ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Книга 1 — Математика и механика
Том 91, 1997

ANNUAIRE DE L'UNIVERSITE DE SOFIA „ST. KLIMENT OHRIDSKI“

FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Livre 1 — Mathématiques et Mecanique
Tome 91, 1997

ON THE ALGEBRAIC PROPERTIES OF CONVEX BODIES AND RELATED ALGEBRAIC SYSTEMS

SVETOSLAV MARKOV

To the memory of Prof. Y. Tagamlitzki

The algebraic system of convex bodies with addition and multiplication by scalar is studied. A new operation for convex bodies, called inner addition, is introduced. New distributivity relations for convex bodies, called resp. quasidistributive and q-distributive law, are formulated and proved. The convex bodies form a quasilinear system with respect to addition and multiplication by scalar. The latter is isomorphically embedded in a q-linear system, which is an abelian group with respect to addition and obeys the q-distributive law. A result of H. Radstróm for convex bodies is generalized.

Keywords: convex bodies, quasilinear systems

1991/95 Math. Subject Classification: main 52A01, secondary 13C99

1. INTRODUCTION

Notation. Let $\mathbb{E} = \mathbb{E}^n$, $n \geq 1$, be an n-dimensional real Euclidean vector space with origin 0. A convex compact subset of $\mathbb{E}$ is called *convex body* (*in* $\mathbb{E}$) or just a *body*; a convex body need not have necessarily interior points, e. g. a line segment and a single point in $\mathbb{E}$ are convex bodies [20]. The class of all convex bodies of $\mathbb{E}$ will be denoted by $\mathcal{K} = \mathcal{K}(\mathbb{E})$; in this work the empty set is not an element of $\mathcal{K}$. The elements of $\mathbb{E}$ are called one-point sets or degenerate bodies. The field of reals is denoted by $\mathbb{R}$.

The set $\mathcal{K}$ is closed under the operations

$$A + B = \{c \mid c = a + b,\ a \in A,\ b \in B\},\ \ A, B \in \mathcal{K}, \tag{1.1}$$
$$\alpha * B = \{c \mid c = \alpha b,\ b \in B\},\ \ B \in \mathcal{K},\ \alpha \in \mathbb{R}, \tag{1.2}$$

called resp. (*Minkowski*) *addition* and *multiplication by scalar*. Operation (1.1) is well-known operation in algebra, see e. g. [1, Ch. I]. Operation (1.2) is not so familiar; it is used in comparatively new areas like set-valued, convex and interval analysis. The symbol "$*$" in (1.2) will not be omitted throughout the paper in order to avoid confusion with the multiplication by scalar in a linear system. The latter will be further called a *linear multiplication by scalar* and will be denoted by "$\cdot$"; the dot "$\cdot$" may be omitted as in the expression "αb" in (1.2).

Addition. We recall some properties of (1.1). For A, B, $C \in \mathcal{K}$ we have

$$(A + B) + C = A + (B + C), \tag{1.3}$$
$$A + B = B + A, \tag{1.4}$$

hence $(\mathcal{K}, +)$ is a commutative (abelian) semigroup. There exists a neutral element in $\mathcal{K}$ — the origin 0 of $\mathbb{E}^n$ — such that for all $A \in \mathcal{K}$

$$A + 0 = A, \tag{1.5}$$

hence $(\mathcal{K}, +)$ is an abelian monoid (cf. [9, Ch. 2], which will be also denoted $(\mathcal{K}, 0, +)$ (to avoid misunderstandings, we shall usually denote the algebraic systems together with their operations).

It has been proved (see, e. g., [16, Lemma 2], or [20, p. 41] that the monoid $(\mathcal{K}, +)$ is cancellative, that is, for $A, B, X \in \mathcal{K}$ the cancellation law holds:

$$A + X = B + X \Longrightarrow A = B. \tag{1.6}$$

The extension method. We recall that an abelian group is an ordered quadruple $(\mathcal{G}, +, 0, -)$ satisfying relations (1.3)–(1.5) and (1.7). An abelian monoid $(S, +, 0)$ turns into a (abelian) group if there exists an operation opp : $S \longrightarrow S$ such that

$$\mathrm{opp}(A) + A = 0 \ \text{ for all } \ A \in S; \tag{1.7}$$

instead of $\mathrm{opp}(A)$ we shall also write $-A$ or (whenever needed to avoid confusion) $-_S A$. Abelian cancellative monoids and abelian cancellative groups play important role in this study, for brevity we shall write "a. c." instead of "abelian cancellative".

In the a. c. monoid $(\mathcal{K}, +, 0)$ there is no opposite, hence the latter is not a group. However, there is a standard algebraic construction, further referred to as "the extension method", which allows us to embed isomorphically every a. c. monoid $(\mathcal{Q}, +, 0)$ into an a. c. group $(\mathcal{G}, +, 0, -)$ (see, e. g., [1]–[4], [7], [8]). Briefly, the extension method consists in the following: define $\mathcal{G} = (\mathcal{Q} \times \mathcal{Q})/\rho$ as the set of pairs

(A, B), A, $B \in \mathcal{Q}$, factorized by the equivalence relation $\rho : (A, B)\rho(C, D) \Longleftrightarrow A+D = B+C$. Addition in $\mathcal{G}$ is defined by means of: $(A, B)+(C, D) = (A+C, B+D)$. We shall denote the equivalence class in $\mathcal{G}$, represented by the pair (A, B), again by (A, B), thus $(A, B) = (A+X, B+X)$. The null element of $\mathcal{G}$ is the class (Z, Z); due to the existence of null element in $\mathcal{Q}$, we have $(Z, Z) = (0, 0)$. The opposite element to $(A, B) \in \mathcal{G}$ is $-(A, B) = (B, A)$; indeed $(A, B) + (-(A, B)) = (A, B) + (B, A) = (A + B, B + A) = (0, 0)$. Instead of $(A, B) + (-(C, D))$ we write $(A, B) - (C, D)$; we have $(A, B) - (C, D) = (A, B) + (D, C) = (A + D, B + C)$.

To embed isomorphically $\mathcal{Q}$ into $\mathcal{G}$, we identify $A \in \mathcal{Q}$ with the equivalence class $(A, 0) = (A+X, X)$, $X \in \mathcal{Q}$. Thus all "proper elements" of $\mathcal{G}$ are pairs (U, V), U, $V \in \mathcal{Q}$, such that $V+Y = U$ for some $Y \in \mathcal{Q}$, i. e. $(U, V) = (V+Y, V) = (Y, 0)$.

The group $(\mathcal{G}, +, 0, -)$ obtained by the extension method is minimal in the sense that if $(\mathcal{G}', +, 0, -)$ is any group in which $(\mathcal{Q}, +, 0)$ is embedded, then $(\mathcal{G}, +, 0, -)$ is isomorphic to a subgroup of $(\mathcal{G}', +, 0, -)$ containing $(\mathcal{Q}, +, 0)$. The group $(\mathcal{G}, +, 0, -)$ is unique up to isomorphism; we shall call it the *extension group induced by* $(\mathcal{Q}, +, 0)$.

Multiplication by scalar. Recall now some properties of (1.2). For $A, B \in \mathcal{K}$, $\gamma, \delta \in \mathbb{R}$ we have

$$\gamma * (A + B) = \gamma * A + \gamma * B, \tag{1.8}$$

$$\gamma * (\delta * A) = (\gamma\delta) * A, \tag{1.9}$$

$$1 * A = A, \tag{1.10}$$

where $\gamma\delta$ denotes the (linear) product of $\gamma, \delta \in \mathbb{R}$. The set of convex bodies together with operations (1.1), (1.2) will be denoted $(\mathcal{K}, +, \mathbb{R}, *)$ or $(\mathcal{K}, \mathbb{E}, +, \mathbb{R}, *)$.

Property (1.8) is known as "first distributive law". The so-called "second distributive law" is characteristic for any linear (vector) system, e. g. in the linear system $(\mathbb{E}^n, +, \mathbb{R}, \cdot)$ we have for every $C \in \mathbb{E}^n$

$$(\alpha + \beta) \cdot C = \alpha \cdot C + \beta \cdot C, \quad \alpha,\ \beta \in \mathbb{R}. \tag{1.11}$$

We recall that a system $(\mathcal{G}, +, \mathbb{R}, \cdot)$ is linear if: i) $(\mathcal{G}, +, 0, -)$ is an abelian group; ii) for all $a, b, c \in \mathcal{G}$, $\alpha, \beta, \gamma \in \mathbb{R}$

$$\begin{cases} \gamma \cdot (a + b) = \gamma \cdot a + \gamma \cdot b; \\ \gamma \cdot (\delta \cdot a) = (\gamma\delta) \cdot a; \\ 1 \cdot a = a; \\ (\alpha + \beta) \cdot c = \alpha \cdot c + \beta \cdot c. \end{cases} \tag{1.12}$$

The last relation in (1.12) is the second distributive law. Recall that in a linear system we have $0 \cdot a = 0$ and $(-1) \cdot a = -a$, hence we may omit the symbols "0" and "$-$" in the notation of a linear system.

