

Foundations of the Theory of Groupoids and Groups

12. Basic notions relative to groupoids

In: Otakar Borůvka (author): Foundations of the Theory of Groupoids and Groups. (English). Berlin: VEB Deutscher Verlag der Wissenschaften, 1974. pp. 94--100.

Persistent URL: <http://dml.cz/dmlcz/401551>

Terms of use:

© VEB Deutscher Verlag der Wissenschaften, Berlin

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

3. In 11.3 b, the set G may consist only of the numbers $0, \dots, n - 1$. Construct the appropriate multiplication tables if $n = 1, 2, 3, 4, 5$.
4. If the positive integers a, b are less than or equal to a positive integer $n \geq 5$, then the number of the prime factors of the number $10a + b$ is $\leq n$. Hence a multiplication in the set G , consisting of the numbers $1, 2, \dots, n$, can be defined as follows: The product $a \cdot b$ of an element $a \in G$ and an element $b \in G$ is the number of the prime factors of $10a + b$. The reader may verify that, for $n = 6$, the corresponding table is

	1	2	3	4	5	6
1	1	3	1	2	2	4
2	2	2	1	4	2	2
3	1	5	2	2	2	4
4	1	3	1	3	3	2
5	2	3	1	4	2	4
6	1	2	3	6	2	3

5. In the system of all the subsets of a nonempty set the multiplication can be defined by associating, with each ordered pair of subsets, their sum. May the multiplication be similarly defined by means of intersection?
6. Find some other examples of multiplication in sets.

12. Basic notions relative to groupoids

12.1. Definition

A nonempty set G together with a multiplication \mathbf{M} in G is called a *groupoid*. G is the *field* and \mathbf{M} the *multiplication of or in the groupoid*. The groupoids will generally be denoted by German capitals corresponding to the Latin capitals used for their fields. Thus, for a groupoid whose field is denoted by G , we use the notation \mathfrak{G} ; if a groupoid is denoted by \mathfrak{G} , then G generally stands for its field.

12.2. Further notions. The groupoids $\mathfrak{3}$, $\mathfrak{3}_n$, \mathfrak{S}_n

To groupoids we may apply the notions and symbols defined for their fields. So we speak, for example, about elements of a groupoid instead of elements of the field of a groupoid and write $a \in \mathfrak{G}$ instead of $a \in G$; we speak about subsets of a groupoid and write, e.g., $A \subset \mathfrak{G}$ or $\mathfrak{G} \supset A$, we speak about decompositions in a groupoid and on a groupoid, about the order of a groupoid, a mapping of a group-

oid into a certain set, into a certain groupoid or onto a groupoid, etc. A nonempty subset of a groupoid is also called a *complex*. If G is an abstract set, then the groupoid \mathcal{G} is called *abstract*.

The notions and symbols defined for multiplication apply to groupoids as well. Thus, in particular, every two-membered sequence of elements $a, b \in \mathcal{G}$ has a well determined product $a \cdot b$, briefly ab ; if for each $a, b \in \mathcal{G}$ there holds $ab = ba$, then the groupoid is called *commutative* or *Abelian*. With every finite groupoid we can also associate a multiplication table describing the multiplication in \mathcal{G} . In 11.3 we have given several examples of multiplication; each of them simultaneously applies to a groupoid.

In what follows we shall often refer to three groupoids denoted by $\mathfrak{Z}, \mathfrak{Z}_n, \mathfrak{S}_n$: \mathfrak{Z} consists of the set Z of all integers and its multiplication is defined by the usual addition (11.3a). \mathfrak{Z}_n consists of the set $Z = \{0, \dots, n - 1\}$ where n is a positive integer and the multiplication is defined by addition modulo n (11.3b). The groupoid \mathfrak{S}_n consists of the set S_n formed by all permutations of a finite set H of order n (≥ 1) and the multiplication is defined by the composition of permutations. Any groupoid whose elements are permutations of a (finite or infinite) set and the multiplication is defined by composing permutations is called a *permutation groupoid*, e.g., the groupoid \mathfrak{S}_n .

12.3. Interchangeable subsets

Let \mathcal{G} denote (throughout the book) a groupoid.

