COMPOSITION RINGS*

BY IRVING ADLER

1. Definitions and summary.

1.1. Let $R = A[x]$ be the ring of polynomials over a ring A. If $p, q \in R$, then $p \circ q \in R$, where $(p \circ q)(x) = p(q(x))$. The composition operation, denoted by $\circ$, has these properties:

(C1) $$(f + g) \circ h = f \circ h + g \circ h$$

(C2) $$(fg) \circ h = (f \circ h)(g \circ h) \qquad (f, g, h \in R)$$

(C3) $$f \circ (g \circ h) = (f \circ g) \circ h$$

We use this fact as the point of departure for defining an abstract algebraic structure with three binary operations:

DEFINITION. R is a *composition ring* if it is a commutative ring, not necessarily with 1, and a binary operation $\circ$ is defined in R satisfying axioms C1, C2, and C3. If R contains an identity for the operation $\circ$, we shall denote it by I.

DEFINITION. c is a *constant* if $c \circ f = c$ for all $f \in R$. If N is any subset of R, the set of all constants in N is called the *foundation* of N, and is denoted by Found N.

A composition ring is essentially the same as the "tri-operational algebra" treated by Menger, Mannos, et al. However, they used a different notation and slightly different axioms. Menger assumed for his tri-operational algebra that it contains an identity I, that $I \neq 1$, and that 1 is a constant. He also tacitly assumed that the algebra was an integral domain. Mannos dispensed with these restrictive assumptions, and also eliminated the assumption that the ring was commutative and with unity element, to obtain what he called a T-0 algebra. A composition ring with identity and in which 1 is a constant he called a T^*-0 algebra.

1.2. *Examples of composition rings.*

1. R is any commutative ring, and $\circ$ is defined by $r \circ s = 0$ for all $r, s \in R$. In this case we shall call R a *null* composition ring.

2. R is any commutative ring, and $\circ$ is defined by $r \circ s = r$ for all $r, s \in R$. Then the foundation of R is R. In this case we shall call R a *constant* composition ring. A composition ring is called *trivial* if it is constant or null.

3. Let K be a commutative ring. Let $R = K^K$ (the ring of all functions

* Received November 16, 1961. This research was supported in part by a National Science Foundation Fellowship and is the author's doctoral dissertation, presented to Columbia University.

$K \to K$). Define $\circ$ as composition of functions. Then R is a composition ring with foundation identified with K in the obvious way.

4. Let K be a commutative ring with 1. Let $R = K[x]$ (ring of polynomials over K). Define $\circ$ as composition of polynomials. Then R is a composition ring with foundation K, and with identity element x.

5. Let R be the ring of continuous real-valued functions on the real line, with composition defined as in 3.

6. Let R be the ring of C^∞ real-valued functions on the real line, with composition defined as in 3.

7. Let R be the ring of entire analytic functions, with composition defined as in 3.

8. Let R be any Boolean ring. Define by $r \circ s = rs$.

1.2. *Summary.* What follows is divided into four sections. §2 presents some elementary properties of composition rings. §3 begins with the question, "Can every non-zero commutative ring be given a non-trivial composition ring structure?" The question is answered in the affirmative. We first define a special kind of composition ring structure which we call *automorphic*. We show that every non-zero commutative ring can be given a non-trivial automorphic composition ring structure. We identify a class of rings which can have only automorphic composition ring structures. Some properties of automorphic structures are explored.

In §4 we examine *simple* composition rings whose foundation is a given field K. We find that they are all isomorphic to composition subrings of K^K. Among these we pick out a special set of *partition rings*. If K is finite, we find that the partition rings account for all the composition subrings of K^K. Where K is infinite, we introduce a topology in K^K, and show that a composition subring of K^K is a partition ring if and only if it is closed.

In §5 we deal with composition ring extensions. We initiate a cohomology theory of composition ring extensions analogous to the cohomology theories for extensions of groups, associative algebras, and Lie algebras. If $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an extension of Q by N, we require that there be an additive mapping $u: Q \to R$ such that $fu =$ identity. For each such mapping we introduce two functions, ϕ and ψ, that measure the deviation of the mapping from simple behavior. The main result is that the set of all equivalence classes of extensions of Q by N is in one-to-one correspondence with the set of all equivalence classes of pairs (ϕ, ψ).

2. Elementary properties.

2.1. Unless R is explicitly defined, it is assumed that R is a composition ring with foundation K. A *composition subring* of R is defined as a subring that is closed under composition.

The following conclusions follow immediately from the axioms: $0 \in K$. If $g \in K$, then $f \circ g \in K$ for all $f \in R$. If $f \in R$, then $f \in K$ if and only if $f \circ 0 = f$. If $1 \in R$, then $1 \in K$ if and only if there exists $c \in K$ such that c is not a zero

divisor. K is a composition subring of R. If R is a composition subring of a composition ring R' having foundation K', then $K \subset K'$. For fixed r, $p \in R$, if $r \circ s = p$ for all $s \in R$, then $p \in K$.

2.2. The composition ring structure of a composition ring is determined by a monoid of ring endomorphisms. This fact is expressed in the following proposition:

PROPOSITION 1. *If R is a composition ring, and the functions $\phi_y : R \to R$ are defined by $\phi_y(x) = x \circ y$ for all x, $y \in R$, then the family $(\phi_y)_{y \in R}$ has these properties: (1) each ϕ_y is a ring endomorphism of R; (2) $\phi_{\phi_x(y)} = \phi_x \phi_y$ for all x, $y \in R$. Conversely, if R is a commutative ring, and $(\phi_x)_{x \in R}$ is a family of ring endomorphisms of R satisfying condition (2), then if we define $\circ$ by $x \circ y = \phi_y(x)$, R is a composition ring.*

For a given composition ring R, we shall call $(\phi_r)_{r \in R}$ the family of endomorphisms *belonging to R*.

2.3. DEFINITION. Let R be a composition ring, and N be a subset of R. N is called a *composition ideal* of R if the following three conditions are satisfied:

(I1) N is an ideal of R.
(I2) $n \circ r \in N$ for all $n \in N$ and $r \in R$.
(I3) If r, s, $t \in R$, and $r - s \in N$, then $t \circ r - t \circ s \in N$.

DEFINITION. A composition ring R is *simple* if it does not have a composition ideal different from (0) and R, and $R \neq (0)$.

DEFINITION. If R and R' are composition rings, a mapping $f : R \to R'$ is a *homomorphism* if $f(r + s) = f(r) + f(s)$, $f(rs) = f(r)f(s)$, and $f(r \circ s) = f(r) \circ f(s)$, for all r, $s \in R$.

If N is a composition ideal in R, we can define a composition ring structure for R/N in a natural way. The expected propositions relating homomorphisms, composition ideals, and quotients are easily established. If $\phi : R \to R'$ is a surjective homomorphism of composition rings with kernel N, and if K' is the foundation of R', then $\phi^{-1}(K') = N + K$.

It is possible to define cartesian product and direct sum of composition rings. They are related in the usual way.

2.4. DEFINITION. Let R be a composition ring with foundation K. Let C be any ideal in K. Let $r \in R$. We say r is a *residual element modulo C* if $r \circ K \subset C$. We denote by R_C the set of all residual elements modulo C.

We find that R_C is an ideal in R and satisfies I2. In fact, R_C is the largest ideal of R satisfying I2 and the condition $R_C \cap K = C$. We find, too, that if N is a composition ideal in R, and $C = N \cap K$, then C is an ideal in K, and $N \subset R_C$.

