18. Remarkable kinds of groupoids

In: Otakar Borůvka (author): Foundations of the Theory of Groupoids and Groups. (English). Berlin: VEB Deutscher Verlag der Wissenschaften, 1974. pp. 131--145.

Persistent URL: http://dml.cz/dmlcz/401557

and, moreover, for $\gamma, \mu = 1, \ldots, \alpha + 1$; $\delta, \nu = 1, \ldots, \beta + 1$,

$$\mathring{\mathfrak{A}}_{\gamma,\nu} = [\overline{\mathfrak{A}}_\gamma, (\overline{\mathfrak{A}}_{\gamma-1}, \overline{\mathfrak{B}}_\nu)] = (\overline{\mathfrak{A}}_{\gamma-1}, [\overline{\mathfrak{A}}_\gamma, \overline{\mathfrak{B}}_\nu]),$$

$$\mathring{\mathfrak{B}}_{\delta,\mu} = [\overline{\mathfrak{B}}_\delta, (\overline{\mathfrak{B}}_{\delta-1}, \overline{\mathfrak{A}}_\mu)] = (\overline{\mathfrak{B}}_{\delta-1}, [\overline{\mathfrak{B}}_\delta, \overline{\mathfrak{A}}_\mu]).$$

Then the above co-basally loosely joint refinements of $(\overline{\mathfrak{A}})$, $(\overline{\mathfrak{B}})$ *are expressed by the following formulae*:

$$\begin{aligned}(\mathring{\mathfrak{A}}) =) \ \overline{\mathfrak{U}} &= \mathring{\mathfrak{A}}_{1,1} \geqq \cdots \geqq \mathring{\mathfrak{A}}_{1,\beta+1} \geqq \mathring{\mathfrak{A}}_{2,1} \geqq \cdots \geqq \mathring{\mathfrak{A}}_{2,\beta+1} \geqq \cdots \\ &\geqq \mathring{\mathfrak{A}}_{\alpha+1,1} \geqq \cdots \geqq \mathring{\mathfrak{A}}_{\alpha+1,\beta+1} = \overline{\mathfrak{B}}, \\ (\mathring{\mathfrak{B}}) =) \ \overline{\mathfrak{U}} &= \mathring{\mathfrak{B}}_{1,1} \geqq \cdots \geqq \mathring{\mathfrak{B}}_{1,\alpha+1} \geqq \mathring{\mathfrak{B}}_{2,1} \geqq \cdots \geqq \mathring{\mathfrak{B}}_{2,\alpha+1} \geqq \cdots \\ &\geqq \mathring{\mathfrak{B}}_{\beta+1,1} \geqq \cdots \geqq \mathring{\mathfrak{B}}_{\beta+1,\alpha+1} = \overline{\mathfrak{B}}\end{aligned}$$

If $(\overline{\mathfrak{A}})$, $(\overline{\mathfrak{B}})$ *are complementary, then the refinements* $(\mathring{\mathfrak{A}})$, $(\mathring{\mathfrak{B}})$ *are co-basally joint.*

The correctness of this theorem follows from 10.7, 10.8.

17.7. Exercises

1. If any two factoroids lying on $\mathfrak{G}$ are complementary, then any two series of factoroids on $\mathfrak{G}$ have co-basally joint refinements.

18. Remarkable kinds of groupoids

The study of some remarkable kinds of groupoids closely ties up with our considerations in chapter 11.2. We have not dealt with them before because we wish to emphasize that the preceding deliberations apply to all groupoids regardless of any particular properties. Now we shall be concerned with the groupoids that are of most importance to our theory, namely, the associative groupoids, the groupoids with uniquely defined division and the groupoids with a unit element.

Moreover, we shall pay a brief attention to the Brandt groupoids though they do not belong exactly within the range of our study.

18.1. Associative groupoids (semigroups)

1. *Definition.* The concept of an associative groupoid $\mathfrak{G}$ has already been determined in 12. 7. 2 by the property that *any three-membered sequence of elements of* $\mathfrak{G}$ *has only one product element*; that is to say, for any three elements $a_1, a_2, a_3 \in \mathfrak{G}$ there holds $a_1(a_2a_3) = (a_1a_2)a_3$. Associative groupoids are also called *semigroups.*

2. *The fundamental theorem of semigroups.* Now we shall show that *any associative groupoid* $\mathfrak{G}$ *has the property that every n-membered* ($n \geqq 2$) *sequence of elements of* $\mathfrak{G}$ *has only one product element,* i.e., the symbol $a_1 \dots a_n$ denotes, for $a_1, \dots, a_n \in \mathfrak{G}$ ($n \geqq 2$), exactly one element of $\mathfrak{G}$.

Let us consider an arbitrary associative groupoid and proceed by the method of complete induction. Our statement is correct if $n = 2$, for, in that case, it immediately follows from the definition of the multiplication in $\mathfrak{G}$. It remains to be shown that: if our statement applies to every, at most, $(n-1)$-membered sequence of elements of $\mathfrak{G}$, n being a positive integer > 2, then it also holds for every n-membered sequence of elements of $\mathfrak{G}$.

Let $n > 2$. Suppose our statement holds for every, at most, $(n-1)$-membered sequence of elements of $\mathfrak{G}$. Consider n arbitrary elements $a_1, \dots, a_n \in \mathfrak{G}$.

