

ON A VARIETY OF GROUPOIDS OF RANK 1
Збор. труд., Втор конгрес мат. и инф. Македонија Охрид 2000
(Сојуз мат. Макед., Скопје 2003), 17–23
 Ć Ćurona , V. Celakoska-Jordanova

Abstract: A canonical description of free objects in the variety \mathcal{V} of groupoids defined by the identity $xx^2 = x^2x^2$ is given. Injective groupoids in \mathcal{V} and subgroupoids of free groupoids in \mathcal{V} are considered. It is shown that the class of free groupoids in \mathcal{V} is a proper subclass of the class of injective groupoids in \mathcal{V} and that both classes are hereditary.

0. Introduction

Throughout the paper we denote by $F = (F, \cdot)$ a given absolutely free groupoid with a basis B (i.e. groupoid free in the class of all groupoids). It is well-known ([1; L.1.5.]) that the following two conditions characterizes F : a) F is injective¹⁾; b) the set B of prime elements in F is nonempty and generates F .

The subject of this paper is the variety of groupoids of rank 1,²⁾ defined by the identity³⁾

$$xx^2 = x^2x^2, \tag{0.1}$$

which we denote by \mathcal{V} . The paper is divided into three sections.

In Section 1 we give a description of \mathcal{V} -free groupoids and show that they may be different.

In Section 2, the notion of \mathcal{V} -injective groupoid (i.e. groupoid injective in \mathcal{V}) is introduced. It is shown that: the class of \mathcal{V} -injective groupoids is hereditary, every \mathcal{V} -injective groupoid is infinite and the class of \mathcal{V} -free groupoids is a proper subclass of the class of injective groupoids.

In Section 3 are considered subgroupoids of \mathcal{V} -free (i.e. free in \mathcal{V}) groupoids. We prove that: Bruck Theorem for \mathcal{V} holds, the class of \mathcal{V} -free groupoids is hereditary and that every \mathcal{V} -free groupoid contains a subgroupoid with an infinite basis.

1. Free objects in \mathcal{V}

For a construction of a free object in a variety \mathcal{V} of groupoids with an axiom $f = g$, the following "procedure" is often convenient. We consider one of the two parts of the axiom of \mathcal{V} as "more suitable", and, as a candidate for the carrier of the desired free object, we choose the set R of all elements $t \in F$ ⁴⁾ which contain no parts with a form of the "unsuitable side of the axiom".

Here we consider the variety \mathcal{V} with an axiom $xx^2 = x^2x^2$. Choosing the left side as "unsuitable", we obtain:

$$R = \{ t \in F : (\forall \alpha \in F) \alpha\alpha^2 \notin P(t) \}. \tag{1.1}$$

By (1.1) immediately we obtain:

- a) $(\forall t, u \in F) \{ tu \in R \Leftrightarrow t, u \in R \ \& \ u \neq t^2 \}$.
- b) $t, u \in R \Rightarrow \{ tu \notin R \Leftrightarrow u = t^2 \}$.
- c) $t \in R \Rightarrow (\forall k \in \mathbb{N}) t^k \in R$ ⁶⁾ (t^n is defined in F by: $t^1 = t, t^{n+1} = t^n t$).

Define an operation $*$ on R by:

¹⁾ We do not define here the notions as: injective groupoid, prime element, length $|v|$ and set $P(v)$ of parts of $v \in F, \dots$ (see, for example [2]).

²⁾ A variety defined by identities which contain only one variable is called a variety of rank 1.

³⁾ Here we use the usual abbreviations: $xx^2 = x(xx)$, $x^2x^2 = (xx)(xx)$.

⁴⁾ $F = (F, \cdot)$, as above, is an absolutely free groupoid with the free basis B .

⁵⁾ $P(t)$ is the set of parts (i.e. subterms) of t .

