III. GROUPS

19. Basic concepts relative to groups

19.1. Axioms of a group

The object of our further study are groups. By the definition in 18.5.1, a group is a semigroup with division.

More accurately:

A groupoid $\mathfrak{G}$ is called a *group* if the following *axioms of a group* are satisfied:

1. *For any elements $a, b, c \in \mathfrak{G}$ there holds $a(bc) = (ab)c$.*

2. *To any elements $a, b \in \mathfrak{G}$ there exists an element $x \in \mathfrak{G}$ satisfying $ax = b$ and an element $y \in \mathfrak{G}$ satisfying $ya = b$.*

These axioms are briefly called the *associative law* and the *axiom of division.* From these, as we have shown in 18.5.1, there follows the existence of a unit, i.e., an element $\underline{1}$ such that for $a \in \mathfrak{G}$ there holds $\underline{1}a = a\underline{1} = a$ and, moreover, the uniqueness of the division in $\mathfrak{G}$. Hence *every group is a quasigroup with a unit (loop).*

In what follows, $\mathfrak{G}$ denotes an arbitrary group.

19.2. Inverse elements. Inversion

Since $\mathfrak{G}$ is a quasigroup with a unit, there exists to every element $a \in \mathfrak{G}$ a unique element $x \in \mathfrak{G}$ such that $ax = \underline{1}$ and a unique element $y \in \mathfrak{G}$ such that $ya = \underline{1}$; the symbol $\underline{1}$ denotes (in our study) the unit of $\mathfrak{G}$.

It is easy to show that, in consequence of the associative law, both elements x and y are equal. In fact, first, the product of the element y and the element ax $(= \underline{1})$ is $y(ax) = y\underline{1} = y$. Next, by the associative law there holds $y(ax) = (ya)x = \underline{1}x = x$ and we actually have $x = y$.

Thus *there exists, to every element $a \in \mathfrak{G}$, a unique element a^{-1} such that $aa^{-1} = a^{-1}a = \underline{1}$.* It is called *the inverse element of a* or *the inverse of a.*

The inverse of a is therefore, by the definition, the only solution of the equation $ax = \underline{1}$ and, simultaneously, the only solution of the equation $ya = \underline{1}$. Since the element a satisfies the equation $a^{-1}x = \underline{1}$, it is the inverse of a^{-1}, i.e., $(a^{-1})^{-1} = a$. We also say that the elements a, a^{-1} are inverse of each other. Note that the inverse of a may be a itself because, e.g., $\underline{1} = \underline{1}$.

On the group $\mathfrak{G}$ we therefore have an important decomposition each element of which consists either of one element only, i.e., the inverse of itself, or of two elements inverse of each other.

For example, in the group $\mathfrak{Z}$ we have the unit 0 and the element inverse of an arbitrary element a is $-a$. The mentioned decomposition of $\mathfrak{Z}$ is: $\{0\}, \{1, -1\}, \{2, -2\}, \ldots$

Let a, b denote arbitrary elements of $\mathfrak{G}$. From $aa^{-1} = \underline{1}$ and in accordance with the associative law, we have

$$a(a^{-1}b) = (aa^{-1})b = \underline{1}b = b$$

so that the element $a^{-1}b$ is the (only) solution of the equation $ax = b$. In a similar way we ascertain that ba^{-1} is the (only) solution of $ya = b$. Furthermore, it is easy to verify that the element inverse of the product ab is $b^{-1}a^{-1}$; it is sufficient to realize that $b^{-1}a^{-1}$ is the solution of the equation $(ab)x = \underline{1}$. That follows from:

$$(ab)\,(b^{-1}a^{-1}) = a(bb^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(\underline{1}a^{-1}) = aa^{-1} = \underline{1}.$$

Analogously we arrive at a more general result, namely, that *the element inverse of the product $a_1a_2 \ldots a_n$ of an arbitrary $n(\geqq 2)$-membered sequence of elements $a_1, a_2, \ldots, a_n \in \mathfrak{G}$ is $a_n^{-1} \ldots a_2^{-1}a_1^{-1}$.*