Then every symbol

$$a_1, a_2 \dots a_n, a_1a_2, a_3 \dots a_n, \dots, a_1 \dots a_{n-1}, a_n$$

denotes exactly one element of $\mathfrak{G}$ because, by our assumption, there exists, for example, only one product element $a_2 \dots a_n$ of the $(n-1)$-membered sequence $a_2, \dots, a_n \in \mathfrak{G}$. Our object now is to show that all the elements

$$a_1(a_2 \dots a_n),\ (a_1a_2)\,(a_3 \dots a_n),\ \dots,\ (a_1 \dots a_{n-1})a_n \tag{1}$$

are equal. To that end let us, first, note that each of these elements is the product $(a_1 \dots a_k)\,(a_{k+1} \dots a_n)$ of the elements $a_1 \dots a_k, a_{k+1} \dots a_n \in \mathfrak{G}$, k being one of the numbers $1, \dots, n-1$. In order to prove our statement we must verify that each of the elements (1) is equal to, e.g., $a_1(a_2 \dots a_n)$; that is to say, for every $k = 1, \dots, n-1$ there holds

$$(a_1 \dots a_k)\,(a_{k+1} \dots a_n) = a_1(a_2 \dots a_n). \tag{2}$$

If $k = 1$, then this equality is obvious, hence we may restrict our attention to the case $k > 1$. In that case, $a_1 \dots a_k$ is the product element of an, at least, 2-membered and, at most, $(n-1)$-membered sequence of elements $a_1, \dots, a_k$ and is therefore, by our assumption, equal to the element $a_1(a_2 \dots a_k)$; consequently, we have

$$(a_1 \dots a_k)\,(a_{k+1} \dots a_n) = \big(a_1(a_2 \dots a_k)\big)\,(a_{k+1} \dots a_n).$$

Since $\mathfrak{G}$ is associative, the element on the right-hand side of this equality is equal to the element $a_1\big((a_2 \dots a_k)\,(a_{k+1} \dots a_n)\big)$, i.e., the element $a_1(a_2 \dots a_n)$ and we have (2), which completes the proof.

A similar result applies, of course, to finite sequences of the subsets of $\mathfrak{G}$.

3. *Effects of the fundamental theorem.* a) The uniqueness of a composite permutation. The result we have just arrived at is useful when we are to compose permutations of a (finite or infinite) set of elements. Let $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ ($n \geqq 2$) denote arbitrary permutations of a set H. What do we understand by a permutation composed of the permutations $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ (in this order)? If $n = 2$, then it is, as we know, the composite mapping $\boldsymbol{p}_2\boldsymbol{p}_1$. If $n = 3$, then the concept of a composite permutation of $\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3$ is defined as follows: By a permutation composed of $\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3$ we mean either of the permutations $\boldsymbol{p}_3(\boldsymbol{p}_2\boldsymbol{p}_1)$, $(\boldsymbol{p}_3\boldsymbol{p}_2)\boldsymbol{p}_1$; notation $\boldsymbol{p}_3\boldsymbol{p}_2\boldsymbol{p}_1$. The symbol $\boldsymbol{p}_3\boldsymbol{p}_2\boldsymbol{p}_1$ therefore stands for the permutation composed of $\boldsymbol{p}_2\boldsymbol{p}_1$, $\boldsymbol{p}_3$ as well as for the permutation composed of $\boldsymbol{p}_1, \boldsymbol{p}_3\boldsymbol{p}_2$. If $n = 4$, then a permutation composed of $\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3, \boldsymbol{p}_4$ is any of the permutations $\boldsymbol{p}_4(\boldsymbol{p}_3\boldsymbol{p}_2\boldsymbol{p}_1)$, $(\boldsymbol{p}_4\boldsymbol{p}_3)\,(\boldsymbol{p}_2\boldsymbol{p}_1)$, $(\boldsymbol{p}_4\boldsymbol{p}_3\boldsymbol{p}_2)\boldsymbol{p}_1$; it is denoted by the symbol $\boldsymbol{p}_4\boldsymbol{p}_3\boldsymbol{p}_2\boldsymbol{p}_1$ which stands for any of the following permutations of H: $\boldsymbol{p}_4\big(\boldsymbol{p}_3(\boldsymbol{p}_2\boldsymbol{p}_1)\big)$, $\boldsymbol{p}_4\big((\boldsymbol{p}_3\boldsymbol{p}_2)\boldsymbol{p}_1\big)$, $(\boldsymbol{p}_4\boldsymbol{p}_3)\,(\boldsymbol{p}_2\boldsymbol{p}_1)$, $\big(\boldsymbol{p}_4(\boldsymbol{p}_3\boldsymbol{p}_2)\big)\boldsymbol{p}_1$, $\big((\boldsymbol{p}_4\boldsymbol{p}_3)\boldsymbol{p}_2\big)\boldsymbol{p}_1$.

Generally, for $n \geqq 2$, a permutation composed of $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ is defined as follows: It is any of the permutations

$$\boldsymbol{p}_n(\boldsymbol{p}_{n-1} \cdots \boldsymbol{p}_1),\ (\boldsymbol{p}_n\boldsymbol{p}_{n-1})\,(\boldsymbol{p}_{n-2} \cdots \boldsymbol{p}_1),\ \dots,\ (\boldsymbol{p}_n \cdots \boldsymbol{p}_2)\boldsymbol{p}_1,$$

where each symbol in parentheses stands for an arbitrary permutation composed of the involved permutations and ordered from right to left. A permutation composed of $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ is denoted by $\boldsymbol{p}_n \dots \boldsymbol{p}_1$. The symbol $\boldsymbol{p}_n \dots \boldsymbol{p}_1$ therefore denotes, in accordance with the definition, a product element of the n-membered sequence of permutations $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$; the latter are elements of the groupoid consisting of all permutations of H, the multiplication being defined by the composition of permutations. By the associative law of composing permutations (8.7.3), the groupoid in question is associative and, according to the above result, *there exists only one permutation* $\boldsymbol{p}_n \dots \boldsymbol{p}_1$ *composed of* $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$. This theorem may also be expressed in terms that, if the order of composing the permutations is the same, then the composite permutation does not depend on the way of composition. Consequently, we obtain the image $\boldsymbol{p}_n \dots \boldsymbol{p}_1 x$ of any element $x \in H$ by, e.g., the formula

$$\boldsymbol{p}_n \cdots \boldsymbol{p}_1 x = \boldsymbol{p}_n\big(\boldsymbol{p}_{n-1}\big(\dots\big(\boldsymbol{p}_2(\boldsymbol{p}_1 x)\big)\dots\big)\big),$$

namely, by determining first the $\boldsymbol{p}_1$-image $\boldsymbol{p}_1 x$ of the element x, then the $\boldsymbol{p}_2$-image $\boldsymbol{p}_2(\boldsymbol{p}_1 x)$ of the element $\boldsymbol{p}_1 x$, etc. and, finally, the $\boldsymbol{p}_n$-image $\boldsymbol{p}_n\big(\boldsymbol{p}_{n-1}\big(\dots\big(\boldsymbol{p}_2(\boldsymbol{p}_1 x)\big)\dots\big)\big)$ of the element $\boldsymbol{p}_{n-1}\big(\dots\big(\boldsymbol{p}_2(\boldsymbol{p}_1 x)\big)\dots\big)$. From this it is immediately clear that if the permutations $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ leave some element $x \in H$ invariant, then the same holds for the composite permutation $\boldsymbol{p}_n \dots \boldsymbol{p}_1$.

b) The composition of a permutation of cyclic permutations. Let us make use of the above results to make a few remarks about permutations of a finite set. Suppose the set H is finite.