Suppose A, B are subsets of \mathcal{G} . The subset of \mathcal{G} consisting of the products ab of each element $a \in A$ and each element $b \in B$ is called the *product of the subsets A and B* ; notation: $A \cdot B$ or AB . If any of the subsets A, B is empty, then the symbols $A \cdot B, AB$ denote the empty set. For $a \in \mathcal{G}$ we generally write aA instead of $\{a\}A$ and, similarly, Aa instead of $A\{a\}$; for example, aA denotes the set of all the products of a and each element of A or, if $A = \emptyset$, the empty set. Instead of AA we sometimes write, briefly, A^2 .

If $AB = BA$, then the subsets A, B are called *interchangeable*. In that case the product of any element $a \in A$ and any element $b \in B$ is the product of an element $b' \in B$ and an element $a' \in A$; simultaneously, the product of any element $b \in B$ and any element $a \in A$ is the product of an element $a' \in A$ and an element $b' \in B$. If \mathcal{G} is Abelian, then, of course, every two subsets of \mathcal{G} are interchangeable. In the opposite case there holds, for some elements $a, b \in \mathcal{G}$, the inequality $ab \neq ba$, hence every two subsets $A, B \subset \mathcal{G}$ need not be interchangeable, for example, if $A = \{a\}, B = \{b\}$. The product AB of the subset $A = \{1\}$ and the subset $B = \{\dots, -2, 0, 2, \dots\}$ of the groupoid \mathfrak{Z} is $\{\dots, -1, 1, 3, \dots\}$ and, evidently, equals the product BA ; if $A = \{0, 1\}, B = \{\dots, -2, 0, 2, \dots\}$, then we have $AB = BA = Z$. Note that for every groupoid \mathcal{G} the relation $\mathcal{G}\mathcal{G} \subset \mathcal{G}$ is true.

12.4. Subgroupoids, supergroupoids, ideals

Suppose A stands for a certain complex in \mathfrak{G} . If $AA \subset A$, that is to say, if the product of any $a \in A$ and $b \in A$ is again an element of A , then A is said to be a *groupoidal subset* of \mathfrak{G} . In that case the multiplication M in \mathfrak{G} determines a, so-called *partial multiplication* M_A in A , defined as follows: M_A associates, with any two-membered sequence of elements $a, b \in A$, the same product $ab \in A$ as the multiplication M . The set A together with the partial multiplication M_A is a groupoid \mathfrak{A} . We say that \mathfrak{A} is a *subgroupoid* of \mathfrak{G} and \mathfrak{G} a *supergroupoid* of \mathfrak{A} and we write: $\mathfrak{A} \subset \mathfrak{G}$ or $\mathfrak{G} \supset \mathfrak{A}$. If A is a proper subset of \mathfrak{G} , then \mathfrak{A} is said to be a *proper subgroupoid* of \mathfrak{G} and \mathfrak{G} a *proper supergroupoid* of \mathfrak{A} . \mathfrak{G} always contains the *greatest subgroupoid*, identical with itself.

If even $GA \subset A$ (or $AG \subset A$ or, simultaneously, $GA \subset A \supset AG$), then \mathfrak{A} is called a *left* (or a *right* or a *bilateral*) *ideal* of \mathfrak{G} . The case of $A \neq G$ is again characterized by the attribute: *proper*.

For example, the complex of \mathfrak{Z} , consisting of all integer multiples of a given positive integer m , is groupoidal because the product (i.e., the sum in the usual sense) of any two integer multiples of m is again an integer multiple of m ; this complex together with addition in the usual sense is therefore a subgroupoid of \mathfrak{Z} ; in case of $m > 1$ it is obviously a proper subgroupoid of \mathfrak{Z} . Another example: The subset of all elements of \mathfrak{S}_n that leave a given element $a \in H$ invariant is groupoidal because, if any two permutations $\mathbf{p}, \mathbf{q} \in \mathfrak{S}_n$ do not change the element a , then the same, naturally, holds for their product $\mathbf{p} \cdot \mathbf{q}$ (i.e., for the composite permutation \mathbf{qp}); this subset, together with the composition of permutations in the usual sense, is therefore a subgroupoid of \mathfrak{S}_n .