The second distributive law (1.11) is not valid in $(\mathcal{K}, +, \mathbb{R}, *)$, apart of certain special cases. For example, for $C \in \mathcal{K}$ and equally signed scalars α, β we have

$$(\alpha + \beta) * C = \alpha * C + \beta * C, \quad \alpha\beta \geq 0. \tag{1.13}$$

Convex bodies are a. c. monoids with scalar operator satisfying (1.8)–(1.10), (1.13), see e. g. [16, 17]. It has been shown that such algebraic structure, called $\mathbb{R}$-semigroup with cancellation law, is characteristic for convex bodies [18].

Denote by $(\mathcal{L}, +, 0, -)$ the group induced by the semigroup of convex bodies $(\mathcal{K}, +, 0)$, $\mathcal{L} = (\mathcal{K} \times \mathcal{K})/\rho$. The following question arises:

Question 1. Can we embed isomorphically $(\mathcal{K}, +, \mathbb{R}, *)$ in a linear system $(\mathcal{L}, +, \mathbb{R}, \cdot)$ with $\mathcal{L} = (\mathcal{K} \times \mathcal{K})/\rho$? In other words, can we isomorphically extend (1.2) in $\mathcal{L}$, so that $\mathcal{L}$ (which is a group under addition) becomes a linear system, that is (1.12) are valid in $\mathcal{L}$?

H. Rådström shows that if we define a multiplication by scalar "$\cdot$" in $\mathcal{L}$ in terms of the multiplication by scalar (1.2) in $\mathcal{K}$ using the relation

$$\gamma \cdot (A, B) = \begin{cases} (\gamma * A, \gamma * B), & \gamma \geq 0, \\ (|\gamma| * B, |\gamma| * A), & \gamma < 0, \end{cases} \tag{1.14}$$

then $(\mathcal{L}, +, \mathbb{R}, \cdot)$ is a linear system, that is relations (1.12) hold true in $\mathcal{L}$ (see [16, Theorem 1]).

Formula (1.14) does not induce an isomorphic embedding of $(\mathcal{K}, +, \mathbb{R}, *)$ into the linear system $(\mathcal{L}, +, \mathbb{R}, \cdot)$. To see this, recall that under an isomorphic embedding the element $U \in \mathcal{K}$ is identified with $(U, 0) \in \mathcal{L}$, hence the element $U = \gamma * A \in \mathcal{K}$ is identified with $(\gamma * A, 0) \in \mathcal{L}$. Therefore the equality

$$\gamma \cdot (A, 0) = (\gamma * A, 0) \tag{1.15}$$

should hold true for all $A \in \mathcal{K}$, $\gamma \in \mathbb{R}$. However, (1.15) does not hold true for $\gamma < 0$, $A \in \mathcal{K} \setminus \mathbb{E}$. Indeed, from (1.14)

$$\gamma \cdot (A, 0) = ((-\gamma) * 0, (-\gamma) * A) = (0, -\gamma * A) \neq (\gamma * A, 0),$$

where the last inequality follows from $A + (-1) * A \neq 0$ for $A \in \mathcal{K} \setminus \mathbb{E}$.

An isomorphic extension of the multiplication by scalar (1.2) in $\mathcal{L}$ is given by the expression

$$\gamma * (A, B) = (\gamma * A, \gamma * B), \;\; A,\ B \in \mathcal{K}, \;\; \gamma \in \mathbb{R}. \tag{1.16}$$

For nonnegative scalars, (1.14) and (1.16) coincide, and an embedding theorem for convex cones holds true (see [16, Theorem 2]). Note that: i) the system $(\mathcal{K}, +, \mathbb{R}, *)$ is not linear, and ii) the induced via (1.16) system $(\mathcal{L}, +, \mathbb{R}, *)$ is not linear as well. We shall investigate in more detail the algebraic properties of these two systems of convex bodies. In particular, we shall point our attention towards extending relation (1.13) to include the case $\alpha\beta < 0$ and shall consider the following question:

Question 2. Can we embed isomorphically $(\mathcal{K}, +, \mathbb{R}, *)$ into $(\mathcal{L}, +, \mathbb{R}, *)$, where the operation "$*$" in $(\mathcal{L}, +, \mathbb{R}, *)$ is defined by (1.16), and what are the properties of the system $(\mathcal{L}, +, \mathbb{R}, *)$?

To answer this question we shall formulate some new algebraic properties of the original system $(\mathcal{K}, +, \mathbb{R}, *)$. Since we know that (1.8)–(1.10) hold true, what remains to be studied is distributivity. We therefore concentrate our attention to distributive relations, both in $\mathcal{K}$ and $\mathcal{L}$. We first prove a modification of (1.11) in $\mathcal{K}$, called quasidistributive law, which completes (1.13). We then find out the distributivity relation in $\mathcal{L}$ induced by (1.16) and call it "q-distributive" law. With the establishment of the distributivity relations in $\mathcal{K}$ and $\mathcal{L}$ we are able to give abstract definitions of $\mathcal{K}$ and $\mathcal{L}$ as algebraic systems, arriving thus to the concept of "quasilinear" and "q-linear" systems. We study the isomorphic embedding of the quasilinear system of convex bodies into the q-linear system of factorized pairs of convex bodies. We shall show that in a q-linear system relation (1.14) defines a linear multiplication by scalar, hence every q-linear system involves a linear one. Some of our results related to intervals, i. e. for convex bodies in $\mathbb{E}^1$, are published in [11, 12].

2. MINKOWSKI SUBTRACTION

A set A of the form $A = x + B$, for $x \in \mathbb{E}$, $B \in \mathcal{K}$, is called a *translate* of B (by the vector x). Clearly, if A is a translate of B by x, then B is a translate of A by $-x$, $B = A - x$.

Let $A, B \in \mathcal{K}$. The expression

$$A \stackrel{*}{-} B = \bigcap_{b \in B} (A - b) \tag{2.17}$$

is introduced for convex bodies and studied by H. Hadwiger (see, e. g., [5, 6]) under the name Minkowski difference. We consider (2.17) as a partial operation defined whenever the right-hand side is not empty. The following equivalent presentation of (2.17) holds:

$$A \stackrel{*}{-} B = \{x \in \mathbb{E} \mid x + B \subset A\}. \tag{2.18}$$

Expression (2.18) says that $A \stackrel{*}{-} B$ is the set of all vectors x such that the translate of B by x belongs to A. If there exists at least one $t \in \mathbb{E}$ such that $t + B \subset A$, then $A \stackrel{*}{-} B$ is well defined and $t \in A \stackrel{*}{-} B$; in this case we shall write $B \leq_M A$. As usual, we shall write $B =_M A$ if both $B \leq_M A$ and $A \leq_M B$ hold, that is, there exist $t, s \in \mathbb{E}$ such that $t + B \subset A$ and $s + A \subset B$. In other words, $B =_M A$ iff there exists $p \in \mathbb{E}$ such that $A + p = B$ (then $A = B - p$), that is A and B are translates of each other. In particular, $B \subset A$ implies $B \leq_M A$. From (2.18) we have for $A,\ B \in \mathcal{K}$ [6]

$$(A \stackrel{*}{-} B) + B \subset A, \tag{2.19}$$

$$(A + B) \stackrel{*}{-} B = A. \tag{2.20}$$

For $A, B \in \mathcal{K}$ we say that B is a *summand of* A if there exists $X \in \mathcal{K}$ such that $A = B + X$ (then X is a summand of A, too). Thus, we see from (2.19) that if B is a summand of A, then $A \stackrel{*}{-} B$ is a summand of A (see [20, Lemma 3.1.8]):

$$(A \stackrel{*}{-} B) + B = A. \tag{2.21}$$

In other words, if for $A, B \in \mathcal{K}$ some of the equations $A + X = B$, $B + Y = A$ is solvable, then the corresponding solution is $X = B \stackrel{*}{-} A$, resp. $Y = A \stackrel{*}{-} B$. The following equality has been established in [6]:

$$\lambda * (A \stackrel{*}{-} B) = \lambda * A \stackrel{*}{-} \lambda * B. \tag{2.22}$$