First we shall show that *any permutation of H is composed of a finite number of cyclic permutations whose cycles have no common elements.*

Consider a permutation $\boldsymbol{p}$ of the set H. As we know from 8.5, $\boldsymbol{p}$ is determined by a finite number of pure cyclic permutations $\boldsymbol{p}_{\bar{a}}, \ldots, \boldsymbol{p}_{\bar{m}}$, i.e., there exists a decomposition $\overline{H} = \{\bar{a}, \ldots, \bar{m}\}$ of the set H such that each of its elements $\bar{a}, \ldots, \bar{m}$ is invariant under $\boldsymbol{p}$ and the partial permutations $\boldsymbol{p}_{\bar{a}}, \ldots, \boldsymbol{p}_{\bar{m}}$ are pure cyclic permutations of the elements $\bar{a}, \ldots, \bar{m}$. Let $\bar{x}$ be an arbitrary element of $\overline{H}$ and $\boldsymbol{q}_{\bar{x}}$ the cyclic permutation of H that maps every element $x \in \bar{x}$ onto $\boldsymbol{p}_{\bar{x}}x$ and leaves all the other elements of H, if there are any, invariant. The cyclic permutation $\boldsymbol{q}_{\bar{x}}$ has therefore the same cycle as the pure cyclic permutation $\boldsymbol{p}_{\bar{x}}$ and so both $\boldsymbol{q}_{\bar{x}}$ and $\boldsymbol{p}_{\bar{x}}$ may be expressed by the same simplified symbol. To prove our statement we shall verify that the permutation $\boldsymbol{p}$ is composed of the cyclic permutations $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$, i.e., $\boldsymbol{p} = \boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}$.

Let x denote an arbitrary element of H and $\bar{x}$ the element of $\overline{H}$ containing x so that the permutation $\boldsymbol{q}_{\bar{x}}$ maps x onto the element $\boldsymbol{q}_{\bar{x}}x$ but all the other permutations $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$, if there are any, leave the element x invariant. Since the composite permutation does not depend, for the same ordering, on the way of composition, we have $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = (\boldsymbol{q}_{\bar{m}} \ldots)\boldsymbol{q}_{\bar{x}} (\ldots \boldsymbol{q}_{\bar{a}})x$; then of course, for $\bar{x} = \bar{m}$ and $\bar{x} = \bar{a}$, the symbols of the composite permutation, written in the first and the second parentheses, respectively, are left out. For $\bar{x} \neq \bar{a}$ we have $(\ldots \boldsymbol{q}_{\bar{a}})x = x$, since all the permutations of which $(\ldots \boldsymbol{q}_{\bar{a}})$ is composed leave the element x invariant. So we have, first, $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = (\boldsymbol{q}_{\bar{m}} \ldots)\boldsymbol{q}_{\bar{x}}x$. In a similar way we realize that the element on the right-hand side of this equation is $\boldsymbol{q}_{\bar{x}}x$, and so $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = \boldsymbol{q}_{\bar{x}}x$. By the definition of $\boldsymbol{q}_{\bar{x}}$ there holds $\boldsymbol{q}_{\bar{x}}x = \boldsymbol{p}_{\bar{x}}x$ and, furthermore, according to the definition of $\boldsymbol{p}_{\bar{x}}$ there is $\boldsymbol{p}_{\bar{x}}x = \boldsymbol{p}x$. So we have $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = \boldsymbol{p}x$ and the proof is complete.

Note that in the formula $\boldsymbol{p} = \boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}$ the order of the permutations $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$ may be arbitrarily changed because, for every arrangement of $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$, we may choose such a notation of the elements of $\overline{H}$ that the formula remains the same.

If we have any permutations $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ ($n \geqq 2$) of H expressed by two-rowed or simplified symbols, then the composite permutation $\boldsymbol{p}_n \ldots \boldsymbol{p}_1$ is expressed by writing the symbols of the permutations $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ next to each other and in the inverse order. With regard to this and the way of expressing any permutations by pure cyclic permutations (8.6), we may understand, for example, the formula

$$\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} = (a, d)\,(b, c)$$

either in the sense that the permutation of the set $\{a, b, c, d\}$ expressed by the symbol on the left-hand side is composed of cyclic permutations (b, c), (a, d) or in the sense that it is determined by pure cyclic permutations (a, d), (b, c).

4. *Weakly associative groupoids.* V. DEVIDÉ has generalized the concept of an associative groupoid as follows: The groupoid $\mathfrak{G}$ is called *weakly associative* if there exist simple mappings $\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}$ of $\mathfrak{G}$ onto itself such that, for arbitrary elements $a, b, c \in \mathfrak{G}$, there holds: $(ab)c = \boldsymbol{f}a(\boldsymbol{g}b \,.\, \boldsymbol{h}c)$. Weakly associative groupoids may also be denoted as *weak semigroups.* It is obvious that if every mapping $\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}$ is the identical mapping, then the concept of a weakly associative groupoid coincides with the concept of an associative groupoid.

Example. Suppose the field of $\mathfrak{G}$ is the set of all rational, real or complex numbers different from zero and let the multiplication in $\mathfrak{G}$ be defined by the division. Employ the symbol $\circ$ for the multiplication of numbers. Then, for $a, b, c \in \mathfrak{G}$, we have

$$(ab)c = \frac{a/b}{c} = \frac{a}{b \circ c} = a/\left(b/\frac{1}{c}\right) = a\left(b\ \frac{1}{c}\right).$$

We observe that the simple mappings of $\mathfrak{G}$ onto itself $\boldsymbol{f} = \boldsymbol{g} = \boldsymbol{e}$ (identical mapping) and the mapping $\boldsymbol{h}$ defined by the formula $\boldsymbol{h}c = 1/c$ satisfy the above condition.

