that $\mathbb{Z}(X)$ becomes a brace.*

The extension process is like a knitting procedure. The miracle is that it does not lead to a contradiction.

Definition 6. A group of *I-type* [61, 32] is a finitely generated free abelian group $\mathbb{Z}(X)$ endowed with a second group structure $(\mathbb{Z}(X), \circ)$ with the same neutral element 0 such that

$$\{x \circ a \mid x \in X\} = \{x + a \mid x \in X\}$$

for all $a \in \mathbb{Z}(X)$.

Thus if we regard $\mathbb{Z}(X)$ as a lattice-ordered group with positive cone $\mathbb{N}(X)$, the upper neighbours of any $a \in \mathbb{Z}(X)$ are permuted by multiplication with the generators. Groups of I-type were studied, e. g., by Jespers and Okniński [37]. For a finite cycle set X , the linear extension $\mathbb{Z}(X)$ is a group of I-type. In fact, $x \circ a = x^a + a$. So the permutation of the upper neighbours of a is just $x \mapsto x^a$. The converse was proved in [54, 56].

Proposition 2.5. *There is a one-to-one correspondence between finite cycle sets and groups of I-type.*

An ideal of a brace A is an additive subgroup I such that $a \in I$ and $b \in A$ implies that ab and ba belong to I . As in the case of pseudo-rings, the additive factor group A/I can be made into a brace with a well-defined multiplication by the products ax with $a \in A$ and $x \in I$ is an ideal. Therefore, we have a descending chain of ideals

$$A \supset A^2 \supset A^3 \supset \cdots$$

with $A^{n+1} := A(A^n)$. By contrast, $(A^2)A$ need not be an ideal. On the other hand, the socle

$$\mathrm{Soc}(A) := \{a \in A \mid Aa = 0\}$$

is an ideal of A . Note that $A^n = 0$ for some n implies that $\mathrm{Soc}(A) \neq 0$ whenever $A \neq 0$. For a finite cycle set X , the brace $A(X) := \mathbb{Z}(X)/\mathrm{Soc}(\mathbb{Z}(X))$ is finite, too, and there is a natural morphism $\sigma: X \rightarrow A(X)$. For $x, y \in X$, we have

$$\sigma(x) = \sigma(y) \iff L_x = L_y$$

which shows that $\sigma(x)$ can be identified with the left multiplication L_x . The image $\sigma(X) \subset A(X)$ is again a cycle set, the *retraction* of X . If σ is not injective, the cycle set X is called *retractable*.

So there is a sequence of retractions

$$X \twoheadrightarrow \sigma(X) \twoheadrightarrow \sigma^2(X) \twoheadrightarrow \sigma^3(X) \twoheadrightarrow \cdots$$

which stops at an irretractable cycle set $\sigma^n(X)$. If $\sigma^n(X)$ is trivial, the structure of X is completely resolved. The corresponding solution of the QYBE is then called a *multipermutation solution* [24].

Gateva-Ivanova's "strong conjecture" [29] asserts that every square-free non-degenerate unitary solution of the QYBE is a multipermutation solution. In terms of cycle sets, this can be stated as

Gateva-Ivanova's strong conjecture. Every square-free cycle set X with $1 < |X| < \infty$ is retractable.

Apart from its implications to the quantum Yang-Baxter equation, the truth of this statement would determine the structure of a big class of Artin-Schelter regular rings. The conjecture has been verified in many cases. For example, it is true for braces X or if $\mathbb{Z}^{(X)}$ is a radical ring.

Note that a brace A is retractable if and only if its socle is non-zero. So there is reason to hope that braces will help to decide this fundamental conjecture.

3 Braces in Differential Geometry

We have seen (Proposition 1.3) that braces can be viewed as affine torsors. Let us pursue this approach in the classical geometric context of flat manifolds. Let X be an n -dimensional connected real manifold with a *flat affine structure* [49], in the sense that X is covered by coordinate charts into the affine n -space \mathbb{A}^n such that the coordinate changes between overlapping charts are given by affine automorphisms. Fix a point in the universal covering \tilde{X} and choose an affine neighbourhood. Attach it to an open set of \mathbb{A}^n , and extend this identification to get an affine immersion $D: \tilde{X} \rightarrow \mathbb{A}^n$. This *developing map* D is unique up to affine automorphisms of \mathbb{A}^n . The affine manifold X is *complete* if D is bijective, or equivalently, if any geodesic line segment extends to a full geodesic (see [6]).

Any element g of the fundamental group $\pi_1(X)$ induces an affine automorphism $\alpha(g)$ of \mathbb{A}^n such that the diagram

$$\begin{array}{ccc} \tilde{X} & \xrightarrow{g} & \tilde{X} \\ \downarrow D & & \downarrow D \\ \mathbb{A}^n & \xrightarrow{\alpha(g)} & \mathbb{A}^n \end{array}$$

commutes. The image of the *holonomy representation* $\alpha: \pi_1(X) \rightarrow \text{Aff}(\mathbb{A}^n)$ is called the *holonomy group* of X . If X is complete, \tilde{X} can be identified with \mathbb{A}^n ,

If $\varphi_{\lambda\mu} \neq 0$, then $\varphi_{\mu\lambda} = 0$. At first glance, it looks extremely plausible that the structure constants of the RSA are just $\varphi_{\lambda\mu}(1)$.

Unfortunately, this is not the case! The orientation of the Dynkin diagram (24) is required in order to have $\varphi_{\lambda\mu}(1) \neq 0$ if and only if $e_\lambda e_\mu \neq 0$; however, this just fails for the product $e_{\alpha+\beta+\gamma+\delta} e_\beta$, that is, the downward leftmost entry of the table. Note that the Hall algebra ansatz cannot be corrected by passing to the LSA.

Ringel has shown that the structure constants $\varphi_{\lambda\mu}$ at $q = 1$ yield the universal enveloping algebra:

$$\mathcal{H}(A)_{q=1} = U(\mathfrak{g}^+)$$

which is associative. Indeed, any associative algebra is an RSA. However, such an RSA must be a radical ring, in contrast to the braces of type B-D.

