

By (0.5) and (1.3) we obtain:

$$|u * v| = 2^m |u^{(-m)} v^{(-m)}| = 2^m (2^{-m}|u| + 2^{-m}|v|) = |u| + |v|, \quad (1.10)$$

i.e. the restriction of the norm on R is a homomorphism from \mathbf{R} onto the additive groupoid of positive integers. This restriction will be called the **norm on \mathbf{R}** .

Let $\mathbf{G} = (G, \cdot) \in \mathcal{V}$, $\lambda: B \rightarrow G$ be an arbitrary mapping, and $\varphi: \mathbf{F} \rightarrow \mathbf{G}$ be the homomorphism which is an extension of λ . Denote by ψ the restriction of φ on R . If $u, v \in R$ and $m = \min\{|u|, |v|\}$, then:

$$\begin{aligned} \psi(u * v) &= \varphi \left(\left(u^{(-m)} v^{(-m)} \right)^{(m)} \right) = \left(\varphi \left(u^{(-m)} v^{(-m)} \right) \right)^{(m)} \\ &= \left(\varphi \left(u^{(-m)} \right) \varphi \left(v^{(-m)} \right) \right)^{(m)} = \\ &= \left(\varphi \left(u^{(-m)} \right) \right)^{(m)} \left(\varphi \left(v^{(-m)} \right) \right)^{(m)} \\ &= \varphi \left(\left(u^{(-m)} \right)^{(m)} \right) \varphi \left(\left(v^{(-m)} \right)^{(m)} \right) \\ &= \varphi(u) \varphi(v) \\ &= \psi(u) \psi(v), \end{aligned}$$

i.e. $\psi: \mathbf{R} \rightarrow \mathbf{G}$ is a homomorphism.

Thus \mathbf{R} is a free groupoid in \mathcal{V} , with a basis B . B is the unique basis of \mathbf{R} , for it is a subset of any generating subset of \mathbf{R} . This completes the proof of *Th. 1*.

Remark. The above proof of *Th. 1* is almost a direct consequence of the previously given definitions and results. Of course, some more general results could be used, but they would make the corresponding proof even more complicated. We will not include here discussions of that kind, and the interested reader is addressed to the corresponding books and papers (for example: [2], III.5; [4], §10; [5], 1.4; [6], 2.9).

2. An axiom system for \mathcal{V} -free groupoids

The main object of this section is the proof of **Th. 2**.

Proposition 2.1. Every \mathcal{V} -free groupoid satisfies the conditions (i)–(iv) of **Th. 2**.

Proof. By **Th. 1**., it is enough to show that $\mathbf{R} = (R, *)$ satisfies (i)–(iv).

Below we assume that $x, y, z, u, v \in R$.

1) By (1.10), if $x * y = z$, then $|z| > |x|$, $|z| > |y|$, and this implies that \mathbf{R} satisfies (i).

2) If $x * x = y * y$, then (according to (1.7)) $x^2 = y^2$, and so $x = y$; thus (ii) holds.

Assume that $x * y = u * v$ and $\min\{[x], [y]\} = p \leq q = \min\{[u], [v]\}$. Then, by (0.5) and (1.5):

$$x^{(-p)} y^{(-p)} = \left(u^{(-q)} v^{(-q)} \right)^{(q-p)}. \quad (2.1)$$

If $p = q$, then $x^{(-p)} y^{(-p)} = u^{(-p)} v^{(-p)}$ which implies $x = u$, $y = v$.

If $p < q$, then by (2.1):

$$x^{(-p)} y^{(-p)} = \left(\left(u^{(-q)} v^{(-q)} \right)^{(q-p-1)} \right)^2,$$

which implies $x^{(-p)} = y^{(-p)}$, i.e. $x = y$.

Thus we have:

3) $x * y = u * v$, $x \neq y$, $u \neq v \Rightarrow x = u$, $y = v$, i.e. (iii) is satisfied.

Finally, assume:

4) $x * x = y * z$, $y \neq z$.

Then, if $q = \min\{[y], [z]\}$, by (0.5) and (1.7), we have $x^2 = (y^{(-q)} z^{(-q)})^{(q)}$, i.e.

$$x = \left(y^{(-q)} z^{(-q)} \right)^{(q-1)} = y^{(-1)} * z^{(-1)}.$$

Thus: $x = u * v$, $y = u^2$, $z = v^2$, where $u = y^{(-1)}$, $v = z^{(-1)}$. \square

Now we will show the following

Lemma 2.2. Let $\mathbf{G} = (G, \cdot)$ be a groupoid which satisfies the condition (i) of Th. 2 and the following one:

(v) The set $\text{div}(a)$ of divisors of an arbitrary element $a \in G$ is finite.

Then, for arbitrary $a \in G$, the set of lengths of divisor chains with the first member a is bounded.

(We denote by $L(a)$ the largest member of this set, and we say that $L(a)$ is the **length** of a .)

Proof. Consider the oriented graph of which the nodes are the elements of G , and for $a, b \in G$ there exists an edge with the initial node a and the terminal

node b iff b is a divisor of a . From the given conditions it follows that every node of the graph is a "source" of finitely many edges and that every (directed) path in the graph is finite. Then, by König's Lemma (for example, [3,4]), one obtains that the set of path lengths, of which the origin is a given node, is bounded. \square

To complete the proof of *Th. 2* we have to show the following

Proposition 2.3. If a \mathcal{V} -groupoid \mathbf{H} satisfies the conditions (i)–(iv), then \mathbf{H} is \mathcal{V} -free, and the set B of primes in \mathbf{H} is the basis of \mathbf{H} .

