MATH. SCAND. 22 (1968), 257–265

SOME FUNCTIONAL EQUATIONS IN GROUPS AND RINGS

BØRGE JESSEN, JØRGEN KARPF, ANDERS THORUP

In this paper we shall prove some algebraical theorems, which were used in a simplified proof of Sydler's theorem on polyhedra, see B. Jessen [2].

These theorems are special cases of theorems on ordered groups and rings, which are closely related to known results of homological algebra. In order to make the exposition self-contained we have included proofs of these known results.

The authors are indebted to Mrs. Käthe Fenchel and Mr. Chr. U. Jensen for valuable advice.

THEOREM 1. *Let A and X be commutative groups, and let $f: A \to X$ be an arbitrary function. Then the function $F: A^2 \to X$ defined by the equation*

$$F(a,b) = f(a+b) - f(a) - f(b) \tag{1}$$

satisfies the equations

$$F(a,b) = F(b,a)\,, \tag{α}$$

$$F(a,b) + F(a+b,c) = F(b,c) + F(a,b+c)\,. \tag{β}$$

If A is free or X is divisible, the functions F determined by means of a function f through the equation (1) *are the only functions which satisfy the equations* (α) (β).

The equation $F = 0$ expresses that f is a homomorphism. Thus, for an arbitrary f, the function F may be said to measure how much f deviates from being a homomorphism.

The first part of Theorem 1 is trivial.

The second part of Theorem 1 is known from the theory of factor systems and group extensions; in homological algebra it is expressed by the formula $\mathrm{Ext}_{\mathbf{Z}}^1(A,X) = 0$. It may be proved as follows.

Let A and X be commutative groups and $F: A^2 \to X$ a function satis-

Received August 4, 1967.

fying the equations (α) (β). The further assumption that A is free or X is divisible will be introduced later in the proof.

From (β) we deduce, by putting $b=0$, that $F(a,0)=F(0,c)=F(0,0)$ for all a and c.

In the product set $W=A\times X$ we define an addition by

$$(*) \qquad (a,x)+(b,y) = \big(a+b, x+y+F(a,b)\big) .$$

It is easily verified that W with this composition is a commutative group with the zero element $0_W=(0,-F(0,0))$.

The projection $\varphi\colon (a,x)\mapsto a$ of W onto A is clearly a homomorphism.

It is easily verified that a function $f\colon A\to X$ will satisfy the equation (1) if and only if its graph $\{(a,f(a)) \mid a\in A\}$ is a subgroup of W. Thus the existence of a function $f\colon A\to X$ satisfying (1) is equivalent to the existence of a subgroup S of W which by φ is mapped bijectively onto A.

Case 1. If A is free with a basis $\{a_i \mid i\in I\}$, and x_i, $i\in I$, are arbitrary elements of X, the subgroup S generated by the elements (a_i,x_i), $i\in I$, has the desired property, and accordingly f is determined by its values $f(a_i)=x_i$, $i\in I$, and these values can be arbitrarily chosen.

Case 2. If X is divisible, we first notice that φ maps the subgroup $S_0=\{0_W\}$ of W bijectively onto the subgroup $A_0=\{0\}$ of A. The existence of S will therefore follow by transfinite induction if we prove the following statement:

Let S_1 be a subgroup of W which is mapped bijectively by φ onto a proper subgroup A_1 of A, and let $a\in A\setminus A_1$. Then there exists an element $x\in X$ such that φ maps the subgroup $S_2=S_1+\mathbf{Z}(a,x)$ of W bijectively onto the subgroup $A_2=A_1+\mathbf{Z}a$ of A.

Clearly, φ maps S_2 onto A_2. We must prove that it is possible to choose x such that, whenever for an element $(a_1,x_1)\in S_1$ and a number $n\in\mathbf{Z}$ we have $a_1+na=0$, we also have $(a_1,x_1)+n(a,x)=0_W$, or, equivalently, such that, whenever for a number $n\in\mathbf{Z}$ we have $na\in A_1$, we also have $n(a,x)\in S_1$. The numbers n for which $na\in A_1$ are the multiples of a certain number $q\geqq 0$, and if $q(a,x)\in S_1$, we also have $n(a,x)\in S_1$ whenever n is a multiple of q. Thus the problem is merely to choose x such that $q(a,x)\in S_1$.