18.2. Groupoids with cancellation laws

$\mathfrak{G}$ is said to be a *groupoid with cancellation laws* if it has the following property; If for certain elements $a, x, y \in \mathfrak{G}$ there holds $ax = ay$ or $xa = ya$, then $x = y$.

In a groupoid with cancellation laws we can therefore "cancel" the equality $ax = ay$ or $xa = ya$ by the element a.

A multiplication table of every finite groupoid $\mathfrak{G}$ with cancellation laws has the following characteristic property: In every row and every column of the table there occur, on the rigth of the vertical and under the horizontal heading, the symbols of all elements of $\mathfrak{G}$. In fact: if, for example, in some row $[a]$ (i.e., to the right of the letter a written in the vertical heading) there do not occur the symbols of all the elements of $\mathfrak{G}$, then in the row $[a]$ and in two different columns $[x]$, $[y]$ (i.e., under the symbols x, y of the horizontal heading) there occurs the symbol of the same element b; that means that the equalities $ax = ay = b$ are true and that there simultaneously holds $x \neq y$ which, however, contradicts the cancellation laws. If, conversely, the multiplication table of a certain groupoid $\mathfrak{G}$ has the above property, then for any elements $a, x, y \in \mathfrak{G}$, $x \neq y$, there holds: $ax \neq ay$, $xa \neq ya$. Hence, in $\mathfrak{G}$ the cancellation laws apply.

18.3. Groupoids with division

1. *Definition.* If a groupoid $\mathfrak{G}$ is such that to any two elements $a, b \in \mathfrak{G}$ there exist elements $x, y \in \mathfrak{G}$ satisfying the equalities

$$ax = b, \quad ya = b,$$

it is called a *groupoid with division.*

If there exists only a single element $x \in \mathfrak{G}$ and a single element $y \in \mathfrak{G}$ with the above property, then $\mathfrak{G}$ is called a *groupoid with unique division.*

Groupoids with unique division are also called *quasigroups.*

We leave it to the reader to verify that the theorems set out below are correct:

For every groupoid with division, $\mathfrak{G}$, there holds $\mathfrak{G}\mathfrak{G} = \mathfrak{G}$.

Every quasigroup is a groupoid with cancellation laws.

Every finite groupoid with cancellation laws is a quasigroup.

2. *Examples.* The groupoids $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$ ($n \geqq 1$) are quasigroups: To every two elements $a, b \in \mathfrak{Z}$ there exists a single element $x \in \mathfrak{Z}$ as well as a single element $y \in \mathfrak{Z}$ such that $a + x = b$, $y + a = b$, namely: $x = -a + b$, $y = b - a$. Similarly, to every two elements $a, b \in \mathfrak{Z}_n$ there exists a single element $x \in \mathfrak{Z}_n$ as well as a single element $y \in \mathfrak{Z}_n$ such that the division of $a + x$ by n as well as the division of $y + a$ by n leaves the remainder b, namely: $x = y = -a + b$ and $x = y = n - a + b$ if $-a + b \geqq 0$ and $-a + b < 0$, respectively. To every two permutations $\boldsymbol{p}, \boldsymbol{q} \in \mathfrak{S}_n$ there exists a single permutation $\boldsymbol{x} \in \mathfrak{S}_n$ and a single permutation $\boldsymbol{y} \in \mathfrak{S}_n$ such that $\boldsymbol{p} \,.\, \boldsymbol{x} = \boldsymbol{q}$, $\boldsymbol{y} \,.\, \boldsymbol{p} = \boldsymbol{q}$, i.e., $\boldsymbol{x} = \boldsymbol{q}\boldsymbol{p}^{-1}$, $\boldsymbol{y} = \boldsymbol{p}^{-1}\boldsymbol{q}$ where $\boldsymbol{q}\boldsymbol{p}^{-1}$ denotes the permutation composed of $\boldsymbol{p}^{-1}$ and $\boldsymbol{q}$; similarly, $\boldsymbol{p}^{-1}\boldsymbol{q}$.

18.4. Groupoids with a unit element

1. *Definition.* If an element, let us denote it $\underline{1}$, of a groupoid $\mathfrak{G}$ has the property that the product of $\underline{1}$ and any element $a \in \mathfrak{G}$, in either order, is again a, then $\underline{1}$ is called a *unit element* or a *unit of* $\mathfrak{G}$.

A unit $\underline{1} \in \mathfrak{G}$ is therefore characterized by the equalities $\underline{1}a = a\underline{1} = a$ which hold for any element $a \in \mathfrak{G}$.

We can easily show that *every groupoid has at most one unit.* If $\underline{1}$, x denote units of a groupoid $\mathfrak{G}$, then there holds $\underline{1}x = x$, on the one hand, (since $\underline{1}a = a$ for every element $a \in \mathfrak{G}$), and $\underline{1}x = \underline{1}$, on the other hand (since $ax = a$ for every element $a \in \mathfrak{G}$). Hence $\underline{1} = x$.

If a groupoid $\mathfrak{G}$ has a unit element, then it is called a *groupoid with a unit element* or *with a unit.*

Let us note that the multiplication table of a finite groupoid with a unit has the following characteristic property: The row beginning with the unit contains, in the subsequent places, the same symbols in the same order as the horizontal heading of the table. Similarly, the column beginning with the unit contains, in the subsequent places, the same symbols in the same order as the vertical heading.

2. *Examples.* $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$ ($n \geqq 1$) are groupoids with a unit. The unit of $\mathfrak{Z}$ is 0, since for every element $a \in \mathfrak{Z}$ there holds $0 + a = a + 0 = a$. The unit of $\mathfrak{Z}_n$ is also 0, since for every element $a \in \mathfrak{Z}_n$ the numbers $0 + a$, $a + 0$ divided by n leave the remainder a. The unit of $\mathfrak{S}_n$ is the identical permutation $\boldsymbol{e}$ of the set H, since for every element $\boldsymbol{p} \in \mathfrak{S}_n$ we have $\boldsymbol{pe} = \boldsymbol{ep} = \boldsymbol{p}$. On the other hand, e.g., the groupoid described in 14.5.3 has no unit element.