Remark. The existence of the inverse of any element follows, as we have seen, from the characteristic properties of a group. Conversely, if any element $a \in \mathfrak{G}$ of an associative groupoid with a unit $\underline{1}$, $\mathfrak{G}$, has an inverse a^{-1}, i.e., the element satisfying $aa^{-1} = a^{-1}a = \underline{1}$, then $\mathfrak{G}$ is a quasigroup and therefore (since it is associative) a group. For in that case there exist, to any two elements $a, b \in \mathfrak{G}$, elements $x, y \in \mathfrak{G}$ such that $ax = b$, $ya = b$, i.e., $x = a^{-1}b$, $y = ba^{-1}$; it can easily be verified that x and y are the only elements with this property.

The property that to each element a of a group there exists an inverse a^{-1} is characteristic of groups and distinguishes them among the associative groupoids with a unit.

Making use of the inverse elements, we may define a certain simple mapping of $\mathfrak{G}$ onto itself, important for the following considerations. It is done by way of associating with every $a \in \mathfrak{G}$ the inverse element $a^{-1} \in \mathfrak{G}$. Thus we obtain a simple mapping of $\mathfrak{G}$ onto itself, hence a permutation on $\mathfrak{G}$, uniquely determined by $\mathfrak{G}$. It is called the *inversion of* $\mathfrak{G}$ and denoted by $\boldsymbol{n}$. We observe that $\boldsymbol{n}$ is an involutary mapping (6.7).

19.3. Powers of elements

Let a be an element of $\mathfrak{G}$ and n an arbitrary positive integer. Since $\mathfrak{G}$ is associative, there exists only one element $\underbrace{aa \ldots a}_{n}$ called the n^{th} *power of a* and denoted by a^n. For $n = 1$ we have $a^1 = a$. Similarly, the element $\underbrace{a^{-1} \ldots a^{-1}}_{n}$ is called the $-n^{th}$ *power of a* and denoted by a^{-n}. By these definitions there holds $a^{-n} = (a^{-1})^n$, $a^{-n} = (a^n)^{-1}$. Thus we have defined the positive and the negative powers of a. It is useful to define even the *zeroth power* a^0 *of a* as the unit of $\mathfrak{G}$ so that $a^0 = \underline{1}$.

With each element $a \in \mathfrak{G}$ we have thus associated infinitely many powers of a: $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$, with the exponents $\ldots, -2, -1, 0, 1, 2, \ldots$; some of these elements may, of course, be equal.

For the powers of an element $a \in \mathfrak{G}$ there holds:

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn} \tag{1}$$

for all the integers m, n.

For brevity, we shall only prove the first formula and leave the proof of the second to the reader. If one or both numbers m, n are 0, then the above formula is obviously correct. If both m and n are positive, then we have

$$a^m a^n = \underbrace{(a \ldots a)}_{m} \underbrace{(a \ldots a)}_{n} = \underbrace{a \ldots a}_{m+n} = a^{m+n},$$

and the formula again applies. If both m and n are negative, then we denote $m' = -m$, $n' = -n$, hence m', n' are positive integers and we have

$$a^m a^n = a^{-m'} a^{-n'} = \underbrace{(a^{-1} \ldots a^{-1})}_{m'} \underbrace{(a^{-1} \ldots a^{-1})}_{n'} = \underbrace{a^{-1} \ldots a^{-1}}_{m'+n'}$$
$$= a^{-(m'+n')} = a^{-m'-n'} = a^{m+n}.$$

It remains to consider the case when one of the numbers m, n is positive and the other negative. If m is positive and n negative, we denote $n' = -n$ so that m, n' are positive integers and we have

$$a^m a^n = a^m a^{-n'} = \underbrace{(a \ldots a)}_{m} \underbrace{(a^{-1} \ldots a^{-1})}_{n'}$$
$$= \begin{cases} \underbrace{a \ldots a}_{m-n'} = a^{m-n'} = a^{m+n} & \text{if } m > n'; \\ \underline{1} = a^0 = a^{m-n'} = a^{m+n} & \text{if } m = n'; \\ \underbrace{a^{-1} \ldots a^{-1}}_{n'-m} = a^{-(n'-m)} = a^{m+n} & \text{if } m < n'. \end{cases}$$

