RADICAL RING

In mathematics, a radical ring R is a ring without unity which is equal to its **Jacobson radical** (see **Ring (mathematics)**). Finite radical rings yield set-theoretic solutions of the **Yang-Baxter equation**, and are examples of skew braces. They also yield examples of Hopf-Galois structures on Galois extensions of fields. [1]

Contents

Definitions

Radical ring. A **radical ring** R is with the additional property that R is equal to its Jacobson radical $J(R)$.

A ring R without unity, sometimes called a **rng**, has two operations, $+$ (addition) and $\cdot$ (multiplication), where $a \cdot b$ is typically written ab, and $a \cdot a \cdot \ldots \cdot a$ (n factors) is denoted a^n. With those operations, R satisfies all of the properties of a ring (associativity of multiplication, left and right distributivity of multiplication over addition, etc.) except that there is no multiplicative identity element.

A **radical ring** R is a ring without unity with the additional property that the ring R is equal to its Jacobson radical $J(R)$ (See **Jacobson radical**. More explicitly, given any ring R, define the **circle operation** $\circ$ on R by $a \circ b = a + b + a \cdot b$. It is easy to check that the operation $\circ$ is associative, and $a \circ 0 = 0 \circ a = a$, so $(R, \circ)$, the set R with the circle operation $\circ$, is a monoid $(R, \circ)$ with identity element

Date: February 8, 2022.

equal to the additive identity element 0 of the ring R. Call an element a of R **right quasi-regular** if there exists an element $\overline{a}$ of R so that $a+\overline{a}+a\cdot\overline{a}=0$: that means that a has a right inverse under the circle operation.

Then the ring R is a radical ring if and only if $(R,\circ)$ is a group: that is, every element of R is both right quasi-regular and left quasi-regular. The group $(R,\circ)$ is called the **circle group** or **adjoint group** of R.

Nilpotent ring. A **nilpotent ring of index** n (some positive integer) is a ring without unity in which the product $a_1\cdot a_2\cdot\ldots\cdot a_n=0$ for all elements $a_1,\ldots,a_n$ of R. A nilpotent ring of index n is a radical ring: given a in R, the element

$$\overline{a}=-a+a^2-a^3+a^4+\ldots$$

is a finite sum because $a^n=0$, and is easily seen to be the left and right inverse of a under the circle operation.

Conversely, if R is a finite radical ring, then R is Artinian, that is, satisfies the descending chain condition on left ideals (any descending chain of left ideals must have finite length), hence R is a nilpotent ring, by a theorem of Hopkins [see [Her61]].

Circle group

. An open question is to understand which finite groups can be the circle group of a finite radical ring.

It is known (see [AW73]) that if the radical ring R is nilpotent of index n, then the circle group G of R is a nilpotent group of class at most $n-1$. For setting R^k to be the subring generated by all products of k elements of R, then in the chain of subring

$$R\supset R^2\supset R^3\supset\ldots\supset R^{n-1}\supset R^n=0,$$

each subring R^j is a normal subgroup of the group $(R,\circ)$, and the commutator of any element of R^j is in R^{j+1}. Ault and Watters [AW73] prove a partial converse: if G is a finite nilpotent group of class 2, that is, if $G\supset Z(G)\supset(1)$ with $Z(G)$ the center of G and $G/Z(G)$ is abelian, then G is the circle group of a nilpotent ring of class 3. See also [Kru70].

Some counting results

Radical algebras and rings with unity. A radical algebra R over a field K is a K-vector space which is a radical ring–that is, a K-algebra R without unity for which $R=J(R)$. For R finite dimensional over K, the dimension of R as a K-vector space is called the **rank** of R. Then the ring with unity $R' = K \oplus R = s + a | s \in K, a \in R$ is a ring with multiplication

$$(s + a)(t + b) = st + sb + ta + tb.$$

and multiplicative identity $= 1 = 1 + 0$, the multiplicative identity element of K. For R commutative, then R' is a commutative local ring with unique maximal ideal R, since $R = J(R) = J(R')$. In that setting, there is an isomorphism from $(R, \circ)$ to $(R', \cdot)$ induced by $a \to 1 + a$, for

$$a \circ b = a + b + ab \mapsto 1 + a + b + ab = (1 + a)(1 + b).$$

Counting isomorphism types of commutative nilpotent algebras. In [Po 08b], Poonen determines all 52 of the commutative local algebras of rank ≤ 6 (up to isomorphism as K-algebras) over an algebraically closed field K; they all have the form $A = K \oplus R$ where R is a commutative radical algebra of rank one less than the rank of A. In particular, over an algebraically closed field F of characteristic p, the number of isomorphism types of commutative nilpotent algebras of rank $n \leq 5$ is independent of p. (Nearly all of the algebras can be defined over any field, not just algebraically closed fields, hence yield distinct examples of nilpotent algebras of index ≤ 5 over any field.)