According to (1.13) for $\alpha\beta \geq 0$ the expression $(\alpha + \beta) * C$ can be written as a sum of the two terms of $\alpha * C$ and $\beta * C$. Can we express $(\alpha + \beta) * C$ in a similar way in the case $\alpha\beta < 0$? The answer is positive. H. Hadwiger [6] proves the following equality:

$$(\lambda - \mu) * A = \lambda * A \stackrel{*}{-} \mu * A, \;\; \lambda > \mu > 0. \tag{2.23}$$

Relation (2.23) can be rewritten in the following form, cf. also [14:

$$(\alpha + \beta) * C = \alpha * C \stackrel{*}{-} (-\beta) * C, \;\; \alpha > 0, \, -\alpha < \beta < 0. \tag{2.24}$$

Hence, for $\alpha\beta < 0$, (2.24) can be written more symmetrically as

$$(\alpha + \beta) * C = \begin{cases} \alpha * C \stackrel{*}{-} (-\beta) * C, & \text{if } |\alpha| \geq |\beta|, \\ \beta * C \stackrel{*}{-} (-\alpha) * C, & \text{if } |\alpha| < |\beta|. \end{cases}$$

3. SUMMABILITY

To formulate and prove a generalization of (1.13) in $\mathcal{K}$, which is valid for all α, $\beta \in \mathbb{R}$, we first concentrate on some further properties of the convex bodies, related to Minkowski subtraction. For our purposes we shall make use of the cancellation law (1.6): $A + X = B + X \Longrightarrow A = B$ for $A, B, X \in \mathcal{K}$.

For given $A, B \in \mathcal{K}$, if there exists an $X \in \mathcal{K}$ such that B is a summand of A (i. e. $B + X = A$), then, due to (1.5) and (1.6), we have in $\mathcal{L}$ the presentation $(A, B) = (B + X, B) = (X, 0)$.

Proposition 1. *For $A, B \in \mathcal{K}$, if B is a summand of A, then there exists a unique $X \in \mathcal{K}$ such that $A = B + X$.*

Proof. By assumption, there is some $X \in \mathcal{K}$ such that $A = B + X$. Assume that $X' \in \mathcal{K}$, with $X' \neq X$, is such that $A = B + X'$. Then we have $B + X = B + X'$, which by the cancellation law (1.6) implies $X = X'$, a contradiction. □

Proposition 2. *Let $A, B \in \mathcal{K}$. The equality $A + B = 0$ implies $A, B \in \mathbb{E}$ and $B = -A$.*

In what follows we shall symbolically denote the relation "B is a summand of A" by $B \leq_\Sigma A$, or $A \geq_\Sigma B$; "$\leq_\Sigma$" is a partial order in $\mathcal{K}$. The assertion "B is not a summand of A" will be denoted by $B \not\leq_\Sigma A$. Obviously, $B \leq_\Sigma A$ implies $B \leq_M A$; however, the inverse is not true.

Generally speaking, for every A, $B \in \mathcal{K}$ there exist four possibilities: 1) $B \leq_\Sigma A$ and $A \not\leq_\Sigma B$, denoted $B <_\Sigma A$; 2) $A \leq_\Sigma B$ and $B \not\leq_\Sigma A$, denoted $A <_\Sigma B$; 3) $A \leq_\Sigma B$ and $B \leq_\Sigma A$, denoted $A =_\Sigma B$; 4) $A \not\leq_\Sigma B$ and $B \not\leq_\Sigma A$. Note that $A =_\Sigma B$ is equivalent to $A =_M B$, that is A and B are translates of each other.

In cases 1)–3) we say that the pair $(A, B) \in \mathcal{L}$ is *Σ-comparable.* We shall further denote the set of all Σ-comparable pairs by $\mathcal{L}_\Sigma$. Clearly, if $(A, B) \in \mathcal{L}_\Sigma$, then at least one of the expressions $A \stackrel{*}{-} B$, $B \stackrel{*}{-} A$ is well defined.

In case 3) there exists a unique $X \in \mathcal{K}$ such that $A = B + X$ and a unique $Y \in \mathcal{K}$ such that $B = A + Y$. Summing up both equations, we obtain $A + B = (B+X)+(A+Y) = (A+B)+X+Y$, and by (1.6), $X+Y = 0$. By Proposition 2, the solutions X, Y are opposite to each other; they belong to the set $\mathbb{E}$ of degenerate convex bodies (one-point sets). Thus, in case 3) A is a translate of B by the vector P, and, conversely, B is a translate of A by $-P$, that is $B = A + (-P)$, where $-P = -_{\mathbb{E}}P$ is the opposite of P in $\mathbb{E}$ (the point sets P and $-P$ are symmetric with respect to the origin 0 of $\mathbb{E}$).

We summarize the above arguments in the next proposition.

Proposition 3 (T-property). *Let $A, B \in \mathcal{K}(\mathbb{E})$, $(A, B) \in \mathcal{L}_\Sigma$. For the equations*

$$B + X = A, \tag{3.25}$$

$$A + Y = B \tag{3.26}$$

exactly one of the following three possibilities holds true:

1) *Case $B <_\Sigma A$: there exists a unique nondegenerate convex body $X \in \mathcal{K} \setminus \mathbb{E}$ satisfying* (3.25)*; equation* (3.26) *is not solvable.*

2) *Case $A <_\Sigma B$: there exists a unique nondegenerate convex body $Y \in \mathcal{K} \setminus \mathbb{E}$ satisfying* (3.26)*; equation* (3.25) *is not solvable.*

3) *Case $A =_\Sigma B$: both* (3.25) *and* (3.26) *are solvable for X, resp. Y, and $Y = -X \in \mathbb{E}$.*

From the cancellation law it follows that for arbitrary $A, B \in \mathcal{K}$ each of the equations (3.25), (3.26) may have at most one solution.

Proposition 4. *Let for $A, B, C \in \mathcal{K}$, $A + B = C$ and $0 \in A$. Then $B \subset C$.*

Proof. Equation $A + B = C$, that is $\bigcup_{a \in A} a + B = C$, means $a + B \subset C$ for all $a \in A$. Hence for $a = 0$, $B = 0 + B \subset C$. □

In the next section we study an operator in $\mathcal{K}$ called "negation", which plays an important role for the algebraic description of the properties of the set of convex bodies.

4. NEGATION

Substituting $\alpha = -1$ in (1.2) we obtain the operator

$$(-1) * A = \{-a \mid a \in A\}, \quad A \in \mathcal{K}, \tag{4.27}$$

called *negation*, which will be denoted by $\neg A = (-1) * A$ or $\text{neg}(A)$. Obviously, $\neg(\gamma * A) = (-1) * (\gamma * A) = (-\gamma) * A$.

The following properties of negation are easily verified:

$$\neg(\neg A) = A, \quad A \in \mathcal{K}, \tag{4.28}$$

$$\neg(A + B) = (\neg A) + (\neg B), \quad A,\ B \in \mathcal{K}, \tag{4.29}$$

$$\neg P + P = 0 \Longleftrightarrow P \in \mathbb{E} \Longleftrightarrow \neg P = -P, \tag{4.30}$$

$$\neg A = 0 \Longleftrightarrow A = 0, \quad A \in \mathcal{K}. \tag{4.31}$$

Properties (4.28)–(4.29) mean that negation is a dual automorphism (involution). Property (4.30) means that a convex body $P \in \mathcal{K}$ satisfies $\neg P + P = 0$ if and only if P is a degenerate, in which case the negation $(\neg)$ coincides with the opposite operator $(-)$ in the set $\mathbb{E}$ of degenerate (one-point) elements of $\mathcal{K}$, i. e. $-P + P = 0$. Of course, $\neg A + A = 0$ does not hold in $\mathcal{K} \setminus \mathbb{E}$, since nondegenerate convex bodies have no opposite elements. We see that negation isomorphically extends the opposite from $\mathbb{E}$ to $\mathcal{K}$.

For brevity, we shall denote for $A,\ B \in \mathcal{K}$

$$A \neg B \equiv A + (\neg B) = A + (-1) * B = \{a - b \mid a \in A,\ b \in B\}; \tag{4.32}$$

the operation $A \neg B$ is called an (*outer*) *subtraction*.