⁶⁾ \mathbb{N} is the set of positive integers.

$$t, u \in R \Rightarrow t * u = \begin{cases} tu, & \text{if } tu \in R \\ (t^2)^2, & \text{if } u = t^2 \end{cases} \quad (1.2)$$

By a direct verification we obtain that $\mathbf{R} = (R, *)$ is a groupoid, the equality (0.1) holds in \mathbf{R} (i.e. $t*(t*t) = (t*t)*(t*t)$) is an identity in \mathbf{R} which means that $\mathbf{R} \in \mathcal{V}$ and for any mapping $\lambda: B \rightarrow G$ ⁷⁾, there is a homomorphism $\varphi: F \rightarrow G$ which extends λ . Therefore:

Theorem 1. $\mathbf{R} = (R, *)$ is a free groupoid in \mathcal{V} with the basis B , and B coincides with the set of primes in \mathbf{R} . \square

Bellow we will state some properties of the groupoid \mathbf{R} , but first we will consider the groupoid power $x^{(k)}$, $k \geq 0$, defined by:

$$x^{(0)} = x, \quad x^{(k+1)} = x^{(k)}x^{(k)} = (x^{(k)})^2 \quad (1.3)$$

By induction on m and n one can show that, in any groupoid $\mathbf{G} = (G, \cdot)$, the following statement is true:

$$(\forall x \in G, m, n \geq 0) \quad (x^{(m)})^{(n)} = x^{(m+n)}. \quad (1.4)$$

If $\mathbf{G} \in \mathcal{V}$, then by (1.3) and (0.1) one obtains:

$$(\forall x \in G, p \geq 0) \quad x^{(p)}x^{(p+1)} = x^{(p+2)}. \quad (1.5)$$

We say that an element $a \in G$ is a power in \mathbf{G} if there are $b \in G$ and $k \geq 1$, such that $a = b^{(k)}$. If $b \in G$ is not a power in \mathbf{G} , i.e. $(\forall c \in G) (c = b^{(p)} \Rightarrow p = 0)$, then we say that b is a base in \mathbf{G} .

As a special case of c), one obtains:

$$c') \quad t \in R, k \geq 1 \Rightarrow t^{(k)} \in R.$$

Note that, if $t \in R$, t^n is the n -th power of t in F ; in this sense, t_*^n is the n -th power of t in \mathbf{R} , defined by: $t_*^1 = t$, $t_*^{n+1} = t_*^n * t$.

From (1.2) and c'), by induction on k , we obtain:

$$d) \quad (\forall t \in R, k \geq 0) \quad t_*^{(k)} = t^{(k)} \quad \text{and, for } k \geq 1: \quad t_*^k = t^k.$$

As a consequence of d), we obtain the following two statements.

Proposition 1.1. $(\forall u \in R)(\exists!(t, p) \in R \times N_0)$ ⁸⁾ $u = t_*^{(p)}$, where t is a base in \mathbf{R} . \square

Proposition 1.2. a) If $x \in R \setminus B$ (i.e. x is not prime in \mathbf{R}) and if x is not a power, then there exists a unique pair $(u, v) \in R^2$, such that $x = u * v$. (In this case $x = uv$.)

(We say that (u, v) is the pair of divisors of x and write $(u, v) | x$.)

b) If $x \in R$ is a power, $x = t^{(p+1)}$, $p \geq 0$, then $x = t^{(p)} * t^{(p)}$, and $(t^{(p)}, t^{(p)})$ is the pair of divisors of x . \square

The class of groupoids free in \mathcal{V} will be denoted by \mathcal{V}_{free} . We will show the following

Proposition 1.3. If \mathbf{R} is defined by (1.2), then there exists a mapping $x \mapsto |x|$ from R into N such that

$$|b| = 1, \quad |cd| \geq |c| + |d|, \quad (1.6)$$

for any $b \in B, c, d \in R$.

Proof. Let $\mathbf{R} = (R, *)$ be the \mathcal{V} -canonical groupoid with the basis B (constructed above, Th.1) and let $x \mapsto |x|$ be the restriction of the mapping $|| : F \rightarrow N$. Let $t, u \in R$. Since $t, u \in F$, it follows that $|tu| = |t| + |u|$ and $|t^2| = 3|t|$. From (1.2) we obtain:

$$\begin{aligned} tu \in R &\Rightarrow |t * u| = |t| + |u|, \\ tu \notin R &\Rightarrow u = t^2 \Rightarrow |t * t^2| = |(t^2)^2| = 4|t| > 3|t|. \end{aligned}$$

This shows that $|t * u| \geq |t| + |u|$. \square

⁷⁾The carrier of a given groupoid \mathbf{S} is denoted by the same (light) letter S .

⁸⁾ N_0 is the set of nonnegative integers.