It is easy to see that for any groupoids $\mathfrak{A}, \mathfrak{B}, \mathfrak{G}$ there evidently hold the following statements:

If \mathfrak{B} is a subgroupoid of \mathfrak{A} and \mathfrak{A} a subgroupoid of \mathfrak{G} , then \mathfrak{B} is a subgroupoid of \mathfrak{G} .

If $\mathfrak{A}, \mathfrak{B}$ are subgroupoids of \mathfrak{G} and for their fields A, B there holds $B \subset A$, then \mathfrak{B} is a subgroupoid of \mathfrak{A} .

12.5. Further notions

Since we apply to groupoids the notions and symbols we have defined for their fields, we sometimes speak, e.g., about the intersection of a subset $B \subset \mathfrak{G}$ and a subgroupoid $\mathfrak{A} \subset \mathfrak{G}$ in the sense of the intersection of the subset B and the field A of \mathfrak{A} ; analogously, we speak about the product of a subset B and a subgroupoid \mathfrak{A} , about the product of a subgroupoid \mathfrak{A} and a subset B , about the closure of a subgroupoid \mathfrak{A} in a certain decomposition \bar{A} , about the intersection of \bar{A} and a subgroupoid \mathfrak{A} , etc; notation, e.g., $B \cap \mathfrak{A}$ or $\mathfrak{A} \cap B$, $B\mathfrak{A}$, $\mathfrak{A}B$, $\mathfrak{A} \sqsubset \bar{A}$ or $\bar{A} \supset \mathfrak{A}$, $\bar{A} \cap \mathfrak{A}$ or $\mathfrak{A} \cap \bar{A}$, etc.

12.6. The intersection of groupoids

Let us now consider two subgroupoids $\mathfrak{A}, \mathfrak{B} \subset \mathfrak{G}$ and suppose the intersection $A \cap B$ of their fields A, B is not empty, $A \cap B \neq \emptyset$. For any elements $a, b \in A \cap B$ there holds $ab \in AA \subset A$, on the one hand, and $ab \in BB \subset B$, on the other hand, and so $ab \in A \cap B$; hence $A \cap B$ is a groupoidal subset of \mathfrak{G} . The corresponding subgroupoid of \mathfrak{G} is called the *intersection of \mathfrak{A} and \mathfrak{B}* and denoted by $\mathfrak{A} \cap \mathfrak{B}$ or $\mathfrak{B} \cap \mathfrak{A}$. We observe that any two subgroupoids of \mathfrak{G} whose fields are incident have an intersection which is a subgroupoid of \mathfrak{G} . This intersection is, of course, a subgroupoid of either of the two subgroupoids. Note that the concept of the intersection of two subgroupoids of \mathfrak{G} is defined only if the fields of both subgroupoids have common elements. There exists, for example, the intersection of the subgroupoids $\mathfrak{A}, \mathfrak{B} \subset \mathfrak{S}_n$ where the field A of \mathfrak{A} consists of all the elements of \mathfrak{S}_n that do not change a certain element $a \in H$, whereas the field B of \mathfrak{B} consists of all the elements of \mathfrak{S}_n that do not change a certain element $b \in H$, as both A and B have at least one common element, namely, the identical permutation of H which does not change any of the elements of H .

The concept of the intersection of two subgroupoids of \mathfrak{G} may easily be extended to the intersection of a system of subgroupoids of \mathfrak{G} : If we have a system $\{a_1, a_2, \dots\}$ of subgroupoids of \mathfrak{G} and the intersection of their fields is not empty, then this intersection is a groupoidal subset of \mathfrak{G} ; the corresponding groupoid of \mathfrak{G} is called the intersection of the system of subgroupoids $\{a_1, a_2, \dots\}$ and denoted $a_1 \cap a_2 \cap \dots$, briefly, $\cap a$ or similarly.