11 Finite p -groups

For every p -group G , the lower central series

$$G = G_1 \supset G_2 \supset G_3 \supset \cdots$$

gives rise to a Lie ring $L(G) := \bigoplus G_i/G_{i+1}$ with Lie bracket

$$[xG_i, yG_j] := (x^{-1}y^{-1}xy)G_{i+j}.$$

One may wonder if the natural bijection $G \rightarrow L(G)$ would lead to a brace structure. If yes, this would imply that every finite p -group is an IYB-group.

Alternatively, we could try to find a complete RSA structure on $L(G)$. Or we let G act on the \mathbb{F}_p -space $L(G)$ and look for a triangle-shaped region in the matrices as done for the Sylow subgroup of a finite Chevalley group.

However, there are several obstructions: First, the group G cannot be recovered by its Lie ring. Second, even if G is abelian, G need not admit a bijective 1-cocycle onto an \mathbb{F}_p -vector space. In fact:

Proposition 11.1. *Let p be an odd prime. Then the additive group of any brace with adjoint group C_{p^2} is cyclic.*

Proof. Let \mathbb{F}_p^2 be a right C_{p^2} -module and $\pi: C_{p^2} \rightarrow \mathbb{F}_p^2$ a bijective 1-cocycle. If $C_{p^n} = \langle c \rangle$, then $\pi(c^{j+1}) = \pi(c^j)c + \pi(c)$. With $v := \pi(c^j)$, this shows that

$$v, v + v^c, v + v^c + v^{c^2}, v + v^c + v^{c^2} + v^{c^3}, \dots$$

runs through all of \mathbb{F}_p^2 . On the other hand, $(c-1)^{p^n} = c^{p^n} - 1 = 0$ implies that the automorphism $x \mapsto x^c$ is unipotent. So we can assume that this automorphism γ

This wonderful formula suggests that a product like

$$e_{\alpha} e_{\beta} = \varphi_{\alpha\beta}(1) e_{\alpha+\beta}$$

might give the desired RSA structure on \mathfrak{g}^+ . Let us check this for D_4 :

$$(24) \quad \begin{array}{c} \alpha \longrightarrow \beta \longrightarrow \delta \\ \uparrow \gamma \end{array}$$

The linear part of the Chevalley group matrices is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -e & -b & 0 & 0 & 0 & 0 & 0 & 0 \\ -h & -f & -c & 0 & 0 & 0 & 0 & 0 \\ -i & -g & -d & 0 & 0 & 0 & 0 & 0 \\ -k & -j & 0 & d & c & 0 & 0 & 0 \\ -l & 0 & j & g & f & b & 0 & 0 \\ 0 & l & k & i & h & e & a & 0 \end{pmatrix}$$

with $a, b, c, d, e, f, g, h, i, j, k, l \in K$ corresponding to the 12 positive roots (in this order): $\alpha, \beta, \gamma, \delta, \alpha+\beta, \beta+\gamma, \beta+\delta, \alpha+\beta+\gamma, \alpha+\beta+\delta, \beta+\gamma+\delta, \alpha+\beta+\gamma+\delta$.

Accordingly, the multiplication table of the RSA looks as follows:

	a	b	c	d	e	f	g	h	i	j	k	l
a												
b												
c												
d												
e												
f												
g												
h												
i												
j												
k												
l												

Now let us return to Eq. (23), Here $\varphi_{\lambda\mu} \neq 0$ if and only if there exists a short exact sequence

$$0 \rightarrow M_{\mu} \rightarrow M_{\lambda+\mu} \rightarrow M_{\lambda} \rightarrow 0.$$

and we have a free properly discontinuous action $\pi_1(X) \curvearrowright \text{Aff}(\mathbb{A}^n)$ on \mathbb{A}^n which identifies X with $\mathbb{A}^n/\pi_1(X)$.

There is a number of long-standing unsolved problems related to flat affine manifolds. Recall that a group is said to *virtually* solvable if it has a solvable subgroup of finite index. A similar terminology is used for other “virtual” properties.

Millnor’s first conjecture [49]: If X is complete, the fundamental group $\pi_1(X)$ is virtually solvable.

In his famous solution of Hilbert’s 18th problem, Bieberbach has proved that X is virtually abelian (i. e. crystallographic) if $\pi_1(X)$ consists of isometries. Nevertheless, Millnor’s 1977 conjecture was disproved by Margulis [45, 46]. By the Tits alternative, there are two possibilities: Either $\pi_1(X)$ is virtually polycyclic - or it contains a subgroup isomorphic to $\mathbb{Z} * \mathbb{Z}$. Margulis proved that the second case occurs in dimension 3.

Compact flat affine manifolds need not be complete. A simple example is **Zeno’s Paradox:** The 1-dimensional manifold $X = \mathbb{R}_{>0}/\{2^n \mid n \in \mathbb{Z}\}$ is not complete.

It is not clear whether such a paradox still occurs in the presence of a *parallel volume*. The latter means that the linear part of the holonomy group consists of maps with determinant 1.

Markus’ conjecture [49]: Every unimodular compact flat affine manifold is complete.

The original Markus conjecture states that compactness implies completeness in case of flat Lorentz manifolds. This was proved in 1989 by Carrière [15]. The general conjecture is still open. Another open problem is

Auslander’s 1964 conjecture [4]: If X is a compact complete flat affine manifold, then $\pi_1(X)$ is virtually solvable.

The proof of this in statement in [4] is incorrect. So the problem remains unsolved. For dimensions up to six, the conjecture was recently proved [1]. If X is compact and $\pi := \pi_1(X)$ virtually solvable, Fried and Goldman (see [27], Corollary 1.5) proved that there is a simply transitive subgroup $G \subset \text{Aff}(\mathbb{A}^n)$ such that $\pi \cap G$ has finite index in π and $G/(\pi \cap G)$ is compact. Since $\pi \cap G$ is finitely generated and linear, Selberg’s lemma implies that $\pi \cap G$ is virtually torsion-free. Thus, if Γ is a cofinite torsion-free subgroup of $\pi \cap G$, we obtain a finite covering $\mathbb{A}^n/\Gamma \twoheadrightarrow \mathbb{A}^n/\pi \cong X$. On the other hand, the simply transitive action of G on \mathbb{A}^n lifts to a right-invariant complete affine structure on G , such that the complete affine solvmanifold $\Gamma \backslash G$ is affinely equivalent to the covering space \mathbb{A}^n/Γ of X .