18.5. Further remarkable groupoids. Groups

1. Special groupoids may have some of the above properties, or even all of them, simultaneously. So we speak, for example, of *semigroups with cancellation laws*, of *quasigroups with a unit*, of *semigroups with division*, etc. Some of these groupoids have special names. Quasigroups with a unit are called *loops*.

Of particular importance to our further deliberations are the semigroups with division. Let us first show that *every semigroup with division contains a unit and its division is unique.*

Suppose $\mathfrak{G}$ is a semigroup with division.

a) Choose, in $\mathfrak{G}$, an element a. As $\mathfrak{G}$ is a groupoid with division, there exists an element $e_r \in \mathfrak{G}$ such that $ae_r = a$. We shall show that e_r is a unit of $\mathfrak{G}$. Let b denote an arbitrary element of $\mathfrak{G}$. Since $\mathfrak{G}$ is a groupoid with division, there exists an element $y \in \mathfrak{G}$ such that $ya = b$ and, $\mathfrak{G}$ being associative, there holds: $be_r = (ya)e_r = y(ae_r) = ya = b$. So we have $be_r = b$. In a similar way we find that for the element $e_l \in \mathfrak{G}$ such that $e_l a = a$ there holds $e_l b = b$. Since $e_l e_r = e_l$ (because $be_r = b$ for every $b \in \mathfrak{G}$) as well as $e_l e_r = e_r$ (because $e_l b = b$ for every element $b \in \mathfrak{G}$), we have $e_l = e_r$ and, consequently, $e_r = \underline{1}$.

b) Suppose a, $b \in \mathfrak{G}$ are arbitrary elements. We shall show that the relations $ax_1 = b = ax_2$ ($x_1, x_2 \in \mathfrak{G}$) yield $x_1 = x_2$. First, $\mathfrak{G}$ being a groupoid with division, there exists an element $u \in \mathfrak{G}$ such that $ua = \underline{1}$. Next (since the multiplication is associative), there holds: $ub = u(ax_1) = (ua)x_1 = \underline{1}x_1 = x_1$ and, similarly, $ub = x_2$. So we have, in fact, $x_1 = x_2$. In an analogous way $y_1 a = b = y_2 a$ ($y_1, y_2 \in \mathfrak{G}$) yield $y_1 = y_2$.

Semigroups with division are called *groups*. The above theorem may therefore be expressed by saying that every group is a loop. For example, $\mathfrak{Z}$, $\mathfrak{Z}_n$ and $\mathfrak{S}_n$ ($n \geqq 1$) are groups. In particular, $\mathfrak{S}_n$ is called the *symmetric permutation group of grade n*

All the mentioned kinds of groupoids may, of course, have further properties, they can, for instance, be Abelian; in that case we speak, e.g., about Abelian associative groupoids with a unit, and similarly. Abelian semigroups all the elements of which are idempotent are called *semilattices*. An example of a semilattice is given by the groupoid whose field consists of all the decompositions in G and the product of the elements $\bar{A}$ and $\bar{B}$ is defined as the least common covering $[\bar{A}, \bar{B}]$ (3.7.4).

2. *Brandt groupoids.* In this chapter we shall briefly deal with the so-called Brandt groupoids, introduced into algebra in 1927 by the German mathematician H. BRANDT. He was the first to use the term "groupoid". About ten years later the term groupoid entered into literature in the sense in which it is employed today and introduced in this book.

Brandt groupoids differ from those we are concerned with by the fact that the multiplication is not necessarily defined for *every* two-membered sequence of elements.

Let G be a nonempty set and suppose we are given a rule, let us again call it a multiplication or binary operation, that can be applied to certain two-membered sequences of the elements $a, b \in G$ and uniquely associates with each of them a certain element $c \in G$; to other sequences, however, it may not be applied. In the first case we say that *a can be multiplied by b* and c is called the *product of a and b*. In the second case we say that *a cannot be multiplied by b* and that *the product of a and b does not exist.*

This situation could be adapted so as to appear as one of those we have already considered, namely, when the multiplication is defined for all two-membered sequences of the elements of G. To that purpose it would suffice to introduce a new element for the non-existing products. But we shall not do that because it would only affect the formal part of our study without any particular effect.

The set G together with a multiplication (in the above sense) is called a *Brandt groupoid* if the four postulates set out below are satisfied:

1. If, for some elements a, b, c, there holds $ab = c$, then each of them is uniquely determined by the remaining two.

2. If there exist ab and bc, then the same holds for the products $(ab)c$ and $a(bc)$; if there exist ab and $(ab)c$, then there also exist bc and $a(bc)$; if there exist bc and $a(bc)$, then there also exist ab and $(ab)c$. In each of these cases there holds $(ab)c = a(bc)$; notation abc.

3. To every element a there exist the following uniquely determined elements: the *right-hand side unit* e, the *left-hand side unit* e' and the *inverse element* a^*; for these elements there holds:

$$ae = e'a = a, \quad a^*a = e.$$

4. To any two units e, e' there exist elements for which e and e' are the right-hand side unit and the left-hand side unit (further, briefly, right unit, left unit), respectively.

If the above postulates are satisfied, then, in particular,

$$aa^* = e', \quad ea^* = a^*, \quad a^*e' = a^*, \quad ee = e, \quad e'e' = e'.$$

This can easily be verified; for example, the first equality:

$$e'a = a = ae = a(a^*a) = (aa^*)a$$

yield $e'a = (aa^*)a$, hence $e' = aa^*$.

We see that a is the inverse of a^* and so a and a^* may be referred to as mutually inverse elements.

On passing to the in verse element, the right unit and the left unit interchange.

Furthermore, we observe that the equality $ee = e$ is a characteristic property of the units: Every right or left unit complies with it and, moreover, every element e satisfying it is both the right and the left unit of e. As regards the postulates 2 and 1, it is obvious that each unit e is the right (left) unit of each element a (b) for which there exists the product ae (eb). By means of the units it can easily be expressed when a may be multiplied by b: that occurs if and only if the right unit of a equals the left unit of b.