12.7. Product of a finite sequence of elements

1. *Definition.* Consider an n -membered sequence of elements $a_1, \dots, a_n \in \mathfrak{G}$, where $n \geq 2$. What do we mean by the product of this sequence? The product of a two-membered sequence a_1, a_2 ($n = 2$) has already been defined and denoted $a_1 \cdot a_2$ or $a_1 a_2$. The product of a three-membered sequence a_1, a_2, a_3 ($n = 3$) is defined as follows: It is the set consisting of the so-called product-elements: $a_1(a_2 a_3)$, $(a_1 a_2)a_3$. This product is denoted by $\{a_1 \cdot a_2 \cdot a_3\}$ or $\{a_1 a_2 a_3\}$; the symbol $a_1 \cdot a_2 \cdot a_3$ or $a_1 a_2 a_3$ stands for any of the product-elements so that it denotes the product of a_1 and $a_2 a_3$ as well as the product of $a_1 a_2$ and a_3 . The product of a four-membered sequence a_1, a_2, a_3, a_4 ($n = 4$) is the set consisting of the three product-elements $a_1(a_2 a_3 a_4)$, $(a_1 a_2)(a_3 a_4)$, $(a_1 a_2 a_3)a_4$. It is denoted by $\{a_1 \cdot a_2 \cdot a_3 \cdot a_4\}$ or $\{a_1 a_2 a_3 a_4\}$; the symbol $a_1 \cdot a_2 \cdot a_3 \cdot a_4$ or $a_1 a_2 a_3 a_4$ stands for any of the product-elements so that it denotes any of the elements: $a_1(a_2(a_3 a_4))$, $a_1((a_2 a_3)a_4)$, $(a_1 a_2)(a_3 a_4)$, $(a_1(a_2 a_3))a_4$, $((a_1 a_2)a_3)a_4$. From these examples we can understand the following definition:

The *product of an n -membered sequence of elements a_1, a_2, \dots, a_n* is the set $\{a_1, a_2, \dots, a_n\}$ defined as follows: If $n = 2$, then the set $\{a_1, a_2\}$ consists of one single ele-

ment $a_1 a_2$; if $n > 2$, then it is defined by the formula

$$\{a_1 a_2 \dots a_n\} = \{a_1\} \{a_2 \dots a_n\} \cup \{a_1 a_2\} \{a_3 \dots a_n\} \cup \dots \cup \{a_1 \dots a_{n-1}\} \{a_n\}.$$

Sometimes we also use the notation $\{a_1 \cdot a_2 \dots a_n\}$. The individual elements of this set, the so-called *product-elements*, are denoted by the symbol $a_1 \cdot a_2 \dots a_n$ or $a_1 a_2 \dots a_n$. Naturally, there exists only a finite number of product-elements. If $n = 2$, then we generally do not draw any difference between the product and the corresponding product-element.

2. *Associative groupoids.* From what we have said in the preceding paragraph it follows that every three-membered sequence of elements $a_1, a_2, a_3 \in \mathfrak{G}$ has, at most, two different product-elements: $a_1(a_2 a_3)$, $(a_1 a_2)a_3$. If they always coincide, i.e., if for any three elements $a_1, a_2, a_3 \in \mathfrak{G}$ there holds $a_1(a_2 a_3) = (a_1 a_2)a_3$, then the multiplication in \mathfrak{G} as well as the groupoid itself is called *associative*.

The groupoids that have most been studied in mathematics have the property that every finite sequence of their elements has only one product-element; as we shall show later (18.1), it is exactly the associative groupoids that have this remarkable property.

The groupoid \mathfrak{Z} , for example, is associative because, by the definition of its multiplication, the product-elements $a(bc)$, $(ab)c$ of any three-membered sequence of the elements $a, b, c \in \mathfrak{Z}$ are sums in the usual sense $a + (b + c)$, $(a + b) + c$ and therefore equal.

Analogously, even the groupoid \mathfrak{Z}_n ($n \geq 1$) is associative. Indeed, by the definition of its multiplication, the product-elements $a(bc)$, $(ab)c$ of any three-membered sequence of elements $a, b, c \in \mathfrak{Z}_n$ are the remainders of the division of the numbers $a + r$, $s + c$ by n , r (s) denoting the remainder of the division of $b + c$ ($a + b$) by n . Since $a + r$ and $a + (b + c)$ differ only by an integer multiple of n , $a(bc)$ is the remainder of the division of $a + (b + c)$ by n ; analogously, $(ab)c$ is the remainder of the division of $(a + b) + c$ by n . From $a + (b + c) = (a + b) + c$ there follows $a(bc) = (ab)c$.