The Lie group G is called a *crystallographic hull* of Γ . By Proposition 1.3, G is an \mathbb{R} -brace. Thus, we obtain:

Proposition 3.1. *Modulo Auslander’s conjecture, any compact complete flat affine manifold gives rise to an \mathbb{R} -brace.*

Milnor [49] proved that every virtually polycyclic torsion-free group is the fundamental group of a complete flat affine manifold X . He asked whether X can be chosen to be compact. This led to his second conjecture which can be stated as

Milnor’s second conjecture: Every simply connected solvable Lie group is isomorphic to the adjoint group of an \mathbb{R} -brace.

The converse is due to Auslander [5]. More precisely, Milnor ([49], Theorem 3.2) proved the following

Theorem 3.2. *A connected Lie group G admits a free action by affine transformations on \mathbb{A}^n if and only if G is simply connected and solvable.*

Milnor’s second conjecture was believed to be true for a long while until it was finally disproved in 1995 by Benoist [8] who constructed a non-affine nilvariety by means of an 11-dimensional Lie algebra of nilpotency class 10.

A discrete version [18] of Milnor’s second conjecture is equivalent to the following statement: *Every finite solvable group is isomorphic to the adjoint group of a brace.*

We will return to this question in Section 5.

4 Braces and spaces

The classification of spaces with zero curvature (with a view toward understanding the possible structure of our physical space) has been a central part of the problem to classify Clifford-Klein “space forms” [40, 16]. Killing [40] constructed Euclidean space forms as homogenous spaces \mathbb{R}^n/Γ with a Bieberbach group Γ . Hermann Weyl [66] proved that all Euclidean space forms are of that type. More generally, *affine* space forms are given by cocompact *properly discontinuous* subgroups $\Gamma \subset \text{Aff}(\mathbb{A}^n)$, that is, $\{g \in \Gamma \mid gC \cap C \neq \emptyset\}$ is finite for compact subsets $C \subset \mathbb{A}^n$. These *affine crystallographic groups* Γ were classified in dimension 3 by Fried and Goldman [27].

Here the stabilizer Γ_x of any $x \in \mathbb{A}^n$ is finite. If Γ acts freely, the quotient \mathbb{A}^n/Γ is a compact complete affine manifold. By Section 3, the crystallographic hull G of Γ is the adjoint group of an \mathbb{R} -brace. The following theorem of Auslander ([5], Theorem III.1) relates any \mathbb{R} -brace A to one with a unipotent adjoint group. Consider the *algebraic hull* of A° , the smallest algebraic group G containing A° . The set of unipotent elements of G form a connected normal subgroup U , the *unipotent radical* of G , and $G = T \ltimes U$ with a maximal torus T .

Thus, in particular, every formal real Jordan algebra A is a Lie-theoretic “brace”. Let $I(A)$ denote the set of idempotents $e \in A$ for which the space $\{a \in A \mid ea = a\}$ is one-dimensional. For simple A , Ulrich Hirzebruch [34] has shown that a formal real Jordan algebra is completely characterized by the topological space $I(A)$ which is a two-fold homogenous closed Riemannian manifold. Hsien-Chung Wang classified these manifolds [65]: For odd dimension, $I(A)$ is a Clifford-Klein space form, while for even dimension, $I(A)$ is either an n -sphere, a real, complex or quaternionic projective space, or the Cayley projective plane of dimension 16.

For every \mathbb{R} -brace A , the corresponding bijective 1-cocycle $A^\circ \rightarrow \mathbb{R}^n$ induces a bijective 1-cocycle $\text{Lie}(A^\circ) \rightarrow \mathbb{R}^n$, which gives a right symmetric algebra structure on $\text{Lie}(A^\circ)$. The converse does not hold, unless A is *complete*, that is, the maps $x \mapsto ax + x$ are bijective for each $a \in A$. By [59], Theorem 1, A is complete if and only if the left multiplications $x \mapsto ax$ are nilpotent. So we have

Proposition 9.2. *\mathbb{R} -braces are equivalent to right symmetric algebras \mathfrak{g} such that the left multiplications L_a in \mathfrak{g} are nilpotent.*

10 Hall algebras

Let \mathfrak{g} be a simple Lie algebra with root vectors e_α , $\alpha \in \Phi^+$, such that $[e_\alpha, e_\beta] = N_{\alpha\beta}e_{\alpha+\beta}$ whenever $\alpha, \beta, \alpha + \beta \in \Phi^+$, and $N_{\alpha\beta} \in \mathbb{Z}$. The examples of Sections 7 and 8 suggest that there exists a right symmetric algebra structure on \mathfrak{g}^+ such that the positive root vectors form a monomial basis.

An obvious candidate for an RSA basis comes from the associated Hall algebra. The positive roots $\alpha \in \Phi^+$ can be associated to the indecomposable representations M_α of a hereditary algebra A over a field K such that A and \mathfrak{g} are of the same Dynkin type. Assume that $q := |K| < \infty$.

The *Hall algebra* $\mathcal{H}(A)$ has a basis \mathcal{B} consisting of the isomorphism classes $[M]$ of finite dimensional A -modules M . The structure constants $F_{LM}^N \in \mathbb{N}$ of $\mathcal{H}(A)$ count the number of submodules M' of N with $M' \cong M$ and $N/M' \cong L$. Ringel [50] proved that $\mathcal{H}(A)$ is isomorphic to the positive part $U_q^+(\mathfrak{g})$ of the Drinfeld-Jimbo quantum group $U_q(\mathfrak{g})$. For $\alpha, \beta, \alpha + \beta \in \Phi^+$, he found a finite list of polynomials [51] which occur as Hall polynomials $\varphi_{\alpha\beta} \in \mathbb{Z}[x]$ such that

$$F_{M_\alpha M_\beta}^{M_{\alpha+\beta}} = \varphi_{\alpha\beta}(q).$$

The structure constants $N_{\alpha\beta}$ of \mathfrak{g} are obtained by passing to $q = 1$:

$$N_{\alpha\beta} = \varphi_{\alpha\beta}(1) - \varphi_{\beta\alpha}(1). \quad (23)$$

theory of convex homogeneous cones. Right symmetric algebras and their left-hand version (LSA's) arise in very many areas of mathematics and physics (see, e. g., [12]). Let us mention just a few typical examples.