Remarks. Instead of the symbol "$\neg$" we may use "$-$" as it is well adopted in the literature on interval and set-valued analysis (see, e. g., [10, 19]); however it should be kept in mind that there is no opposite operator in $\mathcal{K}$, and that $A \neg A \neq 0$ for $A \in \mathcal{K} \setminus \mathbb{E}$. Since the notation "$-$" is usually associated with the equality $A - A = 0$, to avoid confusion we write "$\neg$" instead of "$-$". Using "$\neg$", we also avoid confusion with the opposite in $\mathcal{L}$. In mathematical morphology the outer subtraction (4.32) is called *dilatation*, whereas the Minkowski subtraction is called *erosion* [15].

Definition. $A \in \mathcal{K}$ is called *symmetric* (*with respect to the origin*) if $x \in \mathbb{E}$, $x \in A$, implies $-x \in A$.

Obviously, $A \in \mathcal{K}$ is symmetric if and only if $A = \neg A$. For $A \in \mathcal{K}$ the set $A \neg A$ is called the difference body of A (see [20, p. 127]). The set of all symmetric convex bodies is denoted by $\mathcal{K}_S$, that is $\mathcal{K}_S = \{A \in \mathcal{K} \mid A = \neg A\}$.

Proposition 5. *For $A \in \mathcal{K}$ we have $A \neg A \in \mathcal{K}_S$.*

Proof. Let $x \in \mathbb{E}$ be such that $x \in A \neg A$. Then, from (4.32) $-x \in \neg(A \neg A) = (\neg A)\neg(\neg A) = (\neg A) + A = A \neg A$, using properties (4.28), (4.29). □

Proposition 6. *The following two conditions for symmetricity of $A \in \mathcal{K}$ are equivalent:*

i) $A = \neg A$;

ii) *there exists $Z \in \mathcal{K}$ such that $A = Z \neg Z$.*

Proof. i) Let $A = \neg A$. Assume $t \in \mathbb{E}$ and set $Z = A/2 + t$, where $A/2 = (1/2) * A$. Using $A = \neg A$, we obtain $\neg Z = \neg A/2 - t = A/2 - t$. Hence $Z \neg Z = Z + (\neg Z) = (A/2 + t) + (A/2 - t) = A$.

ii) Assume that $A = Z \neg Z$ for some $Z \in \mathcal{K}$. Then we have $\neg A = \neg(Z \neg Z) = \neg Z + Z = Z \neg Z = A$. □

Definition. $A \in \mathcal{K}$ is called *t-symmetric*, with *center* $t \in \mathbb{E}$, if $(A - t) \in \mathcal{K}_S$.

In other words, a t-symmetric element is a translate by t of a symmetric element.

Proposition 7. *Every t-symmetric convex body A is a translate of its negation $\neg A$.*

Proof. Let $A \in \mathcal{K}$ be t-symmetric. We have to show that there exists $P \in \mathbb{E}$ such that $\neg A + P = A$. Since A is t-symmetric, $A - t$ is symmetric, that is $(A - t) = \neg(A - t) = \neg A + t$. This implies $\neg A + 2t = A$, hence A is a translate by $2t$ of $\neg A$; we found $P = 2t$. □

Remark. Let $A \in \mathcal{K}$ be t-symmetric, i. e. $(A - t) \in \mathcal{K}_S$. By Proposition 6 there exists $Z \in \mathcal{K}$ such that $A - t = Z \neg Z$. To find an expression for Z, fix $s \in \mathbb{E}$ and set $Z = (A - t)/2 + s$; we obtain $Z = A/2 + s'$, $s' \in \mathbb{E}$. Thus $A - t = Z \neg Z = A/2 \neg A/2 = (A \neg A)/2$. We thus have $A - t = (A \neg A)/2$, that is for any t-symmetric element $A \in \mathcal{K}$ its symmetric translate by $-t$ is $(A \neg A)/2$.

5. INNER OPERATIONS

Inner addition in $\mathcal{K}$. *Inner sum* $A +^- B$ is defined for (some) $A, B \in \mathcal{K}$ by

$$A +^- B = \begin{cases} \bigcap_{b \in B} (A + b), & \text{if } \neg B \leq_M A, \\ \bigcap_{a \in A} (B + a), & \text{if } \neg A <_M B. \end{cases}$$

Remark. The inner sum is defined whenever one of the conditions in the right-hand side is fulfilled. Note that $\neg B \leq_M A$ is equivalent to $B \leq_M \neg A$. Note also that if both $\neg B \leq_M A$ and $\neg A \leq_M B$ hold, that is $\neg B =_M A$, then $\neg B = A + t$ for some $t \in \mathbb{E}$. In this case it can be shown that both intersections in the right-hand side of the above definition produce the same result. Therefore we can replace the second condition above by $\neg A \leq_M B$ (or $A \leq_M \neg B$).

Inner difference $A -^- B$, for $A, B \in \mathcal{K}$, is defined by the equality $A -^- B \equiv A +^- (\neg B)$ [11, 12].

In the situation when $(A, \neg B) \in \mathcal{L}_\Sigma$, resp. $(A, B) \in \mathcal{L}_\Sigma$, the inner addition, resp. inner subtraction, admits simple presentation. Namely, we have

$$A +^- B = \begin{cases} Y|_{\neg B+Y=A}, & \text{if } \neg B \leq_\Sigma A, \\ X|_{\neg A+X=B}, & \text{if } \neg A \leq_\Sigma B, \end{cases} \tag{5.33}$$

$$A -^- B = \begin{cases} Y|_{B+Y=A}, & \text{if } B \leq_\Sigma A, \\ X|_{A\neg X=B}, & \text{if } A \leq_\Sigma B. \end{cases} \tag{5.34}$$

The inner operations (5.33) and (5.34) are related by $A +^- B = A -^- (\neg B)$. Note that $A \leq_M B$ does imply $\neg A \leq_M \neg B$, but does not necessarily imply $\neg A \leq_M B$. Due to this fact, for some A, $B \in \mathcal{K}$ it may happen that $A +^- B$ is defined, but $A -^- B$ is not, or vice versa.

A relation between the inner operations and the Minkowski difference is given by

$$\begin{aligned} A +^- B &= (A \stackrel{*}{-} (\neg B)) \cup (B \stackrel{*}{-} (\neg A)), \\ A -^- B &= (A \stackrel{*}{-} B) \cup \neg(B \stackrel{*}{-} A). \end{aligned}$$

Inner addition is commutative, $A +^- B = B +^- A$; other important property is $A -^- A = 0$.

Proposition 8. *Let* $(A, \neg B) \in \mathcal{L}_\Sigma$. *Then* $A +^- B \leq_\Sigma A + B$ *and* $A +^- B \subset A + B$.

Proof. From (5.33) we immediately see that $A +^- B$ is a summand of $A + B$. Indeed, if $\neg B \leq_\Sigma A$, we have $\neg B + (A +^- B) = A$, hence $B \neg B + (A +^- B) = A + B$. If $\neg A \leq_\Sigma B$, then $\neg A + (A +^- B) = B$, and hence $A \neg A + (A +^- B) = A + B$. Since in both cases the other summand contains 0 (indeed, $A \neg A \ni 0$ and $B \neg B \ni 0$), we have $A +^- B \subset A + B$, using Proposition 4 and $A +^- B \leq_\Sigma A + B$ as well. □

Remark. The proof can be generalized (cf. [15]) for the more general case when either $B \leq_M A$ or $A \leq_M B$ (in which case it may happen that $(A, \neg B) \notin \mathcal{L}_\Sigma$). Most of the results in the sequel can be extended to this more general case.

Proposition 9. *Let* $(A, \neg B) \in \mathcal{L}_\Sigma$. *Then*

$$(A, \neg B) = \begin{cases} (A +^- B, 0), & \textit{if } \neg B \leq_\Sigma A, \\ (0, \neg(A +^- B)), & \textit{if } \neg B >_\Sigma A. \end{cases}$$

Proof. From (5.33), if $\neg B \leq_\Sigma A$, then $\neg B + (A +^- B) = A$. Hence $(A, \neg B) = (\neg B + (A +^- B), \neg B) = (A +^- B, 0)$. The case $\neg B >_\Sigma A$ is treated analogously, using that $B >_{sig} \neg A$ implies $B = \neg A + (A +^- B)$, hence $\neg B = A + \neg(A +^- B)$.