If $q=0$, we can use any $x\in X$. If $q>0$, we have

$$q(a,x) = \big(qa,\ qx+\textstyle\sum_{i=1}^{q-1}F(a,ia)\big) .$$

Hence, if we denote by (qa,y) the element of S_1 corresponding to qa, the condition $q(a,x)\in S_1$ takes the form

$$qx + \sum_{i=1}^{q-1} F(a,ia) = y\,,$$

and this equation has a solution x, since X is divisible.

THEOREM 2. *Let A be a commutative ring and X a module over A, and let $f\colon A \to X$ be an arbitrary function. Then the functions $F\colon A^2 \to X$ and $G\colon A^2 \to X$ defined by the equations*

$$F(a,b) = f(a+b) - f(a) - f(b)\,, \tag{1}$$

$$G(a,b) = f(ab) - bf(a) - af(b) \tag{2}$$

satisfy the equations

$$F(a,b) = F(b,a)\,, \tag{α}$$

$$F(a,b) + F(a+b,c) = F(b,c) + F(a,b+c)\,, \tag{β}$$

$$G(a,b) = G(b,a)\,, \tag{γ}$$

$$cG(a,b) + G(ab,c) = aG(b,c) + G(a,bc)\,, \tag{δ}$$

$$F(ac,bc) - cF(a,b) = G(a+b,c) - G(a,c) - G(b,c)\,. \tag{ε}$$

Furthermore, if A has a unity 1 and X is unitary, the function F satisfies the equation

$$\sum_{i=1}^{p} F(1,i1) = 0, \qquad p = \operatorname{char} A\,. \tag{ζ}$$

If A is an integral domain and X is a unitary module over A which is uniquely A-divisible, then the pairs of functions F,G determined by means of a function f through the equations (1) (2) *are the only pairs of functions which satisfy the equations* (α) (β) (γ) (δ) (ε) (ζ).

Notice that the equation (ζ) is void if $p=0$.

The equations $F=0$, $G=0$ express that f is a derivation. Thus, for an arbitrary f, the pair of functions F,G may be said to measure how much f deviates from being a derivation.

The first part of Theorem 2 is trivial.

The second part of Theorem 2 was proved by D. K. Harrison [1] in the case where A is a field and $F=0$. It may be proved as follows.

Let A be an integral domain and X a unitary module over A which is uniquely A-divisible, and let $F,G\colon A^2 \to X$ be functions satisfying the equations (α) (β) (γ) (δ) (ε) (ζ).

From (β) we deduce, by putting $b=0$, that $F(a,0)=F(0,c)=F(0,0)$ for all a and c. From (δ) we deduce, by putting $b=1$ and $c=1$, that $G(a,1)=aG(1,1)$ for all a. From (ε) we deduce, by putting $a=0$ and $b=0$, that $G(0,c)=cF(0,0)-F(0,0)$ for all c; in particular, $G(0,0)=-F(0,0)$.

In the product set $W = A \times X$ we define an addition and a multiplication by

$$(*) \qquad (a,x) + (b,y) = \big(a+b, x+y+F(a,b)\big)$$

$$(**) \qquad (a,x)(b,y) = \big(ab, bx+ay+G(a,b)\big) .$$

It is easily verified that W with these compositions is a commutative ring with the zero element $0_W = \big(0, -F(0,0)\big)$ and with a unity, viz. $1_W = \big(1, -G(1,1)\big)$. For an arbitrary $n \in \mathbf{N}$ we find

$$n\,1_W = \big(n1, -nG(1,1) + \textstyle\sum_{i=1}^{n-1} F(1,i1)\big) .$$

Hence, if $p = \operatorname{char} A = 0$, we also have $\operatorname{char} W = 0$, and if $p > 0$, we have $n\,1_W \neq 0_W$ when $n = 1, \ldots, p-1$, whereas $p1_W = 0_W$, so that $\operatorname{char} W = p$. Thus, $\operatorname{char} W = \operatorname{char} A$ in all cases.