Gerstenhaber proved in his fundamental paper [33] that the Hochschild complex of an associative ring is a (graded) right symmetric algebra. The free RSA with one generator has the rooted trees as a basis. It was discovered 1857 by Cayley [17] in his analysis of differential operators. Chapoton and Livernet ([20], 3.1) identified this RSA with a Lie algebra considered by Connes and Kreimer [21] in connection with renormalization of quantum field theories. More generally, every class of graphs (e. g., Feynman graphs) yields an RSA.

Let P be a non-empty open convex cone in \mathbb{R}^n with a transitive action of its automorphism group $\text{Aut}(P) := \{\alpha \in GL_n(\mathbb{R}) \mid \alpha(P) = P\}$. By [64], Theorem 1.1, $G := \text{Aut}(P)$ decomposes into $G = G_x T$, where G_x is the stabilizer of some $x \in P$ and T is a maximal connected split solvable subgroup which acts simply transitively on P . The orbit map $g \mapsto xg$ is a diffeomorphism $T \xrightarrow{\sim} P$ which induces a linear isomorphism $\rho: \mathfrak{t} \xrightarrow{\sim} \mathbb{R}^n$ from the Lie algebra \mathfrak{t} of T onto \mathbb{R}^n . The binary operation

$$a \Delta b := a\rho^{-1}(b)$$

on \mathbb{R}^n makes \mathbb{R}^n into a right symmetric algebra (cf. [64], Chapter 2). Moreover, Vinberg [64] has characterized the RSA's which arise in this way. (To be sure, Vinberg [64] introduced *left* symmetric algebras, which is just a matter of taste!)

A homogeneous cone $P \subset \mathbb{R}^n$ is called *symmetric* if

holds for all $x \in \mathbb{R}^n$. By the famous Koehler-Vinberg theorem [41, 63], there is a one-to-one correspondence between symmetric cones P and *formal real jordan algebras*, that is, real jordan algebras for which $x^2 + y^2 = 0$ implies that $x = y = 0$. The cone associated to a formal real jordan algebra consists of the non-zero squares.

Right symmetric algebras are the Lie-theoretic analogue of braces:

Proposition 9.1. *Right symmetric algebra structures with underlying Lie algebra \mathfrak{g} are equivalent to 1-cocycles of \mathfrak{g} .*

Proof. Let A be a right module of \mathfrak{g} , and let $q: \mathfrak{g} \rightarrow A$ be a 1-cocycle, that is, $q[a, b] = q(a)b - q(b)a$ for all $a, b \in \mathfrak{g}$. Assume that q is bijective, and define a multiplication on \mathfrak{g} by

$$ab = q^{-1}(q(a)b).$$

A straightforward verification shows that Eq. (22) makes \mathfrak{g} into an RSA. Conversely, the right multiplication of an RSA \mathfrak{g} is a \mathfrak{g} -module structure, such that the identity map $\mathfrak{g} \rightarrow \mathfrak{g}$ is a 1-cocycle.

QED

Proposition 4.1. *Let A be an \mathbb{R} -brace, viewed as an affine torsor on \mathbb{A}^n . Let U be the unipotent radical of the algebraic hull (Zariski closure) of A° . Then U is a simply transitive subgroup of $\text{Aff}(\mathbb{A}^n)$.*

In other words, the action of U on \mathbb{A}^n gives another \mathbb{R} -brace with a unipotent adjoint group U . The group U is isomorphic to the *nil-shadow* of A° , defined in [3], III.2. Therefore, we call the corresponding brace the *nil-shadow* of A . Recall (Section 2) that a brace is retractable if and only if its socle is non-zero. For a brace A , the socle consists of the elements $a \in A$ with $Aa = 0$, that is, $b \circ a = b + a$ for all $b \in A$. Thus, if A is an \mathbb{R} -brace, viewed as an affine torsor, the socle consists of the translations. In the language of braces, a weak form of another conjecture of Auslander can be stated as

Auslander's second conjecture [5]: Every non-zero unipotent \mathbb{R} -brace A is contractable.

Auslander's original conjecture assumes that the adjoint group A° is nilpotent. By [58], Theorem 1, this implies that A° is unipotent. Furthermore, Auslander claims that there are non-trivial translations in the center of A° . Auslander [5] mentions Schuennemann's paper [58] where the conjecture is proved. Nine years later, Fried [25] gave a counterexample in dimension 4 which shows that Schuennemann's argument was false. For other counterexamples, see [48, 19].

The \mathbb{R} -brace with group operation

$$\begin{pmatrix} a \\ b \\ x \end{pmatrix} \circ \begin{pmatrix} c \\ y \\ z \end{pmatrix} = \begin{pmatrix} a + bz e^{x-yz} + cy e^{yz-x} + x \\ b e^{x-yz} + y \\ c e^{yz-x} + z \end{pmatrix}$$

has a trivial socle. Here the nil-shadow is a 2-dimensional abelian subbrace. **Fried's counterexample:** A unipotent \mathbb{R} -brace with trivial socle. Multiplication is given by

$$\begin{pmatrix} a \\ b \\ x \end{pmatrix} = \begin{pmatrix} d \\ c \\ y \\ z \end{pmatrix} \quad \left(\begin{array}{l} -bt + cz - ctv - dy + dzv - \frac{2}{3}d tv^2 \\ cv + \frac{1}{2}dv^2 \\ 0 \end{array} \right)$$

where $v := x + yt - \frac{1}{2}z^2$.

The adjoint group of this example has a Lie-algebra of maximal nilpotency class. Such Lie-algebras (and groups) are called *filiform* [62]. For an \mathbb{R} -brace A with filiform adjoint group, Medina and Khakimdjanov [48] have shown that $\text{Soc}(A) \neq 0$ if $\dim A$ is odd. For even dimension ≥ 4 , they were able to extend Fried's counterexample.