Proof. First, (i) implies that the set B of primes in \mathbf{H} is nonempty. By (ii), (iii) and (iv), for each $a \in H$, $\text{div}(a)$ consists of at most 3 elements; thus the conclusion of *L. 2.2* holds. By induction on $L(a)$ we obtain that B is the least generating subset of \mathbf{H} .

Let $\mathbf{G} = (G, \cdot) \in \mathcal{V}$, and $\lambda: B \rightarrow G$ be an arbitrary mapping. Again by induction on $L(a)$ we will show that there is a (unique) homomorphism $\varphi: \mathbf{H} \rightarrow \mathbf{G}$ which is an extension of λ . First we put $\varphi(b) = \lambda(b)$ if $b \in B$. Assume that, for any $x \in H$ such that $L(x) \leq k$, $\varphi(x) \in G$ is well defined, and if $x = uv$, then $\varphi(x) = \varphi(u)\varphi(v)$. Let $t \in H$ be such that $L(t) = k + 1$. Then t is a product, $t = uv$, where $L(u), L(v) \leq k$; and, there exist at most two distinct such pairs. Then we can put $\varphi(t) = \varphi(u)\varphi(v)$. If $t = x^2 = yz$, where $y \neq z$, then, by (iv), there exist u, v such that: $x = uv, y = u^2, z = v^2$, and thus:

$$\begin{aligned} \varphi(x^2) &= \varphi(x)\varphi(x) = (\varphi(u)\varphi(v))^2 = \varphi(u)^2\varphi(v)^2 = \varphi(u^2)\varphi(v^2) = \\ &= \varphi(y)\varphi(z). \end{aligned}$$

Thus $\varphi(t) \in G$ is well defined. Moreover, we have $\varphi(uv) = \varphi(u)\varphi(v)$, for each u, v such that $L(uv) \leq k + 1$. So, there exists a homomorphism $\varphi: \mathbf{H} \rightarrow \mathbf{G}$ which is an extension of λ . \square

The additive groupoid of positive integers belongs to \mathcal{V} , and this implies:

Proposition 2.4. If \mathbf{H} is a \mathcal{V} -free groupoid with the basis B , then there exists a (unique) mapping $x \mapsto |x|$ from \mathbf{H} into the set of positive integers such that:

$$|b| = 1; \quad |xy| = |x| + |y|, \quad (2.2)$$

for each $b \in B, x, y \in H$. (We say that $|x|$ is the **norm** of x .) \square

Now we will show the following:

Proposition 2.5. Every \mathcal{V} -free groupoid \mathbf{H} is a cancellative groupoid.

Proof. First we will show that:

$$x \neq y \Rightarrow x^2 \neq xy, x^2 \neq yx. \quad (2.3)$$

Namely, (2.3) is clear if $x, y \in B$. Assume that $x, y \in H$ are such that $x \neq y$, $x^2 = xy$ and $|x|$ is the least possible. Then, by (iv), there exist $u, v \in H$ such that $x = uv, x = u^2, y = v^2, u \neq v$. Therefore $u^2 = uv, u \neq v$ and $|u| < |x|$.

By symmetry, $x \neq y \Rightarrow x^2 \neq yx$.

Let $xy = xz$ (or $yx = zx$). If $x \neq y$, $x \neq z$, then by (iii): $y = z$. If $x = y$, then: $x^2 = xz \Rightarrow x = z$. Thus:

$$xy = xz \text{ or } yx = zx \Rightarrow y = z, \quad (2.4)$$

i.e. \mathbf{H} is cancellative. \square

Below we assume that \mathbf{H} is a given \mathcal{V} -free groupoid.

As a consequence of (i) we obtain:

Corollary 2.6. For every $k \geq 0$, the mapping $x \mapsto x^{(k)}$ is injective. \square

As in (0.2), the equality $x = y^{(-k)}$ is equivalent with $y = x^{(k)}$, where $k \geq 0$. Thus, for every $x \in H$, there exists the largest nonnegative integer m such that $x^{(-m)} \in H$; it will be denoted by $[x]$. Therefore, we have a mapping $x \mapsto [x]$ from H into the set of nonnegative integers. It can be easily seen that if we replace F by H in (1.2)–(1.5) we obtain relations which hold in a \mathcal{V} -free groupoid \mathbf{H} . Moreover, we obtain the following property which is an "extension" of *L. 1.2*.

Proposition 2.7. If $x, y \in H$ and m are such that $[x] + m \geq 0$, $[y] + m \geq 0$, then $[xy] + m \geq 0$ and:

$$(xy)^{(m)} = x^{(m)} y^{(m)}. \quad \square$$

We note that:

$$x, y \in H \Rightarrow [xy] = \min\{[x], [y]\}. \quad (2.5)$$

Remark. *Th. 2* could be stated in a weaker form; i.e. without the assumption $\mathbf{H} \in \mathcal{V}$, replacing (iv) by:

$$(iva) \quad x^2 = yz, \quad y \neq z \Leftrightarrow (\exists u, v) \quad x = uv, \quad y = u^2, \quad z = v^2, \quad u \neq v.$$

3. Subgroupoids of \mathcal{V} -free groupoids

Below we assume that \mathbf{H} is a given \mathcal{V} -free groupoid with the basis B , and \mathbf{Q} is a subgroupoid of \mathbf{H} with the carrier Q .

From *Th. 2* one obtains:

Proposition 3.1. $\mathbf{Q} \in \mathcal{V}$ and it satisfies the conditions (i), (ii) and (iii) in *Th. 2*. \square

Proposition 3.2. The set of primes in \mathbf{Q} is nonempty and it is the least generating subset of \mathbf{Q} . \square