Remark 1.4. When one decides which side of the identity $xx^2 = x^2x^2$ to consider as "suitable" one, it is natural to choose the "shorter" side, i.e. xx^2 , and expect a shorter construction of \mathcal{V} -free groupoid. However, it turns out the opposite, the construction is longer and more complicated.

Namely, let the first candidate for the carrier of \mathcal{V} -free groupoid be the set F_1 , defined by:

$$F_1 = \{ t \in F : (\forall \alpha \in F) (\alpha^2)^2 \notin P(t) \}.$$

If we define an operation $*_1$ on F_1 by:

$$t, u \in F_1 \Rightarrow t *_1 u = \begin{cases} tu, & \text{if } tu \in F_1 \\ \alpha\alpha^2, & \text{if } t = u = \alpha^2 \end{cases}$$

then we obtain that $F_1 = (F_1, *_1)$ is a groupoid. However, the equality (0.1), which has the form here

$$t *_1 (t *_1 t) = (t *_1 t) *_1 (t *_1 t) \quad (1.7)$$

is not satisfied in F_1 , i.e. $F_1 \notin \mathcal{V}$. Namely, if $t = \alpha^2$, the left side of (1.7) is $\alpha^2(\alpha\alpha^2)$ and the right one is $(\alpha\alpha^2)^2$. This result implies that

$$\alpha^2(\alpha\alpha^2) = (\alpha\alpha^2)^2 \quad (1.7')$$

is an identity in \mathcal{V} . This suggests a definition of a new "candidate" $F_2 = (F_2, *_2)$:

$$F_2 = \{ t \in F_1 : (\forall \alpha \in F_1) (\alpha\alpha^2)^2 \notin P(t) \},$$

$$t, u \in F_2 \Rightarrow t *_2 u = \begin{cases} t *_1 u, & \text{if } t *_1 u \in F_2 \\ \alpha^2(\alpha\alpha^2), & \text{if } t = u = \alpha\alpha^2 \end{cases}.$$

Checking (1.7) (when $*_1$ is substituted by $*_2$), we obtain $F_2 \notin \mathcal{V}$ and one more identity in \mathcal{V} :

$$(\alpha\alpha^2)(\alpha^2(\alpha\alpha^2)) = ((\alpha^2(\alpha\alpha^2))^2). \quad (1.7'')$$

Continuing this procedure, we can see a regularity in the consequences of the identity (1.7), which suggests to introduce a special kind of groupoid power $x \mapsto x^{<n>}$, defined by:

$$x^{<0>} = x, \quad x^{<1>} = x^2, \quad x^{<k+2>} = x^{<k>} x^{<k+1>}. \quad (1.8)$$

Using this, we define the following infinite set of groupoids $\{F_n = (F_n, *_n) : n \geq 1\}$:

$$F_1 = \{ t \in F : (\forall \alpha \in F) (\alpha^{<1>})^2 \notin P(t) \}, \quad t, u \in F_1 \Rightarrow t *_1 u = \begin{cases} tu, & \text{if } tu \in F_1 \\ \alpha\alpha^2, & \text{if } t = u = \alpha^{<1>} \end{cases},$$

$$F_{n+1} = \{ t \in F_n : (\forall \alpha \in F_n) (\alpha^{<n>})^2 \notin P(t) \}, \quad t, u \in F_{n+1} \Rightarrow t *_n u = \begin{cases} t *_n u, & \text{if } tu \in F_{n+1} \\ \alpha^{<n+2>}, & \text{if } t = u = \alpha^{<n+1>} \end{cases}.$$

One can show that F_{n+1} is a groupoid such that $F_{n+1} \notin \mathcal{V}$.

Using the fact that $F \supseteq F_1 \supseteq \dots \supseteq F_n \supseteq \dots$ and that F_{n+1} is "better" than F_n , we obtain the following definition of the carrier R' of a free groupoid in \mathcal{V} :

$$R' = \{ t \in F : (\forall \alpha \in F, n \geq 1) (\alpha^{<n>})^2 \notin P(t) \} (= \bigcap \{F_n : n \geq 1\}).$$

(Note that it is not necessary to define the whole sequence, because the desired "good candidate" can be noticed after several steps.)