Finally, if m is negative and n positive, then we write $m' = -m$, so that m', n are positive integers and we have:

$$\begin{aligned} a^m a^n &= a^{-m'}a^n = (a^{-1})^{m'}[(a^{-1})^{-1}]^n = (a^{-1})^{m'}(a^{-1})^{-n} = (a^{-1})^{m'-n} \\ &= a^{-(m'-n)} = a^{-m'+n} = a^{m+n}, \end{aligned}$$

which completes the proof.

If, for example, a stands for an arbitrary element of $\mathfrak{Z}$, then the individual powers of a are: $\ldots, -2a, -a, 0, a, 2a, \ldots$; in particular, for $a = 1$ we have: $\ldots, -2, -1, 0, 1, 2, \ldots$ and we observe that the set of all the powers of $1 \in \mathfrak{Z}$ coincides with the field of $\mathfrak{Z}$.

19.4. Subgroups and supergroups

1. *Definition.* Let $\mathfrak{A}$ be a subgroupoid of $\mathfrak{G}$. By 12.9.8, $\mathfrak{A}$ is an associative groupoid. If $\mathfrak{A}$ is a group, then we say that $\mathfrak{A}$ is a *subgroup of* $\mathfrak{G}$ or that $\mathfrak{G}$ is a *supergroup of* $\mathfrak{A}$ and write, as usual, $\mathfrak{A} \subset \mathfrak{G}$ or $\mathfrak{G} \supset \mathfrak{A}$.

$\mathfrak{A} \subset \mathfrak{G}$ is called a *proper subgroup of* $\mathfrak{G}$ if the field A of $\mathfrak{A}$ is a proper subset of $\mathfrak{G}$. Then we say that $\mathfrak{G}$ is a *proper supergroup of* $\mathfrak{A}$. There exist at least two subgroups of $\mathfrak{G}$, namely, the *greatest subgroup* which is identical with $\mathfrak{G}$ and the *least subgroup* $\mathfrak{G}$ whose field consists of the single element $\underline{1}$. These are the *extreme subgroups of* $\mathfrak{G}$.

To any groups $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{G}$ there evidently apply the following statements:

a) *If* $\mathfrak{B}$ *is a subgroup of* $\mathfrak{A}$ *and* $\mathfrak{A}$ *a subgroup of* $\mathfrak{G}$, *then* $\mathfrak{B}$ *is a subgroup of* $\mathfrak{G}$.

b) *If* $\mathfrak{A}$, $\mathfrak{B}$ *are subgroups of* $\mathfrak{G}$ *and for their fields* A, B *there holds* $B \subset A$, *then* $\mathfrak{B}$ *is a subgroup of* $\mathfrak{A}$.

2. *Characteristic properties of subgroups.* Consider a subgroup $\mathfrak{A}$ of $\mathfrak{G}$. Denote by j the unit of $\mathfrak{A}$. Is there any relation between the unit $\underline{1}$ of $\mathfrak{G}$ and the unit j of $\mathfrak{A}$? By the definition of j there applies to every element $a \in \mathfrak{A}$ the equality $a = ja$ and, simultaneously, there of course holds $a = \underline{1}a$. Hence, in accordance with 19.1.2, we have $j = \underline{1}$. We see that *the unit of* $\mathfrak{G}$ *is, at the same time, the unit of* $\mathfrak{A}$. Consequently, *the inverse of an arbitrary element* $a \in \mathfrak{A}$ *is the element* a^{-1}, namely, the inverse of a in $\mathfrak{G}$.