The groupoid \mathfrak{S}_n ($n \geq 1$) is associative as well because, if $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are arbitrary elements of \mathfrak{S}_n , then, by the definition of the multiplication in \mathfrak{S}_n , the product-elements $\mathbf{p} \cdot (\mathbf{q} \cdot \mathbf{r})$, $(\mathbf{p} \cdot \mathbf{q}) \cdot \mathbf{r}$ are composite permutations $(\mathbf{r}\mathbf{q})\mathbf{p}$, $\mathbf{r}(\mathbf{q}\mathbf{p})$ and, with respect to the results in 8.7.3, equal.

3. *Example.* To illustrate the process of determining a product, let us find the product $\{1 \cdot 2 \cdot 3 \cdot 4\}$ in the groupoid described in 11.5.4. By the appropriate multiplication table we have

$$\begin{aligned} \{1 \cdot 2 \cdot 3\} &= \{1\} \cdot \{2 \cdot 3\} \cup \{1 \cdot 2\} \cdot \{3\} = \{1\} \cdot \{1\} \cup \{3\} \cdot \{3\} \\ &= \{1\} \cup \{2\} = \{1, 2\}; \\ \{2 \cdot 3 \cdot 4\} &= \{2\} \cdot \{3 \cdot 4\} \cup \{2 \cdot 3\} \cdot \{4\} = \{2\} \cdot \{2\} \cup \{1\} \cdot \{4\} \\ &= \{2\} \cup \{2\} = \{2\}; \end{aligned}$$

$$\begin{aligned} \{1 \cdot 2 \cdot 3 \cdot 4\} &= \{1\} \cdot \{2 \cdot 3 \cdot 4\} \cup \{1 \cdot 2\} \cdot \{3 \cdot 4\} \cup \{1 \cdot 2 \cdot 3\} \cdot \{4\} \\ &= \{1\} \cdot \{2\} \cup \{3\} \cdot \{2\} \cup \{1, 2\} \cdot \{4\} = \{3\} \cup \{5\} \cup \{2, 4\} \\ &= \{2, 3, 4, 5\}. \end{aligned}$$

All the product-elements $1 \cdot 2 \cdot 3 \cdot 4$ are therefore 2, 3, 4, 5.

12.8. The product of a finite sequence of subsets

1. *Definition.* Now let A_1, \dots, A_n ($n \geq 2$) stand for arbitrary subsets of \mathcal{G} .

The *product of the n -membered sequence of subsets* A_1, A_2, \dots, A_n is the sum of all the products $\{a_1 a_2 \dots a_n\}$, the elements $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ running over all the elements of the corresponding subsets A_1, A_2, \dots, A_n . We denote it by $A_1 \cdot A_2 \dots A_n$ or $A_1 A_2 \dots A_n$. If any of the subsets A_1, \dots, A_n is empty, then the product in question is defined as the empty set. By the above definition and the meaning of the symbol $\{a_1 \dots a_n\}$, each element $a \in A_1 A_2 \dots A_n$ is the result of the multiplication of a product-element $a_1 \dots a_k$ and one of the elements $a_{k+1} \dots a_n$ where $1 \leq k \leq n - 1$; hence

$$a \in (A_1 \dots A_k) (A_{k+1} \dots A_n).$$

Conversely, the product of any element of the set $A_1 \dots A_k$ and any element $A_{k+1} \dots A_n$ is an element $a \in A_1 \dots A_n$. So we have

$$A_1 \dots A_n = A_1 (A_2 \dots A_n) \cup (A_1 A_2) (A_3 \dots A_n) \cup \dots \cup (A_1 \dots A_{n-1}) A_n.$$

If A denotes a subset of \mathcal{G} , then we write A^n instead of $\underbrace{A \dots A}_n$ so that, for $n \geq 2$, we have

$$A^n = A A^{n-1} \cup A^2 A^{n-2} \cup \dots \cup A^{n-1} A.$$

The above definitions of the product of a finite sequence of elements or sets obviously generalize the definitions of the product of a two-membered sequence of elements or sets, respectively.