We define an operation $*$ on R' by

$$t, u \in R' \Rightarrow t * u = \begin{cases} tu, & \text{if } tu \in R' \\ \alpha^{<n+1>}, & \text{if } t = u = \alpha^{<n>}, n \geq 1 \end{cases}$$

and obtain:

Proposition 1.5. R' is a V -free groupoid with the basis B . \square

Therefore, there exist at least two distinct V -free groupoids, R and R' . Since R and R' have the same basis B , they are isomorphic.

2. Injective groupoids in V

We obtain the class of injective groupoids in V from the class of V -free groupoids in the same way as in the variety of all groupoids (and, namely, by omitting the condition that the set of primes is a generating set).

Using Pr.1.1 – 1.2, we come to the following definition of injective groupoids in V .

We say that a groupoid $H = (H, \cdot) \in V$ is *injective in V* (i.e. V -injective) iff the following conditions are satisfied:

(i₁) $(\forall a \in H)(\exists!(b, p) \in H \times N_0) a = b^{(p)}$ and b is a base in H .

(We say that b is the *base* and p the *exponent* of a .)

(i₂) $b^{(p+2)} = cd$ iff $[c = d = b^{(p)}$ or $(c = b^{(p)} \ \& \ d = b^{(p+1)})]$.

(ii) If b is a base in H , then: $b^{(1)} = cd \Leftrightarrow c = d = b$.

(iii) If $a \in H$ is a base which is not prime in H , then

$$(\exists!(c, d) \in H^2) \quad a = cd, c \neq d.$$

The pair of divisors (c, d) of an element $a \in H$ which is not prime in H (we write: $(c, d) \mid a$) is defined as follows.

1) If b is a base in H and $p \geq 0$, then $(b^{(p)}, b^{(p)}) \mid b^{(p+1)}$.

2) If $a = cd$ is a base in H , then $(c, d) \mid a$.

We denote by V_{inj} the class of injective groupoids. By Pr.1.1–1.2 we obtain:

Proposition 2.1. $V_{free} \subseteq V_{inj}$. \square

Proposition 2.2. Let $H \in V_{inj}$, $Q \leq H$, $a = b^{(p)} \in Q$ and $b \notin Q$, where b is the base of a in H . If $r = \min\{k : b^{(k)} \in Q\}$, then $b^{(r)}$ is a prime in Q . \square

As a corollary of Pr.2.2, we obtain the following

Proposition 2.3. The class V_{inj} is hereditary. \square

If $c^{(p)} = d^{(q)}$ and c, d are bases in $H \in V_{inj}$, then $c = d \ \& \ p = q$. Therefore, if a is a base in H , then the powers $a^{(n)}$, $n \geq 1$, are mutually distinct and thus the set $\{a, a^{(1)}, a^{(2)}, \dots\}$ is infinite. Therefore:

Proposition 2.4. Every $H \in V_{inj}$ is infinite. \square

Bellow we will give a construction of V -injective groupoids (and show that there are V -injective groupoids which are not V -free).

Let A be an infinite set and $H = A \times N_0$. Define a partial operation \bullet on H by:

$$(a, p) \bullet (a, p) = (a, p+1), \quad (a, p) \bullet (a, p+1) = (a, p+2)$$

and put

$$D = \{((a, p), (b, q)) : a \neq b \text{ or } (a = b \ \& \ q \notin \{p, p+1\})\}.$$

Since A and D have the same cardinality, there is an injection $\varphi: D \rightarrow A$ and we can put

$$(\forall (a, p), (b, q) \in D) \quad (a, p) \bullet (b, q) = (\varphi((a, p), (b, q)), 0).$$

Then we obtain that (H, \bullet) is a groupoid injective in V .

If φ is a bijection, then the set $A \times \{0\} \setminus \text{im} \varphi$ of primes in H is empty, and thus (H, \bullet) is not free in V . This and Cor.2.1 proves the following

Theorem 2. The class V_{free} is a proper subclass of V_{inj} . \square

3. Subgroupoids of V -free groupoids

In this section we will show that the class V_{free} is hereditary, but first we will give a characterization of V -free groupoids (analogous to a), b) in Introduction, for absolutely free groupoids).

Theorem 3 (Bruck Theorem for V). A groupoid $H \in V$ is V -free iff:

(i) H is V -injective.