The projection $\varphi\colon (a,x) \mapsto a$ of W onto A is clearly a ring-homomorphism.

For arbitrary elements $(0,x)$ and $(0,y)$ we find $(0,x)(0,y) = \big(0, G(0,0)\big) = 0_W$. For an arbitrary element $(0,x)$ and an arbitrary element (b,y) we find $(b,y)(0,x) = \big(0, bx + G(b,0)\big)$. Since X is uniquely A-divisible, we conclude that, for every element (b,y) with $b \neq 0$ and every element $(0,z)$, the equation $(b,y)(0,x) = (0,z)$ has a unique solution $(0,x)$. In particular, for every (b,y) with $b \neq 0$ the equation $(b,y)(0,x) = 0_W$ has only the one solution $(0,x) = 0_W$.

It is easily verified that a function $f\colon A \to X$ will satisfy the equations (1) (2) if and only if its graph $\{(a,f(a)) \mid a \in A\}$ is a subring of W. Thus, the existence of a function $f\colon A \to X$ satisfying (1) (2) is equivalent to the existence of a subring S of W which is mapped bijectively by φ onto A.

We define A_0 as $\mathbf{Z}1$ if $p = 0$, and as $\{a^p \mid a \in A\}$ if $p > 0$, and we define S_0 as $\mathbf{Z}1_W$ if $p = 0$, and as $\{(a,x)^p \mid (a,x) \in W\}$ if $p > 0$. Clearly, A_0 is a subring of A, and S_0 is a subring of W, and S_0 is mapped onto A_0 by φ. This map is bijective. This is clear if $p = 0$; and if $p > 0$, it follows by observing that, if $\varphi\big((a,x)^p\big) = 0$, we must have $a^p = 0$, and hence $a = 0$ so that $(a,x)^p = (0,x)^p = (0,x)^2(0,x)^{p-2} = 0_W$.

The existence of S will therefore follow by transfinite induction if we prove the following statement:

Let $S_1 \supseteq S_0$ be a subring of W which is mapped bijectively by φ onto a proper subring A_1 of A, and let $a \in A \setminus A_1$. Then there exists an element $x \in X$ such that φ maps the subring $S_2 = S_1[(a,x)]$ of W bijectively onto the subring $A_2 = A_1[a]$ of A.

The restriction of φ to S_1 is an isomorphism of S_1 onto A_1. This isomorphism extends to an isomorphism of the polynomial ring $S_1[T]$

onto the polynomial ring $A_1[T]$. For an arbitrary element P of $A_1[T]$, let $\bar{P}$ denote the element of $S_1[T]$ which is carried into P by the isomorphism. Now, A_2 consists of all $P(a)$, and S_2 consists of all $\bar{P}((a,x))$, and the image by φ of an element $\bar{P}((a,x))$ is $P(a)$. Thus we must prove that it is possible to choose x such that, whenever $P(a)=0$ for an element P of $A_1[T]$, we also have $\bar{P}((a,x))=0_W$.

CASE 1. $p=0$. If a is transcendental over A_1, we can obviously use any x.

If a is algebraic over A_1, let $Q\neq 0$ be an element of $A_1[T]$ of the lowest possible degree such that $Q(a)=0$. For an arbitrary x we have $(a,x)=(a,x_0)+(0,x)$, where $x_0=-F(0,0)$. Hence, by Taylor's formula, since $(0,x)^2=0_W$,

$$\bar{Q}((a,x)) = \bar{Q}((a,x_0))+\bar{Q}'((a,x_0))(0,x)\,.$$

Since $Q(a)=0$, we have $\bar{Q}((a,x_0))=-(0,z)$ for some z. Furthermore, since Q' is of lower degree than Q, and $Q'\neq 0$, we have $\bar{Q}'((a,x_0))=(b,y)$ for some y, where $b=Q'(a)\neq 0$. The equation $\bar{Q}((a,x))=0_W$ therefore takes the form $(b,y)(0,x)=(0,z)$. Thus the equation $\bar{Q}((a,x))=0_W$ has a unique solution x.