The existence of the inverse element implies that if, for certain elements a, b, c, there holds $ab = c$, then there simultaneously holds $a^*c = b$, $cb^* = a$, $b^*a^* = c^*$, $c^*a = b^*$, $bc^* = a^*$. The inverse element a^* is also denoted a^{-1}. The products aa^{-1} or $a^{-1}a$ are only important when they stand alone, otherwise they may be omitted. If $n = ab \ldots m$ is the product of a finite sequence of an arbitrary number of elements, then the inverse element n^{-1} is given by the formula: $n^{-1} = m^{-1} \ldots b^{-1}a^{-1}$.

We shall content ourselves with these remarks without studying the theory of Brandt groupoids in detail. The latter is, after all, closely related to the theory of groups which we are concerned with in Part III of this book. To illustrate the concept of the Brandt groupoid we introduce the following simple example.

Let G be the Cartesian square of a nonempty set A (1.8). The elements of G are therefore two-membered sequences (a, b) where a, b run over the individual elements of A. The multiplication in G is defined as follows: The element (a, b) may be multiplied by $(c, d) \in G$ if and only if $b = c$ and in that case the product is given by the formula:

$$(a, b)\,(b, d) = (a, d).$$

The set G with this multiplication is a Brandt groupoid. In fact, first, it is obvious that the postulates 1 and 2 are satisfied. Next, the same holds for 3 and 4: To every element $(a, b) \in G$ there exists the right unit (b, b), the left unit (a, a) and the inverse element (b, a); to every two units (b, b), (a, a) there exists an element $(a, b) \in G$ for which (b, b) is the right and (a, a) the left unit.

If, for example, A is the set of all points in a plane, then we can associate, with every element (a, b) $(a \neq b)$ or (a, a) of the Cartesian square of A, the oriented

line segment $\overrightarrow{ab}$ or the point a, respectively. In this way we obtain a Brandt groupoid whose field consists of points and oriented line segments and whose multiplication is given by the connection of these elements.

18.6. Lattices

Let us conclude this chapter with a short exposition of lattices the concept of which closely ties up with our previous deliberations. Lattices are, essentially, pairs of co-field, that is to say, in the same field defined groupoids with special properties and with multiplications connected by certain laws. The theory of lattices plays an important part in modern mathematics not only for its extent and formal elegance but chiefly because it describes, from a unifying view, the properties of the special lattices actually occuring in various branches of mathematics.

Assume two given multiplications on G; let us call them the *upper* and the *lower multiplication*, respectively. The product of an element $a \in G$ and an element $b \in G$ under the upper (lower) multiplication is called the *meet* (the *join*) *of a and b* and is denoted by $a \cup b$ ($a \cap b$). The groupoid whose field is the set G and whose multiplication is the upper (lower) multiplication is called the *upper* (*lower*) *groupoid*. We shall make use of the same symbols as for the sum and intersection of sets (1.5, 1.6), i.e. $\cup$, $\cap$; there is no danger of misunderstanding.

1. *The definition of a lattice.* A pair consisting of an upper and a lower groupoid is called a *lattice on the field G*, briefly, a *lattice* if for any elements $a, b, c \in G$ the following equalities are true:

a) $a \cup b = b \cup a$,	a') $a \cap b = b \cap a$,
b) $a \cup a = a$,	b') $a \cap a = a$,
c) $a \cup (b \cup c) = (a \cup b) \cup c$,	c') $a \cap (b \cap c) = (a \cap b) \cap c$,
d) $a \cup (a \cap b) = a$,	d') $a \cap (a \cup b) = a$.

Either of the two groupoids of the lattice is therefore Abelian [a), a')], associative [c), c')] and all its elements are idempotent [b), b')]. The multiplications in both groupoids are connected according to the formulae d), d')'; the latter express the *absorptive laws of the lattice.*

A lattice may also be described as a pair of semilattices defined in the same field and connected by the absorptive laws.

2. *Examples.* [1] G is the set of all positive integers 1, 2, 3, ... For $a, b \in G$, $a \cup b$ is the least common multiple and $a \cap b$ the greatest common divisor of a and b.

[2] G is the set of all subsets of a certain set. For $A, B \in G$, $A \cup B$ is the sum and $A \cap B$ the intersection of A and B.

[3] G is the set of all decompositions of a certain nonempty set. For $\bar{A}, \bar{B} \in G$, $\bar{A} \cup \bar{B}$ is the least common covering $[\bar{A}, \bar{B}]$ and $\bar{A} \cap \bar{B}$ the greatest common refinement $(\bar{A}, \bar{B})$ of $\bar{A}$ and $\bar{B}$.

3. *Fundamental partial ordering of a lattice.* Let Γ be a lattice on G and a, b, $c \in G$ denote arbitrary elements.

Note that *both relations*

$$a \cup b = b, \quad b \cap a = a \tag{u}$$

are simultaneously valid.

In fact, if $a \cup b = b$, then by a') and d'):

$$b \cap a = (a \cup b) \cap a = a \cap (a \cup b) = a;$$

analogously, if $b \cap a = a$, then by a) and d):

$$a \cup b = (b \cap a) \cup b = b \cup (b \cap a) = b.$$

Associating with every element $a \in G$ any element $b \in G$ satisfying (u), we obtain a generalized mapping of G onto itself; notation $\boldsymbol{u}$.

The mapping $\boldsymbol{u}$ is an antisymmetric congruence on G. Indeed, from b) and b') we see that it is reflexive. On taking account of c), we conclude that $a \cup b = b$, $b \cup c = c$ yield: $a \cup c = a \cup (b \cup c) = (a \cup b) \cup c = b \cup c = c$, hence $\boldsymbol{u}$ is transitive. Therefore it is a congruence on G. Finally, from $a \cup b = b$, $b \cup a = a$ there follows, by a), the equality $a = b$.

Thus we have verified that the congruence $\boldsymbol{u}$ is antisymmetric, that is to say, is a partial ordering of G. We call it the *upper partial ordering of the lattice Γ.*

Note that the following symbols have the same meaning: $a \leqq b$ $(\boldsymbol{u})$, $a \cup b = b$, $b \cap a = a$.

