Математички Билтен
25 (LI)
2001 (5–12)
Скопје, Македонија

ISSN 0351–336X

GROUPOID POWERS

Ǵorǵi Čupona *, Naum Celakoski **, Snežana Ilić ***

Abstract

The following statement is the main result of the paper.

If $\mathcal{V}$ is the variety of groupoids (commutative groupoids), or $\mathcal{V}$ is the variety of n-idempotent groupoids (commutative n-idempotent groupoids), i.e. groupoids (commutative groupoids) with an axiom $x^{n+1} = x$, $n \geq 2$, then the monoid of powers is free with a countable infinite basis.

0. Preliminaries

A pair $\mathbf{G} = (G, \cdot)$, where G is a nonempty set, and $\cdot : (x, y) \mapsto xy$ a mapping from G^2 into G, is called a *groupoid*. A groupoid $\boldsymbol{G} = (G, \cdot)$ is said to be *injective* iff

$$(\forall x, y, u, v \in G)\big(xy = uv \Rightarrow (x, y) = (u, v)\big). \tag{0.1}$$

An element $a \in G$ is *prime* in $\boldsymbol{G}$ [1] iff

$$(\forall x, y \in G)\ a \neq xy. \tag{0.2}$$

---

[1] The notions as subgroupoid, semigroup, monoid, generating set, homomorphism, variety of groupoids, . . . have usual meanings.

We note that by a "free groupoid" we mean "free groupoid in the variety of groupoids" (i.e. an *"absolutely free groupoid"*). Recall that the following *Theorem of Bruck* characterizes free groupoids ([1; L.1.5]).

Theorem 0.1. *A groupoid $\boldsymbol{F} = (F, \cdot)$ is free iff it satisfies the following conditions:*

(i) *$\boldsymbol{F}$ is injective,*

(ii) *The set B of primes in $\boldsymbol{F}$ is nonempty and generates $\boldsymbol{F}$. (In that case B is the unique free basis of $\boldsymbol{F}$.)*

Throughout the paper we denote by $\boldsymbol{F}$ a free groupoid with the basis B, and $t, u, v, \dots, \alpha, \beta, \dots$ elements of F.

For any $v \in F$ we define the *length* $|v|$ of v and the *set $P(v)$ of parts* of v in the following way:

$$|b| = 1, \quad |tu| = |t| + |u|, \tag{0.3}$$

$$P(b) = \{b\}, \quad P(tu) = \{tu\} \cup P(t) \cup P(u), \tag{0.4}$$

for any $b \in B$, $t, u \in F$.

1. Groupoid powers

From now on, we will denote by $\boldsymbol{E} = (E, \cdot)$ a free groupoid with a one-element basis $\{e\}$. The elements of E will be denoted by $f, g, h, \dots$ and called *groupoid powers*. Note that E is a countable infinite set.

If $\boldsymbol{G} = (G, \cdot)$ is a groupoid, then each $f \in E$ induces a transformation f^G of G (called the *interpretation* of f in $\boldsymbol{G}$) defined by:

$$f^{\mathbf{G}}(x) = \varphi_x(f),$$

where $\varphi_x \colon E \to G$ is the homomorphism from $\boldsymbol{E}$ into $\boldsymbol{G}$ such that $\varphi_x(e) = x$. In other words

$$e^{\boldsymbol{G}}(x) = x, \quad (fh)^{\boldsymbol{G}}(x) = f^{\boldsymbol{G}}(x) h^{\mathbf{G}}(x), \tag{1.1}$$

for any $f, h \in E$, $x \in G$. (We will usually write $f(x)$ instead of $f^{\boldsymbol{G}}(x)$ when we work with a fixed groupoid $\boldsymbol{G}$.)

By induction on lenght, for any $f, g \in E$, $t, u \in F$, the following statements can be shown. (Most of these results are stated in [4], as well.)

Proposition 1.1. $|f(t)| = |f|\,|t|$. □

Proposition 1.2. $t \in P\big(f(t)\big)$. □

Proposition 1.3. $(\forall n \in \boldsymbol{N})\big(f(t)\big)^n = f^n(t)$. □

Proposition 1.4. $f(t) = g(u)$ & $|t| = |u| \Leftrightarrow (f = g$ & $t = u)$. □

Proposition 1.5. $f(t) = g(u)$ & $|t| \geq |u| \Leftrightarrow (\exists!\, h \in E)(t = h(u)$ & $g = \ (\ ))$. □

Corresponding translations (0.3′), (0.4′) and Prop.1.1′–Prop.1.5′ (for E) of (0.3), (0.4) and Prop.1.1–Prop.1.5 are obvious and we will not state them explicitely.