If C is a given ideal in K, under what conditions does there exist a composition ideal of R that has C as its foundation? The answer takes this form: There exists a composition ideal in R with foundation C if and only if $a \equiv b \bmod C$

for $a, b \in K$ implies $r \circ a \equiv r \circ b \bmod C$ for all $r \in R$. If there exists a composition ideal with foundation C, then there is a largest one, viz. R_C, and a smallest one. In particular, R_0 is always a composition ideal. Note that $R_0 = R$ if and only if $K = 0$.

Definition. We call an element n of R such that $n \circ R = 0$ a *nullifier* of R, and denote the set of all nullifiers of R by N_R. We find that N_R is a composition ideal in R. If $N_R = 0$ and $r_1 \circ s = r_2 \circ s$ for all $s \in R$, then $r_1 = r_2$. In particular, if $r \circ s = p$ for all $s \in R$, then $r = p \in K$.

If the mapping $T : R \rightarrow R^R$ is defined by $T(r) = f_r$, where $f_r(s) = r \circ s$ for all $s \in R$, then T is a homomorphism with kernel N_R.

If the mapping $V : R \rightarrow K^K$ is defined by $V(r) = g_r$, where $g_r(c) = r \circ c$ for all $c \in K$, then V is a homomorphism with kernel R_0.

If C is an ideal in K, and (C) is the ideal in R generated by C, then $K \cap (C) = C$.

2.5. Definition. A composition ring which is a field is called a *composition field*.

Proposition 2. *Let R be a composition field with foundation K. If $K \neq \{0\}$, then $R = K$.*

Proof. $K \neq \{0\}$ implies that $1 \in K$. $0 \in K$. Define $\phi_0 : R \rightarrow K$ by $\phi_0(r) = r \circ 0$ for all $r \in R$. ϕ_0 is a surjective K-ring homomorphism which is not 0 (since $K \neq \{0\}$) and therefore is an isomorphism. Since $\phi_0(c) = c$ $(c \in K)$, we see that $R = K$.

Corollary 1. *Let R be a composition ring with constant unity element and foundation K. Let N be a composition ideal in R. Let $C = N \cap K$. Then N is a maximal ideal if and only if* 1) $R = N + K$, 2) $N = R_C$, *and* 3) C *is a maximal ideal in* K.

Corollary 2. *Let $1 \in K$ and N be a composition ideal of R which is a maximal ideal. Then the following conditions are equivalent:* 1) K *is a field;* 2) $N = R_0$; 3) $C = 0$; 4) $R = N \oplus K$ *(direct sum of composition subrings).*

Some other related results are: If R is an integral domain, then $1 \circ y = 0$ or 1 for all $y \in R$. If R contains an identity I, and if K is an infinite field, then I is transcendental over K. (If K is a finite field, I may be algebraic over K. For example, if $R = K^K$, and q denotes the number of elements of K, then I is a root of $x^q - x = 0$.) There is one and only one composition field that contains an identity element; it is the prime field of characteristic 2, with composition defined by $a \circ b = ab$.

Let N be a composition ideal in R, and suppose that $1 \in K$. If N is a maximal ideal, then R does not contain an identity.

If $R = N + K$, with N a composition ideal in R, and $N \cap K = 0$, then: 1) $N = R_0$; 2) for $r, s, t \in R$, if $r \circ s$ and $r \circ t \in K$, then $r \circ s = r \circ t$. Conversely, if $r \circ s, r \circ t \in K$ implies $r \circ s = r \circ t$, then $R = R_0 \oplus K$.

3. Automorphic composition rings.

3.1. Can every non-zero commutative ring be given a non-trivial composition ring structure? We find that it can, generally in many ways. We make use of the automorphisms of the ring to produce such structures.

Let R be a commutative ring. The endomorphisms of R form a monoid relative to the operation of composition, and the invertible elements of this monoid, that is the automorphisms of R, form a group Aut R. Consider any subgroup Ω of Aut R. Ω induces a partition of R into orbits; for any $y \in R$ the orbit of y is the set $P_y = \{\phi(y) : \phi \in \Omega\}$. Of course, if $x \in P_y$ then $P_x = P_y$; also $P_0 = \{0\}$. An orbit P is said to be *principal* if, whenever $x \in P, \phi \in \Omega, \phi \neq Id$, then $\phi(x) \neq x$, that is, if for every $x \in P$ the mapping $\Omega \to P$ carrying each $\phi \in \Omega$ into $\phi(x)$ is a bijection. When Ω is the group $\{Id\}$, then every orbit is principal.

3.2 DEFINITION. A composition ring is said to be *automorphic* if every nonzero endomorphism ϕ_y belonging to R (see 2.2) is a ring automorphism.

The following proposition is easily established with the help of the facts noted in 3.1.

THEOREM 1. *Let $(\phi_y)_{y \in R}$ be the family of endomorphisms belonging to a nontrivial automorphic composition ring R, and let Ω denote the set of all ϕ_y with $y \in R$ and $\phi_y \neq 0$. Then Ω is a group, and there exists a nonempty set $\mathcal{V}$ of principal orbits, with $\{0\} \notin \mathcal{V}$, such that $\phi_y \in \Omega$ whenever $y \in \bigcup_{P \in \mathcal{V}} P$ and $\phi_y = 0$ whenever $y \notin \bigcup_{P \in \mathcal{V}} P$; for each $P \in \mathcal{V}$ there exists a unique element $a_P \in P$ such that $\phi_y(a_P) = y$ for every $y \in P$.*

Conversely, let R be any commutative ring, Ω be a group of automorphisms of R, $\mathcal{V}$ be any nonempty set of principal orbits with $\{0\} \notin \mathcal{V}$, and (for each $P \in \mathcal{V}$) a_P be an element of P. For each $y \in R$ define the mapping $\phi_y : R \to R$ as follows: if y is an element of an orbit $P \in \mathcal{V}$ then ϕ_y is the element of Ω which carries a_p into y; if $y \notin \bigcup_{P \in \mathcal{V}} P$ then $\phi_y = 0$. Then $(\phi_y)_{y \in R}$ is the family of endomorphisms belonging to a non-trivial automorphic composition ring.

Thus, for a given commutative ring R, the set of all non-trivial automorphic composition ring structures is in one-to-one correspondence with the set of triples $(\Omega, \mathcal{V}, (a_p)_{P \in \mathcal{V}})$ described above. (We can include the two trivial composition ring structures in this correspondence by allowing Ω and $\mathcal{V}$ to be empty (null composition ring) and by taking $\Omega = \{Id\}$ and $\mathcal{V}$ to be the set of all sets $\{x\}$ with $x \in R$ (constant composition ring); in the null composition ring case Ω is not a group.) For any such structure, we shall call $a = (a_P)_{P \in \mathcal{V}}$ the base of the structure, and a_P the base point of P.

DEFINITION. A commutative ring is an *automorphic ring* if each of its nonzero endomorphisms is an automorphism.

It is clear that the only composition ring structures an automorphic ring may have are those of an automorphic composition ring.

Examples of automorphic rings: 1) The ring $\mathbf{Z}$ of rational integers; 2) The field $\mathbf{R}$ of real numbers; 3) $\mathbf{Z}/p^n$, where p is a prime, n a positive integer; 4) Any

absolutely algebraic field (algebraic over a prime field); 5) Any algebraically closed field of finite transcendence degree over a prime field.