Analogous considerations are correct if the roles of the upper and the lower groupoids are exchanged. Then we have the following results:

Both relations

$$b \cup a = a, \quad a \cap b = b \tag{l}$$

are simultaneously valid.

Associating with every element $a \in G$ any element $b \in G$ satisfying (l), *we obtain, on G, an antisymmetric congruence $\boldsymbol{l}$.* It is called the *lower partial ordering of Γ.*

It is easy to see that the following symbols have the same meaning: $a \leqq b$ $(\boldsymbol{l})$, $b \cup a = a$, $a \cap b = b$.

The upper and the lower ordering of Γ are called the *fundamental partial orderings of Γ.*

The fundamental partial orderings of Γ are inverse of each other and so $\boldsymbol{l} = \boldsymbol{u}^{-1}$, $\boldsymbol{u} = \boldsymbol{l}^{-1}$ because, under $\boldsymbol{u}$, every $b \in G$ is the image of all elements $a \in G$ satisfying the equations (u); precisely these elements are, as we see from (l), images of b under the congruence $\boldsymbol{l}$.

The symbols $a \leqq b$ $(\boldsymbol{u})$ and $b \leqq a$ $(\boldsymbol{l})$ have the same meaning.

On the above lattice [1], for example, the upper or the lower partial ordering is obtained by associating, with every positive integer, each of its positive multiples or divisors, respectively; on lattice [2], by associating, with every set $A \in G$, each of its supersets or subsets $B \in G$, respectively; on lattice [3], by associating, with every decomposition $\bar{A} \in G$, each of its coverings or refinements $\bar{B} \in G$, respectively.

The elements $a \cup b$ and $a \cap b$ are, with regard to the upper (lower) partial ordering of the lattice, the least upper (the greatest lower) and the greatest lower (the least upper) bounds of the elements a, b, respectively.

Since the upper and the lower partial orderings are mutually inverse, it is sufficient to restrict the proof to the upper partial ordering (9.4.2). Let us consider the element $a \cup b$.

Our object is to show that, with regard to $\boldsymbol{u}$, there holds $a \leqq a \cup b$, $b \leqq a \cup b$ and, furthermore, that $a \leqq c$, $b \leqq c$ yield $a \cup b \leqq c$.

The correctness of $a \leqq a \cup b$, $b \leqq a \cup b$ follows from the formulae 18.6.1 c), b), a):

$$a \cup (a \cup b) = (a \cup a) \cup b = a \cup b,$$

$$b \cup (a \cup b) = b \cup (b \cup a) = (b \cup b) \cup a = b \cup a = a \cup b.$$

The relations $a \leqq c$, $b \leqq c$ are expressed by the equalities

$$a \cup c = c, \qquad b \cup c = c$$

which yield, by 18.6.1 c),

$$(a \cup b) \cup c = a \cup (b \cup c) = a \cup c = c,$$

i.e., $a \cup b \leqq c$ and the proof is complete.

We observe that, *with regard to the upper (lower) partial ordering of a lattice, each pair of its elements has both the least upper and the greatest lower bounds; the least upper bound is the meet (join) of the pair and the greatest lower bound is its join (meet).*

4. *Comment on the definition of a lattice.* A lattice has been described as a pair of groupoids defined on the same field, with special properties and multiplications bound by certain laws. We have shown that on every lattice there are certain mutually inverse partial orderings with regard to which each pair of elements has a least upper bound and a greatest lower bound; both the least upper bound and

the greatest lower bound are the products of the relative elements under the multiplications in the groupoids of which the lattice consists.

The definition of a lattice may, conversely, be based on the concept of antisymmetric congruence. If we have, on G, an arbitrary antisymmetric congruence with regard to which each pair of elements $a, b \in G$ has a least upper bound $a \cup b$ and a least lower bound $a \cap b$, then two multiplications on G can be defined in the way that the product of the ordered pair of elements a, b is $a \cup b$ or $a \cap b$, respectively. It is easy to show that the pair of groupoids on G with these multiplications is a lattice and that the initial antisymmetric congruence and its inverse are the corresponding upper partial ordering and the lower partial ordering, respectively.

5. *Remarkable kinds of lattices.* Let Γ be a lattice on the field G.

a) Lattices with extreme elements. If some element $O \in G$ is such that for every element $a \in G$ there holds $a \leqq O$ $(\boldsymbol{u})$ $[a \leqq O$ $(\boldsymbol{l})]$, then it is said to be the *greatest element with regard to the upper* (*lower*) *partial ordering*; any element $o \in G$ such that there always applies $o \leqq a$ $(\boldsymbol{u})$ $[o \leqq a$ $(\boldsymbol{l})]$ is called the *least element with regard to the upper* (*lower*) *partial ordering*. Since the relations (u) or (l) (see 18.6.3) are simultaneously valid, it is easy to see that *the greatest* (*least*) *element with regard to the upper* (*lower*) *partial ordering is the least* (*greatest*) *with regard to the lower* (*upper*) *partial ordering*. It is also obvious that in a lattice there may be, with regard to the same fundamental partial ordering, at most one greatest and one least element. The greatest and the least elements with regard to either fundamental partial ordering of a lattice are called the *extreme elements*.

If, in the lattice Γ, both extreme elements with regard to the fundamental partial orderings exist, then Γ is said to be a *lattice with extreme elements*.

For example, the above lattice [1] has, with regard to the upper partial ordering, the least element 1 but has no greatest element; with regard to the lower partial ordering it therefore has the greatest element 1 but has no least element. [2] is a lattice with extreme elements; the greatest (least) element with regard to the upper partial ordering is the sum of all the elements of G (the empty set). Even [3] is a lattice with extreme elements; the greatest (least) element with regard to the upper partial ordering is the greatest (least) decomposition of the corresponding set.

b) Modular (Dedekind) lattices. If for some elements a, b, $c \in G$ such that $a \leqq c$ $(\boldsymbol{u})$ there holds

$$a \cup (b \cap c) = (a \cup b) \cap c,$$

then we say that the sequence a, b, c satisfies the *upper modular* or *upper Dedekind relation*; similarly, if $a \leqq c$ $(\boldsymbol{l})$ and there holds

$$a \cap (b \cup c) = (a \cap b) \cup c,$$

then the sequence a, b, c satisfies the *lower modular* or *lower Dedekind relation*.