Flat spacetimes. In analogy to the Clifford-Kleinian problem of Euclidean space forms, Fried [26] classified compact complete 4-manifolds with zero curvature which are covered by the Minkowski space. The corresponding braces are two exceptional (non-algebraic) ones and a series of unipotent braces $U_{\beta,\varepsilon}$ where the right operation by $(xyz t)^T$ is given by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -\beta z + \frac{\beta \varepsilon t^2}{2} & 1 & 0 & 0 \\ -\varepsilon t & 0 & 1 & 0 \\ -\frac{\beta^2 z^2}{2} + \frac{\beta^2 \varepsilon z t^2}{2} - \frac{\beta^2 \varepsilon^2 t^4}{8} - \frac{\varepsilon^2 t^2}{2} & \beta z - \frac{\beta \varepsilon t^2}{2} & \varepsilon t & 1 \end{pmatrix}.$$

The parameters $\beta, \varepsilon \geq 0$ are unique up to rescaling $(\beta, \varepsilon) \mapsto (\lambda\beta, \lambda^2\varepsilon)$ with $\lambda > 0$. All these braces are retractable.

5 Braces versus radical rings

In view of a long-standing ring-theoretic tradition, notwithstanding the geometric examples of the preceding two sections (where braces arise as groups with an affine connection), braces may still be regarded as a kind of radical rings where something is missing. Indeed, the concept of brace is one-sided, and a two-sided brace is nothing else than a radical ring.

So it is time to point out that this perspective is *one-sided*, as it evaluates braces from the viewpoint of ring theory. A more appropriate comparison should take into account how far the two structures are invariant under natural operations. We will show that the category of braces is closed with respect to semidirect products, while this fails to be true in the case of radical rings. Of course, this failure could not be detected in the classical framework of ring theory where a semidirect product of radical rings does not exist!

Let M be an abelian group. With Jacobson's circle operation $f \circ g = fg + f + g$, the ring $R(M)$ of right endomorphisms is a monoid with neutral element 0.

Definition 7. A module M over a brace A is given by a monoid homomorphism $A^\circ \rightarrow R(M)$.

Explicitly, this means that there is a right operation $M \times A \rightarrow M$ which satisfies $x0 = 0$ and

$$(x + y)a = xa + ya \quad (8)$$

$$x(a \circ b) = (xa)b + xa + xb \quad (9)$$

for all $x, y \in M$ and $a, b \in A$.

find a canonical construction of the diagram (16) simultaneously for all Chevalley groups, including the exceptional ones. We shall return to this problem in Section 10. Using the brace structure in cases A-D, the matrices (17)-(19) could also be given in a form like (20), at the expense of increasing the dimension of the representation. The triangle-shaped area then turns into a straight line.

9 Right symmetric algebras

Let A be an \mathbb{R} -brace with adjoint group $G = A^\circ$, viewed as an affine torsor. The additive group $(A, +)$ is an \mathbb{R} -vector space \mathbb{R}^n , and the map $x \mapsto x \circ a$ yields a simply transitive action $\alpha: G \rightarrow \text{Aff}(A)$ on A as an affine space. The differential of α gives an affine representation $d\alpha: \mathfrak{g} \rightarrow \text{aff}(A)$ of the Lie algebra \mathfrak{g} which fits into a commutative diagram

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{d\alpha} & \text{aff}(A) \\ \downarrow \exp & & \downarrow \exp \\ G & \xrightarrow{\alpha} & \text{Aff}(A) \end{array}$$

The identification $\mathfrak{g} = A$ turns \mathfrak{g} into a right module over itself. This gives a bilinear map $\mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ with

$$\begin{aligned} [a, b] &= ab - ba \\ a[b, c] &= (ab)c - (ac)b \end{aligned}$$

for all $a, b, c \in \mathfrak{g}$. Hence

$$(ab)c - a(bc) = (ac)b - a(cb) \quad (21)$$

for all $a, b, c \in \mathfrak{g}$.

Definition 10. A (non-associative) algebra satisfying Eq. (21) is called a *right symmetric algebra*.

With $[a, b] := ab - ba$, Eq. (21) can be written as

$$[Rb, R_c] = R_{[b, c]},$$

another version of the Jacobi identity!

In fact, every right symmetric algebra (RSA) is a Lie algebra with bracket $[a, b] := ab - ba$. Therefore, we also speak of a Lie algebra with a *right symmetric structure*. The concept was introduced by Vinberg [64] in connection with his

$$\begin{pmatrix} 1 & e & ef-d & 2c & ce-b & a-bf+cef-cd & c^2+ae-bd \\ 0 & 1 & f & 2d & de-c & def-cf-d^2 & \\ 0 & 0 & 1 & 2e & e^2 & e^2f-de-c & b \\ 0 & 0 & 0 & 1 & e & ef-d & c \\ 0 & 0 & 0 & 0 & 1 & f & d \\ 0 & 0 & 0 & 0 & 0 & e & \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

where the parameters a, b, c, d, e, f are located in a stretched triangle-shaped part. As above, we obtain a brace A with $A^\circ = U$. Now the operation $x \mapsto x \circ a$ in A yields an affine matrix representation for U :

$$(20) \quad \begin{pmatrix} 1 & f & 2d & de-c & def-cf-d^2 & 0 & a \\ 0 & 1 & 2e & e^2 & e^2f-de-c & 0 & b \\ 0 & 0 & 1 & e & ef-d & 0 & c \\ 0 & 0 & 0 & 1 & f & 0 & d \\ 0 & 0 & 0 & 0 & e & 1 & e \\ 0 & 0 & 0 & 0 & 1 & 0 & f \end{pmatrix}$$

Here the matrices take a very simple form. The parameters a, b, c, d, e, f , indicating the root subgroups, appear in the last row. They correspond, respectively, to the roots

$$2\alpha + 3\beta, \alpha + 3\beta, \alpha + 2\beta, \alpha + \beta, \beta, \alpha,$$

where α denotes the long root. So we obtain

Theorem 8.1. *The positive part of a simple Lie algebra \mathfrak{g} of type A, B, C, D, G over a field K is a brace with adjoint group $X(\mathfrak{g}^+)$.*

With some patience, a similar construction should yield a brace with adjoint group the unipotent part of F_4 , the automorphism group of the exceptional Jordan algebra of 3×3 self-adjoint matrices over \mathbb{O} . For the remaining type E_6 , the representations given in [68] may be useful. Already for E_6 , the matrices are too large to be depicted.