If R is the finite field $\mathbf{F}_{p^n}$ of characteristic p with p^n elements, we can count all possible composition ring structures on R as follows: Let $a \in R$ be a primitive $(p^n - 1)$th root of 1. $R = \{0, a, a^2, \cdots, a^{p^n-1} = 1\}$. Let $\phi : R \to R$ be defined by $x \to x^p$. The group of automorphisms of R is Aut $R = \{Id, \phi, \phi^2, \cdots, \phi^{n-1}\}$. For every $\nu | n$, there exists one and only one subgroup Ω_ν of Aut R with order ν and generator $\phi^{n/\nu}$. $\Omega_n =$ Aut R; $\Omega_1 = Id$. These composition ring structures are possible: 1) The null structure obtained by taking $\phi_y = 0$ for all $y \in R$; 2) The constant structure obtained by taking $\phi_y = Id$ for all $y \in R$; 3) Non-trivial structures using $\mathfrak{V} =$ a subset of the set of principal orbits under Ω_1. They are in one-to-one correspondence with the non-empty subsets of $R - \{0\}$. Hence their number is $2^{p^n-1} - 1$; 4) Non-trivial structures using $\mathfrak{V} =$ a subset of the set of principal orbits under Ω_ν, for each $\nu > 1$. The number of such structures for fixed ν is

$$\sum_{r=1}^{b_\nu} \binom{b_\nu}{r} \nu^r = (1 + \nu)^{b_\nu} - 1$$

where b_ν is the number of principal orbits under Ω_ν (or, what is the same thing, is the number of irreducible polynomials in $\mathbf{F}_{p^{n/\nu}}[x]$ of degree ν and with highest coefficient 1) and is given by

$$\nu b_\nu = p^n - \sum_{\pi_1 | \nu} p^{n/\pi_1} + \sum_{\substack{\pi_1, \pi_2 | \nu \\ \pi_1 < \pi_2}} p^{n/\pi_1 \pi_2} - \cdots$$

where $\pi_1, \pi_2, \cdots$ run through the distinct prime divisors of ν. Therefore the total number of composition ring structures on the finite field of characteristic p with p^n elements is

$$1 + 2^{p^n-1} + \sum_{\substack{\nu | n \\ \nu > 1}} [(1 + \nu)^{b_\nu} - 1].$$

3.3. Let R be an automorphic ring with 1 whose only automorphism is the identity. Then, applying the method of 3.2, we find that all possible composition ring structures for R can be constructed with the aid of subsets of R as follows: Let S be any subset of R such that if $S \neq R$ then $0 \notin S$. Let F_S be the characteristic function of S. Define $x \circ y = xF_S(y)$. This applies, for example, to $\mathbf{Z}$, the prime fields, $\mathbf{R}$, and the rings $\mathbf{Z}/(p^n)$.

The rings $\mathbf{Z}/(m)$, where m is not a power of a prime, are not automorphic. The possibilities of composition ring structure are completely described by the following result, which is easy to prove.

Proposition 3. *Let R be a commutative ring with* 1, *and let* $(d_y)_{y \in R}$ *be a family of idempotent elements of R such that* $d_{x \circ y} = d_x d_y$; *then the formula* $x \circ y = xd_y$ *defines a composition ring structure on R. If* $R = \mathbf{Z}/(m)$, *where m is any integer, then every composition ring structure on R is defined in this way.*

In $\mathbf{Z}/(6)$, for example, we can take $d_0 = 0$, $d_1 = 3$, $d_2 = 0$, $d_3 = 3$, $d_4 = 0$ $d_5 = 1$; or we may take $d_0 = 0$, $d_1 = 3$, $d_2 = 4$, $d_3 = 3$, $d_4 = 0$, $d_5 = 3$; ther are, of course, many other possibilities.

We observe that if N is any ideal of the ring R we may define $d_y = 0$ or 1 according as $y \epsilon N$ or $y \not\epsilon N$, and in the resulting composition ring N is a composition ideal. This composition ring is obviously automorphic, and is non-trivial if N is different from (0) and R.

3.4. Theorem 2. *Let R be a non-trivial automorphic composition ring with composition given by $(\Omega, \mathcal{V}, (a_P)_{P \epsilon \mathcal{V}})$, and let $f : R \longrightarrow R'$ be a surjective composition ring homomorphism with $R' \neq \{0\}$. Then R' is also a non-trivial automorphic composition ring. If composition in R' is given by $(\Omega', \mathcal{V}', (a'_{P'})_{P' \epsilon \mathcal{V}'})$ then:* (a) *for each $y \epsilon R$, $\phi_y \epsilon \Omega$ if and only if $\phi_{f(y)} \epsilon \Omega'$;* (b) *there is a unique surjective group homomorphism $f_* : \Omega \longrightarrow \Omega'$ such that $f_*(\phi_y) = \phi_{f(y)}$ whenever $y \epsilon R$ and $\phi_y \epsilon \Omega$, and* Ker $f_* = \{\phi \mid \phi \epsilon \Omega, \phi(x) - x \epsilon$ Ker $f\ (x \epsilon R)\}$; (c) $\mathcal{V}' = \{f(P) \mid P \epsilon \mathcal{V}\}$, *and $a'_{f(P)} = f(a_P)$ for each $P \epsilon \mathcal{V}$.*

Proof. 1) If $\phi_y = 0$, $y \epsilon R$, then $x \circ y = 0$ for all $x \epsilon R$. Applying f, we find that $0 = f(x \circ y) = f(x) \circ f(y) = \phi_{f(y)}(f(x)) = \phi_{f(y)}(R')$, since f is a surjective homomorphism. That is, if $\phi_y = 0$, then $\phi_{f(y)} = 0$. 2) Let N be the kernel of f, $\phi \epsilon \Omega$, x, $y \epsilon R$. By property I2 of composition ideals, if $x \equiv y$ mod N, then $\phi(x - y) \epsilon N$, and consequently $\phi(x) \equiv \phi(y)$ mod N. 3) Suppose $\phi_y \epsilon \Omega$, $y \epsilon R$, and let $z' \epsilon R'$. There exists $z \epsilon R$ such that $f(z) = z'$. There exists $x \epsilon R$ such that $x \circ y = \phi_y(x) = z$. Then $f(x) \circ f(y) = f(z) = z'$, or $\phi_{f(y)}(f(x)) = z'$. Therefore $\phi_{f(y)}$ is surjective. Suppose $\phi_{f(y)}(r') = \phi_{f(y)}(s')$ where r', $s' \epsilon R'$. Since f is surjective, there exist $r, s \epsilon R$ such that $r' = f(r)$, $s' = f(s)$. Then $f(r) \circ f(y) = f(s) \circ f(y)$, or $f(r \circ y) = f(s \circ y)$. Then $\phi_y(r) \equiv \phi_y(s)$ mod N. Applying ϕ_y^{-1}, and the result of (2) above, we have $r \equiv s$ mod N, and $r' = s'$. Therefore, if $\phi_y \epsilon \Omega$, $\phi_{f(y)}$ is a ring automorphism. Then R' is automorphic, and a) is established. 4) Suppose $\phi_{y_1} = \phi_{y_2}$, y_1, $y_2 \epsilon R$. Then $x \circ y_1 = x \circ y_2$ for all $x \epsilon R$, and $f(x) \circ f(y_1) = f(x) \circ f(y_2)$. Since f is surjective, this means that $\phi_{f(y_1)}(x') = \phi_{f(y_2)}(x')$ for all $x' \epsilon R'$, and therefore $\phi_{f(y_1)} = \phi_{f(y_2)}$. Hence, if we define $f_* : \Omega \longrightarrow \Omega'$ by $f_*(\phi_y) = \phi_{f(y)}$, f_* is well defined. It is easy to verify that f_* is a surjective group homomorphism, and that $\phi \epsilon \Omega$ is in the kernel of f_* if and only if $\phi(x) \equiv x$ mod N $(x \epsilon R)$. The proof of (c) is direct.