For K the field of p elements, the number of commutative nilpotent K-algebras A of rank n a over K satisfying $A^3 = 0$ is a fixed number independent of p for $n < 5$, but examples in [ST68] show that the number of isomorphism types of commutative nilpotent K-algebras of rank 6 is at least $(p - 5)/6$, resp. $(p - 1)/6$ if p is congruent to 5, resp. 1 modulo 6. So the number of isomorphism types for rank ≥ 6 goes to infinity with p. Whether this is also true for algebras of rank 5 is apparently unknown (c.f. [Ch15]).

Number of rank n commutative nilpotent $\mathbb{F}_p$-algebras for large n. Kruse and Price [KP70] determined that the number of isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras A of rank n over $\mathbb{F}_p$ and index 3, that is, with $A^3 = 0$, is $p^{\frac{2}{27}n^3 - \frac{4}{9}n^2 + O(n)}$ as $n \to \infty$. For $p > 3$, the circle group of any $\mathbb{F}_p$-algebra A with $A^3 = 0$ is an elementary abelian p-group, a consequence of a lemma of Caranti [2].

Poonen [Po08b] determined that for large m the number of rank m commutative local $\mathbb{F}_p$-algebras is $p^{\frac{2}{27}m^3 + O(m^{8/3})}$. Since local $\mathbb{F}_p$-algebras of rank m coincide with nilpotent $\mathbb{F}_p$-algebras of rank $m - 1$, this gives an asymptotic estimate of the number of commutative nilpotent $\mathbb{F}_p$-algebras of rank n, independent of index.

Number of nilpotent K-algebras of dimension ≤ 4. In [DeG18], DeGraaf determined all isomorphism types of nilpotent associative (but not necessarily commutative) K-algebras of dimension ≤ 4 over any field K: if K is a finite field with q elements, then there are $5q + 20$ isomorphism types for q odd and $5q + 17$ for q even.

Radical rings and skew braces

A set B with two operations, $*$ and $\circ$, is a **left skew brace** if $(B, *)$ is a group (where the inverse of a is called a^{-1}), $(B, \circ)$ is a group (where the inverse of a is called $\overline{a}$), and the single defining relation relating the two operations is: for all a, b, c in B,

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c).$$

If $(B, *)$ is an abelian group, then B is called a brace. In that setting $(B, *)$ is usually called the "additive group" and the operation $*$ is usually replaced by $+$; in that case the defining relation is

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

Given a radical algebra $A = (A, +, \cdot)$, the circle operation $\circ$ on A defined by

$$a \circ b = a + b + a \cdot b$$

makes $(A, \circ)$ into a group, and then $(A, +, \circ)$ is then a brace: for

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

while

$$(a \circ b) - a + (a \circ c) = a + b + ab - a + a + c + ac.$$

and the defining relation for a brace holds. (see [GV17], [SV18]).

Radical algebras and the set-theoretic Yang-Baxter equation

The question of finding set-theoretic solutions of the Yang-Baxter equation was first raised by V. G. Drinfel'd in 1990 [Dr92]. That question has motivated considerable work in algebra since that time.

Any radical K-algebra A yields a set-theoretical solution of the Yang-Baxter equation:

Given A, define $\lambda_a : A \to A$ by $\lambda_a(b) = a^{-1}(a \circ b)$. Then $a \circ b = a\lambda_a b$. We let $R : A \times A \to A \times A$ by

$$R(a, b) = (\sigma_a(b), \tau_b(a) = (\lambda_a(b), \overline{\lambda_a(b)} \circ a \circ b$$

where $\sigma_a(b) = a^{-1}(a \circ b)$ and $\tau_b(a) = \overline{\lambda_a(b)} \circ a \circ b$. The claim ([GV], Theorem 3.1) is that if A is a skew left brace, then for all x, y, z in A,

$$(R \times id)(id \times R)(R \times id)(x, y, z) = (id \times R)(R \times id)(id \times R)(x, y, z).$$

Thus,

$$\begin{aligned}&\sigma_{\sigma_x(y)}(\sigma_{\tau_y(x)}(z)), \tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y)), \tau_z(\tau_y(x)))\\ &= (\sigma_x(\sigma_y(z)), \sigma_{\tau_{\sigma_y(z)}(x))}(\tau_z(y)), \tau_{\tau_z(y)}(\tau_{\sigma_y(z)}(x)).\end{aligned}$$

So there are three equalities to show:

$$\sigma_{\sigma_x(y)}(\sigma_{\tau_y(x)}(z)) = \sigma_x(\sigma_y(z)),$$

$$\tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y)) = \sigma_{\tau_{\sigma_y(z)}(x)}(\tau_z(y))$$

and

$$\tau_z(\tau_y(x))) = \tau_{\tau_z(y)}(\tau_{\sigma_y(z)}(x)).$$

The fact that any radical algebra yields a set-theoretic solution to the YBE motivated the concept of left brace by W. Rump [Ru06], and subsequently the concept of skew left brace ([GV17]), as generalizations of a radical algebra: every skew brace yields a solution to the YBE and every solution to the set-theoretic YBE corresponds to a skew brace. (see, e. g [Ven19])