It is clear that *if the sequence a, b, c satisfies the upper (lower) Dedekind relation, then the inverse sequence c, b, a satisfies the lower (upper) Dedekind relation.*

The lattice Γ is called *modular* or *Dedekind* if every sequence of elements $a, b, c \in G$ in which there is $a \leqq c$ $(\boldsymbol{u})$ $(a \leqq c$ $(\boldsymbol{l}))$ satisfies the upper (lower) Dedekind relation.

For example, the above lattice [2] is a Dedekind lattice because, for any parts A, B, C of an arbitrary set such that $A \subset C$, there holds $A \cup (B \cap C) = (A \cup B) \cap C$ (1.10.5; 1.10.3). Note that this lattice has, at the same time, extreme elements.

6. *Homomorphic mappings (deformations) of lattices.* The notion of homomorphic mapping defined for groupoids (13.1) may easily be applied to lattices.

Let Γ, Γ^* be arbitrary lattices.

The mapping $\boldsymbol{d}$ of the lattice Γ into Γ^* is called a *homomorphic mapping* or a *deformation* if it preserves both lattice multiplications, that is to say, if for any elements $a, b \in \Gamma$ there holds:

$$\boldsymbol{d}(a \cup b) = \boldsymbol{d}a \cup \boldsymbol{d}b, \qquad \boldsymbol{d}(a \cap b) = \boldsymbol{d}a \cap \boldsymbol{d}b.$$

In the same way further notions connected with the concept of deformation may be applied to lattices. In particular, a simple deformation of Γ into Γ^* is called an *isomorphic mapping* and, in case of a mapping onto Γ^*, an *isomorphism*. If Γ is, under an isomorphism $\boldsymbol{i}$, mapped onto Γ^*, then Γ^* is said to be the *isomorphic image of Γ under the isomorphism $\boldsymbol{i}$* or the *$\boldsymbol{i}$-image of Γ*: $\Gamma^* = \boldsymbol{i}\Gamma$.

13.7. Exercises

1. If a permutation $\boldsymbol{p}$ of a set is composed of the permutations $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ $(n \geqq 2)$, then the inverse permutation $\boldsymbol{p}^{-1}$ is composed of $\boldsymbol{p}_n^{-1}, \ldots, \boldsymbol{p}_1^{-1}$.
2. Every cyclic permutation of a finite set whose cycle consists of at least two members may be composed of transpositions as follows: $(a, b, c, \ldots, k, l, m) = (a, b)\,(b, c) \ldots (k, l)\,(l, m)$.
3. Denote, for convenience, the elements of a set H of order n $(\geqq 2)$ by the numbers $1, \ldots, n$. Every transposition $(i, i + j)$ of H may be composed of some transpositions $(1, 2)$, $(2, 3)$, $\ldots$, $(n - 1, n)$ as follows:

$$(i, i + j) = (i + j - 1, i + j) \ldots (i + 1, i + 2)\,(i, i + 1)\,(i + 1, i + 2) \ldots (i + j - 1, i + j).$$

Every permutation of H may be composed of some transpositions

$$(1, 2), (2, 3), \ldots, (n - 1, n).$$

4. If the groupoid $\mathfrak{G}$ has a unit, then the image of the latter under any deformation $\boldsymbol{d}$ of $\mathfrak{G}$ into $\mathfrak{G}^*$ is a unit of $\boldsymbol{d}\mathfrak{G}$.
5. Every factoroid $\overline{\mathfrak{G}}$ on an arbitrary groupoid with a unit, $\mathfrak{G}$, has a unit; the element $\bar{a} \in \overline{\mathfrak{G}}$ containing the unit of $\mathfrak{G}$ is the unit of $\overline{\mathfrak{G}}$.

6. Give examples of groupoids that have only one or (with the exception of groups) exactly two properties described in 18.1, 18.3 and 18.4.

7. Every finite semigroup is a group.

8. In a semigroup the product of an arbitrary n-membered sequence of elements $a_1, \ldots, a_n$ ($n \geqq 2$) does not depend on their order if any two elements a_i, a_j are interchangeable. In an Abelian semigroup the product of a finite sequence of elements does not depend on their order.

9. In a Brandt groupoid there follow, from $ab = c$, for the right and the left units of the elements a, b, c; a^{-1}, b^{1}, c^{-1} the relations: b and c, c^{-1} and a^{-1}, a and b^{-1} have the same right units; b^{-1} and c^{-1}, c and a, a^{-1} and b have the same left units (equal to the corresponding right units). Each of these relations is sufficient for $ab = c$ to apply.

10. In any Brandt groupoid the elements having simultaneously the same unit on the right and on the left are called *doubly corresponding*. All elements doubly corresponding to some unit form a group. The sets of doubly corresponding elements form again a Brandt groupoid; its units are groups consisting of elements doubly corresponding to the units.

11. The properties of the upper and the lower groupoid required in the definition of the lattice (18.6.1) are not independent, since the properties b), b′) are a consequence of the others. Make sure of this by applying the equality d′) [d)] to the elements a, $b = a$ and the equality d) [d′)] to the elements a, $b = a \cup a$ [a, $b = a \cap a$].

12. If a lattice consists of decompositions on G every two of which are complementary and if the multiplications are defined as in 18.6.2. [3], then it is modular.

13. A lattice is modular if and only if any three of its elements a, b, c satisfy the equality:

$$(a \cup b) \cap [c \cup (a \cap b)] = (a \cap b) \cup [c \cap (a \cup b)].$$

14. An isomorphic image of a modular lattice is again modular.

15. Let Γ be an arbitrary lattice of decompositions on G with lattice operations [ ] and ( ). A series of decompositions on G all the members of which are elements of Γ is called a *main series of* Γ if each of its refinements containing only elements of Γ is its lengthening. The following theorems apply: a) *if* Γ *contains the greatest (least) element, then the latter is the initial (final) element of every main series of* Γ; b) *all mutually complementary main series of* Γ *have the same reduced length.*