On the other hand, the above example for G_2 shows that Wildberger's marvelous basis [67] is not optimal for our purpose. We leave it as a challenge to

Proposition 5.1. *Modules over a brace A are the same as right A° -modules.*

Proof. For an A -module, define a new operation $x \mapsto x^a$ by

$$x^a := xa + x.$$

Then $x^0 = x$, and (8) and (9) turn into

$$(x + y)^a = x^a + y^a$$

$$x^{(ab)} = (x^a)^b.$$

$$\square \square \square$$

In particular, any brace is a module over itself. By Proposition 5.1, every (right) module can be turned into a left module, and vice versa: $(^ax)^a = x$.

Definition 8. We say that a brace A acts on a brace B if there is a map $A \times B \rightarrow B$ which satisfies

$$\begin{aligned} \alpha(a + b) &= \alpha a + \alpha b \\ \alpha(ab) &= (\alpha a)(\alpha b) \\ (\alpha \circ \beta)a &= \alpha(\beta a) \end{aligned}$$

and $0a = a$ for all $\alpha, \beta \in A$ and $a, b \in B$.

In other words, the action of A on B is given by a group homomorphism

$$A \rightarrow \text{Aut}(B),$$

which shows that Definition 8 is quite natural. Less obvious is the following result (see [55], Corollary of Proposition 4) which defines a *semidirect product* for braces:

Theorem 5.2. *Let A be a brace which acts on a brace B . The operations*

$$(10) \quad (a, \alpha) + (b, \beta) = ((\alpha \cdot \beta)a + (\beta \cdot \alpha)b, \alpha + \beta)$$

$$(11) \quad (a, \alpha) \circ (b, \beta) = (a \circ \alpha b, \alpha \circ \beta)$$

with $\alpha, \beta \in A$ and $a, b \in B$ make the cartesian product $B \times A$ into a brace $A \ltimes B$.

Theorem 5.2 has no analogue in ring theory. Indeed, the following example shows that the semidirect product of radical rings need not be a radical ring.

Example 2. Let R be a discrete valuation domain with quotient field K and radical $\mathfrak{p} = R\pi$. For an integer $n \geq 2$, let Γ_n be a Morita-reduced hereditary R -order with n simple modules, and $J_n := \text{Rad } \Gamma_n$. For example,

$$\Gamma_4 = \begin{pmatrix} R & \mathfrak{p} & \mathfrak{p} & \mathfrak{p} \\ R & R & \mathfrak{p} & \mathfrak{p} \\ R & R & R & \mathfrak{p} \\ R & R & R & R \end{pmatrix} \quad J_4 = \begin{pmatrix} \mathfrak{p} & \mathfrak{p} & \mathfrak{p} & \mathfrak{p} \\ R & \mathfrak{p} & \mathfrak{p} & \mathfrak{p} \\ R & R & \mathfrak{p} & \mathfrak{p} \\ R & R & R & \mathfrak{p} \end{pmatrix}$$

Let e_{ij} denote the matrix units in $M_n(K)$, and let g be the canonical generator of J_n . For $n = 4$:

$$e_{21} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad g = \begin{pmatrix} 0 & 0 & 0 & \pi \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Then $gJ_ng^{-1} = J_n$. Therefore, conjugation by g is an automorphism σ of J_n , and $\langle \sigma \rangle \subset \text{Aut}(J_n)$ is a cyclic subgroup of order n . So the radical ring $\langle \sigma \rangle$ with trivial multiplication operates on the radical ring J_n , and thus $\langle \sigma \rangle \ltimes J_n$ is a brace. However, a direct calculation shows that left distributivity fails for this brace:

$$(e_{32}, 1)((-e_{21}, 1) + (0, \sigma)) \neq (e_{32}, 1)(-e_{21}, 1) + (e_{32}, 1)(0, \sigma).$$

Whence $\langle \sigma \rangle \ltimes J_n$ is not a radical ring.

Eq. (11) shows that every semidirect product $A \ltimes B$ of braces satisfies

$$(A \ltimes B)^\circ = A^\circ \ltimes B^\circ.$$

Now let us return to the question raised at the end of Section 3, concerning the solvable groups arising as adjoint group of a brace. In [18] they are called *involutive Yang-Baxter groups* (*IYB-groups* for short).

Corollary 1. *Let A be a brace, and let G be an IYB-group acting on A° by automorphisms of A . Then $G \ltimes A^\circ$ is an IYB-group.*

Corollary 2. *Every semidirect product $G \ltimes A$ of an IYB group G with an abelian group A is an IYB group.*

Proof. The abelian group A is a radical ring with trivial multiplication. Every group automorphism of A is thus a brace automorphism. QED

Type D_n : The even orthogonal group $\Omega_{2n}(K)$ of $(2n, 2n)$ -matrices A with $AJA^T = J$, where

$$J = \begin{pmatrix} O & & & & 1 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 1 & & & & O \end{pmatrix}.$$

For $n = 3$, the matrices in the unipotent part U of $\Omega_{2n}(K)$ are of the form

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -f & 1 & 0 & 0 & 0 & 0 \\ df-e & -d & 1 & 0 & 0 & 0 \\ bf-c & -b & 0 & 1 & 0 & 0 \\ bdf-be-cd-a & -bd & b & d & 1 & 0 \\ -af-ce & a & c & e & f & 1 \end{pmatrix} \quad (19)$$

with $a, b, c, d, e, f \in K$. Again, the parameters are located in a triangle-shaped part of A , and there is a canonical brace \mathfrak{g}^+ with adjoint group U .

Note that for all cases A-D, the unipotent group U is a subgroup of the Chevalley group G_a of adjoint type as well as a subgroup of its simply connected covering $\sigma: G_u \rightarrow G_a$: The kernel of σ is just the center of G_u .