Thus, *if a subgroupoid of* $\mathfrak{G}$ *is a subgroup of* $\mathfrak{G}$, *it contains the unit of* $\mathfrak{G}$ *and with each of its elements* a, *the element* a^{-1}; *conversely, if a subgroupoid of* $\mathfrak{G}$ *has these properties, then it is a subgroup of* $\mathfrak{G}$.

Owing to this result we can easily deduce a certain property of subgroups by which they are distinguishable among the subgroupoids. A subgroup $\mathfrak{A} \subset \mathfrak{G}$

contains, as we know, with each of its elements even the inverse of the latter, and so, if it contains any elements a, b, then it also contains the element ab^{-1}. If, conversely, a certain subgroupoid of $\mathfrak{G}$ contains with every two elements a, b even the element ab^{-1}, then it contains (for $b = a$) the unit $\underline{1}$ of $\mathfrak{G}$ and (for $a = \underline{1}$) the element b^{-1}; hence it is a subgroup of $\mathfrak{G}$.

The subgroups of $\mathfrak{G}$ are distinguishable among the subgroupoids of $\mathfrak{G}$ by that they contain, with every two elements a, b, even the element ab^{-1}.

Note, moreover, that any nonempty subset $A \subset \mathfrak{G}$ containing, with every two elements a, b, even the element ab^{-1} is groupoidal and therefore is the field of a subgroup of $\mathfrak{G}$. A similar observation applies to the element $a^{-1}b$.

3. *Examples.* Let us again consider the group $\mathfrak{Z}$ and let $\mathfrak{A}$ be a subgroup of $\mathfrak{Z}$. Since $\mathfrak{A}$ contains, with each of its elements b even the inverse, $-b$, $\mathfrak{A}$ consists either only of the element 0 or comprises both negative and positive numbers. In the first case, $\mathfrak{A}$ is the least subgroup of $\mathfrak{Z}$. In the second case, denote by a the least positive integer contained in $\mathfrak{A}$. The subgroup $\mathfrak{A}$, naturally, comprises all the powers of a, i.e., the multiples of a:

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots$$

Let b denote an arbitrary element of $\mathfrak{A}$. As we know, there exist integers q, r such that $b = qa + r$, $0 \leqq r \leqq a - 1$. Since $\mathfrak{A}$ contains b, qa, it also includes $b - qa = r$ and, as it contains no positive integers $<a$, we have $r = 0$. Hence $b = qa$ so that $\mathfrak{A}$ contains only multiples of a certain non-negative integer. Conversely, it is obvious that the set of all multiples of an arbitrary non-negative integer together with the adequate multiplication is a subgroup of $\mathfrak{Z}$.

The result: *all subgroups of $\mathfrak{Z}$ consist of all the multiples of the single non-negative integers.* Note that all *positive* multiples of a *positive* integer form a subgroupoid but not a subgroup of $\mathfrak{Z}$. Thus groups may comprise subgroupoids that are not subgroups.

4. *Remark.* Though we have succeeded in determining all the subgroups of $\mathfrak{Z}$, we must not expect a similar success in case of other groups where the multiplication is more complicated. No law by which it would be possible to determine all the subgroups of any group has, so far, been found.

19.5. The intersection and the product of subgroups

1. *The intersection of subgroups.* Consider two arbitrary subgroups $\mathfrak{A}, \mathfrak{B} \subset \mathfrak{G}$. Since both $\mathfrak{A}$ and $\mathfrak{B}$ contain the element $\underline{1} \in \mathfrak{G}$, there exists, as we know from our study of the groupoids, their intersection $\mathfrak{A} \cap \mathfrak{B}$. It is easy to show that $\mathfrak{A} \cap \mathfrak{B}$ is again a subgroup of $\mathfrak{G}$. $\mathfrak{A} \cap \mathfrak{B}$ is evidently an associative subgroupoid

of $\mathfrak{G}$ with the unit $\underline{1}$; it will therefore be sufficient to make sure that it contains, with every element a, even the inverse element a^{-1}. If $a \in \mathfrak{A} \cap \mathfrak{B}$, then simultaneously $a \in \mathfrak{A}$, $a \in \mathfrak{B}$ and, as $\mathfrak{A}$, $\mathfrak{B}$ are subgroups, there follows $a^{-1} \in \mathfrak{A}$, $a^{-1} \in \mathfrak{B}$ whence $a^{-1} \in \mathfrak{A} \cap \mathfrak{B}$ and the proof is complete. Consequently, *every two subgroups of $\mathfrak{G}$ have an intersection which is a subgroup of* $\mathfrak{G}$. It is also, as we see, a subgroup of each of the mentioned subgroups. This result may easily be applied to any number of subgroups of $\mathfrak{G}$.