For this x we must now have $\bar{P}((a,x))=0_W$ for every element P of $A_1[T]$ for which $P(a)=0$. In fact, when $P(a)=0$, we have $dP=QR$ for some $d\in A_1\setminus\{0\}$ and some element R of $A_1[T]$. Hence, denoting by (d,u) the element of S_1 corresponding to d, we have $(d,u)\bar{P}=\bar{Q}\bar{R}$, and hence $(d,u)\bar{P}((a,x))=0_W$. Since $d\neq 0$, this equation implies that $\bar{P}((a,x))=0_W$.

CASE 2. $p>0$. In this case, since $a^p\in A_0$, we have $P(a)=0$ for the polynomial $P=T^p-a^p\in A_1[T]$, and, more generally, for every polynomial $P=(T^p-a^p)R$, where R is any element of $A_1[T]$. For these P we evidently also have $\bar{P}((a,x))=0_W$ for every x. Thus, if these are the only P for which $P(a)=0$, we can use any x.

Otherwise, let $Q\neq 0$ be an element of $A_1[T]$ of the lowest possible degree such that $Q(a)=0$. Then, since $T^p-a^p=(T-a)^p$, we must have $Q=b(T-a)^q$ for some $b\in A_1\setminus\{0\}$ and some $q\in\{1,\ldots,p-1\}$. Thus $b(-a)^q=Q(0)\in A_1$. The numbers $n\in\mathbf{N}$ for which $ka^n\in A_1$ for some $k\in A_1\setminus\{0\}$ are clearly the multiples of a certain number; since p is a prime, we conclude that $q=1$. Hence $Q'(a)=b\neq 0$ and we find, just as in the previous case, that the equation $\bar{Q}((a,x))=0_W$ has a unique solution x. We also find, just as in the previous case, that for this x we must have $\bar{P}((a,x))=0_W$ for every element P of $A_1[T]$ for which $P(a)=0$.

REMARK. In the case $p=0$ it follows from the proof that, if

$\{a_i \mid i \in I\}$ is a transcendence basis of A over Z, and x_i, $i \in I$, are arbitrarily chosen elements of X, there exists one and only one function $f: A \to X$ satisfying (1) (2), such that $f(a_i) = x_i$, $i \in I$. It also follows that all functions $f: A \to X$ satisfying (1) (2) must coincide on the set of elements of A which are algebraic over Z.

In particular we find the known results that a derivation $f: A \to X$ from a field A with $\operatorname{char} A = 0$ into a vector space X over A vanishes on the set of elements of A which are algebraic over Z, and that every function from a transcendence basis of A over Z into X is the restriction of a unique derivation.

LEMMA 1. *Let A be an ordered commutative group and X a commutative group, and let $A_+ = \{a \in A \mid a > 0\}$. Let $F: {A_+}^2 \to X$ be a function which satisfies the equations* (α) (β) *for all $a,b,c \in A_+$. Then the function can be extended to a function $\overline{F}: A^2 \to X$ which satisfies* (α) (β) *for all $a,b,c \in A$.*

We define $\overline{F}(a,b)$ as 0 when (at least) one of the elements $a, b, a+b$ is 0. When $a, b, a+b$ are $\neq 0$, we define $\overline{F}(a,b)$ by table 1, where '+' and '−' stand for '>0' and '<0'.

a	b	$a+b$	$\overline{F}(a,b)$
+	+	+	$F(a,b)$
+	−	+	$-F(a+b,-b)$
+	−	−	$F(-a-b,a)$
−	+	+	$-F(a+b,-a)$
−	+	−	$F(-a-b,b)$
−	−	−	$-F(-a,-b)$

Table 1.

One easily verifies that the function $\overline{F}: A^2 \to X$ thus defined satisfies the conditions.

The verification requires the consideration of a number of cases. We therefore also give a second proof, in which we do not have to distinguish between cases, and which moreover has the advantage that it leads to all extensions with the desired properties.