We define an other operation "∘" in E by:

$$f \circ g = f(g)\,. \tag{1.2}$$

So, we obtain an algebra $(E, \circ, \cdot)$ with two operations, $\circ$ and $\cdot$, such that

$$e \circ g = g \circ e = g\,, \quad (f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)\,,$$

for any $g, f_1, f_2 \in E$.

Using (1.1), (1.2) and Prop.1.4, one can show the following proposition.

Proposition 1.6. *$(E, \circ, e)$ is a cancellative monoid.* □

A power $f \in E$ is said to be *irreducible* iff

$$f \neq e \;\&\; (f = g \circ h \Rightarrow g = e \text{ or } h = e)\,. \tag{1.3}$$

The proofs of the following propositions are obvious.

Proposition 1.7. *If the length $|f|$ of f is a prime integer, then f is irreducible.* □

Proposition 1.8. *If $p, q \in E$ are irreducible and $f \circ p = h \circ q$, then $f = h$ and $p = q$.* □ (OTAP)

Proposition 1.9. *For every $f \in E \setminus \{e\}$ there is a unique sequence $p_1, p_2, \ldots, p_n$ of irreducible elements in $\boldsymbol{E}$, such that $f = p_1 \circ p_2 \circ \ldots \circ p_n$.* □

By Prop.1.6, 1.7 and Prop.1.9 it follows:

Proposition 1.10. *The monoid $(E, \circ, e)$ is free with a countable infinite basis. (The set of irreducible powers is the basis of the monoid.)* □

If $\mathcal{V}$ is a variety of groupoids, then we denote by $\boldsymbol{E_\mathcal{V}} = (E_\mathcal{V}, \cdot)$ a free groupoid in $\mathcal{V}$, with a one-element basis $\{e\}$. The elements of $E_\mathcal{V}$ can be considered as powers in groupoids of $\mathcal{V}$. Namely, for every $\boldsymbol{G} \in \mathcal{V}$, and $f \in E_\mathcal{V}$, we can define a transformation $f^{\boldsymbol{G}}$, as an interpretation of f; we say that $f^{\boldsymbol{G}}$ is a *$\mathcal{V}$-power* in $\boldsymbol{G}$. [$(\forall a \in G)\ \langle a \rangle = \{ f^G(a) \mid f \in E \}$].

2014

In the case of the variety of commutative groupoids, we can use the corresponding Bruck Theorem, modifying the notion of an injective groupoid. Namely, if $\boldsymbol{G}$ is a commutative groupoid such that

$$\big(\forall x, y, u, v \in G\big)\big(xy = uv \iff \{x, y\} = \{u, v\}\big), \tag{1.4}$$

we say that $\boldsymbol{G}$ is *injective* in the variety of commutative groupoids. We will not formulate Bruck Theorem for commutative groupoids, because it is formally the same as Th.0.1.

Further on, in the paper, we denote by $\boldsymbol{F}_c = (F_c, \cdot)$ a free commutative groupoid with the basis B; also, $\boldsymbol{E}_c = (E_c, \cdot)$ is a free commutative groupoid with a one-element basis $\{e\}$.

We assume the definitions (0.3), (0.4), (1.1)–(1.3), replacing F, E by F_c, E_c respectively, as definitions (0.3_c), (0.4_c), (1.1_c)–(1.3_c) for the corresponding notions in commutative groupoids. Then, the Pr.1.1–1.10, replacing F, E by F_c, E_c respectively, become Pr.1.1_c–1.10_c , which hold for commutative groupoids. (We will not formulate explicitly the Pr.1.1_c–1.10_c, because they are formally the same as Pr.1.1–1.10.) By Pr.1.10 and Pr.1.10_c it follows:

Proposition 1.11. *The monoids $(E, \circ, e)$ and $(E_c, \circ, e)$ are isomorphic.* □

We will end this part with a short discussion about the number $\varepsilon(n)$ of elements in the set

$$\{f \in E \colon |f| = n\}, \tag{1.5}$$

and the number $\varepsilon_c(n)$ of elements in the set

$$\{f \in E_c \colon |f| = n\}. \tag{1.6}$$

Since the groupoid $\boldsymbol{E}$ is injective and e is a prime, we obtain that $\varepsilon(1) = 1$, and that for any $n \geq 2$, the following relation holds

$$\varepsilon(n) = \sum_{k=1}^{n} \varepsilon(k)(n-k). \tag{1.7}$$

By a result of P.Hall (see for example: [2], III 2, Ex.2, p.125), one obtains the following result:

$$\varepsilon(n) = (2n-2)!/\big((n-1)!\,n!\big).\ ^2 \tag{1.8}$$

---

[2] Consider the power series $\sigma(x) = \varepsilon_1 x + \varepsilon_2 x^2 + \cdots$, where $\varepsilon_n = \varepsilon(n)$. One can show that $\sigma(x)^2 - \sigma(x) + x = 0$, which implies $2\sigma(x) = \sqrt{1-4x}$. Then, using the binomial series for $\sqrt{1-4x}$, one obtains (1.8).