2. *The product of subgroups.* Suppose the subgroups $\mathfrak{A}$, $\mathfrak{B}$ are interchangeable, i.e., $AB = BA$ where A and B stand for the fields of $\mathfrak{A}$ and $\mathfrak{B}$, respectively. Under this assumption there exists the product $\mathfrak{A}\mathfrak{B}$ of the subgroups $\mathfrak{A}$, $\mathfrak{B}$ (12.9.9) which is a subgroup of $\mathfrak{G}$. In fact, it is associative and, in accordance with the relations: $\underline{1} \in \mathfrak{A}$, $\underline{1} \in \mathfrak{B}$, $\underline{1} = \underline{1}\underline{1} \in \mathfrak{A}\mathfrak{B}$, comprises the unit $\underline{1}$ of $\mathfrak{G}$. Moreover, each element of $\mathfrak{A}\mathfrak{B}$ is the product ab of an element $a \in \mathfrak{A}$ and an element $b \in \mathfrak{B}$. The inverse of ab is $b^{-1}a^{-1}$ which lies, by the relation $BA = AB$, in the subgroupoid $\mathfrak{A}\mathfrak{B}$. Hence $\mathfrak{A}\mathfrak{B}$ is a subgroup of $\mathfrak{G}$. Note that there also holds 19.7.6. Furthermore, $\mathfrak{A}\mathfrak{B} \supset \mathfrak{A}$, $\mathfrak{A}\mathfrak{B} \supset \mathfrak{B}$; in particular $\mathfrak{A}^2$, i.e., $\mathfrak{A}\mathfrak{A}$ is the subgroup $\mathfrak{A}$ of $\mathfrak{G}$. It is also important to realize that in every Abelian group (any two subgroups are interchangeable and therefore) there exists a product of any two subgroups which is again a subgroup.

3. *Example.* Any two subgroups of $\mathfrak{Z}$ have an intersection and a product. Determine, for example, the intersection and the product of the subgroups $\mathfrak{A}$, $\mathfrak{B}$ whose fields are

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$\{\ldots, -14, -7, 0, 7, 14, \ldots\}.$$

Every element of the intersection $\mathfrak{A} \cap \mathfrak{B}$ is, simultaneously, a multiple of the numbers 4 and 7; hence it is a multiple of the least common multiple of 4 and 7, i.e., of 28. The intersection $\mathfrak{A} \cap \mathfrak{B}$ therefore consists of the members

$$\ldots, -56, -28, 0, 28, 56, \ldots$$

As for the product $\mathfrak{A}\mathfrak{B}$, it obviously contains $4 + 7 = 11$. Moreover, as a subgroup of $\mathfrak{Z}$, $\mathfrak{A}\mathfrak{B}$ consists of all multiples of a certain non-negative integer a (19.4.3). Consequently, 11 is a multiple of a and therefore $a = 1$ or $a = 11$. Since $\mathfrak{A}\mathfrak{B}$ obviously comprises even, e.g., the number 4, there holds $a = 1$ because 4 is not a multiple of 11. It follows that the subgroup $\mathfrak{A}\mathfrak{B}$ consists of all multiples of 1, hence it is equal to $\mathfrak{Z}$.