Proposition 10. *Let $C \in \mathcal{K}$, $\alpha \in \mathbb{R}$, $\alpha \geq 0$. Then*

$$C \geq_\Sigma \alpha * C, \quad \text{if} \quad 0 \leq \alpha \leq 1,$$
$$C \leq_\Sigma \alpha * C, \quad \text{if} \quad \alpha \geq 1.$$

Proof. Let $0 \leq \alpha \leq 1$. We have to verify that $\alpha * C$ is a summand of C, that is $\alpha * C + X = C$ for some $X \in \mathcal{K}$. Take $X = (1-\alpha) * C$. Substituting $\beta = 1 - \alpha \geq 0$ in

$$\alpha * C + \beta * C = (\alpha + \beta) * C, \;\; \alpha\beta \geq 0,$$

we obtain $\alpha * C + (1-\alpha) * C = (\alpha + 1 - \alpha) * C = C$, showing that $C \geq_\Sigma \alpha * C$, for $\alpha \in [0,1]$. Let $\alpha \geq 1$. We look for Y such that $\alpha * C = Y + C$. Taking $Y = (\alpha - 1) * C$, we see that $C \leq_\Sigma \alpha * C$ for $\alpha \geq 1$. □

The above proposition shows that for $\alpha \in (0,1)$ the solution of $C = \alpha * C + X$ is $X = (1-\alpha) * C$.

Proposition 11. *Let $\alpha, \beta \in \mathbb{R}$, $C \in \mathcal{K}$. If $\alpha\beta > 0$, then $(\alpha * C, \beta * C) \in \mathcal{L}_\Sigma$. If $\alpha\beta < 0$, then $(\neg\alpha * C,\ \beta * C) \in \mathcal{L}_\Sigma$.*

Proof. The case $\alpha\beta = 0$ is obvious. Let $\alpha\beta > 0$, say $\alpha \geq \beta > 0$. We shall show that the pair $(\alpha * C, \beta * C)$ is Σ-comparable, and $\beta * C \leq_\Sigma \alpha * C$. By Proposition 10 we have that C and $(\alpha/\beta) * C$, $\alpha/\beta > 1$ are Σ-comparable with $(\alpha/\beta) * C \geq_\Sigma C$, that is $C + X = (\alpha/\beta) * C$ is solvable. Then $\beta * C + Y = \alpha * C$ is solvable, i. e. $\alpha * C \geq_\Sigma \beta * C$. The other subcases of $\alpha\beta > 0$ are treated similarly. The case $\alpha\beta < 0$ is reduced to the previous case by setting $\alpha = -\gamma$. □

Proposition 12. *Let α, $\beta \in \mathbb{R}$, $\alpha\beta < 0$, $C \in \mathcal{K}$. Then*

$$(\alpha + \beta) * C = \alpha * C +^- \beta * C.$$

Proof. Without a loss of generality we may assume that $\alpha > 0$, $\beta < 0$. Denote $-\beta = \gamma > 0$. Using (5.33), we obtain

$$\begin{aligned}
\alpha * C +^- \beta * C &= \begin{cases} Y|_{\gamma * C + Y = \alpha * C}, & \text{if } \gamma * C \leq_\Sigma \alpha * C, \\ X|_{\alpha * C + (\neg X) = \gamma * C}, & \text{if } \alpha * C \leq_\Sigma \gamma * C; \end{cases} \\
&= \begin{cases} (\alpha - \gamma) * C, & \gamma \leq \alpha, \\ \neg(\gamma - \alpha) * C, & \alpha \leq \gamma; \end{cases} \\
&= (\alpha - \gamma) * C = (\alpha + \beta) * C.
\end{aligned}$$

In the proof we make use of Proposition 10. □

Denote the sign of the real number $\alpha \in \mathbb{R}$ by $\sigma(\alpha) \in \{+, -\}$, that is:

$$\sigma(\alpha) = \begin{cases} +, & \text{if } \alpha \geq 0, \\ -, & \text{if } \alpha < 0. \end{cases}$$

Assuming $+^+ = +$, we can combine Proposition 12 and relation (1.13) in the following general *quasidistributive law*: for every $\alpha, \beta \in \mathbb{R}$, $C \in \mathcal{K}$,

$$(\alpha + \beta) * C = \alpha * C +^{\sigma(\alpha\beta)} \beta * C. \tag{6.35}$$

7. QUASILINEAR SYSTEMS OF CONVEX BODIES

As already mentioned, due to (1.3)–(1.6) the system $(\mathcal{K}, +, 0)$ is an (additive) a. c. monoid. This system is a *proper* semigroup (i. e. not a group itself), which means that there exists at least one pair (A, B) such that $A + X = B$ has no solution for $X \in \mathcal{K}$. The monoid $(\mathcal{K}, +, 0)$ has a unique idempotent element e (such that $e + e = e$), which is the null element ($e = 0$). For a semigroup $(\mathcal{Q}, +)$ with only one idempotent element it is known that the set $\mathcal{Q}_0$ of all invertable elements $u \in \mathcal{Q}$ (i. e., such that $u + v = 0$ for some v) is a group $(\mathcal{Q}_0, +, 0, -)$, which is the unique maximal subgroup of the semigroup (see, e. g., [1, Section 1.7]). Recall that a subgroup $(\mathcal{M}, +)$ of a semigroup $(\mathcal{Q}, +)$ is called maximal (with respect to "$\subset$") if there is no other subgroup $(\mathcal{M}', +)$ of $(\mathcal{Q}, +)$ such that $\mathcal{M}' \supset \mathcal{M}$ and $\mathcal{M} \neq \mathcal{M}'$. If no doubt occurs, we shall further say "the subgroup of the monoid" instead of "the unique maximal subgroup of the monoid".

Using the above terminology, we can say that the system of convex bodies $(\mathcal{K}, +, 0)$ involves the group $(\mathbb{E}, +, 0)$, which is the (maximal) subgroup of $\mathcal{K}$ comprising all invertible elements of $\mathcal{K}$.

Given a semigroup $(\mathcal{Q}, +)$, we shall call $\pi : \mathcal{Q} \longrightarrow \mathcal{Q}$ an *involution in* $\mathcal{Q}$ if it is a dual automorphism, that is:

i) $\pi(\pi(A)) = A$ for $A \in \mathcal{Q}$;

ii) $\pi(A + B) = \pi(A) + \pi(B)$ for $A, B \in \mathcal{Q}$.

A proper a. c. monoid $(\mathcal{Q}, +, 0)$ with (maximal) subgroup $(\mathcal{Q}_0, +, 0, -)$ will be further denoted $(\mathcal{Q}, \mathcal{Q}_0, +)$. The subgroup $(\mathcal{Q}_0, +, 0, -)$ contains the trivial group, and, in particular, it may happen that $\mathcal{Q}_0 = \{0\}$. In $(\mathcal{Q}, \mathcal{Q}_0, +)$ we define negation as follows:

Definition. Let $(\mathcal{Q}, \mathcal{Q}_0, +)$ be a proper a. c. monoid. An involution neg : $\mathcal{Q} \to \mathcal{Q}$ is called *negation* in $(\mathcal{Q}, \mathcal{Q}_0, +)$ if it extends the operator opposite from $\mathcal{Q}_0$ to $\mathcal{Q}$: $\mathrm{neg}(P) = -_{\mathcal{Q}_0} P$ for $P \in \mathcal{Q}_0$ (i. e. $\mathrm{neg}(P) + P = 0$, $P \in \mathcal{Q}_0$).

It is easily seen that $\mathrm{neg}(A) = 0 \iff A = 0$ for $A \in \mathcal{Q}$, which corresponds to (4.31).

We shall further require that negation is unique (sufficient conditions for uniqueness will be discussed elsewhere).

Definition [12]. A proper a. c. monoid $(\mathcal{Q}, \mathcal{Q}_0, +)$ with unique operator negation "neg = $\neg$" is called a *quasimodule* and is denoted by $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$.

Remark. Note that a quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$ is not a group, but it possesses the same number of basic operations as a group does: one binary "+", one unary "¬", and one nullary operation "0", and the algebraic properties of $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$ are close to those of a group.

The relation "$\leq_\Sigma$" is defined in a general semigroup in the same manner as it is done in the semigroup $(\mathcal{K}, +)$, see Sections 2, 3. Inner addition "$+^-$" and inner subtraction "$-^-$" in a quasimodule are partial operations defined by (5.33)–(5.34), hence the quasidistributivity law (6.35) mentioned in the next definition makes sense.

Definition. Multiplication by scalar $* : \mathbb{R} \times \mathcal{Q} \longrightarrow \mathcal{Q}$, in a quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$ is a scalar operator over $\mathbb{R}$ satisfying relations (1.8)–(1.10), (6.35), and such that $(-1) * A = \neg A$ for all $A \in \mathcal{Q}$.