Because of the commutativity of $\boldsymbol{E}_c$, one obtains that $\varepsilon_c(1) = \varepsilon_c(2) = \varepsilon_c(3) = 1$, and that for each $n \geq 1$, the following relations hold

$$\varepsilon_c(2n) = \sum_{k=1}^{n} \varepsilon_c(k)\varepsilon_c(2n-k)\,, \tag{1.9}$$

$$\varepsilon_c(2n+1) = \sum_{k=1}^{n} \varepsilon_c(k)\varepsilon_c(2n+1-k)\,. \tag{1.10}$$

But we do not know any "elementary function" which expresses $\varepsilon_c(n)$ as (1.8) expresses $\varepsilon(n)$.

2. Powers in n-idempotent groupoids

Let $\mathcal{V}^{(n)}$ be the variety of groupoids with the axiom $x^{n+1} = x$,[3] where $n \geq 1$. $\mathcal{V}^{(1)}$ is the variety of idempotent groupoids, and thus $E^{(1)} = \{e\}$ is a one-element set; this implies that the monoid $(E^{(1)}, \circ, e)$ is free with empty basis.

Below, we assume that $n \geq 2$ and we will write $E^{(n)}$ instead of $E_{\mathcal{V}^{(n)}}$.

By the main result of [3] it follows that the monoid $\boldsymbol{E}^{(n)}$ is defined as follows:

$$E^{(n)} = \{f \in E \mid (\forall g \in E) g^{n+1} \notin P(f)\}\,, \tag{2.1}$$

$$(\forall f, g \in E^{(n)})[(f \bullet g = fg \text{ if } fg \in E^{(n)} \ \&\ (f \bullet g = g \text{ if } f = g^n)]\,. \tag{2.2}$$

The main result of this section is the following statement.

Proposition 2.1. *For each $n \geq 2$, $(E^{(n)}, \circ, e)$ is a free monoid with an infinite basis, and the basis consists of the irreducible elements of E which belong to $E^{(n)}$.*

In order to prove Prop.2.1, we will use some lemmas.

Lemma 2.2. $(\forall f \in E) f \in E^{(n)} \Rightarrow P(f) \subseteq E^{(n)}$.

Proof. This is an obvious corollary from (2.1) and the definition of $P(f)$. □

---

[3] For $k \in N$, x^k have the usual meaning, i.e. $x^1 = x$, $x^{k+1} = x^k x$.

Lemma 2.3. $(\forall f, g \in E)(f \circ g \in E^{(n)} \Rightarrow \{f, g\} \subseteq E^{(n)}$.

Proof. Assume $f \circ g \in E^{(n)}$. Clearly, if $e \in \{f, g\}$, then $\{f, g\} \subseteq E^{(n)}$. Thus we can assume that $|f| \geq 2$, $|g| \geq 2$. Moreover, by L.2.2, $g \in P(f \circ g)$ implies $g \in E^{(n)}$. We have to show that $f \in E^{(n)}$, as well. If $f = f_1 f_2$, then $(f_1 \circ g)(f_2 \circ g) = f \circ g \in E^{(n)}$, and by L.2.2, this implies $\{f_1 \circ g, f_2 \circ g\} \subseteq E^{(n)}$; by induction on length we obtain $\{f_1, f_2\} \subseteq E^{(n)}$. Then $f \notin E^{(n)}$ implies $f_1 = f_2^n$, and then we would have

$$f \circ g = (f_1 f_2) \circ g = (f_2^{n+1}) \circ g = (f_2 \circ g)^{n+1} \notin E^{(n)},$$

a contradiction. □

Lemma 2.4. $E^{(n)}$ *is a submonoid of* $(E, \circ, e)$.