2. *Example.* Let A denote the subset $\{1, 2, 4\}$ of the groupoid described in 11.5.4. Then:

$$\begin{aligned} A^2 &= \{1, 2, 4\} \cdot \{1, 2, 4\} \\ &= \{1 \cdot 1, 1 \cdot 2, 1 \cdot 4, 2 \cdot 1, 2 \cdot 2, 2 \cdot 4, 4 \cdot 1, 4 \cdot 2, 4 \cdot 4\} \\ &= \{1, 2, 3, 4\}; \\ A^3 &= \{1, 2, 4\} \cdot \{1, 2, 3, 4\} \cup \{1, 2, 3, 4\} \cdot \{1, 2, 4\} \\ &= \{1, 2, 3, 4, 5\}; \\ A^4 &= \{1, 2, 4\} \cdot \{1, 2, 3, 4, 5\} \cup \{1, 2, 3, 4\} \cdot \{1, 2, 3, 4\} \\ &\quad \cup \{1, 2, 3, 4, 5\} \cdot \{1, 2, 4\} \\ &= \{1, 2, 3, 4, 5\}. \end{aligned}$$

12.9. Exercises

1. If $A \subset \mathcal{G}$ and $B \subset \mathcal{G}$ are the sums of some subsets $\bar{a}_1, \bar{a}_2, \dots$ and $\bar{b}_1, \bar{b}_2, \dots$, respectively, then AB is the sum of the products of each subset $\bar{a}_1, \bar{a}_2, \dots$ and each $\bar{b}_1, \bar{b}_2, \dots$.
2. If the subsets $A \subset \mathcal{G}$ and $B \subset \mathcal{G}$ are the intersections of some subsets $\bar{a}_1, \bar{a}_2, \dots$ and $\bar{b}_1, \bar{b}_2, \dots$, respectively, then AB is a part of the intersection of the products of each subset $\bar{a}_1, \bar{a}_2, \dots$ and each $\bar{b}_1, \bar{b}_2, \dots$. Thus for any subsets $A, B, C \subset \mathcal{G}$ there hold, in particular, the relations: a) $(A \cap B)C \subset AC \cap BC$; b) $C(A \cap B) \subset CA \cap CB$. Give suitable examples to show that the symbol \subset can, in these relations, not always be replaced by $=$.
3. Show that the number N_n of the product-elements of an n -membered sequence of elements of \mathcal{G} ($n \geq 2$) is expressed, in general, by the formula $N_n = (2n - 2)!/(n - 1)!n!$
4. Let A stand for a subset of \mathcal{G} and m, n denote arbitrary positive integers. Then the following relations are true: a) $A^m A^n \subset A^{m+n}$; b) $(A^m)^n \subset A^{mn}$.
5. Suppose $A \subset B$ are subsets of \mathcal{G} and n denotes an arbitrary positive integer. There holds $A^n \subset B^n$.
6. Let n be an arbitrary positive integer. For the field G of \mathcal{G} there holds the relation $G^n \supset G^{n+1}$ so that $G \supset G^2 \supset G^3 \supset \dots$.
7. Let G, n be the same as in Exercise 6. G^n is a groupoidal subset of \mathcal{G} and the corresponding subgroupoid of \mathcal{G} is a bilateral ideal. — Remark. The latter is denoted by \mathcal{G}^n .
8. If \mathcal{G} is an associative groupoid, then: a) every subgroupoid of \mathcal{G} is associative; b) for any subsets $A, B, C \subset \mathcal{G}$ there holds $A(BC) = (AB)C$.
9. If \mathcal{G} is an associative groupoid and A, B are groupoidal and interchangeable subsets of \mathcal{G} , then the subset AB is groupoidal as well. — Remark. If $\mathfrak{A}, \mathfrak{B}$ are interchangeable subgroupoids of \mathcal{G} , then the subgroupoid of \mathcal{G} , corresponding to the product of their fields, is called the *product of the subgroupoids* $\mathfrak{A}, \mathfrak{B}$ and denoted by $\mathfrak{A}\mathfrak{B}$ or $\mathfrak{B}\mathfrak{A}$.
10. If \mathcal{G} is an associative groupoid, then the set of all the elements of \mathcal{G} that are interchangeable with each element of \mathcal{G} is groupoidal unless it is empty. — Remark. The corresponding subgroupoid of \mathcal{G} is called the *center of* \mathcal{G} .
11. Suppose \mathcal{G} is a groupoid whose field consists of all positive integers, and the multiplication is defined, as follows: The product of any element $a \in \mathcal{G}$ and any element $b \in \mathcal{G}$ is the least common multiple or the greatest common divisor of the numbers a and b . Show that in both cases \mathcal{G} is Abelian and associative.