The last assumption $(-1) * A = \neg A$ means that negation is a special case of multiplication by scalar. Note also that the multiplication by integers $n * A = A + A + \cdots + A$ is consistent with the multiplication by (real) scalar (1.2), hence the symbol "$*$" makes sense in expressions like $2 * A = A + A$; we also have $\neg(n * A) = (-1) * (n * A) = (-n) * A$.

Definition. A quasimodule endowed with multiplication by scalar is called *quasilinear system (over the field* $\mathbb{R}$), or $\mathbb{R}$-*quasimodule*, and is denoted by $(\mathcal{Q}, \mathcal{Q}_0, +, \mathbb{R}, *)$.

We borrow the notion "quasilinear" from [13], where this notion is used to denote a similar algebraic system of convex bodies over $\mathbb{E}^1$, that is intervals.

If the subgroup of a quasimodule $\mathcal{Q}$ is $\mathcal{Q}_0 = (\{0\}, +)$, then negation and identity coincide. Due to $\neg A = A$, in a quasimodule with (maximal) subgroup 0 we have $A + B = A \neg B$ and $A +^- B = A -^- B$.

Example 1. The subgroup of the monoid of convex bodies is $(\mathbb{E}, +, 0)$, hence the corresponding $\mathbb{R}$-quasimodule is $(\mathcal{K}, \mathbb{E}, +, \mathbb{R}, *)$ (also to be further referred to as *quasilinear system of convex bodies*).

Example 2. The system of symmetric elements $(\mathcal{K}_S, 0, +)$ is a quasimodule with subgroup $(\{0\}, +)$. The quasilinear system of symmetric elements is $(\mathcal{K}_S, 0, +, \mathbb{R}, *)$. Due to $\neg B = (-1) * B = B$ it is easy to check that $\alpha * B = |\alpha| * B$ for $B \in \mathcal{K}_S$. Using (1.2), this implies $\alpha * B = \{\alpha x \mid x \in B\} = \{|\alpha| x \mid x \in B\}$.

Example 3 [17]. Another instructive example of a quasilinear system with (maximal) subgroup 0 is the system $(\mathbb{R}^+, 0, +, \mathbb{R}, *)$, where $(\mathbb{R}^+, +)$ is the semigroup of nonnegative reals with subgroup $(\{0\}, +)$. The system $(\mathbb{R}^+, 0, +, \mathbb{R}, *)$ can be considered as a subsystem of $(\mathcal{K}_S, 0, +, \mathbb{R}, *)$ whenever $\mathcal{K}_S$ is replaced by a subset of symmetric bodies of the form $\mathcal{K}'_S = r * B$, $r \in \mathbb{R}^+$, with $B \in \mathcal{K}_S$, $B \neq 0$, fixed; then $\mathcal{K}'_S \cong \mathbb{R}^+$. The multiplication by scalar $* : \mathbb{R} \times \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ satisfies $\alpha * A = |\alpha| * A$. In this system we have $A +^- B = A -^- B = |A - B|$, where $|A - B|$

is defined in $\mathbb{R}^+$ by $\{A - B, \text{ if } B \leq A;\ B - A, \text{ if } A < B\}$. By definition, $A - B$ for $B \leq A$ is the solution of $B + X = A$.

8. THE Q-LINEAR SYSTEM

Here we shall further stay within the framework of abstract algebraic systems. This approach allows us to summarize several important special cases, such as the ones considered in Examples 1–3.

Recall that every quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$ is an a. c. monoid, and, according to the extension method mentioned in the introduction, the quasimodule induces an extension group with supporting set $\mathcal{G} = (\mathcal{Q} \times \mathcal{Q})/\rho$. The extension group has opposite $\text{opp}(A, B) = (B, A)$, which will be denoted symbolically by "$-_{\mathcal{G}}$" or just "$-$". Negation ($\text{neg} = \neg$) in the quasimodule induces a corresponding operator in the extension group $(\mathcal{G}, +)$ by means of $\text{neg}(A, B) = (\text{neg}(A), \text{neg}(B))$, $A, B \in \mathcal{Q}$, which will be again called *negation* (in $\mathcal{G}$) and denoted symbolically by "$\neg$": $\neg(A, B) = (\neg A, \neg B)$. The set of invertable elements $\mathcal{Q}_0$ of the monoid is isomorphic to a subset of $\mathcal{G}$ of the form $\mathcal{G}_0 = \{(P, 0) \mid P \in \mathcal{Q}_0\}$, which is subgroup of the extension group: $(\mathcal{G}_0, +, 0, -) \cong (\mathcal{Q}_0, +, 0, -)$. We shall incorporate the important elements "$\mathcal{G}_0$", "$-$", "$\neg$" (and, of course, "$+$") in the notation of the extension group induced by the quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$, writing thus $(\mathcal{G}, \mathcal{G}_0, +, -, \neg)$.

Let us first discuss in some detail the automorphisms in the extension group $(\mathcal{G}, \mathcal{G}_0, +, -, \neg)$. Denote the identity in $\mathcal{G}$ by "id" and the operator, which is a composition "$\circ$" of negation and opposite, by dual: $\text{dual} = \text{neg} \circ \text{opp}$, that is $\text{dual}(a) = \text{neg}(\text{opp}(a))$ for $a \in \mathcal{G}$; the operator $\text{dual}(a)$ is called *dualization* (or *conjugation*). Since negation and opposite are involutions, dualization is also involution. Any two of the four involutions id, neg, opp and dual in $\mathcal{G}$ are composed to each other according to Table 1.

TABLE 1
Composition table for the involutions in $\mathcal{G}$

$\circ$	id	neg	opp	dual
id	id	neg	opp	dual
neg	neg	id	dual	opp
opp	opp	dual	id	neg
dual	dual	opp	neg	id

Let $(\mathcal{G}, \mathcal{G}_0, +, \neg)$ with $\mathcal{G} = (\mathcal{Q} \times \mathcal{Q})/\rho$ and $\mathcal{G}_0 \cong \mathcal{Q}_0$ be the extension group generated by the quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$, and let π be any of the operators opposite or negation in $\mathcal{G}$. As already mentioned, π is an involution in the sense that:

C1) $\pi(\pi(a)) = a$ for $a \in \mathcal{G}$;

C2) $\pi(a + b) = \pi(a) + \pi(b)$ for $a, b \in \mathcal{Q}$;

C3) $\pi(a) = 0 \Longleftrightarrow a = 0$ for $a \in \mathcal{G}$.

It is important to note that the both involutions "opp" and "neg" extend the operator "opp" from $\mathcal{Q}_0$ into $\mathcal{G}$, that is:

C4) $\pi(p) = -_{\mathcal{Q}_0}(p)$, i. e. $\pi(p) + p = 0$, for $p \in \mathcal{G}_0 \cong \mathcal{Q}_0$.

Since both opposite and negation satisfy conditions C1)–C4), it is interesting to formulate characteristic conditions for the distinction of these two operators. One such distinctive property is that $\text{opp}(p) + p = 0$ for every $p \in \mathcal{G}$, whereas $\text{neg}(p) + p \neq 0$ for $p \in \mathcal{G} \setminus \mathcal{G}_0$. We shall next consider another distinctive property.

The class $\mathcal{G}_\Sigma$ of Σ-comparable elements of $\mathcal{G}$ is

$$\mathcal{G}_\Sigma = \{(U, 0) \mid U \in \mathcal{Q}\} \bigcup \{(0, V) \mid V \in \mathcal{Q}\}. \tag{8.36}$$

The function *type* (or *direction*) of an element of $\mathcal{G}_\Sigma$ is defined by

$$\tau(A, B) = \begin{cases} +, & \text{if } B \leq_\Sigma A, \\ -, & \text{if } A <_\Sigma B. \end{cases} \tag{8.37}$$

The form of presentation $(U, 0)$, resp. $(0, V)$, appearing in (8.36) is similar to the form used for real numbers; indeed, we may write $(U; +)$ for $(U, 0)$ and $(V; -)$ for $(0, V)$ as we do with positive, resp. negative, numbers.