(ii) The set B of primes in H is nonempty and generates H .

Proof. If H is V -free with the basis B , then $H \in V_{inj}$ (by Th.2), B is the set of primes in H and generates H .

For the converse, define an infinite sequence of subsets B_1, B_2, \dots of H :

$$B_1 = B, \quad B_2 = \{cd : c, d \in B_1\},$$

$$B_{k+1} = \{a \in HH : (c, d) \mid a \Rightarrow \{c, d\} \subseteq B_1 \cup \dots \cup B_k \text{ \& } \{c, d\} \cap B_k \neq \emptyset\}.$$

Then the following statements are true:

$$1) (\forall k \geq 1) B_k \neq \emptyset; \quad 2) p \neq q \Rightarrow B_p \cap B_q = \emptyset; \quad 3) H = \bigcup \{B_k : k \geq 1\}.$$

Let $G \in V$ and $\lambda : B \rightarrow G$ be a mapping. Defining a sequence of mappings $\varphi_k : B_k \rightarrow G$ inductively ($\varphi_1 = \lambda; \dots$) and continuing in a similar way as in [2; Th.1], one can show that the mapping $\varphi = \bigcup \{\varphi_k : k \geq 1\}$ is a homomorphism from H into G which extends λ . \square

Below we assume that R is as above and Q is a subgroupoid of R .

Proposition 3.1. The set P of primes in Q is nonempty and generates Q .

Proof. By Pr.1.3, there is a mapping in R with the property (1.6). Let $c \in Q$ be such that

$$|c| = \{\min |a| : a \in Q\} \quad (3.1)$$

By (1.6) and (3.1), c is prime in Q . Thus the set P of primes in Q is nonempty.

Denote by T the groupoid generated by P . Clearly, $T \subseteq Q$. We will show that $Q \subseteq T$, using induction on length.

First of all, $P \subseteq T$. If $b \in Q$ and $|b|=1$, then b is prime in R , and thus b is prime in Q , i.e. $b \in P$. Therefore $b \in T$. Suppose $c \in Q$ & $|c| \leq k \Rightarrow c \in T$. Let $c \in Q$ and $|c|=k+1$. If $c \in P$, then $c \in T$. Therefore let $c \in Q \setminus P$. Then $c = de$ ($d, e \in Q$), and $|c| = |de| \geq |d| + |e| \Rightarrow |d|, |e| \leq k \Rightarrow d, e \in T \Rightarrow c = de \in T$.

Thus $Q \subseteq T$ and therefore P generates Q . \square

Proposition 3.2. $Q \in V_{free}$.

Proof. By Pr.2.1, $H \in V_{free}$ implies $H \in V_{inj}$, and by Pr.2.3, $Q \in V_{inj}$. Now, applying Bruck Theorem for V we obtain that $Q \in V_{free}$. \square

As a corollary of Pr.3.2 we obtain

Proposition 3.3. The class V_{free} is hereditary. \square

Finally, we will prove the following

Proposition 3.4. If $H \in V_{free}$, then there is a subgroupoid Q such that Q has an infinite basis.

Proof. Let B be the basis of H and $a \in B$. Put

$$c_1 = a \cdot a, \quad c_2 = c_1 a, \dots, \quad c_{k+1} = c_k a, \dots$$

and let Q be the subgroupoid of H generated by the set $C = \{c_k : k \geq 0\}$. Then: 1) C is infinite; 2) all the elements in C are prime in Q ; 3) C is a basis of Q . Namely, the elements of C are mutually distinct ($c_p = c_q \Rightarrow p = q$) and thus C is infinite. Secondly, every element $c_k \in C$ is a base in Q : $c_1 = aa = a^2$, but $a \notin Q$ and thus c_1 is a base in Q ; $c_1 = a^2 a = a^3$, $a^2 \in Q$, but $a \notin Q$, and thus c_2 is a base in Q ; inductively, $c_{k+1} = a^k a$ is a base in Q . Thirdly, C is the set of primes in Q , $C \neq \emptyset$ and generates Q . Therefore, C is the basis of Q . \square

References

- [1] R. H. Bruck: *A Survey of Binary Systems*, Springer-Verlag 1958
- [2] Ā. Čupona, N. Celakoski, B. Janeva: *Injective groupoids in some varieties of groupoids* (this volume)