4. Simple composition rings.

4.1. Proposition 3. *Let K be a non-zero commutative ring with unity element. Then* (a) *K^K is a simple composition ring with constant unity element, having foundation K;* (b) *Every simple composition ring with constant unity element, having foundation K, is K-isomorphic to a composition subring of K^K;* (c) *A necessary and sufficient condition that every composition subring of K^K with foundation K be simple is that K be a field.*

Proof. a) Let $S = K^K$. It is obvious that S is a composition ring with foundation K, and that $1 \epsilon K$. Suppose N is a composition ideal in S different

from (0) and S. Then $1 \not\varepsilon N$. K is the foundation of S. Let C be the foundation of N. If $C \neq (0)$, there exists a $c \neq 0$, $c \varepsilon C$. Let $a \varepsilon K$. $a + c \equiv a \bmod N$, $a + c \neq a$. There exists an $f \varepsilon S$ such that $f \circ a = 0$ and $f \circ (a + c) = 1$. Therefore $f \circ (a+c) - f \circ a = 1 \varepsilon N$, a contradiction. If $C = (0)$, $N \subset S_0 = (0)$, a contradiction. Therefore K^K is simple.

b) Let R be a simple composition ring with foundation K and $1 \varepsilon K$. Then the composition ideal R_0 is either (0) or R. Since $1 \varepsilon K$, $1 \circ K = 1$. Therefore $1 \not\varepsilon R_0$, and $R_0 \neq R$. Therefore $R_0 = (0)$, and $V : R \rightarrow K^K$ (defined in 2.4) is a K-monomorphism.

c) Let K be a field, and suppose R is a composition ring such that $K \subset R \subset K^K = S$. If N is a composition ideal of R, then $N \cap K$ is an ideal in K, and so $N \cap K = (0)$ or K. If $N \cap K = K$, then $1 \varepsilon N$, and $N = R$. If $N \cap K = (0)$, then $N \subset R_0 \subset S_0 = 0$. Consequently R is simple.

If K is not a field, let $R = K[I]$, where I is the identity element of K^K. $K \subset R \subset K^K$. It is easily verified that for every ideal C of K, (C) is a composition ideal of R with foundation C. Hence R is not simple.

4.2. If W is any partition of K, that is, any disjoint set of nonempty subsets of K whose union is K, then the functions $f \varepsilon K^K$ which are constant on each element of W obviously form a composition subring of K^K having foundation K; we denote this composition ring by T_W. By a *partition ring* (with foundation K) we shall mean any composition ring T_W with W a partition of K. It is obvious that if W' is a refinement of a partition W of K then $T_W \subset T_{W'}$ and conversely; in particular, $T_{\{K\}} = K$ is the smallest partition ring with foundation K, and $T_{\{\{x\}|x \varepsilon K\}} = K^K$ is the biggest.

Conversely, if R is any composition ring with $K \subset R \subset K^K$, the relation $f(x) = f(y)$ $(f \varepsilon R)$ is an equivalence $x \sim y$ on K, and therefore induces a partition of K (the set of equivalence classes); we denote this partition of K by $W(R)$. Obviously $R \subset T_{W(R)}$.

PROPOSITION 4. *Let K be a finite field. The mapping $R \rightarrow W(R)$ of the set of all composition rings between K and K^K into the set of all partitions of K, and the mapping $W \rightarrow T_W$ in the opposite direction, are bijective and inverse to each other.*

Proof. Let R be a composition ring between K and K^K. Let $A_1, \cdots, A_n$ be the distinct elements of $W(R)$, and select an $a_i \varepsilon A_i$ $(1 \leq i \leq n)$. For each $i \neq 1$ there exists an $f_i \varepsilon R$ with $f_i(a_1) \neq f_i(a_i)$; then the function $g_1 = \prod_{i=2}^{n} (f_i - f_i(a_i))/\prod_{i=2}^{n} (f_i(a_1) - f_i(a_i))$ is in R and

$$g_1(a_j) = \begin{cases} 1 & (j = 1), \\ 0 & (j \neq 1). \end{cases}$$

Similarly there exist functions $g_i \varepsilon R$ $(2 \leq i \leq n)$ such that

$$g_i(a_j) = \begin{cases} 1 & (i = j), \\ 0 & (i \neq j). \end{cases}$$

For any $f \in T_{W(R)}$ then $f = \sum_{i=1}^{n} f(a_i)g_i \in R$, so that $T_{W(R)} = R$. Thus the mapping $R \rightarrow W(R)$ followed by the mapping $W \rightarrow T_W$ is the identity mapping of the set of composition rings between K and K^K. As the composite in the opposite order is obviously the identity mapping of the set of partitions of K, the result follows.

PROPOSITION 5. *Let K be any commutative ring with unity element. For each element ϕ of the group of composition ring automorphisms of K^K the restriction ϕ_0 of ϕ to K is an element of the group of ring automorphisms of K, and the mapping $\phi \rightarrow \phi_0$ is an isomorphism of the former group onto the latter. If R is any composition ring with $K \subset R \subset K^K$, then every composition ring monomorphism of R into K^K is the restriction of a unique composition ring automorphism of K^K.*

Proof. It is clear that the mapping $\phi \rightarrow \phi_0$ is a homomorphism. It is surjective because for any ring automorphism F of K there is a composition ring automorphism ϕ of K^K defined by $\phi(f) = F \circ f \circ F^{-1}$ for all $f \in K^K$, and $\phi_0 = F$. It is easily shown that if ψ is a composition ring monomorphism of R into K^K such that ψ restricted to K coincides with ϕ_0, then $\psi = \phi$ restricted to R. Hence $\phi \rightarrow \phi_0$ is one-to-one.

PROPOSITION 6. *If K is a finite field, then the number of K-isomorphism classes of simple composition rings with foundation K is equal to the number of partitions of K, and the number of isomorphism classes of such composition rings is equal to the number of equivalence classes of partitions of K, two partitions being equivalent if one of them is carried into the other by an automorphism of K.*

Proof. This is an immediate consequence of the preceding propositions. The number of partitions P_n of a finite set of n distinct elements is easily computed from the well-known recursion formula

$$P_{n+1} = \sum_{i=0}^{n} \binom{n}{i} P_i\,, \qquad P_0 = 1.$$

For the finite fields with 2, 3, 4, 5, 7 or 8 elements respectively we have $P_2 = 2$, $P_3 = 5$, $P_4 = 15$, $P_5 = 52$, $P_7 = 877$, $P_8 = 4{,}140$.

If K is a finite prime field with characteristic p, isomorphism of simple composition rings with foundation K reduces to K-isomorphism, and the number of isomorphism classes of such rings is equal to P_p. If K is a finite field with n elements where n is not prime, then the number of isomorphism classes of such rings is less than P_n. For example, if K is the field with 4 elements, while $P_4 = 15$, the number of isomorphism classes of simple composition rings with foundation K is 11.