The above matrix representations exhibit the root subgroups of U . These are bijectively associated to the entries of the triangle-shaped region in the matrices A .

Remark. In contrast to case A, the braces of type B,C,D are not radical rings. To verify this for B_2 , consider $x := e_{54} - e_{21}$, $y := e_{43} - 2e_{32} - e_{42} \in \mathfrak{g}^+$. Then

$$x(y + y) \neq xy + xy.$$

8 The exceptional group G_2

The 14-dimensional exceptional simple Lie group G_2 has a faithful matrix representation of dimension 7. As a real group, G_2 is the automorphism group of the division algebra \mathbb{O} of octonions. The action of G_2 on the imaginary part $\text{Im}(\mathbb{O})$ of \mathbb{O} yields an embedding into the orthogonal group $O(\text{Im}(\mathbb{O}))$:

$$G_2 \hookrightarrow O_7(\mathbb{R}).$$

Compact Riemannian manifolds with G_2 -holonomy were constructed in 1994 by D. Joyce. They carry the hidden dimensions in 11-dimensional supergravity theory.

According to the root system of G_2 , the unipotent part U of G_2 is of dimension 6. Using Wildberger's basis [67] for \mathfrak{g}_2 , the matrices in U can be put into the form

Precisely, the *simply connected* group $\Omega_{2n+1}(K)$ is the commutator group of the orthogonal group $O_{2n+1}(K)$ with respect to J , and $P\Omega_{2n+1}(K)$ is the Chevalley group of adjoint type.

For $n = 2$, the unipotent part U consists of the matrices

$$A = \begin{pmatrix} 1 & & & & & \\ & 0 & & & & \\ & & -d & & & \\ & & 2bd-2c & & & \\ & & -b^2 & & & \\ & & & -ad-c^2 & & \\ & & & & 1 & \\ & & & & & \triangle \\ & & & & & c & d \\ & & & & & & 1 \end{pmatrix} \quad (17)$$

with $a, b, c, d \in K$. The subspace

$$M := Ke_{21} \oplus Ke_{31} \oplus Ke_{32} \oplus Ke_{41} \oplus Ke_{42} \oplus Ke_{51}$$

of $\mathfrak{u}_5(K)$ is a right $U_5(K)$ -submodule, and the epimorphism

$$p: \mathfrak{u}_5(K)/M \cong \mathfrak{g}^+$$

provides a bijective 1-cocycle $\gamma = p\delta|_U: U \rightarrow \mathfrak{g}^+$ which makes \mathfrak{g}^+ into a brace with adjoint group U .

Type C_n : The symplectic group $Sp_{2n}(K)$. With

$$J = \begin{pmatrix} & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \\ & & & & & & & & \end{pmatrix},$$

this group consists of the $(2n, 2n)$ -matrices A which satisfy $AJA^T = J$. For $n = 3$, the unipotent part U consists of the matrices

$$A = \begin{pmatrix} 1 & & & & & & & & \\ & -i & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & & & \\ & & & & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & -g & & \\ & & & & & & & 1 & \\ & & & & & & & & 1 \\ & & & & & & & & & \triangle \\ & & & & & & & & & c & f & h \\ & & & & & & & & & & & 1 \end{pmatrix} \quad (18)$$

with $a, b, c, d, e, f, g, h, i \in K$. As in case B, the parameters can be found in a triangle-shaped part of the matrix A . So we can apply exactly the same method to obtain a canonical brace structure on the nilpotent Lie algebra \mathfrak{g}^+ with adjoint group U .

6 Amalgamation of cycle sets

Example 2 shows that semidirect products of radical rings naturally lead to braces. Let us now have a closer look upon Eq. (10) which defines addition in a semidirect product $A \ltimes B$ of braces. Subtraction can be inferred from Eq. (10) as

$$(a, \alpha) - (b, \beta) = ((\alpha \cdot -\beta)a - (\alpha \cdot -\beta)\alpha(\beta \cdot -\beta)b, \alpha - \beta).$$

Recall that $b \mapsto a \cdot b$ is the inverse map of $b \mapsto b^a$. Using the formula $a \circ b = a^b + b$ which holds in any brace, Eq. (10) transforms into

$$(a, \alpha)^{(b, \beta)} = ((\alpha \cdot \beta')(a^{ab}), \alpha^{\beta'}), \quad (12)$$

where β' is the inverse of β in the adjoint group. Now Eq. (12) can be rewritten as

$$(a, \alpha) \cdot (b, \beta) = ((\alpha \cdot \beta)a \cdot (\beta \cdot \alpha)b, \alpha \cdot \beta), \quad (13)$$

an expression of Eq. (10) in terms of the cycle set structure! This leads to the following

Definition 9. We say that a cycle set X acts on a cycle set Y if there is a map $X \rightarrow S(Y)$ into the symmetric group $S(Y)$ which satisfies

$$\alpha(x \cdot y) = \alpha x \cdot \alpha y \quad (14)$$

$$(\alpha \cdot \beta)\alpha x = (\beta \cdot \alpha)\beta x \quad (15)$$

for $\alpha, \beta \in X$ and $x, y \in Y$.

While the first equation is obvious, the second one becomes clear in case that X is a brace: Then $(\alpha \cdot \beta) \circ \alpha = (\beta \cdot \alpha) \circ \beta = \alpha + \beta$ holds for all $\alpha, \beta \in X$. Generalizing Theorem 5.2, we have

Theorem 6.1 ([55]). *If a cycle set X acts on a cycle set Y , Eq. (13) makes $Y \times X$ into a cycle set $X \ltimes Y$.*

Firstly, this theorem shows that every semidirect product of braces is a semidirect product of the underlying cycle sets. Secondly, in combination with Proposition 2.1, Theorem 6.1 can be used to construct non-degenerate unitary set-theoretic solutions of the quantum Yang-Baxter equation by amalgamation of given solutions.