An element $(A, B) \in \mathcal{G}_\Sigma$ is *proper* if $(A, B) = (U, 0)$ for some $U \in \mathcal{Q}$. According to the extension method the element $W \in \mathcal{Q}$ is identified with the proper element $(W, 0) \in \mathcal{G}_\Sigma$. Improper Σ-comparable elements are of the form $(A, B) = (0, V)$, $V \in \mathcal{Q} \setminus \mathcal{Q}_0$. A special case of proper elements are the degenerate $(U, 0)$ with $U \in \mathcal{Q}_0$. Using the notation (8.37), $a \in \mathcal{G}_\Sigma$ is proper if $\tau(a) = +$, and improper if $\tau(a) = -$. According to Proposition 9, using inner addition we can present any Σ-comparable element of $\mathcal{G}$ in the "$(\pm)$-form $(U, 0)$ or $(0, V)$, resp. $(A; \pm)$.

If an element $a \in \mathcal{G}_\Sigma$ is proper, then $\text{neg}(a)$ is also proper, since $a = (A, 0)$ implies $\text{neg}(A, 0) = (\text{neg}(A), 0)$ for $A, B \in \mathcal{Q}$. If an element b is improper, then $\text{neg}(b) = \text{neg}(0, B) = (0, \text{neg}(B))$, showing that negation preserves the type, that is:

C5) $\tau(\text{neg(a)}) = \tau(\text{a})$ for $a \in \mathcal{G}_\Sigma$.

On the other side, for a nondegenerate a:

C6) $\tau(\text{opp(a)}) = -\tau(\text{a})$ for $a \in \mathcal{G}_\Sigma$,

where $-\tau$ is defined by $-- = +$, $-+ = -$.

The operators identity "id" and "dual" satisfy C1)–C3) and, instead of C4), the condition:

C7) $\pi(p) = p$ for $p \in \mathcal{G}_0$.

However, unlike identity, dualization changes the type of a Σ-comparable element. We summarize the above observations as follows:

Proposition 13. *The quasimodule $(\mathcal{Q}, \mathcal{Q}_0, +, \neg)$ generates (by means of the extension method) a system $(\mathcal{G}, \mathcal{G}_0, +, -, \neg)$ such that:*

1) $\mathcal{G} = (\mathcal{Q} \times \mathcal{Q})/\rho$; $(\mathcal{G}_0, +, 0, -) \cong (\mathcal{Q}_0, +, 0, -)$; *the opposite in* $\mathcal{G}$ *is*: $\mathrm{opp}(A, B) = -(A, B) = (B, A)$, $A, B \in \mathcal{Q}$.

2) *Negation in* $\mathcal{G}$ *is given by* $\mathrm{neg}(A, B) = (\mathrm{neg}(A), \mathrm{neg}(B))$, $A, B \in \mathcal{Q}$; *dualization, which is a composition of negation and opposite, is*: $\mathrm{dual}(A, B) = \mathrm{neg}(B, A) = (\mathrm{neg}(B), \mathrm{neg}(A))$, $A, B \in \mathcal{Q}$. *Opposite and negation coincide on* $\mathcal{G}_0$ *and dual coincides on* $\mathcal{G}_0$ *with identity. Opposite and dualization change the type of the* Σ-*comparable elements, whereas negation does not influence the type. The four automorphisms on* $\mathcal{G}$*: identity, opposite, negation and dualization, obey composition rules according to Table* 1.

The following symbolic notation will be used: for $a \in \mathcal{G}$ we write $\mathrm{dual}(a) = a_-$, $a = a_+$; then a_σ is either a or $\mathrm{dual}(a)$ according to the value of $\sigma \in \{+, -\}$. In such notation we have for $U, V \in \mathcal{Q}$: $(U, V)_- = (\neg V, \neg U)$.

The multiplication by scalar "$*$" in the quasilinear system $(\mathcal{Q}, \mathcal{Q}_0, +, \mathbb{R}, *)$ induces a corresponding multiplication in the extension group $(\mathcal{G}, \mathcal{G}_0, +, -, \neg)$ by means of the relation

$$\gamma * (A, B) = (\gamma * A, \gamma * B),\ A, B \in \mathcal{Q}. \tag{8.38}$$

Applying the extension method to the quasilinear system $(\mathcal{Q}, \mathcal{Q}_0, +, \mathbb{R}, *)$ (that is, extending the multiplication by scalar), we obtain a new system with basic properties given in the next proposition; below we assume $\alpha, \beta, \gamma \in \mathbb{R}$, $a, b, c \in \mathcal{G}$ [12].

Proposition 14. *Let* $(\mathcal{Q}, \mathcal{Q}_0, +, \mathbb{R}, *)$ *be a quasilinear system,* $(\mathcal{G}, \mathcal{G}_0, +, -, \neg)$ *be the extension group according to Proposition* 13 *, and multiplication by scalar "$*$" be defined in* $\mathcal{G}$ *by* (8.38). *Then*:

i) $\neg a = (-1) * a$;

ii) $\alpha * (\beta * c) = (\alpha\beta) * c$;

iii) $\gamma * (a + b) = \gamma * a + \gamma * b$;

iv) $1 * a = a$;

v) $(\alpha + \beta) * c_{\sigma(\alpha+\beta)} = \alpha * c_{\sigma(\alpha)} + \beta * c_{\sigma(\beta)}$;

vi) $(-1) * a + a = 0$ *for* $a \in \mathcal{G}_0$.

Proof. Relations i)–iv) and vi) are obvious. To prove v), note that it is equivalent to v′) $(\alpha + \beta) * c = (\alpha * c + \beta * c_{\sigma(\alpha)\sigma(\beta)})_{\sigma(\alpha)\sigma(\alpha+\beta)}$; we shall prove v) in this latter form. Substitute $c = (U, V) \in \mathcal{G}$ with $U, V \in \mathcal{Q}$. The right-hand side of v′) is

$$r = (\alpha * (U, V) + \beta * (U, V)_{\sigma(\alpha)\sigma(\beta)})_{\sigma(\alpha)\sigma(\alpha+\beta)}.$$

If $\sigma(\alpha)\sigma(\beta) = +$, using that $\sigma(\alpha)\sigma(\alpha + \beta) = +$ as well, we see that r is identical to the left-hand side

$$l = (\alpha + \beta) * (U, V) = ((\alpha + \beta) * U,\ (\alpha + \beta) * V).$$

Consider now the case $\sigma(\alpha)\sigma(\beta) = -$. The right-hand side becomes

$$\begin{aligned} r &= (\alpha * (U,V) + \beta * (U,V)_-)_{\sigma(\alpha)\sigma(\alpha+\beta)} \\ &= (\alpha * (U,V) + \beta * (\neg V, \neg U))_{\sigma(\alpha)\sigma(\alpha+\beta)} \\ &= ((\alpha * U, \alpha * V) + ((-\beta) * V, (-\beta) * U)_{\sigma(\alpha)\sigma(\alpha+\beta)} \\ &= (\alpha * U + (-\beta) * V,\ \alpha * V + (-\beta) * U)_{\sigma(\alpha)\sigma(\alpha+\beta)}. \end{aligned}$$

We must now consider a number of subcases. Consider, e. g., the subcase $\sigma(\alpha) = +$, $\sigma(\beta) = -$, $\sigma(\alpha + \beta) = +$ (in this subcase we have $\alpha \geq -\beta > 0$). Adding the zero term $(-\beta) * (U + V, U + V) = (0,0)$ to the left-hand side and using the quasidistributive law (6.35), we obtain

$$\begin{aligned} l &= (\alpha+\beta) * (U,V) + (-\beta) * (U+V, U+V) \\ &= ((\alpha+\beta) * U, (\alpha+\beta) * V) + ((-\beta) * U + (-\beta) * V, (-\beta) * U + (-\beta) * V) \\ &= ((\alpha+\beta) * U + (-\beta) * U + (-\beta) * V,\ (\alpha+\beta) * V) + (-\beta) * V + (-\beta) * U) \\ &= (\alpha * U + (-\beta) * V,\ \alpha * V) + (-\beta) * U) = r. \end{aligned}$$

The rest of the cases are treated analogously. □

Relation v) (or v′)) will be called q-distributive law. The q-distributive law can be also written in the form $(\alpha + \beta)c = \alpha c_\lambda + \beta c_\mu$ with $\lambda = \sigma(\alpha)\sigma(\alpha + \beta)$, $\mu = \sigma(\beta)\sigma(\alpha + \beta)$.

Definition. The system obtained in Proposition 14 will be further denoted $(\mathcal{G}, \mathcal{G}_0, +, -, \mathbb{R}, *)$ and called *q-linear system.*

Proposition 14 is a generalization of Radström's embedding theorem [16] in two directions: a) no restrictions for the signs of the scalar multipliers in the second distributive law (that is in the quasi- and q-distributive laws) are required (leading to embedding of cones in Radström case), and b) our theorem is formulated for abstract algebraic systems, comprising the system of convex bodies as special case. Clearly, (8.38) isomorphically extends multiplication by scalar from $\mathcal{Q}$ into $\mathcal{G}$; briefly, Proposition 14 says that a quasilinear system can be isomorphically embedded into a q-linear system. Thus the proposition answers fully the questions posed in the introduction.