4.3. We have seen that if K is a finite field, every composition subring of K^K containing k is a partition ring. This property distinguishes finite fields from all other non-zero commutative rings with unity element. Indeed, if K is not a field, so that K contains a non-zero element a which has no reciprocal, and if we let W be some partition of K into two sets J, J', and if f, f' denote the charac-

teristic functions of J, J' respectively, then $K + Kaf + Kaf'$ is easily seen to be a composition subring of K^K which is not a partition ring. On the other hand, if K is infinite, the set of all functions $f \in K^K$ with finite range is a composition subring of K^K which is not a partition ring.

To generalize Proposition 4 to infinite fields we introduce a topology in K^K. Let F be the set of all finite subsets of K. For any $A \in F$, and any $g \in K^A$, let $O_{A,g} = \{f \in K^K : f \mid A = g\}$. Let $\Theta = \{O_{A,g} : A \in F, g \in K^A\}$. Then Θ is an open basis for a topology on K^K. The topology is Hausdorff, and with this topology K^K becomes a topological composition ring. (That is, addition, multiplication, and composition are all continuous operations.) We denote the closure of any set $X \subset K^K$ by $\bar{X}$.

THEOREM 3. *Let K be a field. Then* (a) *for every partition W of K the partition ring T_W is closed*; (b) *if R is any composition ring between K and K^K then $\bar{R} = T_{W(R)}$*.

Proof. a) If $g \notin T_W$, there exists a set $J \in W$ and $a, b \in J$ such that $g(a) \neq g(b)$. Let $A = \{a, b\}$, and let $h \in K^A$ be defined by $h(a) = g(a)$, $h(b) = g(b)$. Then $O_{A,h}$ is a neighborhood of g that does not meet T_W.

b) Let R be given and let $f \in T_{W(R)}$. We must show that every neighborhood $O_{A,g}$ of f intersects R, that is, that for every finite subset A of K there exists an $f' \in R$ which coincides with f on A. Now, we may write $A = A_1 \cup \cdots \cup A_n$ where each A_i is a subset of a set $B_i \in W(R)$ and $B_i \neq B_j$ when $i \neq j$; let $a_i \in A_i$ $(1 \leq i \leq n)$. Just as in the proof of Proposition 4 we find functions $g_1, \cdots, g_n \in R$ such that

$$g_i(a_j) = \begin{cases} 1 & (i = j), \\ 0 & (i \neq j). \end{cases} \quad \text{Setting} \quad f' = \sum_{i=1}^{n} f(a_i)g_i$$

we see that $f' \in R$ and f' coincides with f on A.

5. Extensions.

5.1. We find it convenient to introduce a new operation that may be defined in any composition ring:

DEFINITION. Let R be a composition ring with foundation K. We define a binary operation in R, $(r, s) \to r * s$ as follows: $r * s = r \circ s - r \circ 0$. The operation $*$ has these properties:

$$(r + s) * t = r * t + s * t, \qquad (r, s, t \in R);$$

$$c * s = 0, \qquad (c \in K, s \in R);$$

if N is a composition ideal in R, then $r * n \in N$, $(r \in R, n \in N)$.

We state immediately the hypotheses and main result of this section:

Given: Two composition rings N, Q with $NN = 0$, $N * N = 0$, and two operations of Q on N

1. $(q, n) \to qn$, 2. $(q, n) \to n \circ q$,

subject to the following conditions:

1. N is a Q-module with respect to the first operation;

2. $n \circ 0_Q = n \circ 0_N$, $(n_1+n_2) \circ q = n_1 \circ q + n_2 \circ q$, $(n \circ q_1) \circ q_2 = n \circ (q_1 \circ q_2)$, $(n_1 \circ n_2) \circ q = n_1 \circ (n_2 \circ q)$;

1–2. $(q_1 n) \circ q_2 = (q_1 \circ q_2)(n \circ q_2)$.

Definition. An *extension of Q by N* is an exact sequence of composition ring homomorphisms $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ such that

$$g(f(r)n) = rg(n), \qquad g(n \circ f(r)) = g(n) \circ r$$

and such that there exists an additive mapping $u : Q \to R$ for which $f(u(q)) = q$. This extension is *equivalent* to an extension $0 \to N \xrightarrow{g'} R' \xrightarrow{f'} Q \to 0$ if there exists a composition ring homomorphism $h : R \to R'$ such that the diagram is commutative; h must then be an isomorphism. $E(Q, N)$ denotes the set of equivalence classes of extensions of Q by N.

$$\begin{tikzcd}
& R \arrow[dr, "f"] \arrow[dd, "h"] & \\
N \arrow[ur, "g"] \arrow[dr, "g'"'] & & Q \\
& R' \arrow[ur, "f'"'] &
\end{tikzcd}$$

Definition. $S(Q, N)$ is the set of all pairs (ϕ, ψ) such that:

$\phi : Q^2 \times N \to N$, ϕ is additive in the first argument,
$\psi : Q^2 \to N$, ψ is additive in each argument, ψ is symmetric, and

$$\phi(q_1 \circ q_2, q_3, n_1) - \phi(q_1, q_2 \circ q_3, n_2 \circ q_3 + \phi(q_2, q_3, n_1)) + \phi(q_1, q_2, n_2) \circ q_3 = 0, \tag{1}$$

$$q_1\psi(q_2, q_3) - \psi(q_1q_2, q_3) + \psi(q_1, q_2q_3) - q_3\psi(q_1, q_2) = 0, \tag{2}$$

$$(q_1 \circ q_3)\phi(q_2, q_3, n) - \phi(q_1q_2, q_3, n) + (q_2 \circ q_3)\phi(q_1, q_3, n) = \psi(q_1, q_2) \circ q_3 - \psi(q_1 \circ q_3, q_2 \circ q_3). \tag{3}$$

The pairs (ϕ, ψ), $(\phi', \psi') \in S(Q, N)$ are equivalent if there exists an additive mapping $b : Q \to N$ such that

$$\phi(q_1, q_2, n) = \phi'(q_1, q_2, n + b(q_2)) - b(q_1 \circ q_2) + b(q_1) \circ q_2, \tag{4}$$

$$\psi(q_1, q_2) = \psi'(q_1, q_2) + q_1b(q_2) - b(q_1q_2) + q_2b(q_1). \tag{5}$$

$S^*(Q, N)$ denotes the set of equivalence classes of $S(Q, N)$.

Theorem 4. *If $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an extension of Q by N and u is ohosen as above, then $y = u(q_1) \circ (g(n) + u(q_2)) - u(q_1 \circ q_2)$ is an element of $\operatorname{Ker} f = \operatorname{Im} g$, and so is $z = u(q_1)u(q_2) - u(q_1q_2)$, so we may define $\phi(q_1, q_2, n) =$*

$g^{-1}(y)$ and $\psi(q_1, q_2) = g^{-1}(z)$; we then have $(\phi, \psi) \in S(Q, N)$. If u is chosen differently, then (ϕ, ψ) is replaced by an equivalent pair; if the extension is replaced by an equivalent one, then (ϕ, ψ) is replaced by an equivalent pair. Thus we have a mapping $E(Q, N) \to S^*(Q, N)$.