Example 3. Let V be the Klein Four group, the additive group of $\mathbb{F}_2 \oplus \mathbb{F}_2$. Then the cyclic group $C_3 = \langle \sigma \rangle$ acts on V by permuting the three non-zero vectors. The semidirect product $C_3 \ltimes V$ is the alternating group A_4 . An easy calculation shows that $(a, \sigma) \in C_3 \ltimes V$ has order 6 if $a \neq 0$. So we get a brace A with adjoint group A_4 and additive group $C_6 \times C_2$.

Example 4. Every brace A acts on itself. If it acts by brace automorphisms, there is a *double* $A \ltimes A$ which is again a brace. The existence of a double is determined by the following criterion.

Proposition 6.2. *A brace A admits a double $A \ltimes A$ if and only if $A^3 = 0$.*

For $a \in A$, let a' denote the inverse of a in A° . We need the following

Lemma. *Every ideal of a brace A is a normal subgroup of the adjoint group A° .*

Proof. Let I be an ideal of A . For $a \in I$ and $b \in A$, we have $b' \circ a \circ b = (b'a + b' + a) \circ b = (b'a + b' + a)b + (b'a + b' + a) + b = (b'a + a)b + (b'a + a) \in I$. QED

Proof of Proposition 6.2. The brace A acts on itself by automorphisms if and only if $(a \circ b)^c = a^c \circ b^c$, that is, $(a^b + b)^c = (a^c)^{b^c} + b^c$ for all $a, b, c \in A$. This is equivalent to $(a^b)^c = (a^c)^{b^c}$ or, by Eqs. (2), $a^{b \circ c} = a^{c \circ b^c}$. Now this equation can be written as $a = a^{c \circ b^c \circ c' \circ b'}$, which means that $c \circ b^c \circ c' \circ b' \in \text{Soc}(A)$ for all $b, c \in A$. By the lemma, this condition can be replaced by $b^c \circ c' \circ b' \circ c \in \text{Soc}(A)$. Now $b^c \circ c' \circ b' = ((b^c)^{c'} + c') \circ b' = (c' + b) \circ b' = ((c')^{b'} \circ b) \circ b' = (c')^{b'}$. So the condition turns into $(c')^{b'} \circ c \in \text{Soc}(A)$. Since $(c')^c + c = c' \circ c = 0$, the substitution $b' = c \circ d \circ c'$ gives $(c')^{b'} \circ c = (-c)^{d \circ c'} \circ c = (-c)^{d \circ c' \circ c} + c = (-c)^d + c = (-c)d - c + c = (-c)d$. So the condition states that $A^2 \subset \text{Soc}(A)$, that is, $A^3 = 0$. QED

7 Chevalley groups

The adjoint group of a finite dimensional \mathbb{R} -brace is solvable. So there is no way to make a simple Lie group into a brace. On the other hand, Proposition 4.1 shows that every \mathbb{R} -brace A gives rise to a unipotent \mathbb{R} -brace where the adjoint group is replaced by the nil-shadow of A . In this section, we will show that the unipotent part of a Chevalley group of type A-D has a natural structure of a brace.

Remark. For a finite Chevalley group G over a prime field \mathbb{F}_p , it may happen that G itself is a brace: In Example 3, we proved that $PSL_2(3) = A_4$ is the adjoint group of a brace with additive group $C_6 \times C_2$. Of course, a finite non- p -group G cannot be the adjoint group of an \mathbb{F}_p -brace.

Let $\mathfrak{g} = \mathfrak{g}^+ \oplus \mathfrak{h} \oplus \mathfrak{g}^-$ be a simple Lie algebra over a field K . The corresponding Chevalley group of *adjoint type* is the subgroup of $\text{Aut}(\mathfrak{g})$ generated by the root subgroups $X_\alpha := \{x_\alpha(t) \mid t \in K\}$, where $x_\alpha(t) := \exp(t \text{ad } e_\alpha)$ for any root α with root vector $e_\alpha \in \mathfrak{g}$. Consider the unipotent subgroup

$$X(\mathfrak{g}^+) := \langle x_\alpha(t) \mid \alpha \in \Phi^+ \rangle$$

generated by the X_α with α positive. The Chevalley groups of type A-D can be represented as classical groups. Using their matrix representation, we have

Proposition 7.1. *For every simple Lie algebra \mathfrak{g} of type A-D, \mathfrak{g}^+ is a brace with adjoint group $X(\mathfrak{g}^+)$.*

Type A_n . The Lie algebra $\mathfrak{sl}_{n+1}(K)$ corresponds to the matrix group $SL_{n+1}(K)$ with unipotent part $X(\mathfrak{sl}_{n+1}(K)^+) = U_{n+1}(K)$, the group of unipotent lower triangular matrices of size $n+1$. The Lie algebra $\mathfrak{u}_{n+1}(K)$ of $U_{n+1}(K)$ coincides with the radical of the lower triangular matrix ring. Hence $\mathfrak{u}_{n+1}(K)$ is a K -brace with adjoint group $U_{n+1}(K)$. The corresponding bijective 1-cocycle is given by

$$\delta: U_{n+1}(K) \rightarrow \mathfrak{u}_{n+1}(K)$$

with $\delta(g) := g - 1$. In particular, there are braces of type A for finite fields K of characteristic $p > 0$. Here $U_{n+1}(K)$ is a Sylow p -subgroup of $SL_{n+1}(K)$.

For the unipotent groups U of type B-D, the affine structure is given by a bijective 1-cocycle $\gamma: U \rightarrow A$ induced by δ via a commutative diagram

$$\begin{array}{ccc} U & \hookrightarrow & U_m(K) \\ \downarrow \gamma & & \downarrow \delta \\ A & \xleftarrow{p} & \mathfrak{u}_m(K) \end{array} \quad (16)$$

with a $U_m(K)$ -linear epimorphism p . In any case, $\gamma = p\delta|_U$ is a 1-cocycle. Thus, to obtain γ , it is enough to find a factor module A of $\mathfrak{u}_m(K)$ with γ bijective. We will show that this can be done in a natural way.

Type B_n : The odd orthogonal group $\Omega_{2n+1}(K)$ consisting of the $(2n+1, 2n+1)$ -matrices A with $AJA^T = J$, where

$$J = \begin{pmatrix} 0 & & & & 1 \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ 1 & & & & 0 \end{pmatrix}.$$