In the product set $W_+ = A_+ \times X$ we define an addition by (*). It is easily verified that W_+ with this composition is a commutative semigroup in which the cancellation law holds. Let $\overline{W}$ be the (unique) commutative group containing W_+ in which every element is a difference of elements of W_+. The projection $\varphi_+: (a,x) \mapsto a$ of W_+ onto A_+ extends uniquely to a homomorphism $\bar{\varphi}$ of $\overline{W}$ onto A. An arbitrary element $(a,x)-(b,y)$ of $\overline{W}$ is mapped by $\bar{\varphi}$ onto $a-b$. Thus the subgroup $\overline{W}_0 = \bar{\varphi}^{-1}(0)$ consists of all elements of the form $w_0 = (a,x)-(a,y)$. It is easily

seen that the difference $x-y$ is independent of the representation of w_0 and that $\pi: w_0 \mapsto x-y$ is an isomorphism of $\overline{W}_0$ onto X. Let s_a for every $a \in A$ be an element of $\overline{W}$ such that $\bar{\varphi}(s_a)=a$. Then for arbitrary $a,b \in A$ we have

$$s_a+s_b-s_{a+b} \in \overline{W}_0,$$

and it is easily verified that the function $\overline{F}: A^2 \to X$ defined by

$$\overline{F}(a,b) = \pi(s_a+s_b-s_{a+b})$$

satisfies the equations (α) (β), and also that, if for $a>0$ we choose $s_a=(a,0)$, the function $\overline{F}$ is an extension of F.

In particular, we find $\overline{F}(0,0)=\pi(s_0)$ and $\overline{F}(a,-a)=\pi(s_a+s_{-a}-s_0)$. These equations show that, for an arbitrary function $k: A \to X$ satisfying the equation $k(a)=k(-a)$, we can choose s_a for $a \leqq 0$ such that for the corresponding extension $\overline{F}$ we have $\overline{F}(a,-a)=k(a)$. On the other hand, one easily shows that an extension of F which satisfies (α) (β) is uniquely determined by its values on the set $\{(a,-a) \mid a \in A\}$. Thus we have actually obtained all extensions with the desired properties.

The extension given in the first proof corresponds to the choice $k=0$.

Professor Calvin C. Moore has shown us another way, to appear in [3], of extending functions satisfying the equations (α) (β) on a subset of A^2 to functions satisfying these equations on the whole of A^2, in which the group A is not supposed to be ordered. The subsets to which his method applies contain in case of an ordered group the sets ${A_+}^2$.

LEMMA 2. *Let A be an ordered commutative ring and X a module over A, and let $A_+=\{a \in A \mid a>0\}$. Let $F,G: {A_+}^2 \to X$ be functions which satisfy the equations (α) (β) (γ) (δ) (ε) for all $a,b,c \in A_+$. Then the functions can be extended to functions $\overline{F},\overline{G}: A^2 \to X$ which satisfy (α) (β) (γ) (δ) (ε) for all $a,b,c \in A$.*

We define $\overline{F}: A^2 \to X$ as in the first proof above. We define $\overline{G}(a,b)$ as 0 when (at least) one of the elements a,b is 0. When a,b are $\neq 0$, we define $\overline{G}(a,b)$ by table 2.

a	b	$\overline{G}(a,b)$
+	+	$G(a,b)$
+	−	$-G(a,-b)$
−	+	$-G(-a,b)$
−	−	$G(-a,-b)$

Table 2.

One easily verifies that the functions $\overline{F},\overline{G}: A^2 \to X$ thus defined satisfy the conditions.

The second proof above can also be extended to this case and leads to all extensions with the desired properties.

In the product set $W_+ = A_+ \times X$ we now define an addition and a multiplication by (*) and (**). As in the previous case, W_+ as additive semigroup is imbedded in the group $\overline{W}$, and one easily sees that the multiplication can be uniquely extended so that $\overline{W}$ becomes a commutative ring. The extension $\bar{\varphi}$ of the projection $\varphi_+ : (a,x) \mapsto a$ will now be a ring-homomorphism of $\overline{W}$ onto A. We define $\overline{W}_0$ and π as in the previous case. Then $\overline{W}_0$ is an ideal, π is an additive isomorphism of $\overline{W}_0$ onto X, and for every $w_0 \in \overline{W}_0$ and every $w \in \overline{W}$ we have the relation $\pi(ww_0) = \bar{\varphi}(w)\pi(w_0)$ connecting ring-multiplication with scalar multiplication. Let again s_a for every $a \in A$ be an element of $\overline{W}$ such that $\bar{\varphi}(s_a) = a$. Then for arbitrary $a, b \in A$ we have both