19.6. Comments on the multiplication tables of finite groups

1. *Characteristic properties of the tables.* Let $\mathfrak{G}$ denote an arbitrary finite group and consider the corresponding multiplication table. Since there hold, in $\mathfrak{G}$, the

cancellation laws (18.3.1), we find in every row and every column of the multiplication table, to the right of the vertical and under the horizontal heading, the symbols of all the elements of $\mathfrak{G}$. There occurs, in particular, $\underline{1}$ and simultaneously with each element even the symbol of its inverse. These properties are characteristic of the multiplication table of a finite group only if there simultaneously applies the associative law. For example, the multiplication tables for groups of the order 1, 2, 3 whose members have been denoted by $\underline{1}$, a, b are:

	$\underline{1}$
$\underline{1}$	$\underline{1}$

	$\underline{1}$	a
$\underline{1}$	$\underline{1}$	a
a	a	$\underline{1}$

	$\underline{1}$	a	b
$\underline{1}$	$\underline{1}$	a	b
a	a	b	$\underline{1}$
b	b	$\underline{1}$	a

For groups of order 4 whose elements have been denoted by $\underline{1}$, a, b, c we have two different multiplication tables:

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	a	$\underline{1}$
c	c	b	$\underline{1}$	a

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	$\underline{1}$	a
c	c	b	a	$\underline{1}$

The above multiplication tables are found in the following way: one considers all the products of two equal or different elements and (taking account of the fact that in the multiplication table there occur, in every row and every column, the symbols of all the elements of the group, each only once) one decides which of the elements the product could be; finally, one verifies that the associative law is satisfied. But this procedure is, without further knowledge of the groups, rather tedious. Though we know rules by means of which the multiplication tables of all groups of certain orders may be determined, the main and hitherto unsolved problem is the enumeration of all finite groups of an arbitrary order.

2. *Normal tables.* Every multiplication table of a group of an arbitrary order may, first, be simplified by omitting both headings. Then we write, as the first, that row which contains the symbol $\underline{1}$ in the first place; as the second, that row which contains the symbol $\underline{1}$ in the second place, and so on until, as the last, that row which contains the symbol $\underline{1}$ in the last place. Such a multiplication table is called *normal*. Examples of normal multiplication tables of groups of the orders 1, 2, 3, 4 with the symbols $\underline{1}$, a, b, c of their elements are set out below:

$\underline{1}$

$\underline{1}$	a
a	$\underline{1}$

$\underline{1}$	a	b
b	$\underline{1}$	a
a	b	$\underline{1}$

$\underline{1}$	a	b	c
a	$\underline{1}$	c	b
c	b	$\underline{1}$	a
b	c	a	$\underline{1}$

$\underline{1}$	a	b	c
a	$\underline{1}$	c	b
b	c	$\underline{1}$	a
c	b	a	$\underline{1}$

3. *The rectangle rule.* In every normal multiplication table there is, at each place of the main diagonal, the symbol of the unit. Consider the normal multiplication table of a finite group. The symbol of the product of two elements a and b is, naturally, at the intersection of the row beginning with a and the column beginning with b. If a and b are symmetrically placed with regard to the main diagonal, then we have $ab = \underline{1}$ and, of course, a, b are inverse of each other. We observe that in the first row of the table there are the symbols of the elements inverse of those written in the first column.

Now consider any three elements x, y, z whose symbols together with $\underline{1}$ form the vertices of a rectangle so that, for example, x is in the same column and y in the same row as $\underline{1}$ and so z is in the same row as x and in the same column as y. Let a and b stand for the first letters of the rows containing $\underline{1}$ and x, respectively, and let, similarly, c and d be the first letters of the columns containing $\underline{1}$ and y, respectively. Then, for example, x lies at the intersection of the row beginning with b and the column beginning with c, so that $x = bc$ and, similarly, we have $y = ad$, $z = bd$, $\underline{1} = ac$. From $\underline{1} = ac$ we see that a and c are inverse of each other, hence there simultaneously holds $ca = \underline{1}$. So we have: $xy = (bc)\,(ad) = b(ca)d = b\underline{1}d = bd = z$, hence $xy = z$, which expresses the rectangle rule:

If, on a normal multiplication table, the symbols of four elements one of which is $\underline{1}$ form the vertices of a rectangle, then the element lying on the vertex opposite to $\underline{1}$ is the product of the element lying on the vertex in the same column as $\underline{1}$ and the element lying on the remaining vertex.