Proof. From (2.1) it follows that $e \in E^{(n)}$. Let $f, g \in E^{(n)}$. If $f = e$, then $f \circ g = g \in E^{(n)}$, and thus we can assume that $f = f_1 f_2$, where $f_1, f_2 \in E^{(n)}$. Assume $f_1 \circ g, f_2 \circ g \in E^{(n)}$, but

$$f \circ g = (f_1 \circ g)(f_2 \circ g) \notin E^{(n)}.$$

Then $f_1 \circ g = (f_2 \circ g)^n = f_2^n \circ g$, and this (because of the cancellative law) implies $f_1 = f_2^n$, which is impossible, for then we would have $f = f_2^{n+1} \in E^{(n)}$. □

As a corollary of L.2.3, we have:

Lemma 2.5. *If* $f \in E^{(n)}$ *and* $f = f_1 \circ f_2 \circ \ldots \circ f_n$, *then* $f_1, f_2, \ldots, f_n \in E^{(n)}$. □

Lemma 2.6. *If* $p \in E^{(n)}$ *is irreducible in* $\boldsymbol{E}$, *then* p *is irreducible in* $\boldsymbol{E}^{(n)}$, *as well.* □

Lemma 2.7. *The set of irreducible elements in* $\boldsymbol{E}^{(n)}$ *is infinite.*

Proof. If $q_1 = e^2$, $q_{k+1} = eq_k$, then $\{q_1, q_2, \ldots, q_k, q_{k+1}, \ldots\} = Q$ is an infinite set of irreducible elements in $\boldsymbol{E}^{(n)}$. Namely, from $|q_k| = k + 1$, it follows that Q is infinite.

Also, from (2.1) and $n \geq 2$, we have $q_1 \in E^{(n)}$. Assume that $q_k \in E^{(n)}$. Then $e^2 \neq q_k^n$, which implies that $q_{k+1} \in E^{(n)}$. Thus $Q \subseteq E^{(n)}$.

It remains to show that the elements of Q are irreducible. Namely, by Prop.1.7, q_1 is irreducible. Let $q_1, q_2, \ldots, q_p$, for any integer $p \leq k$, be irreducible. Assume that $q_{k+1} = f \circ g$, where $f, g \in E^{(n)}$, $f \neq e$, $g \neq e$. Then, $eq_k = f \circ g = (f_1 \circ g)(f_2 \circ g)$, i.e. $e = f_1 \circ g$, which is impossible. □

Finally, Prop.2.1 is a corollary of L.2.3–L.2.7. □

As usual, by $\mathcal{V}_c^{(n)}$ we denote the variety of commutative groupoids in $\mathcal{V}^{(n)}$. The corresponding groupoid $\boldsymbol{E}_c^{(n)} \in \mathcal{V}_c^{(n)}$ can be defined by (2.1_c) and (2.2_c), replacing $E^{(n)}$ in (2.1) and (2.2) by $E_c^{(n)}$ and E by E_c.

In the same maner we obtain Lemmas 2.2_c–2.7_c. We only need a modification in the proof that the set of irreducible elements in $(E_c^{(n)}, \circ, e)$ is infinite. Namely, in $\boldsymbol{E}_c^{(n)}$ we have $q_k = e^{k+1}$, and therefore (for example) $q_n \notin E_c^{(n)}$. But we can obtain an infinite set of irreducible elements in $\boldsymbol{E}_c^{(n)}$, as follows:

$$p_1 = e(e^2)^2, \quad p_{k+1} = ep_k\,.$$

Thus we would obtain the following, analogy of Prop.2.1.

Proposition 2.1$_c$. *For each $n \geq 2$, $(E_c^{(n)}, \circ, e)$ is a free monoid with an infinite basis, and the basis consists of the irreducible elements of E_c which belong to $\boldsymbol{E}_c^{(n)}$.* □

References

[1] R. H. Bruck: *A Survey of Binary Systems*, Springer-Verlag, 1958.

[2] P. M. Cohn: *Universal Algebra*, Harper & Row, 1965.

[3] Ǵ. Čupona, N. Celakoski, *Free groupoids with $x^n = x$*, Proceed. of the First Congress of Math. and Informat. of Rep. of Macedonia, Ohrid 1996, p. 19-25.

[4] Ǵ. Čupona, S. Ilic, *Free groupoids with $x^n = x$*, II, Novi Sad, J. Math., Vol. 29, No.1, 1999, 147-154.

ГРУПОИДНИ СТЕПЕНИ

Ѓорѓи Чупона*, Наум Целакоски**, Снежана Илиќ***

Р е з и м е

Следното тврдење е главен резултат на работава.

Ако $\mathcal{V}$ е многуобразието групоиди (комутативни групоиди), или $\mathcal{V}$ е многуобразието од n-идемпотентни групоиди (комутативни n-идемпотентни групоиди), т.е. групоиди (комутативни групоиди) со аксиомата $x^{n+1} = x$, $n \geq 2$, тогаш моноидот од степени е слободен со бесконечна пребројлива база.

* Macedonian Academy of Sciences and Arts
P.O. Box 428, 1000 Skopje,
Republic of Macedonia

** Faculty of Mechanical Engineering
P.O. Box 464, 1000 Skopje,
Republic of Macedonia

*** Faculty of Sciences, University of Nis
SR Yugoslavia