Conversely, if $(\phi, \psi) \in S(Q, N)$ and if we set $R = N \times Q$ and define addition, multiplication, and composition in R by the formulas

$$(6) \qquad (n_1, q_1) + (n_2, q_2) = (n_1 + n_2, q_1 + q_2),$$

$$(7) \qquad (n_1, q_1)(n_2, q_2) = (n_1q_2 + n_2q_1 + \psi(q_1, q_2), q_1q_2),$$

$$(8) \qquad (n_1, q_1) \circ (n_2, q_2) = (n_1 \circ q_2 + \phi(q_1, q_2, n_2), q_1 \circ q_2),$$

then R is a composition ring; and if we define $g : N \to R$, and $f : R \to Q$, by the formulas $g(n) = (n, 0)$, $f(n, q) = q$, then $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an extension of Q by N; if (ϕ, ψ) is replaced by an equivalent pair in $S(Q, N)$, then this extension is replaced by an equivalent extension. Thus we have a mapping $S^*(Q, N) \to E(Q, N)$.

These mappings $E(Q, N) \to S^*(Q, N)$ and $S^*(Q, N) \to E(Q, N)$ are inverse to each other (and therefore are bijective).

5.2. *Proof.* Suppose $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an extension of Q by N, and $u : Q \to R$ is chosen so that u is additive and $f(u(q)) = q$. To simplify the notation, we shall identify $g(N)$ with N. We can verify directly that ϕ is additive in the first argument, ψ is additive in each argument, and ψ is symmetric. Every $r \in R$ has a unique representation in the form $n + u(q)$, $(n \in N, q \in Q)$. ϕ and ψ are related to multiplication and composition in R as follows:

$$(9) \qquad (n_1 + u(q_1))(n_2 + u(q_2)) = n_1q_2 + n_2q_1 + \psi(q_1, q_2) + u(q_1q_2).$$

$$(10) \qquad (n_1 + u(q_1)) \circ (n_2 + u(q_2)) = n_1 \circ q_2 + \phi(q_1, q_2, n_2) + u(q_1 \circ q_2).$$

Since multiplication in R is associative,

$$[(n_1 + u(q_1))(n_2 + u(q_2))](n_3 + u(q_3)) = (n_1 + u(q_1))[(n_2 + u(q_2))(n_3 + u(q_3))].$$

Applying equation (9) repeatedly, we find that ψ satisfies equation (2). Since composition in R is associative,

$$[(n_1 + u(q_1)) \circ (n_2 + u(q_2))] \circ (n_3 + u(q_3))$$
$$= (n_1 + u(q_1)) \circ [(n_2 + u(q_2)) \circ (n_3 + u(q_3))].$$

Applying equation (10) repeatedly we find that ϕ satisfies equation (1). Since composition in R is right distributive with respect to multiplication,

$$[(n_1 + u(q_1))(n_2 + u(q_2))] \circ (n_3 + u(q_3))$$
$$= [(n_1 + u(q_1)) \circ (n_3 + u(q_3))][(n_2 + u(q_2)) \circ (n_3 + u(q_3))].$$

Applying (9) and (10), we find that (ϕ, ψ) satisfies equation (3). Consequently $(\phi, \psi) \in (S(Q, N)$.

If u' is another additive mapping $Q \to R$ such that $f(u'(q)) = q$, then u' determines a pair $(\phi', \psi') \in S(Q, N)$. Let $r_1, r_2 \in R$. Then if $q_1 = f(r_1)$ and $q_2 = f(r_2)$, we have $r_1 = n_1 + u(q_1) = n_1' + u'(q_1)$, and $r_2 = n_2 + u(q_2) = n_2' + u'(q_2)$. Equation (9) expresses $r_1 r_2$ in terms of u and ψ. A similar equation expresses $r_1 r_2$ in terms of u' and ψ'. Equating the two expressions, and denoting $(u - u')(q)$ by $b(q)$, we find that

$$\psi(q_1, q_2) = \psi'(q_1, q_2) + q_1 b(q_2) - b(q_1 q_2) + q_2 b(q_1).$$

Equation (10) expresses $r_1 \circ r_2$ in terms of u and ϕ. A similar equation expresses $r_1 \circ r_2$ in terms of u' and ϕ'. Equating the two expressions, we find that

$$\phi(q_1, q_2, n_2) = \phi'(q_1, q_2, n_2 + b(q_2)) - b(q_1 \circ q_2) + b(q_1) \circ q_2 .$$

Therefore (ϕ, ψ) is equivalent to (ϕ', ψ').

Suppose $0 \to N \xrightarrow{g'} R' \xrightarrow{f'} Q \to 0$ is another extension of Q by N equivalent to $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$. (See the figure in 5.1.) Choose u' as defined in 5.1, and determine the pair (ϕ', ψ') as above. As before, we identify $g(N)$ with N, and $g'(N)$ with N. Then $h(n) = n$, $(n \in N)$. For each $n + u(q) \in R$, $h(n + u(q)) = n' + u'(q)$. Then from the fact that $q = f'h(n + u(q)) = f'(n' + u'(q))$ we find that $hu(q) - u'(q) = b(q) \in N$ where b is additive. Then $n' = n + b(q)$. Equating $h[(n_1 + u(q_1))(n_2 + u(q_2))]$ with $(n_1' + u'(q_1))(n_2' + u'(q_2))$, we find that ψ and ψ' satisfy (5). Equating $h[(n_1 + u(q_1)) \circ (n_2 + u(q_2))]$ with $(n_1' + u'(q_1)) \circ (n_2' + u'(q_2))$ we find that ϕ and ϕ' satisfy (4). Therefore (ϕ, ψ) is equivalent to (ϕ', ψ'), and we have established that there is a mapping $E(Q, N) \to S^*(Q, N)$.

Conversely if $(\phi, \psi) \in S(Q, N)$, and if we set $R = N \times Q$ with addition, multiplication and composition defined by (6), (7), and (8), it is easily verified that R is a composition ring. If we define $g : N \to R$ and $f : R \to Q$ by $g(n) = (n, 0)$, $f(n, q) = q$, then $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an exact sequence satisfying the conditions $g(f(r)n) = rg(n)$, $g(n \circ f(r)) = g(n) \circ r$. Moreover, if we define $u : Q \to R$ by $q \to (0, q)$, then u is additive and $f(u(q)) = q$.

If we replace (ϕ, ψ) by an equivalent pair (ϕ', ψ'), we obtain in the same way an extension $0 \to N \xrightarrow{g'} R' \xrightarrow{f'} Q \to 0$. There exists an additive mapping $b : Q \to N$ satisfying (4) and (5). Define $h : R \to R'$ by $h(n, q) = (n + b(q), q)$. Then the figure in 5.1 is commutative and h is a homomorphism. Hence we have a mapping $S^*(Q, N) \to E(Q, N)$.

To show that the mapping $S^*(Q, N) \to E(Q, N)$ is the inverse of the mapping $E(Q, N) \to S^*(Q, N)$ we observe that $y = (0, q_1) \circ ((n, 0) + (0, q_2)) - (0, q_1 \circ q_2)$ and $z = (0, q_1)(0, q_2) - (0, q_1 q_2)$. (See the definitions of y and z in 5.1.) It follows at once that $g^{-1}(y) = \phi$, and $g^{-1}(z) = \psi$, and the composite mapping $S^*(Q, N) \to E(Q, N) \to S^*(Q, N)$ is the identity mapping. On the other hand, if for a given extension we take $\phi = g^{-1}(y)$ and $\psi = g^{-1}(z)$, and then, as above, construct the extension using $N \times Q$ and operations defined by (6), (7) and (8), then the mapping $h : n + u(q) \to (n, q)$ is an isomorphism. Hence the composite mapping $E(Q, N) \to S^*(Q, N) \to E(Q, N)$ is the identity mapping.