Proposition 15. *Let $(\mathcal{G}, \mathcal{G}_0, +, -, \mathbb{R}, *)$ be a q-linear system and the operation "$\cdot$": $\mathbb{R} \times \mathcal{G} \longrightarrow \mathcal{G}$ be defined by*

$$\alpha \cdot c = \alpha * c_{\sigma(\alpha)}, \quad \alpha \in \mathbb{R},\ c \in \mathcal{G}. \tag{8.39}$$

Then $(\mathcal{G}, +, \mathbb{R}, \cdot)$ is a linear system.

Proof. Let us check that "$\cdot$" satisfies the axioms for linear multiplication.

1. Let us prove that $\alpha \cdot (\beta \cdot d) = (\alpha\beta) \cdot d$. Substitute $c = d_{\sigma(\beta)}$ in the relation $\alpha * (\beta * c) = (\alpha\beta) * c$ to obtain $\alpha * (\beta * d_{\sigma(\beta)}) = (\alpha\beta) * d_{\sigma(\beta)}$. Using (8.39), we

have $\alpha * (\beta \cdot d) = (\alpha\beta) * d_{\sigma(\beta)}$. "Dualizing" by $\sigma(\alpha)$, we obtain $\alpha * (\beta \cdot d)_{\sigma(\alpha)} = (\alpha\beta) * d_{\sigma(\beta)\sigma(\alpha)} = (\alpha\beta) * d_{\sigma(\beta\alpha)}$, or $\alpha \cdot (\beta \cdot d) = (\alpha\beta) \cdot d$, for all $d \in \mathcal{G}$, $\alpha, \beta \in \mathbb{R}$.

2. To prove the relation $\gamma \cdot (a+b) = \gamma \cdot a + \gamma \cdot b$, substitute $a = c_{\sigma(\gamma)}$, $b = d_{\sigma(\gamma)}$ in $\gamma * (a+b) = \gamma * a + \gamma * b$. We obtain $\gamma * (c_{\sigma(\gamma)} + d_{\sigma(\gamma)}) = \gamma * c_{\sigma(\gamma)} + \gamma * d_{\sigma(\gamma)}$, or $\gamma * (c+d)_{\sigma(\gamma)} = \gamma * c_{\sigma(\gamma)} + \gamma * d_{\sigma(\gamma)}$. This implies that $\gamma \cdot (c+d) = \gamma \cdot c + \gamma \cdot d$ for all $c, d \in \mathcal{G}$, $\gamma \in \mathbb{R}$.

The relations $1 \cdot a = a$, $(\alpha + \beta) \cdot c = \alpha \cdot c + \beta \cdot c$ and $(-1) \cdot a + a = 0$ can be proved similarly. □

We proved that the system $(\mathcal{G}, +, \mathbb{R}, \cdot)$ is a linear system (and, hence, "$\cdot$" is a linear multiplication by scalar). The operation "$\cdot$" is involved in the q-linear system — therefore the latter can be written in the form $(\mathcal{G}, \mathcal{G}_0, +, \mathbb{R}, *, \cdot)$.

9. CONCLUSIONS

Algebraic properties of convex bodies with respect to Minkowski operations for addition and multiplication by real scalar are studied. To this end two new operations, called inner addition, resp. inner subtraction, are introduced, and a new analogue of the second distributive law, called quasidistributive law, is proved. With the latter the system of convex bodies becomes a quasilinear system. A quasilinear system of convex bodies can be isomorphically embedded into a q-linear system, having group properties with respect to addition. The quasidistributive law induces in the q-linear system a corresponding distributivity relation, called q-distributive law. A q-linear system has much algebraic structure and is rather close to a linear system and differs from the latter by:

i) existence of two new automorphic operators — "negation" and "dualization" — in addition to the familiar automorphism "opposite" (and, of course, identity);

ii) the distributivity relation (q-distributive law) resembles the usual linear distributive law with the difference that the operator dualization is involved.

From our study it becomes clear that quasilinear and q-linear systems summarize some of the most characteristic algebraic properties of convex bodies. However, the following methodological question remains open: Which are the algebraic properties of the abstract systems corresponding to the notion of "convexity"? In our abstract study we circumvent this question by stepping directly on the fundament of abelian cancellative monoids — algebraic systems comprising well-known properties of convex bodies. Another approach could be to take into account that the set of convex bodies is a power set of certain type over a vector (or Euclidean) space (or lattice). For the latter approach results from [21] may be used, where the concept of convexity has been considered in abstract algebraic systems, which are more general than semigroups — the so-called associative spaces. Another similar approach offers the mathematical morphology (see, e. g., [15]), where vector lattices are used as fundament.

ACKNOWLEDGEMENTS. The present article arose from a talk at a seminar commemorating Prof. Y. Tagamlitzki, organized by Prof. D. Skordev and Prof. V.

Chakalov. The author is grateful to the anonymous referee for his extraordinary careful reading of the paper and remarks. This work was partially supported by the Bulgarian National Science Fund under Grant No I-507/95.

REFERENCES

1. Clifford, A. H., G. B. Preston. The Algebraic Theory of Semigroups. I, AMS, 1964.
2. Cohn, P. M. Universal Algebra. Harper and Row, 1965.
3. Fuchs, L. Abelian Groups. Publ. House Hung. Acad. Sci., Budapest, 1958.
4. Fuchs, L. Infinite Abelian Groups. I and II. Academic Press, 1970 and 1973.
5. Hadwiger, H. Minkowskische Addition und Subtraktion beliebiger Punktmengen und die Theoreme von Rirhard Schmidt. *Math. Z.*, **53**, Heft 3, 1953, 210–218.
6. Hadwiger, H. Vorlesungen über Inhalt, Oberfläche und Isoperimetrie. Springer, Berlin, 1957.
7. Kaucher, E. Interval Analysis in the Extended Interval Space $I\mathbb{R}$. *Computing Suppl.*, **2**, 1980, 33–49.
8. Kurosh, A. G. Lectures on General Algebra. Chelsea, 1963.
9. MacLane S., G. Birkhoff. Algebra. II ed., Macmillan, N. Y., 1979.
10. Markov, S. On Two Interval-arithmetic Structures and Their Properties. *Ann. Univ. Sofia, Fac. Math. Inf.*, **89**, 1995, 129–164 (in Bulgarian).
11. Markov, S. Isomorphic Embedding of Abstract Interval Systems. *Reliable Computing*, **3**, 3, 1997, 199–207.
12. Markov, S. On the Algebra of Intervals and Convex Bodies. *J. UCS*, **4**, 1, 1998, 34–47.
13. Mayer, O. Algebraische und metrische Strukturen in der Intervallrechnung und einige Anwendungen. *Computing*, **5**, 1970, 144–162.
14. Ohmann, D. Ungleichungen für die Minkowskische Summe und Differenz konvexer Körper. *Comment. Math. Helvet.*, **30**, 1956, 297–307.
15. Popov, A. A Relation between Morphological and Interval Operations. *Reliable Computing*, **4**, 2, 1998, 167–178.
16. Rådström, H. An Embedding Theorem for Spaces of Convex Sets. *Proc. Amer. Math. Soc.*, **3**, 1952, 165–169.
17. Ratschek, H., G. Schröder. Über den quasilinearen Raum. Forsch.-Zentr. Graz, 1975.
18. Ratschek, H., G. Schröder. Representation of Semigroups as Systems of Compact Convex Sets. *Proc. Amer. Math. Soc.*, **65**, 1977, 24–28.
19. Rockafellar, R. T. Convex Analysis. Princeton, 1970.
20. Schneider, R. Convex Bodies: The Brunn-Minkowski Theory. Cambridge Univ. Press, 1993.
21. Tagamlitzki, Y. On the Separability Principle in Abelian Associative Spaces. *Bull. Inst. Math.*, Bulg. Acad. Sci., **7**, 1963, 169–183 (in Bulgarian).

Received February 27, 1998
Revised May 22, 1998

Institute of Mathematics and Computer Sciences
Bulgarian Academy of Sciences,
"Acad. G. Bonchev" st., Bl. 8
BG-1113 Sofia, BULGARIA
E-mail: smarkov@iph.bio.acad.bg