$$s_a + s_b - s_{a+b} \in \overline{W}_0 \quad \text{and} \quad s_a s_b - s_{ab} \in \overline{W}_0 ,$$

and it is easily verified that the functions $\overline{F}, \overline{G} : A^2 \to X$ defined by

$$\begin{aligned} \overline{F}(a,b) &= \pi(s_a + s_b - s_{a+b}) , \\ \overline{G}(a,b) &= \pi(s_a s_b - s_{ab}) \end{aligned}$$

satisfy the equations (α) (β) (γ) (δ) (ε), and also that, if for $a > 0$ we choose $s_a = (a, 0)$, the functions $\overline{F}, \overline{G}$ are extensions of F, G.

One easily shows that in this way we have obtained all extensions with the desired properties. We can prescribe the values of $\overline{F}$ on the set $\{(a, -a) \mid a \in A\}$ subject to the condition $\overline{F}(a, -a) = \overline{F}(-a, a)$; then $\overline{F}$ and $\overline{G}$ are uniquely determined.

By combining Theorems 1 and 2 with Lemmas 1 and 2 we obtain the following theorems.

THEOREM 3. *Let A be an ordered commutative group and X a commutative group, and let $A_+ = \{a \in A \mid a > 0\}$. Then, if A is free or X is divisible, the class of functions $F : {A_+}^2 \to X$ determined by means of a function $f : A_+ \to X$ through the equation* (1) *is identical with the class of functions $F : {A_+}^2 \to X$ which satisfy the equations* (α) (β).

THEOREM 4. *Let A be an ordered integral domain and X a unitary module over A which is uniquely A-divisible, and let $A_+ = \{a \in A \mid a > 0\}$. Then the class of pairs of functions $F, G : {A_+}^2 \to X$ determined by means of a function $f : A_+ \to X$ through the equations* (1) (2) *is identical with the class of pairs of functions $F, G : {A_+}^2 \to X$ which satisfy the equations* (α) (β) (γ) (δ) (ε).

[For an ordered integral domain A we have $\mathrm{char}\, A = 0$, so that the equation (ζ) falls out.]

The special cases used in [2] in the proof of Sydler's theorem are the following.

THEOREM 5. *Let V be a vector space over* R. *Then the class of functions $F\colon]0,1[^2 \to V$ determined by means of a function $f\colon]0,1[\to V$ through the equation*

$$F(a,b) = f(ab) - f(a) - f(b)$$

is identical with the class of functions $F\colon]0,1[^2 \to V$ which satisfy the equations

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

$$F(a,b) + F(ab,c) = F(b,c) + F(a,bc)\,.$$

We obtain this theorem from Theorem 3 by taking $A =]0,+\infty[$ with multiplication as composition and '$>$' as order relation, and $X = V$.

THEOREM 6. *Let V be a vector space over* R. *Then the class of functions $F\colon]0,+\infty[^2 \to V$ determined through the equation*

$$F(a,b) = f(a+b) - f(a) - f(b)$$

by means of a function $f\colon]0,+\infty[\to V$ satisfying the equation

$$f(ab) = bf(a) + af(b)$$

is identical with the class of functions $F\colon]0,+\infty[^2 \to V$ which satisfy the equations

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

$$F(a,b) + F(a+b,c) = F(b,c) + F(a,b+c)\,,$$

$$F(ac,bc) = cF(a,b)\,.$$

We obtain this theorem from Theorem 4 by taking $A = \mathsf{R}$, $X = V$, and $G = 0$.

REFERENCES

1. D. K. Harrison, *Commutative algebra and cohomology*, Trans. Amer. Math. Soc. 104 (1962), 191–204.
2. B. Jessen, *The algebra of polyhedra and the Dehn–Sydler theorem*, Math. Scand. 22 (1968), 241–256.
3. C. C. Moore, *Group extensions of p-adic and adèlic linear algebraic groups*, in preparation.

UNIVERSITY OF COPENHAGEN, DENMARK