Definition. An extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ of Q by N is *inessential* if there exists a composition ring homomorphism $u : Q \to R$ such that $fu =$ identity.

If an inessential extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is equivalent to an extension $0 \to N \xrightarrow{g'} R' \xrightarrow{f'} Q \to 0$ (with the commutative figure of 5.1), then $hu : Q \to R'$ is a homomorphism and $f'(hu) =$ identity. Hence all extensions equivalent to an inessential extension are inessential.

Suppose an element P of $S^*(Q, N)$ determines inessential extensions. Choose any $(\phi, \psi) \in P$, and construct the extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ as described in 5.1. Then it is an inessential extension, and the homomorphism $u : Q \to R$ takes the form $u(q) = (b(q), q)$, where b is an additive mapping $Q \to N$. From $(b(q_1), q_1)(b(q_2), q_2) - (b(q_1q_2), q_1q_2) = (0, 0)$ and $(b(q_1), q_1) \circ (b(q_2), q_2) - (b(q_1 \circ q_2), q_1 \circ q_2) = (0, 0)$ we find that

$$\psi(q_1, q_2) + q_1 b(q_2) - b(q_1 q_2) + q_2 b(q_1) = 0, \tag{11}$$

and

$$\phi(q_1, q_2, b(q_2)) - b(q_1 \circ q_2) + b(q_1) \circ q_2 = 0. \tag{12}$$

Conversely, if $(\phi, \psi) \in S(Q, N)$, and conditions (11) and (12) hold for some additive $b : Q \to N$, and the extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is constructed via the formulas of 5.1, and $u : Q \to R$ is defined by $u(q) = (b(q), q)$, then u is a homomorphism and $fu =$ identity.

Proposition 7. *$(\phi, \psi) \in S(Q, N)$ determines an inessential extension of Q by N if and only if ϕ and ψ satisfy equations* (11) *and* (12) *with some additive $b : Q \to N$.*

5.3. We call an extension of Q by N *special* if there exists an additive mapping $u : Q \to R$ such that $f(u(q)) = q$ and u (Found Q) $\subset$ Found R. We call a pair $(\phi, \psi) \in S(Q, N)$ *special* if ϕ ((Found Q) $\times Q \times N) = 0$. It is easily verified that if an extension of Q by N is special and a u with the properties listed above is used to construct $\phi = g^{-1}(y)$ and $\psi = g^{-1}(z)$, then (ϕ, ψ) is special. Conversely, if $(\phi, \psi) \in S(Q, N)$ is special, and an extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is constructed via (6), (7), (8) and the formulas for g and f in 5.1, then this extension is special. If two extensions of Q by N are equivalent, and one of them is special, then so is the other. Consequently there is a one-to-one correspondence between the subset of $S^*(Q, N)$ whose elements contain at least one special (ϕ, ψ) and the subset of $E(Q, N)$ whose elements are the equivalence classes of special extensions of Q by N.

If $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is a special extension of Q by N constructed via (6), (7), (8), and the formulas for g and f in 5.1, then Found $R =$ (Found N, Found Q).

5.4. The operation $*$ in a composition ring is not, in general, left distributive with respect to addition. This defect is partially remedied in a class of composition rings defined as follows:

Definition. Let R be a composition ring, and N a composition ideal in R. *R is semi-distributive over N* if $r * (s \circ n - s \circ 0) = r * (s \circ n) - r * (s \circ 0)$, and $r * (m + n) = r * m + r * n$, for all $r, s \in R$ and $m, n \in N$.

For the remainder of this section we modify the assumptions about Q and N by imposing these additional requirements: There is a third operation of Q on N, $(q, n) \to q * n$ subject to these conditions: $(q_1 + q_2) * n = q_1 * n + q_2 * n$, $q * (n_1 + n_2) = q * n_1 + q * n_2$, $(q_1 \circ q_2) * n = q_1 * (q_2 * n)$, $(q_1 * n) \circ q_2 = q_1 * (n \circ q_2)$.

We also modify the definitions of 5.1 as follows: We require of an extension of Q by N the additional property that $g(f(r) * n) = r * g(n)$, and we require of $(\phi, \psi) \in S(Q, N)$ that $\phi(q, 0, n) - \phi(q, 0, 0) = q * n$. With these modified assumptions and definitions the theorem of 5.1 still holds. However, under these conditions, an extension of Q by N is necessarily semi-distributive over $g(N)$.

Definition. If N is a composition ideal in R, R is *distributive* over N if $r * (n + s) = r * n + r * s$ for all $r, s \in R$ and $n \in N$. An extension $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ of Q by N is distributive over N if R is distributive over $g(N)$.

We shall determine the conditions under which there exist extensions of Q by N that are distributive over N, and we identify these extensions. We shall show that the set of equivalence classes of such extensions is in one-to-one correspondence with a certain cohomology group which we now define.

Definition. Let $C^t(Q, N)$ be the group of all functions $f(q_1, \cdots, q_t)$ of t variables in Q with values in N, additive with respect to each variable. Define δ by

$$(\delta f)(q_1, \cdots, q_{t+1}) = q_1 f(q_2, \cdots, q_{t+1})$$
$$+ \sum_{i=1}^{t} (-1)^i f(q_1, \cdots, q_i q_{i+1}, \cdots, q_{t+1}) + (-1)^{t+1} f(q_1, \cdots, q_t) q_{t+1}.$$

δ is a homomorphism, and $\delta\delta = 0$. Let $Z^2_s(Q, N)$ be the second group of symmetric cocycles mod δ.

Let $D^t(Q, N)$ be the group of all functions $f(q_1, \cdots, q_t)$ of t variables in Q with values in N that are additive in q_1. Define Δ by

$$(\Delta f)(q_1, \cdots, q_{t+1}) = q_1 * f(q_2, \cdots, q_{t+1})$$
$$+ \sum_{i=1}^{t} (-1)^i f(q_1, \cdots, q_i \circ q_{i+1}, \cdots, q_{t+1}) + (-1)^{t+1} f(q_1, \cdots, q_t) \circ q_{t+1}.$$

Δ is a homomorphism, and $\Delta\Delta = 0$. Let $W^2(Q, N)$ be the second group of cocycles mod Δ.

Let $S'(Q, N)$ be the set of pairs $(F, \psi) \in W^2(Q, N) \times Z^2_s(Q, N)$ which satisfy

$$(13) \qquad \psi(q_1, q_2) \circ q_3 - \psi(q_1 \circ q_3, q_2 \circ q_3)$$
$$= (q_2 \circ q_3) F(q_1, q_3) - F(q_1 q_2, q_3) + (q_1 \circ q_3) F(q_2, q_3).$$

S' is clearly a group. Let $\Theta = \{(\Delta b, \delta b) : b \in D^1(Q, N)\}$.