For a radical algebra A, $\sigma_x(y) = y + xy$ and $\tau_y(x) = \frac{x}{1+y+xy}$. Note that by embedding A into $A' = K \oplus A$ by $a \to 1 + a$, we can identify A as the set of elements $1 + a$ in A', and they are all invertible in A'. For if $\overline{a}$ is the inverse of A in the circle group $(A, \circ)$, then in A', $1 + a$ for a in R has an inverse, $1 + \overline{a}$. where $\overline{a}$ is the inverse of a in the circle group $(R, \circ)$:

$$0 = a \circ a' = a + a' + aa'$$

iff $1 = (1 + a)(1 + \overline{a})$. Thus $\tau_y(x)$ makes sense in A'.

Thus for a radical algebra A (or $A' = K \oplus A$), the three equations that must hold for the function R to yield a set-theoretic solution of the YBE are as follows: The left equation (L) is:

$$\sigma_{\sigma_x(y)}(\sigma_{\tau_y(x)}(z)) = \sigma_x(\sigma_y(z)) :$$

both sides of equation (L) equal

$$(1 + x)(1 + y)z.$$

The middle equation (C) is

$$\tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y)) = \sigma_{\tau_{\sigma_y(z)}(x)}(\tau_z(y)) :$$

both sides of equation (C) equal

$$\frac{(y(1+x)}{1+z(1+x)(1+y)}.$$

The right equation is (R):

$$\tau_z(\tau_y(x))) = \tau_{\tau_z(y)}(\tau_{\sigma_y(z)}(x)) :$$

both sides of equation (R) equal

$$\frac{x}{(1+z)(1+y+yx)+xz}.$$

Thus a radical algebra yields a solution of the Yang-Baxter equation.

See also

Jacobson radical, Yang-Baxter equation; for connections to Hopf-Galois theory and local algebraic number theory, see [CGKKKTU21]; for brace theory, see [GV17] and [SV18] and the references therein.

Notes

[1]. For the connection between radical rings and Hopf-Galois extensions, see, for example, [Ch15] or [CGKKKTU21] and the references therein.

[2]. Caranti's Lemma says that if A is a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n and index $\leq e$ (that is, $A^e = 0$) where $e < p$, then the circle group $(A, \circ)$ is isomorphic to the additive group $(A, +)$.

References

[Ch15] Childs, L. N., On abelian Hopf Galois structures and finite commutative nilpotent rings, New York J. Math. 21 (2015), 205–229.

[CGKKKTU21] Childs, L. N., Greither, C., Keating, K. P., Koch, A., Kohl, T., Truman, P. J., Underwood, R.G., Hopf Algebras and Galois Module Theory, Amer. Math. Soc. Math. Surveys and Monographs, vol.260, 2021.

[DeG18] DeGraaf, W., Classification of nilpotent associative algebras of small dimension, Int. J. Algebra Com. 28 (2018), 133–161.

[Dr92] Drinfel'd, V., On some unsolved problems in quantum group theory, Lecture Notes in Mathematics 1510 (1992), 1–8.

[FCC12] Featherstonhaugh, S. C., Caranti, A., Childs, L. N., Abelian Hopf Galois structures on prime-power Galois field extensions, Trans. Amer. Math. Soc. 364 (2012), 3675–3684.

[GV17] Guarnieri, L., Ventramin, L., Skew braces and the Yang-Baxter equation, Math. Comp. 86 (2017), 2519–2534.

[Her61] Herstein, I. N., Theory of Rings, University of Chicago Mathematics Lecture Notes, Spring, 1961

[KP70] Kruse, R. L., Price, D. T., Enumerating finite rings, J. London Math. Soc. (2) 2 (1970), 149–159.

[Kr70] Kruse, R. L., On the circle group of a nilpotent ring, American Math. Monthly 77 (1970), 168–170.

[Po08b] Poonen, B., Isomorphism types of commutative algebras of finite rank over an algebraically closed field, in Computational Algebraic Geometry, Contemp. Math. 463, Amer. Math. Soc., 2008, 817–836.

[Po08a] Poonen, B., The moduli space of commutative algebras of finite rank, J. European Math. Soc. 10 (2008), 817–836.

[Ru07] Rump, W., Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), 153–170.

[ST68] Suprunenko, D. A., Tyskevic, R. I., Commutative Matrices, Academic Press, New York, NY, 1968.

[SV18] Smoktunowicz, A., Vendramin, L., On skew braces (with an appendix by N. Byott and L. Vendramin), J. Combinatorial Algebra 2 (2018), 47–86.

[Ven19], Vendramin, L., Problems on skew braces, Advances in Group Theory and Applications 7 (2019), 15–37.