For example, in the last normal multiplication table introduced in 19.6.2, the elements $\underline{1}$, c in the second row together with the elements b, a in the fourth row form the vertices of a rectangle. In accordance with the above rule, we have $bc = a$ and, in fact, at the intersection of the row beginning with b and the column beginning with c there is a.

19.7. Exercises

1. A groupoid whose field is the set of all Euclidean motions on a straight line $f[a]$, $g[a]$ or in a plane $f[\alpha; a, b]$, $g[\alpha; a, b]$, the multiplication being defined by the composition of the motions (11.5.1), is a group called the *complete group of Euclidean motions on a straight line* or *in a plane*, respectively. In the latter all the elements $f[a]$ or $f[\alpha; a, b]$ form a subgroup. Find some further subgroups of the mentioned groups.
   Remark. The Euclidian geometry in a plane describes the properties of figures consisting of points and straight lines such as configurations of points and straight lines,

triangles, conics, etc. It is based on the complete group of Euclidean motions in a plane in the sense that two figures are considered equal if one can be mapped onto the other under an Euclidean motion.

2. The groupoid whose field is the set of $2n$ permutations of the vertices of a regular n-gon in a plane ($n \geqq 3$), described in Exercise 8.8.4, and whose multiplication is defined by the composition of permutations, is a group called the *diedric permutation group of order* $2n$. The latter contains, besides the least subgroup, further proper subgroups: the subgroup of order n which consists of all the elements corresponding to the rotations of the vertices about the center; n subgroups of order 2 each of which consists of the identical permutation and the permutation associating, with the vertices of the n-gon, the vertices symmetric with regard to an axis of symmetry.

3. In every finite group of an even or an odd order, the number of elements inverse of themselves is even or odd, respectively.

4. Every subgroupoid of a finite group is a subgroup (cf. 18.7.7).

5. The inversion of every Abelian group is an automorphism of itself.

6. In every Abelian group all the elements inverse of themselves form a subgroup.

7. In every Abelian group $\mathfrak{G}$ there applies, to any two elements $a, b \in \mathfrak{G}$ and an integer n, the equality $(ab)^n = a^n b^n$. Show that in a non-Abelian group this formula is not necessarily true.

8. If $\mathfrak{A}$, $\mathfrak{B}$ are subgroups of $\mathfrak{G}$ and the product of their fields, AB, is the field of a subgroup of $\mathfrak{G}$, then $\mathfrak{A}$, $\mathfrak{B}$ are interchangeable.

9. If $\mathfrak{A} \subset \mathfrak{B}$ are subgroups of $\mathfrak{G}$, then $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{B}$, $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{A}$. If even $\mathfrak{C}$ is a subgroup of $\mathfrak{G}$ and is interchangeable with $\mathfrak{A}$, then the subgroup $\mathfrak{C} \cap \mathfrak{B}$ is also interchangeable with $\mathfrak{A}$.

10. Every group has a center.

11. Assuming $p \in \mathfrak{G}$ to be an arbitrary element of $\mathfrak{G}$, let a new multiplication in $\mathfrak{G}$, marked with the sign $\circ$, be defined as follows: For arbitrary elements $x, y \in \mathfrak{G}$, the product $x \circ y$ is given by $x \circ y = xp^{-1}y$. Then there holds: a) the groupoid $\overset{\circ}{\mathfrak{G}}$ whose field is the field G of $\mathfrak{G}$, the multiplication being defined in the mentioned way, is a group; b) the unit of $\overset{\circ}{\mathfrak{G}}$ is the element p, the inverse of $x \in \overset{\circ}{\mathfrak{G}}$ is $px^{-1}p$.

    Remark. The group $\overset{\circ}{\mathfrak{G}}$ will henceforth be called the *(p)-group associated with the group* $\mathfrak{G}$.