Theorem 5. *There exist extensions of Q by N that are distributive over N if and only if*

$$(14)\qquad (q_1 \circ q_2)(q_3 * n) - (q_1 q_2) * n + (q_2 \circ q_1)(q_1 * n) = 0, \qquad (q_1, q_2, q_3 \in Q, n \in N).$$

If an extension of Q by N is distributive over N, an extension of Q by N equivalent to it is also distributive over N. If there exist extensions of Q by N that are distributive over N, an element P of $S^*(Q, N)$ determines an equivalence class of such extensions if and only if, for each $(\phi, \psi) \in P$, $\phi = F(q_1, q_2) + q_1 * n$ and $(F, \psi) \in S'(Q, N)$. Then $(\Delta b, \delta b) \in S'(Q, N)$ for all $b \in D^1(Q, N)$, and the set of equivalence classes of such extensions is in one-to-one correspondence with the group S'/O. Under this correspondence the inessential extensions (that are distributive over N) correspond to the zero of the group.

Proof. 1) Suppose $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ and $0 \to N \xrightarrow{g'} R' \xrightarrow{f'} Q \to 0$ are equivalent extensions of Q by N, with commutative figure as in 5.1, and R is distributive over N. Let $h(r) = r'$, $h(s) = s'$. Identify $g(N)$ and $g'(N)$ with N. Then $h(n) = n$ for all $n \in N$. Since R is distributive over N,

$$r \circ (n + s) = r \circ n + r \circ s - r \circ 0, \qquad (r, s \in R, n \in N).$$

Under h this equation transforms to

$$r' \circ (n + s') = r' \circ n + r' \circ s' - r' \circ 0, \qquad (r', s' \in R', n \in N),$$

which implies that R' is distributive over N.

2) We define a mapping d of the set of functions on $Q^2 \times N$ with values in N into itself by

$$d(\phi(q_1, q_2, n)) = \phi(q_1, q_2, n) - \phi(q_1, q_2, 0) - q_1 * n.$$

If $0 \to N \xrightarrow{g} R \xrightarrow{f} Q \to 0$ is an extension of Q by N, with $u : Q \to R$ defined as in 5.1, and $\phi = g^{-1}(y)$, then $\phi(q_1, q_2, 0) = g^{-1}(u(q_1) \circ u(q_2) - u(q_1 \circ q_2))$. If R is distributive over N, it is easily verified that $d\phi = 0$. Conversely, if $d\phi = 0$, equation (10) reduces to

$$(15)\qquad (n_1 + u(q_1)) \circ (n_2 + u(q_2)) = n_1 \circ q_2 + \phi(q_1, q_2, 0) + q_1 * n_2 + u(q_1 \circ q_2).$$

Let $r = n_1 + u(q_1)$, $s = n_2 + u(g_2)$, and $m \in N$. Using (15) we find that $r * (m + s) = r * m + r * s$, and hence R is distributive over N.

3) Let $(\phi, \psi) \in S(Q, N)$ such that $d\phi = 0$. In equation (3) take $n = 0$. By subtracting the resulting equation from equation (3) we find that Q and N must satisfy equation (14). If we identify $g(N)$ with N, $\phi(q_1, q_2, 0) = u(q_1) \circ u(q_2) - u(q_1 \circ q_2)$. If we write $\phi^0(q_1, q_2)$ for $\phi(q_1, q_2, 0) \in D^2(Q, N)$, and substitute $\phi^0(q_1, q_2) + q_1 * n$ for $\phi(q_1, q_2, n)$ in equation (1) we find that $\Delta\phi^0 = 0$. Hence $\phi^0 \in W^2(Q, N)$. $\psi \in C^2(Q, N)$ and is symmetric. Moreover, ψ satisfies equation (2) which asserts that $\delta\psi = 0$. Substituting $\phi^0(q_1, q_2) + q_1 * n$ for $\phi(q_1, q_2, n)$ in

equation (3), and applying (14), we find that (ϕ^0, ψ) satisfies (13). Thus $(\phi^0, \psi) \in S'(Q, N)$.

4) Suppose Q and N satisfy (14). If $(F, \psi) \in S'(Q, N)$, and we let $\phi(q_1, q_2, n) = F(q_1, q_2) + q_1 \circ n$, then $(\phi, \psi) \in S(Q, N)$, $d\phi = 0$, and $F = \phi^0$. It is clear then that we have a one-to-one correspondence between the set $S'(Q, N)$ and the set of elements (ϕ, ψ) in $S(Q, N)$ for which $d\phi = 0$.

5) We define an equivalence relation in $S'(Q, N)$ by $(\phi_1^0, \psi_1) \sim (\phi_2^0, \psi_2)$ if $(\phi_1, \psi_1) \sim (\phi_2, \psi_2)$. $(\phi_1, \psi_1) \sim (\phi_2, \psi_2)$ if and only if equations (4) and (5) are satisfied. Equation (5) asserts that $\psi_1 - \psi_2 = \delta b$, and equation (4) asserts that $\phi_1^0 - \phi_2^0 = \Delta b$, where $b \in D^1(Q, N)$. Since (ϕ_1^0, ψ_1) and (ϕ_2^0, ψ_2) satisfy (13), so does $(\Delta b, \delta b)$.

Suppose $(\phi_1^0, \psi_1) \in S'(Q, N)$, and b is any element of $D^1(Q, N)$. (ϕ_1, ψ_1) is associated with a mapping $u : Q \rightarrow R$. Let $u' = u - b$. Then there is associated with the mapping u' a pair $(\phi_2, \psi_2) \in S(Q, N)$, and $(\phi_2^0, \psi_2) \sim (\phi_1^0, \psi_1)$. Moreover, $\psi_1 - \psi_2 = \delta b$, and $\phi_1^0 - \phi_2^0 = \Delta b$. It follows that the set of equivalence classes of extensions of Q by N that are distributive over N is in one-to-one correspondence with the group S'/Θ.

5) Suppose (ϕ, ψ) determines an extension of Q by N that is distributive over N. Equations (11) and (12) constitute a necessary and sufficient condition that the extension be inessential. (11) has the form $\psi = \delta(-b)$, and (12) has the form $\phi^0 = \Delta(-b)$. Hence the set of inessential extensions that are distributive over N corresponds to the zero of S'/Θ.

References

1. Henri Cartan and Samuel Eilenberg, *Homological Algebra*, Princeton, 1956, pp. 289–314.
2. Claude Chevalley and Samuel Eilenberg, *Cohomology theory of Lie groups and Lie algebras*, Transactions of the American Mathematical Society, vol. 63(1948), pp. 85-124.
3. Samuel Eilenberg and Saunders MacLane, *Cohomology theory in abstract groups. II. Group extensions with a non-Abelian kernel*, Annals of Mathematics, vol. 48(1947), pp. 326-341.
4. Samuel Eilenberg, *Topological methods in abstract algebra. Cohomology theory of groups*, Bulletin of the American Mathematical Society, vol. 55(1949), pp. 3-27.
5. G. Hochschild, *On the cohomology groups of an associative algebra*, Annals of Mathematics, vol. 46(1945), pp. 58-67.
6. Murray Mannos, *Ideals in tri-operational algebra* I. Reports of a Mathematical Colloquium, second series, Issue 7, Notre Dame, 1946.
7. Karl Menger, *Algebra of analysis*, Notre Dame Mathematical Lectures, Number 3, 1944.
8. Karl Menger, *General algebra of analysis*, Reports of a Mathematical Colloquium, second series, Issue 7, Notre Dame, 1946.
9. Karl Menger, *Tri-operational algebra*, Reports of a Mathematical Colloquium, second series, Issue 5-6, Notre Dame, 1944.

Bennington College